

# GW2300 Series User Manual

Issue: 1.2  
Date: 28 February 2020

---

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>Introduction .....</b>                                       | <b>11</b> |
| 1.1      | Document scope .....  | 11        |
| 1.2      | Using this documentation.....                                   | 11        |
| <b>2</b> | <b>GW2300 Series hardware .....</b>                             | <b>14</b> |
| 2.1      | Hardware specification.....                                     | 14        |
| 2.2      | Compliance .....  | 17        |
| 2.3      | Antenna.....  | 17        |
| 2.4      | Components.....   | 17        |
| 2.5      | Inserting SIM cards.....  | 19        |
| 2.6      | Connecting the SIM cover .....                                  | 20        |
| 2.7      | Connecting cables.....  | 20        |
| 2.8      | Connecting the antenna .....                                    | 20        |
| 2.9      | Connecting the WiFi antenna .....                               | 20        |
| 2.10     | Powering up .....   | 20        |
| 2.11     | Reset button .....  | 20        |
| <b>3</b> | <b>GW2300 Series LED behaviour.....</b>                         | <b>22</b> |
| 3.1      | Main LED behaviour.....   | 22        |
| 3.2      | Ethernet port LED behaviour .....                               | 23        |
| <b>4</b> | <b>Factory configuration extraction from SIM card .....</b>     | <b>24</b> |
| <b>5</b> | <b>Accessing the router.....</b>                                | <b>25</b> |
| 5.1      | Configuration packages used .....                               | 25        |
| 5.2      | Accessing the router over Ethernet using the web interface..... | 25        |
| 5.3      | Accessing the router over Ethernet using an SSH client .....    | 26        |
| 5.4      | Accessing the router over Ethernet using a Telnet client .....  | 27        |
| 5.5      | Configuring the password.....                                   | 27        |
| 5.6      | Configuring the password using the web interface.....           | 27        |
| 5.7      | Configuring the password using UCI.....                         | 28        |
| 5.8      | Configuring the password using package options.....             | 28        |
| 5.9      | Accessing the device using RADIUS authentication .....          | 29        |
| 5.10     | Accessing the device using TACACS+ authentication .....         | 30        |
| 5.11     | SSH .....   | 34        |
| 5.12     | Package dropbear using UCI.....                                 | 36        |
| 5.13     | Certs and private keys.....                                     | 36        |
| 5.14     | Configuring a router's web server .....                         | 37        |
| 5.15     | Basic authentication (httpd conf) .....                         | 43        |
| 5.16     | Securing uhttpd .....   | 43        |
| 5.17     | Displaying custom information via login screen .....            | 43        |
| <b>6</b> | <b>Router file structure .....</b>                              | <b>46</b> |
| 6.1      | System information .....  | 46        |
| 6.2      | Identify your software version .....                            | 47        |

---

|           |   |            |
|-----------|---|------------|
| 6.3       | Image files.....  | 48         |
| 6.4       | Directory locations for UCI configuration files .....           | 48         |
| 6.5       | Viewing and changing current configuration .....                | 48         |
| 6.6       | Configuration file syntax .....                                 | 49         |
| 6.7       | Managing configurations .....                                   | 49         |
| 6.8       | Exporting a configuration file.....                             | 50         |
| 6.9       | Importing a configuration file .....                            | 51         |
| <b>7</b>  | <b>Using the Command Line Interface.....</b>                    | <b>55</b>  |
| 7.1       | Overview of some common commands .....                          | 55         |
| 7.2       | Using Unified Configuration Interface (UCI) .....               | 58         |
| 7.3       | Configuration files.....  | 63         |
| 7.4       | Configuration file syntax .....                                 | 63         |
| <b>8</b>  | <b>Upgrading router firmware.....</b>                           | <b>65</b>  |
| 8.1       | Software versions .....   | 65         |
| 8.2       | Upgrading firmware using CLI .....                              | 71         |
| 8.3       | Firmware recovery .....   | 73         |
| <b>9</b>  | <b>System settings .....</b>                                    | <b>74</b>  |
| 9.1       | Syslog overview.....  | 74         |
| 9.2       | Configuration package used .....                                | 74         |
| 9.3       | Configuring system properties .....                             | 75         |
| 9.4       | System settings using command line.....                         | 83         |
| 9.5       | System diagnostics .....  | 85         |
| 9.6       | Advanced filtering of syslog messages .....                     | 88         |
| <b>10</b> | <b>Configuring an Ethernet interface.....</b>                   | <b>93</b>  |
| 10.1      | Configuration packages used .....                               | 93         |
| 10.2      | Configuring an Ethernet interface using the web interface ..... | 93         |
| 10.3      | Interface configuration using command line .....                | 106        |
| 10.4      | Configuring port maps .....                                     | 109        |
| 10.5      | Port map packages.....  | 109        |
| 10.6      | Interface diagnostics .....                                     | 111        |
| <b>11</b> | <b>Configuring VLAN .....</b>                                   | <b>113</b> |
| 11.1      | Maximum number of VLANs supported .....                         | 113        |
| 11.2      | Configuration package used .....                                | 113        |
| 11.3      | Configuring VLAN using the web interface .....                  | 113        |
| 11.4      | Viewing VLAN interface settings.....                            | 116        |
| 11.5      | Configuring VLAN using the UCI interface.....                   | 117        |
| <b>12</b> | <b>Configuring Power over Ethernet.....</b>                     | <b>118</b> |
| 12.1      | PoE overview.....   | 118        |
| 12.2      | Configuration package used .....                                | 118        |
| 12.3      | Configuring PoE .....   | 118        |

---

|           |  |            |
|-----------|--|------------|
| 12.4      | Restarting a PoE port.....   | 120        |
| 12.5      | PoE diagnostics.....   | 120        |
| <b>13</b> | <b>Configuring AC power sense .....</b>                                | <b>122</b> |
| 13.1      | Configuration packages used .....                                      | 122        |
| 13.2      | Configuring vapowermond using the web interface.....                   | 122        |
| 13.3      | Configuring vapowermond using the command line .....                   | 124        |
| 13.4      | AC power sense diagnostics .....                                       | 125        |
| <b>14</b> | <b>Configuring a WiFi connection .....</b>                             | <b>126</b> |
| 14.1      | Configuration packages used .....                                      | 126        |
| 14.2      | Configuring a WiFi interface using the web interface.....              | 126        |
| 14.3      | Configuring WiFi in AP mode.....                                       | 132        |
| 14.4      | Configuring WiFi using UCI.....  | 134        |
| 14.5      | Creating a WiFi interface in client mode using the web interface ..... | 137        |
| 14.6      | Configuring WiFi in client mode using command line.....                | 138        |
| <b>15</b> | <b>Configuring an xDSL interface .....</b>                             | <b>140</b> |
| 15.1      | xDSL overview.....   | 140        |
| 15.2      | xDSL connection options on your router.....                            | 140        |
| 15.3      | Configuration package used .....                                       | 141        |
| 15.4      | Configuring a DSL device .....   | 141        |
| 15.5      | Configuring an upper layer for the DSL device .....                    | 145        |
| 15.6      | xDSL diagnostics.....  | 184        |
| <b>16</b> | <b>Configuring a mobile connection .....</b>                           | <b>187</b> |
| 16.1      | Configuration package used .....                                       | 187        |
| 16.2      | Configuring a mobile connection using the web interface.....           | 187        |
| 16.3      | Configuring a mobile connection using CLI .....                        | 194        |
| 16.4      | Diagnositcs .....  | 195        |
| <b>17</b> | <b>Configuring mobile manager.....</b>                                 | <b>199</b> |
| 17.1      | Configuration package used .....                                       | 199        |
| 17.2      | Configuring mobile manager using the web interface.....                | 199        |
| 17.3      | Configuring mobile manager using command line.....                     | 204        |
| 17.4      | Monitoring SMS .....   | 206        |
| 17.5      | Sending SMS from the router .....                                      | 207        |
| 17.6      | Sending SMS to the router .....  | 207        |
| <b>18</b> | <b>Configuring multi-APNs for mobile interfaces.....</b>               | <b>208</b> |
| 18.1      | Supported mobile modules.....  | 208        |
| 18.2      | Multi-APN overview .....   | 208        |
| 18.3      | Configuration package used .....                                       | 208        |
| 18.4      | Configuring multi-APN .....  | 209        |
| 18.5      | Multi-APN diagnostics .....  | 212        |
| <b>19</b> | <b>Configuring a GRE interface.....</b>                                | <b>217</b> |

---

|           |  |            |
|-----------|--|------------|
| 19.1      | Configuration packages used .....                        | 217        |
| 19.2      | Creating a GRE connection using the web interface .....  | 217        |
| 19.3      | GRE configuration using command line .....               | 222        |
| 19.4      | GRE configuration using UCI.....                         | 222        |
| 19.5      | GRE configuration using package options .....            | 222        |
| 19.6      | GRE diagnostics .....                                    | 223        |
| <b>20</b> | <b>Configuring VRF (Virtual Router Forwarding) .....</b> | <b>225</b> |
| 20.1      | VRF overview .....                                       | 225        |
| 20.2      | Configuration package used .....                         | 225        |
| 20.3      | Configuring VRF .....                                    | 225        |
| 20.4      | VRF diagnostics .....                                    | 228        |
| <b>21</b> | <b>Configuring static routes .....</b>                   | <b>229</b> |
| 21.1      | Configuration package used .....                         | 229        |
| 21.2      | Configuring static routes using the web interface .....  | 229        |
| 21.3      | Configuring IPv6 routes using the web interface .....    | 230        |
| 21.4      | Configuring routes using command line .....              | 230        |
| 21.5      | IPv4 routes using UCI.....                               | 231        |
| 21.6      | IPv4 routes using package options .....                  | 232        |
| 21.7      | IPv6 routes using UCI.....                               | 232        |
| 21.8      | IPv6 routes using package options .....                  | 232        |
| 21.9      | Static routes diagnostics .....                          | 233        |
| <b>22</b> | <b>Configuring BGP (Border Gateway Protocol) .....</b>   | <b>234</b> |
| 22.1      | Configuration package used .....                         | 234        |
| 22.2      | Configuring BGP using the web interface.....             | 234        |
| 22.3      | Configuring BGP using command line.....                  | 238        |
| 22.4      | View routes statistics.....                              | 241        |
| <b>23</b> | <b>Configuring OSPF (Open Shortest Path First) .....</b> | <b>242</b> |
| 23.1      | Introduction .....                                       | 242        |
| 23.2      | Configuration package used .....                         | 247        |
| 23.3      | Configuring OSPF using the web interface .....           | 248        |
| 23.4      | Configuring OSPF using the command line .....            | 251        |
| 23.5      | OSPF using UCI .....                                     | 252        |
| 23.6      | OSPF using package options.....                          | 253        |
| 23.7      | OSPF diagnostics .....                                   | 254        |
| 23.8      | Quagga/Zebra console.....                                | 255        |
| <b>24</b> | <b>Configuring VRRP .....</b>                            | <b>261</b> |
| 24.1      | Overview .....   | 261        |
| 24.2      | Configuration package used .....                         | 261        |
| 24.3      | Configuring VRRP using the web interface .....           | 261        |
| 24.4      | Configuring VRRP using command line.....                 | 265        |

---

|           |  |            |
|-----------|--|------------|
| 24.5      | VRRP diagnostics .....   | 267        |
| <b>25</b> | <b>Configuring Routing Information Protocol (RIP) .....</b>          | <b>268</b> |
| 25.1      | Introduction .....   | 268        |
| 25.2      | Configuration package used .....                                     | 269        |
| 25.3      | Configuring RIP using the web interface.....                         | 270        |
| 25.4      | Configuring RIP using command line .....                             | 274        |
| 25.5      | RIP diagnostics .....  | 278        |
| <b>26</b> | <b>Configuring Multi-WAN .....</b>                                   | <b>282</b> |
| 26.1      | Configuration package used .....                                     | 282        |
| 26.2      | Configuring Multi-WAN using the web interface.....                   | 282        |
| 26.3      | Configuring Multi-WAN using UCI .....                                | 287        |
| 26.4      | Multi-WAN diagnostics .....  | 288        |
| <b>27</b> | <b>Automatic operator selection.....</b>                             | <b>291</b> |
| 27.1      | Configuration package used .....                                     | 291        |
| 27.2      | Configuring automatic operator selection via the web interface ..... | 291        |
| 27.3      | Configuring via UCI .....  | 314        |
| 27.4      | Configuring no PMP + roaming using UCI.....                          | 319        |
| 27.5      | Automatic operator selection diagnostics via the web interface ..... | 321        |
| 27.6      | Automatic operator selection diagnostics via UCI .....               | 322        |
| <b>28</b> | <b>Configuring Connection Watch (cwatch) .....</b>                   | <b>327</b> |
| 28.1      | Configuration package used .....                                     | 327        |
| 28.2      | Configuring Connection Watch using the web interface .....           | 327        |
| 28.3      | Configuring cwatch using command line.....                           | 330        |
| 28.4      | cwatch diagnostics .....   | 331        |
| <b>29</b> | <b>Configuring DHCP server and DNS (Dnsmasq).....</b>                | <b>333</b> |
| 29.1      | Configuration package used .....                                     | 333        |
| 29.2      | Configuring DHCP and DNS using the web interface .....               | 333        |
| 29.3      | Configuring DHCP and DNS using command line .....                    | 343        |
| <b>30</b> | <b>Configuring DHCP client.....</b>                                  | <b>348</b> |
| 30.1      | Configuration packages used .....                                    | 348        |
| 30.2      | Configuring DHCP client using the web interface .....                | 348        |
| 30.3      | Configuring DHCP client using command line.....                      | 354        |
| 30.4      | DHCP client diagnostics .....  | 355        |
| <b>31</b> | <b>Configuring DHCP forwarding .....</b>                             | <b>358</b> |
| 31.1      | Configuration packages used .....                                    | 358        |
| 31.2      | Configuring DHCP forwarding using the web interface.....             | 358        |
| 31.3      | Configuring DHCP forwarding using command line .....                 | 359        |
| 31.4      | DHCP forwarding over IPSec.....                                      | 360        |
| 31.5      | DHCP forwarding diagnostics .....                                    | 363        |
| <b>32</b> | <b>Configuring Dynamic DNS.....</b>                                  | <b>365</b> |

---

|           |   |            |
|-----------|---|------------|
| 32.1      | Overview .....  | 365        |
| 32.2      | Configuration packages used .....                                     | 365        |
| 32.3      | Configuring Dynamic DNS using the web interface .....                 | 365        |
| 32.4      | Dynamic DNS using UCI.....  | 367        |
| <b>33</b> | <b>Configuring hostnames.....</b>                                     | <b>369</b> |
| 33.1      | Overview .....  | 369        |
| 33.2      | Local host file records.....  | 369        |
| 33.3      | PTR records.....  | 371        |
| 33.4      | Static leases.....  | 373        |
| <b>34</b> | <b>Configuring firewall .....</b>                                     | <b>376</b> |
| 34.1      | Configuration package used .....                                      | 376        |
| 34.2      | Configuring firewall using the web interface .....                    | 376        |
| 34.3      | Configuring firewall using UCI.....                                   | 388        |
| 34.4      | IPv6 notes .....  | 391        |
| 34.5      | Implications of DROP vs. REJECT .....                                 | 391        |
| 34.6      | Connection tracking .....   | 392        |
| 34.7      | Firewall examples .....   | 393        |
| <b>35</b> | <b>Configuring IPSec.....</b>   | <b>400</b> |
| 35.1      | Configuration package used .....                                      | 400        |
| 35.2      | Configuring IPSec using the web interface.....                        | 400        |
| 35.3      | Configuring IPSec using UCI.....                                      | 409        |
| 35.4      | Configuring an IPSec template for DMVPN via the web interface .....   | 413        |
| 35.5      | Configuring an IPSec template to use with DMVPN .....                 | 420        |
| 35.6      | IPSec diagnostics using the web interface .....                       | 422        |
| 35.7      | IPSec diagnostics using UCI .....                                     | 422        |
| <b>36</b> | <b>Configuring SCEP (Simple Certificate Enrolment Protocol) .....</b> | <b>423</b> |
| 36.1      | Configuration package used .....                                      | 423        |
| 36.2      | Configuring SCEP using the web interface .....                        | 423        |
| 36.3      | SCEP certificate diagnostics.....                                     | 429        |
| <b>37</b> | <b>Dynamic Multipoint Virtual Private Network (DMVPN) .....</b>       | <b>431</b> |
| 37.1      | Prerequisites for configuring DMVPN.....                              | 431        |
| 37.2      | Advantages of using DMVPN.....  | 431        |
| 37.3      | DMVPN scenarios .....   | 432        |
| 37.4      | Configuration packages used .....                                     | 434        |
| 37.5      | Configuring DMVPN using the web interface .....                       | 434        |
| 37.6      | DMVPN diagnostics.....  | 436        |
| <b>38</b> | <b>Configuring multicasting using PIM and IGMP interfaces .....</b>   | <b>439</b> |
| 38.1      | Overview .....  | 439        |
| 38.2      | Configuration package used .....                                      | 439        |
| 38.3      | Configuring PIM and IGMP using the web interface.....                 | 439        |

---

|           |   |            |
|-----------|---|------------|
| 38.4      | Configuring PIM and IGMP using UCI .....                          | 441        |
| <b>39</b> | <b>QoS: VLAN 802.1Q PCP tagging .....</b>                         | <b>443</b> |
| 39.1      | Configuring VLAN PCP tagging .....                                | 443        |
| <b>40</b> | <b>QoS: type of service.....</b>                                  | <b>446</b> |
| 40.1      | QoS configuration overview.....                                   | 446        |
| 40.2      | Configuration packages used .....                                 | 446        |
| 40.3      | Configuring QoS using the web interface.....                      | 446        |
| 40.4      | Configuring QoS using UCI .....                                   | 448        |
| 40.5      | Example QoS configurations.....                                   | 451        |
| <b>41</b> | <b>Management configuration settings .....</b>                    | <b>452</b> |
| 41.1      | Activator.....  | 452        |
| 41.2      | Monitor.....  | 452        |
| 41.3      | Configuration packages used .....                                 | 452        |
| 41.4      | Autoload: boot up activation.....                                 | 453        |
| 41.5      | Autoload packages .....   | 453        |
| 41.6      | Autoload using UCI .....  | 455        |
| 41.7      | HTTP Client: configuring activation using the web interface ..... | 456        |
| 41.8      | Httpclient: Activator configuration using UCI .....               | 459        |
| 41.9      | Httpclient: Activator configuration using package options.....    | 459        |
| 41.10     | User management using UCI .....                                   | 460        |
| 41.11     | Configuring the management user password using UCI.....           | 461        |
| 41.12     | Configuring management user password using package options.....   | 462        |
| 41.13     | User management using UCI .....                                   | 462        |
| 41.14     | User management using package options .....                       | 462        |
| 41.15     | Configuring user access to specific web pages .....               | 463        |
| <b>42</b> | <b>Configuring Monitor.....</b>                                   | <b>464</b> |
| 42.1      | Introduction .....  | 464        |
| 42.2      | Reporting device status to Monitor .....                          | 464        |
| 42.3      | Reporting GPS location to Monitor .....                           | 470        |
| 42.4      | Reporting syslog to Monitor.....                                  | 472        |
| 42.5      | Configuring ISAD .....  | 473        |
| 42.6      | Speedtest reporting.....  | 476        |
| <b>43</b> | <b>Configuring SNMP.....</b>                                      | <b>477</b> |
| 43.1      | Configuration package used .....                                  | 477        |
| 43.2      | Configuring SNMP using the web interface.....                     | 477        |
| 43.3      | Configuring SNMP using command line .....                         | 484        |
| 43.4      | Configuring SNMP interface alias with static SNMP index.....      | 492        |
| 43.5      | Automatic SNMP traps .....  | 494        |
| 43.6      | SNMP diagnostics.....   | 494        |
| <b>44</b> | <b>Event system .....</b>   | <b>497</b> |



---

|           |   |            |
|-----------|---|------------|
| 44.1      | Configuration package used .....  | 497        |
| 44.2      | Event system overview .....   | 497        |
| 44.3      | Configuring the event system using the web interface .....              | 498        |
| 44.4      | Configuring the event system using command line .....                   | 510        |
| 44.5      | Event system diagnostics .....  | 518        |
| <b>45</b> | <b>Configuring data usage monitor .....</b>                             | <b>521</b> |
| 45.1      | Introduction .....  | 521        |
| 45.2      | Configuration package used .....  | 521        |
| 45.3      | Configuring data usage using the web interface .....                    | 521        |
| 45.4      | Data usage status .....   | 524        |
| 45.5      | Data usage diagnostics .....  | 524        |
| <b>46</b> | <b>Configuring terminal server .....</b>                                | <b>526</b> |
| 46.1      | Overview .....  | 526        |
| 46.2      | Configuration packages used .....                                       | 526        |
| 46.3      | Configuring terminal server using the web interface .....               | 526        |
| 46.4      | Configuring terminal server using UCI .....                             | 537        |
| 46.5      | Configuring terminal server using package options .....                 | 538        |
| 46.6      | Configuring terminal server DSR signal management network .....         | 538        |
| 46.7      | Serial mode GPIO control .....  | 540        |
| 46.8      | Terminal server diagnostics .....                                       | 540        |
| <b>47</b> | <b>Configuring terminal package .....</b>                               | <b>543</b> |
| 47.1      | Configuration packages used .....                                       | 543        |
| 47.2      | Configuring terminal package using the web interface .....              | 543        |
| 47.3      | Configuring terminal package using UCI .....                            | 543        |
| 47.4      | Configuring terminal using package options .....                        | 544        |
| 47.5      | Terminal diagnostics .....  | 544        |
| <b>48</b> | <b>Configuring GPIO on the GW2300 Series router .....</b>               | <b>545</b> |
| 48.1      | GPIO connectors .....   | 545        |
| 48.2      | GPIO diagnostics .....  | 545        |
| <b>49</b> | <b>Configuring SCADA RTU (RTUD) .....</b>                               | <b>546</b> |
| 49.1      | Terminology .....   | 546        |
| 49.2      | SCADA RTU overview .....  | 546        |
| 49.3      | Configuration package used .....  | 546        |
| 49.4      | Configuring SCADA RTUD using the web interface .....                    | 547        |
| 49.5      | Controlling the RTUD application manually using the web interface ..... | 552        |
| 49.6      | Viewing RTUD statistics using the web interface .....                   | 553        |
| 49.7      | Configuring RTUD using command line .....                               | 553        |
| 49.8      | RTUD diagnostics .....  | 556        |
| <b>50</b> | <b>SCADA IEC104 gateway .....</b>                                       | <b>557</b> |
| 50.1      | Overview .....  | 557        |

---

|           |  |            |
|-----------|--|------------|
| 50.2      | Configuration packages used .....                          | 558        |
| 50.3      | IEC104 gateway configuration using the web interface ..... | 558        |
| 50.4      | IEC104 gateway configuration using command line .....      | 575        |
| 50.5      | Configuring the terminal server .....                      | 588        |
| 50.6      | Configuring IEC61850 to IEC101 conversion.....             | 597        |
| 50.7      | Diagnostics .....  | 606        |
| <b>51</b> | <b>DNP3 outstation application .....</b>                   | <b>609</b> |
| 51.1      | Configuration packages used .....                          | 609        |
| 51.2      | Configuring using the web interface.....                   | 609        |
| 51.3      | Configuring DNP3 outstation using command line.....        | 610        |
| 51.4      | DNP3 outstation diagnostics .....                          | 611        |
| <b>52</b> | <b>Serial interface .....</b>                              | <b>613</b> |
| 52.1      | Overview .....   | 613        |
| 52.2      | Monitoring serial interfaces using the web interface.....  | 613        |
| 52.3      | Monitoring serial interfaces using command line .....      | 614        |

# 1 Introduction

This user manual describes the features and how to configure Virtual Access GW2300 Series routers.

The Virtual Access GW2300 Series router is an industrial router designed for harsh environments such as roadside cabinets and other remote monitoring and control sites. PoE+ capability supplies up to 30W per Ethernet port to power cameras and other PoE devices. Serial ports and digital IO options make this a very versatile device for many industrial applications. Support for cellular radio modules provides very high availability for critical communications solutions.

## 1.1 Document scope

This document covers models in the GW2300 Series. For general references, we refer to the GW2300 Series throughout.

## 1.2 Using this documentation

You can configure your router using either the router's web interface or via the command line using UCI commands. Each chapter explains first the web interface settings, followed by how to configure the router using UCI. The web interface screens are shown along with a path to the screen for example, 'In the top menu, select **Service -> SNMP.**' followed by a screen grab.

After the screen grab there is an information table that describes each of the screen's fields.

### 1.2.1 Information tables

We use information tables to show the different ways to configure the router using the router's web and command line. The left-hand column shows three options:

- **Web:** refers the command on the router's web page,
- **UCI:** shows the specific UCI command, and
- **Opt:** shows the package option.

The right-hand column shows a description field that describes the feature's field or command and shows any options for that feature.

Some features have a drop-down menu and the options are described in a table within the description column. The default value is shown in a **grey cell**.

Values for enabling and disabling a feature are varied throughout the web interface, for example, 1/0; Yes/No; True/False; check/uncheck a radio button. In the table descriptions, we use **0** to denote Disable and **1** to denote Enable.

Some configuration sections can be defined more than once. An example of this is the routing table where multiple routes can exist and all are named 'route'. For these sections, the UCI command will have a code value [**0**] or [**x**] (where x is the section number) to identify the section.

| Web Field/UCI/Package Option                                | Description                        |
|---|------------------------------------|
| Web: Metric<br>UCI: network.@route[0].metric<br>Opt: metric | Specifies the route metric to use. |

**Note:** these sections can be given a label for identification when using UCI or package options.

```
network.@route[0]=route
network.@route[0].metric=0
```

can be written as:

```
network.routename=route
network.routename.metric=0
```

However the documentation usually assumes that a section label is not configured.

The table below shows fields from a variety of chapters to illustrate the explanations above.

| Web Field/UCI/Package Option  | Description  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
|---|--|---|-----------|---|----------|---|----------|---|-------|---|---------|---|--------|---|---------------|---|-------|
| Web: Enable<br>UCI: cesop.main.enable<br>Opt: enable                        | Enables CESoPSN services.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0 | Disabled. | 1 | Enabled. |   |          |   |       |   |         |   |        |   |               |   |       |
| 0   | Disabled.  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 1   | Enabled.   |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| Web: Syslog Severity<br>UCI: cesop.main.severity<br>Opt: log_severity       | Selects the severity used for logging events CESoPSN in syslog. The following levels are available.<br><table border="1"> <tr> <td>0</td> <td>Emergency</td> </tr> <tr> <td>1</td> <td>Alert</td> </tr> <tr> <td>2</td> <td>Critical</td> </tr> <tr> <td>3</td> <td>Error</td> </tr> <tr> <td>4</td> <td>Warning</td> </tr> <tr> <td>5</td> <td>Notice</td> </tr> <tr> <td>6</td> <td>Informational</td> </tr> <tr> <td>7</td> <td>Debug</td> </tr> </table> | 0 | Emergency | 1 | Alert    | 2 | Critical | 3 | Error | 4 | Warning | 5 | Notice | 6 | Informational | 7 | Debug |
| 0   | Emergency  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 1   | Alert  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 2   | Critical   |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 3   | Error  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 4   | Warning  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 5   | Notice   |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 6   | Informational  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 7   | Debug  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| Web: Agent Address<br>UCI: snmpd.agent[0].agentaddress<br>Opt: agentaddress | Specifies the address(es) and port(s) on which the agent should listen.<br>[[udp tcp]:]port[@address][,...]  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |

**Table 1: Example of an information table**

## 1.2.2 Definitions

Throughout the document, we use the host name 'VA\_router' to cover all router models.

UCI commands and package option examples are shown in the following format:

```
root@VA_router:~# vacmd show current config
```

## 1.2.3 Diagnostics

Diagnostics are explained at the end of each feature's chapter.

## 1.2.4 UCI commands

For detailed information on using UCI commands, read chapters 'Router File Structure' and 'Using Command Line Interface'.

## 2 GW2300 Series hardware

### 2.1 Hardware specification

#### 2.1.1 GW2300 Series router model variants

| Model                      | VDSL2<br>ADSL2+ | GigE | POE+ | 2G/3G/4G | SIM slots | RS232/<br>RS485 | GPIO | WiFi |
|----------------------------|-----------------|------|------|----------|-----------|-----------------|------|------|
| GW2302-PE2-2S-2DI2O-RFW    | -               | 2    | 2    | 1        | 2         | 2               | Yes  | -    |
| GW2302-PE2-WF-RFW          | -               | 2    | 2    | 1        | 2         | -               | -    | Yes  |
| GW2304-PE4-V-2S-2DI2O-RFW  | Yes             | 4    | 4    | 1        | 2         | 2               | Yes  | -    |
| GW2304-PE4-2S-2DI2O-WF-RFW | -               | 4    | 4    | 1        | 2         | 2               | Yes  | Yes  |

Table 2: GW2300 series feature set per model

#### 2.1.2 GW2300 Series hardware features

- Secure boot
- Designed for IP54
- Dual antenna SMA connectors for each mobile module
- Dual antenna SMA connectors for WiFi
- GPS SMA connector
- SD card
- Operates in ambient temperature range of -30 °C to +70 °C
- WiFi: dual band 2.4Ghz and 5Ghz where WiFi is present
- Mini PCI express slot
- Power over Ethernet Plus, each port supplying up to 30 Watts at between 52V and 57V DC.
- Digital I/O
- Dual serial ports where present. Each is software configurable to act as RS232 or RS485
- Two or four 1Gbps Ethernet ports

#### 2.1.3 GSM and LTE technology

- HSPA+
- EDGE/GPRS
- Download up to 150Mbps
- Upload up to 50Mbps
- LTE FDD: B1/B3/B7/B8/B20/B28A
- LTE TDD: B38/B40/B41

## 2.1.4 WiFi

- 2.4GHz and 5GHz
- 802.11b/g/n
- 802.11ac

## 2.1.5 Power supply

The GW2300 Series router is powered by a 120W 100V-240V AC PSU.

A low-voltage option supports input voltages of 24V to 57V.

## 2.1.6 Dimensions

Unit size: 50W 125D 170H mm

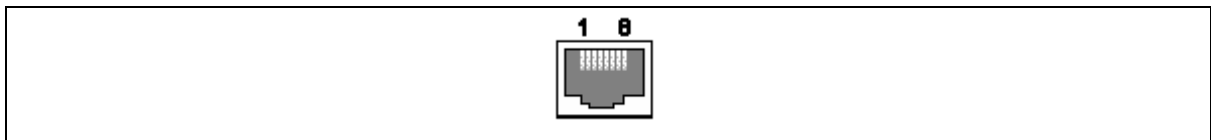
Unit weight: Approx 920g

## 2.1.7 Serial ports

A pair of asynchronous serial ports may be present on a router, for more information on how many serial ports are populated on each model, see Table 1: GW2300 Series feature set per model.

Each serial port is configurable to operate in either RS232 or RS485 mode. The default mode is RS232 for the first port and RS485 for the second port.

The pin numbering of the serial port connector is shown below.



**Figure 1: RJ45 connector front view pin numbering**

### 2.1.7.1 RS232 ports

When you configure a serial port to operate as an RS232 interface, it supports the following signals:

- TX DATA
- RX DATA
- CTS
- RTS
- DSR
- DTR

The pin numbering of RJ45 sockets is as shown below.

The RS232 interface is wired as a DTE, and the pinout is shown in the table below.

| RJ45 Pin | Signal Name | Direction          |
|----------|-------------|--------------------|
| 1        | RTS         | Output from router |
| 2        | DTR         | Output from router |
| 3        | TXD         | Output from router |
| 4        | GND         | -                  |
| 5        | GND         | -                  |
| 6        | RXD         | Input to router    |
| 7        | DSR         | Input to router    |
| 8        | CTS         | Input to router    |

Table 3: RS232 port pinout

### 2.1.7.2 RS485 ports

When you configure a serial port to operate as an RS485 interface, it supports both two-wire (half-duplex) and four-wire (full-duplex) modes. Configurations between two-wire and four-wire RS485 modes will be under software control.

The pin-out of the RJ45 connector in RS485 mode is shown below.

| RJ45 Pin | Four-wire mode |                    | Two-wire mode |           |
|----------|----------------|--------------------|---------------|-----------|
|          | Signal         | Direction          | Signal        | Direction |
| 1        |                |                    |               |           |
| 2        | RXD+           | Input to router    |               |           |
| 3        | RXD-           | Input to router    |               |           |
| 4        |                |                    |               |           |
| 5        |                |                    |               |           |
| 6        | TXD-           | Output from router | D-            | In/Out    |
| 7        | TXD+           | Output from router | D+            | In/Out    |
| 8        |                |                    |               |           |

Table 4: RS485 port pinout

### 2.1.8 Digital I/O interface

On the digital I/O socket, there is a 4x2 pin connector comprising two inputs and two outputs.

The output is a connected to a pair of relay contacts that are normally open, that is open when no power is applied.

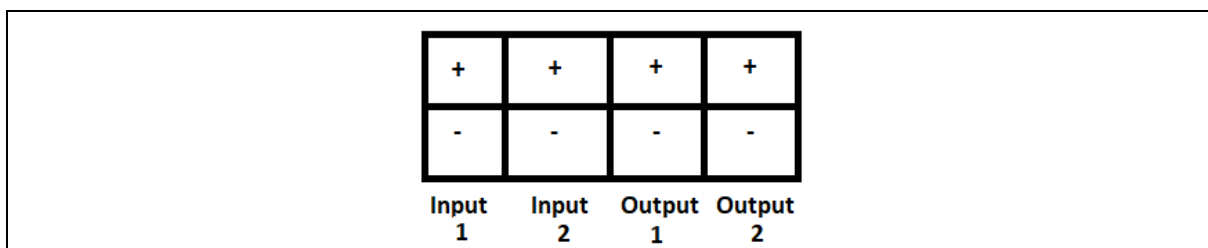


Figure 2: Pinout of digital I/O socket



### 2.1.9 Ethernet

The GW2300 Series router has up to four 1Gbps Ethernet ports. Each Ethernet port can be configured to deliver Power over Ethernet (PoE) with a total power of 120W; each port supplying up to 30 Watts at between 52V and 57V DC.

The ports support 802.3at Type 2 (Power over Ethernet Plus).

## 2.2 Compliance

GW2300 Series routers are compliant and tested to the following standards:

- CE approved including CE RED
- EMC declaration
- Safety declaration based on IEC 62368
- IEC 61000-6-2:2016

### 2.2.1 Vibration standards

The GW2300 Series router complies with these requirements:

- Freefall drop test to EN60068-2-32:2008
- Bump test to EN60068-2-27:2009
- Random vibration test to EN60068-2-64:2008
- Mechanical shock test to EN60068-2-27:2009

## 2.3 Antenna

GW2300 Series routers can have up to seven SMA connectors for connection of up to seven antennas. Depending on the model variant:



- Two LTE antennas for each mobile radio module (optionally up to two mobile radio modules)
- Two WiFi antennas for WiFi
- Single antenna for GPS

## 2.4 Components

To enable and configure connections on your router, it must be correctly installed.




GW2300 Series routers contain an internal web server that you use for configurations. Before you can access the internal web server and start the configuration, ensure the components are correctly connected and that your PC has the correct networking setup.

All GW2300 Series routers come with the following components as standard:

|   |  |
|---|--|
| 1 x GW2300 Series router (models vary)        |  |
| 1 x 120W 52V-57V power supply unit (2 parts). |   |

**Table 5: GW2300 series router standard components**

Optional components include:

|   |   |
|---|---|
| 1 x ADSL cable: RJ11 to RJ11 (purple)     |    |
| 1 x Ethernet cable RJ45 to RJ45 (yellow). |    |
| 2 x 4G/LTE antennas                       |   |
| Extra antennas                            | Virtual Access supplies a wide range of antennas for 3G, 4G/LTE and WiFi. Please visit our website: <a href="http://virtualaccess.com/antenna-options/">http://virtualaccess.com/antenna-options/</a> or contact Virtual Access for more information. |

**Table 6: GW2300 series router optional components**

## 2.5 Inserting SIM cards

### 2.5.1 Inserting SIM 1 card

- Ensure the unit is powered off.
- Remove the SIM cover using a Torx key
- Hold the SIM 1 card with the chip side facing down and the cut corner facing away from you, to the left.
- Gently push the SIM card into the upper SIM slot 1 until it clicks in.



Figure 3: Inserting SIM card into SIM1 slot

### 2.5.2 Inserting SIM 2 card




- If you are using a second SIM, hold the SIM 2 card with the chip side facing up and the cut corner front right facing away from you.
- Gently push the SIM card into the lower SIM slot 2 until it clicks in.



Figure 4: Inserting SIM card into SIM2 slot

## 2.6 Connecting the SIM cover

Connect the SIM cover using a Torx key.

|   |   |
|---|---|
|  | SIM cover                                     |
|  | Torx key (not provided)                       |
|  | GW2300 Series router with SIM cover in place. |

## 2.7 Connecting cables

Connect one end of the Ethernet cable into port A and the other end to your PC or switch.

## 2.8 Connecting the antenna

If you are only connecting one antenna, screw the antenna into the MAIN SMA connector.

If you are using more than one antenna, screw the main antenna into the MAIN SMA connector and the secondary antenna into the 3G-AUX SMA connector.

## 2.9 Connecting the WiFi antenna

If you are connecting one antenna, screw the antenna into either of the WiFi SMA connectors. You can use a second WiFi antenna if necessary.

## 2.10 Powering up

Plug the power cable into an electrical socket suitable for the power supply.

The GW2300 takes less than a minute to boot up. During this time, the power LED flashes.

Other LEDs display different diagnostic patterns during boot up.

Booting is complete when the power LED stops flashing and stays on steady.

## 2.11 Reset button

Use the reset button to request a system reset.

When you press the reset button all LEDs turn on simultaneously. The length of time you hold the reset button will determine its behaviour.

| <b>Press duration</b>             | <b>PWR/CONFIG LED behaviour</b> | <b>Router behaviour on depress</b>  |
|-----------------------------------|---------------------------------|---|
| 0-3 seconds                       | Solid on                        | Normal reset to running config. No special LED activity.                          |
| Between 3 and 15 seconds          | Flashing fast                   | Releasing between 3-15 seconds switches the router back to factory configuration. |
| Between 15 and 20 seconds         | Solid on                        | Releasing between 15-20 seconds performs a normal reset to running config.        |
| Between 20 seconds and 30 seconds | Flashing slowly                 | Releasing between 20-30 seconds reboots the router in recovery mode.              |
| Over 30 seconds                   | Solid on                        | Releasing after 30 seconds performs a normal reset.                               |

**Table 7: GW2300 series router reset behaviour**

### 2.11.1 Recovery mode

Recovery mode is a fail-safe mode where the router can load a default configuration from the routers firmware. If your router goes into recovery mode, all config files are kept intact. After the next reboot, the router will revert to the previous config file.

You can use recovery mode to manipulate the config files, but should only be used if all other configs files are corrupt. If your router has entered recovery mode, contact your local reseller for access information.

## 3 GW2300 Series LED behaviour

### 3.1 Main LED behaviour

The GW2300 Series router has single colour LEDs. When the router is powered on, the power LED is green. There are five variants of GW2300.

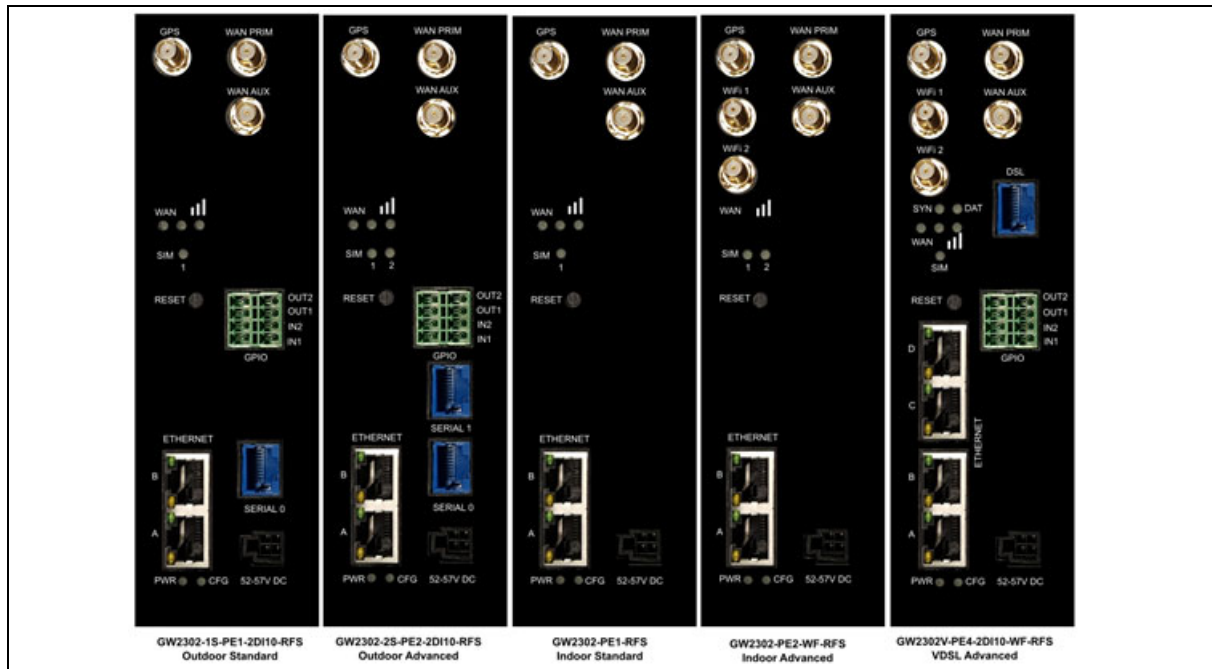


Figure 5: The various front plates of the GW2300 series

The possible LED states are:

- Off
- Flashing slowing
- Flashing quickly
- On

|                  |                  |  |
|------------------|------------------|--|
| Booting up       |                  | The router takes less than a minute to boot up. During this time, the power LED flashes. Other LEDs display different diagnostic patterns during boot up. Booting is complete when the power LED stops flashing and stays on steady. |
| Power LED        | On               | Power  |
|                  | Off              | No power. Boot loader does not exist.  |
|                  | Flashing         | Booting.   |
| Config LED       | On               | Unit running a valid configuration file.   |
|                  | Flashing slowly  | Unit running in recovery mode (2.5 flashes per second).  |
|                  | Flashing quickly | Unit running in factory configuration (5 flashes per second).  |
| SIM1 & SIM2 LEDs | On               | SIM selected and registered on the 3G/4G network.  |
|                  | Off              | Not selected or SIM not inserted.  |
|                  | Flashing         | SIM selected and not registered on the network.  |

|  |                  |   |
|--|------------------|---|
| 3G/LTE<br>Cellular Signal<br>Strength LEDs | None             | Data link not connected or signal strength $\leq -113\text{dBm}$ .                    |
|  | 1                | Data link connected and signal strength $\leq -89\text{dBm}$ .                        |
|  | 2                | Data link connected and signal strength between $-89\text{dBm}$ and $-69\text{dBm}$ . |
|  | 3                | Data link connected and signal strength $> -69\text{dBm}$ .                           |
| DSL SYN<br>available on<br>models:         | On               | Connected and established to ADSL or VDSL DSLAM.                                      |
|  | Off              | Not active.   |
|  | Flashing slowly  | Searching for DSL connection.   |
|  | Flashing quickly | Connection negotiating.   |
| DSL DAT                                    | On               | Transmit data.  |
|  | Off              | No data transmit.   |

**Table 8: LED behaviour and descriptions**

## 3.2 Ethernet port LED behaviour

The Ethernet port has two LEDs: a LINK LED (green) and a SPEED LED (amber). When looking at the port, the LED on the top is the LINK LED, and the SPEED LED is on the bottom.



**Figure 6: Ethernet LED activity**

|                      |          |  |
|----------------------|----------|--|
| LINK LED<br>(green)  | On       | Physical Ethernet link detected.                     |
|                      | Off      | No physical Ethernet link detected.                  |
|                      | Flashing | Data is being transmitted or received over the link. |
| SPEED LED<br>(amber) | On       | Link operating at 10/100mbps mode.                   |
|                      | Off      | Link operating at 1Gb/s.                             |

**Table 9: Ethernet LED behaviour and descriptions**

## 4 Factory configuration extraction from SIM card

Virtual Access routers have a feature to update the factory configuration from a SIM card. This allows you to change the factory configuration of a router when installing the SIM.

1. Make sure the SIM card you are inserting has the required configuration written on it.
2. Ensure the router is powered off.
3. Hold the SIM 1 card with the chip side facing down and the cut corner front left.
4. Gently push the SIM card into SIM slot 1 until it clicks in.
5. Power up the router.

Depending on the model, the power LED and/or the configuration LED flash as usual.

The SIM LED starts flashing. This indicates the application responsible for 3G and configuration extraction management is running. It also means the update of the configuration is happening.

When the update is finished, depending on the model, the power LED and/or the configuration LED blink alternatively and very fast for 20 seconds.

**Note:** factory configuration extraction is only supported on mobile modules that support phone book operations.



## 5 Accessing the router

Access the router through the web interface or by using SSH. By default, Telnet is disabled.

### 5.1 Configuration packages used

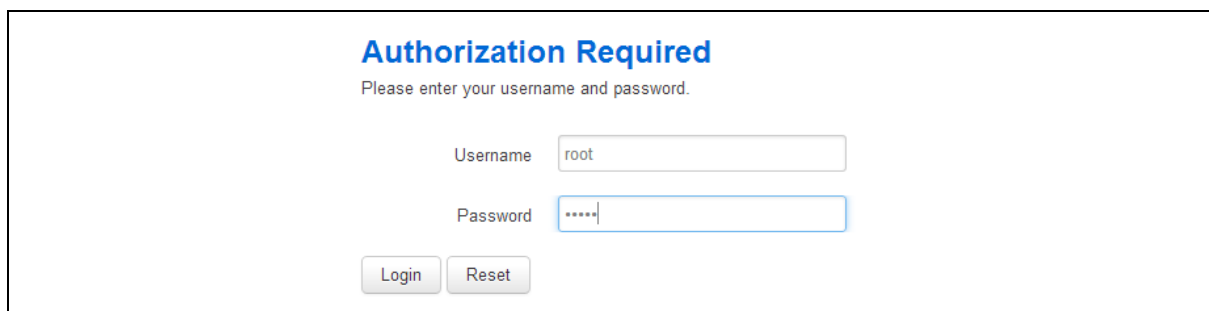
| Package  | Sections     |
|----------|--------------|
| dropbear | dropbear     |
| system   | main         |
| uhttpd   | main<br>cert |

### 5.2 Accessing the router over Ethernet using the web interface

DHCP is disabled by default, so if you do not receive an IP address via DHCP, assign a static IP to the PC that will be connected to the router.

|                 |                 |
|-----------------|-----------------|
| PC IP address   | 192.168.100.100 |
| Network mask    | 255.255.255.0   |
| Default gateway | 192.168.100.1   |

Assuming that the PC is connected to Port A on the router, in your internet browser, type in the default local IP address 192.168.100.1, and press **Enter**. The Authorization page appears.



**Figure 7: The login page**

The password may vary depending on the factory configuration the router has been shipped with. The default settings are shown below. The username and password are case sensitive.

In the username field, type **root**.

In the Password field, type **admin**.

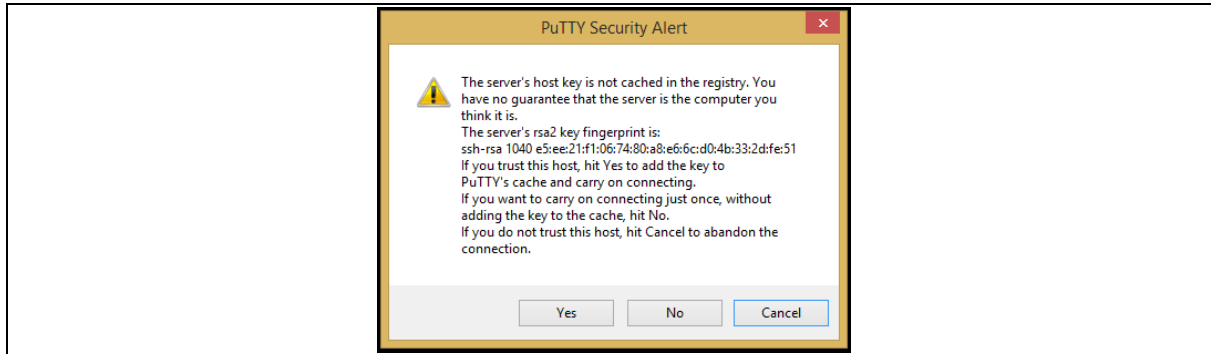
Click **Login**. The Status page appears.

## 5.3 Accessing the router over Ethernet using an SSH client

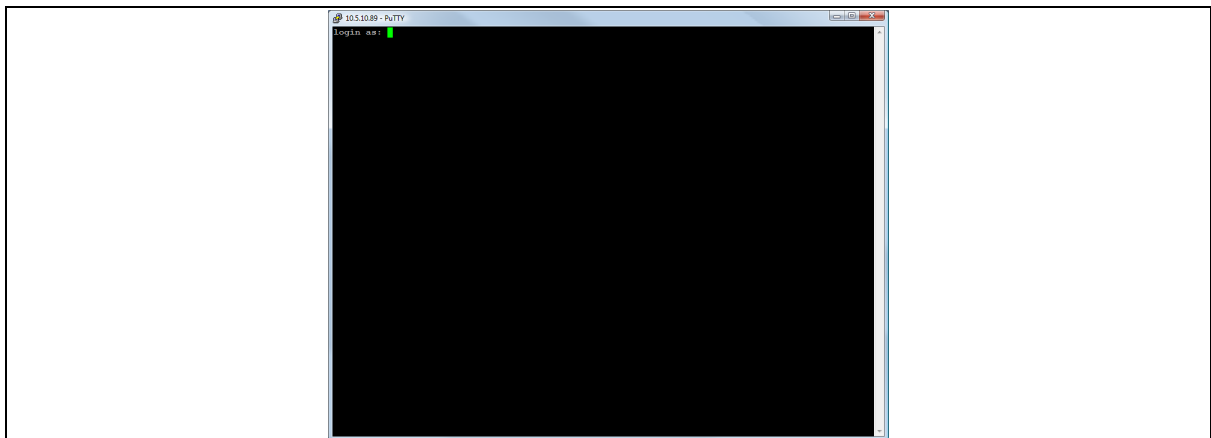
You can also access the router over Ethernet, using Secure Shell (SSH) and optionally over Telnet.

To access CLI over Ethernet start an SSH client and connect to the router's management IP address, on port **22: 192.168.100.1/24**.

On the first connection, you may be asked to confirm that you trust the host.



**Figure 8: Confirming trust of the routers public key over SSH**



**Figure 9: SSH CLI logon screen**

In the SSH CLI logon screen, enter the default username and password.

Username: **root**

Password: **admin**

### 5.3.1 SCP (Secure Copy Protocol)

As part of accessing the router over SSH, you can also use SCP protocol. Use the same user authentication credentials as for SSH access. You can use SCP protocol to securely, manually transfer files from and to the router's SCP server.

No dedicated SPC client is supported; select the SCP client software of your own choice.

## 5.4 Accessing the router over Ethernet using a Telnet client

Telnet is disabled by default, when you enable Telnet, SSH is disabled.

To enable Telnet, enter:

```
root@VA_router: ~# /etc/init.d/dropbear disable
root@VA_router: ~# reboot
```

To re-enable SSH, enter:

```
root@VA_router: ~# /etc/init.d/dropbear enable
root@VA_router: ~# reboot
```

**Note:** as SSH is enabled by default, initial connection to the router to enable Telnet must be established over SSH.

## 5.5 Configuring the password

### 5.5.1 Configuration packages used

| Package | Sections |
|---------|----------|
| system  | main     |

## 5.6 Configuring the password using the web interface

To change your password, in the top menu click **System -> Administration**. The Administration page appears.

**Figure 10: The router password section**

In the Router Password section, type your new password in the password field and then retype the password in the confirmation field.

Scroll down the page and click **Save & Apply**.

**Note:** the username 'root' cannot be changed.

| Web Field/UCI/Package Option                                | Description   |
|---|---|
| Web: Password<br>UCI: system.main.password<br>Opt: password | Defines the root password. The password is displayed encrypted via the CLI using the 'hashpassword' option.<br>UCI: system.main.hashpassword<br>Opt: hashpassword |

## 5.7 Configuring the password using UCI

The root password is displayed encrypted via the CLI using the hashpassword option.

```
root@VA_router:~# uci show system
system.main=system
system.main.hostname=VA_router
system.main.hashpassword=$1$jRX/x8A/$U5kLCMpi9dcahRh017eZV1
```

If you are changing the password using UCI, enter the new password in plain text using the password option.

```
root@VA_router:~# uci system.main.password=newpassword
root@VA_router:~# uci commit
```

The new password will take effect after a reboot and will now be displayed in encrypted format via the hashpassword option.

## 5.8 Configuring the password using package options

The root password is displayed encrypted via the CLI using the hashpassword option.

```
root@VA_router:~# uci export system
package system

config system 'main'
    option hostname 'VA_router'
    option hashpassword '$1$wRYyiJOz$EeHN.GQcxXhRgNPVbqxVw
```

If you are changing the password using UCI, enter the new password in plain text using the password option.

```
package system

config system 'main'
    option hostname 'VA_router'
    option hashpassword '$1$wRYyiJOz$EeHN.GQcxXhRgNPVbqxVw
    option password 'newpassword'
```

The new password will take effect after reboot and will now be displayed in encrypted format via the hashpassword option.

## 5.9 Accessing the device using RADIUS authentication

You can configure RADIUS authentication to access the router over SSH, web or local console interface.

```
package system

config system 'main'
    option hostname 'VirtualAccess'
    option timezone 'UTC'

config pam_auth
    option enabled 'yes'
    option pamservice 'login'
    option pammodule 'auth'
    option pamcontrol 'sufficient'
    option type 'radius'
    option servers '192.168.0.1:3333|test|20 192.168.2.5|secret|10'

config pam_auth
    option enabled 'yes'
    option pamservice 'sshd'
    option pammodule 'auth'
    option pamcontrol 'sufficient'          it checks package
management_users
    option type 'radius'
    option servers '192.168.0.1:3333|test|20 192.168.2.5|secret|10'

config 'pam_auth'
    option enabled 'yes'
    option pamservice 'luci'
    option pammodule 'auth'
    option pamcontrol 'sufficient'
    option type 'radius'
    servers '192.168.0.1:3333|test|20 192.168.2.5|secret|10'
```

| UCI/Package Option  | Description  |            |   |          |   |   |   |
|---|--|------------|---|----------|---|---|---|
| UCI: system.@pam_auth[0].enabled=yes<br>Opt: enabled                              | Enables and disables RADIUS configuration sections.<br><table border="1"> <tr> <td>yes</td> <td>Enables the following RADIUS configuration section.</td> </tr> <tr> <td>no</td> <td>Disables the following RADIUS configuration section.</td> </tr> </table>   | yes        | Enables the following RADIUS configuration section.   | no       | Disables the following RADIUS configuration section.  |   |   |
| yes   | Enables the following RADIUS configuration section.  |            |   |          |   |   |   |
| no  | Disables the following RADIUS configuration section.   |            |   |          |   |   |   |
| UCI: system.@pam_auth[0].pamservice<br>Opt: pamservice                            | Selects the method which users should be authenticated by.<br><table border="1"> <tr> <td>login</td> <td>User connecting over console cable.</td> </tr> <tr> <td>sshd</td> <td>User connecting over SSH.</td> </tr> <tr> <td>luci</td> <td>User connecting over web.</td> </tr> </table>   | login      | User connecting over console cable.   | sshd     | User connecting over SSH.   | luci  | User connecting over web.   |
| login   | User connecting over console cable.  |            |   |          |   |   |   |
| sshd  | User connecting over SSH.  |            |   |          |   |   |   |
| luci  | User connecting over web.  |            |   |          |   |   |   |
| UCI: system.@pam_auth[0].pamcontrol<br>Opt: pamcontrol                            | Specifies authentication behaviour after authentication fails or connection to RADIUS server is broken.<br><table border="1"> <tr> <td>Sufficient</td> <td>First authenticates against remote RADIUS if password authentication fails then it tries the local database (user defined in package management_users).</td> </tr> <tr> <td>Required</td> <td>If either authentication fails or the RADIUS server is not reachable then the user is not allowed to access the router.</td> </tr> <tr> <td>[success=done<br/>new_authtok_reqd=done<br/>authinfo_unavail=ignore<br/>default=die]</td> <td>Local database is only checked if the RADIUS server is not reachable.</td> </tr> </table> | Sufficient | First authenticates against remote RADIUS if password authentication fails then it tries the local database (user defined in package management_users). | Required | If either authentication fails or the RADIUS server is not reachable then the user is not allowed to access the router. | [success=done<br>new_authtok_reqd=done<br>authinfo_unavail=ignore<br>default=die] | Local database is only checked if the RADIUS server is not reachable. |
| Sufficient  | First authenticates against remote RADIUS if password authentication fails then it tries the local database (user defined in package management_users).  |            |   |          |   |   |   |
| Required  | If either authentication fails or the RADIUS server is not reachable then the user is not allowed to access the router.  |            |   |          |   |   |   |
| [success=done<br>new_authtok_reqd=done<br>authinfo_unavail=ignore<br>default=die] | Local database is only checked if the RADIUS server is not reachable.  |            |   |          |   |   |   |
| UCI:<br>system.@pam_auth[0].pammodule.auth<br>Opt: pammodule                      | Enables user authentication.   |            |   |          |   |   |   |
| UCI: system.@pam_auth[0].type.radius<br>Opt: type                                 | Specifies the authentication method.   |            |   |          |   |   |   |
| UCI: system.@pam_auth[0].servers<br>Opt: servers                                  | Specifies the RADIUS server along with port number, password and timeout in seconds.<br>Port and timeout are optional. The default port for RADIUS is 1812; default timeout is 10 seconds.<br>Multiple servers are entered using a space separator.<br>Syntax:<br><server ip address>[:<port>] <secret>[[timeout]<br>Examples:<br>option servers `192.168.0.1test`<br>option servers `192.168.0.1 test 192.168.2.5:1234 secret 10`   |            |   |          |   |   |   |

Table 10: Information table for RADIUS authentication

## 5.10 Accessing the device using TACACS+ authentication

You can configure TACACS+ authentication for accessing the router over SSH, web or local console interface.

```
package system

config system 'main'
```

```
option hostname 'VirtualAccess'
option timezone 'UTC'

config pam_auth
option enabled 'yes'
option pamservice 'sshd'
option pammodule 'auth'
option pamcontrol 'sufficient'
option type 'tacplus'
option servers '192.168.0.1:49|secret'

config pam_auth
option enabled 'yes'
option pamservice 'sshd'
option pammodule 'account'
option pamcontrol 'sufficient'
option type 'tacplus'
option servers '192.168.0.1:49|secret'
option args 'service=ppp'

config pam_auth
option enabled 'yes'
option pamservice 'sshd'
option pammodule 'session'
option pamcontrol 'sufficient'
option type 'tacplus'
option servers '192.168.0.1:49|secret'
option args 'service=ppp'

config pam_auth
option enabled 'yes'
option pamservice 'luci'
option pammodule 'auth'
option pamcontrol 'sufficient'
option type 'tacplus'
option servers '192.168.0.1:49|secret'
```

```
config pam_auth
    option enabled 'yes'
    option pamservice 'luci'
    option pammodule 'account'
    option pamcontrol 'sufficient'
    option type 'tacplus'
    option servers '192.168.0.1:49|secret'
    option args 'service=ppp'
```

```
config pam_auth
    option enabled 'yes'
    option pamservice 'luci'
    option pammodule 'session'
    option pamcontrol 'sufficient'
    option type 'tacplus'
    option servers '192.168.0.1:49|secret'
    option args 'service=ppp'
```

```
config pam_auth
    option enabled 'yes'
    option pamservice 'login'
    option pammodule 'auth'
    option pamcontrol 'sufficient'
    option type 'tacplus'
    option servers '192.168.0.1:49|secret'
```

```
config pam_auth
    option enabled 'yes'
    option pamservice 'login'
    option pammodule 'account'
    option pamcontrol 'sufficient'
    option type 'tacplus'
    option servers '192.168.0.1:49|secret'
    option args 'service=ppp'
```

```
config pam_auth
    option enabled 'yes'
    option pamservice 'login'
```



```

option pammodule 'session'
option pamcontrol 'sufficient'
option type 'tacplus'
option servers '192.168.0.1:49|secret'
option args 'service=ppp'

```

| UCI/Package Option  | Description  |            |   |          |  |   |  |
|---|--|------------|---|----------|--|---|--|
| UCI: system.@pam_auth[0].enabled=yes<br>Opt: enabled                              | Enables and disables TACACS configuration sections. <table border="1"> <tr> <td>yes</td> <td>Enables following the TACACS configuration section.</td> </tr> <tr> <td>no</td> <td>Disables following the TACACS configuration section.</td> </tr> </table>  | yes        | Enables following the TACACS configuration section.   | no       | Disables following the TACACS configuration section.   |   |  |
| yes   | Enables following the TACACS configuration section.  |            |   |          |  |   |  |
| no  | Disables following the TACACS configuration section.   |            |   |          |  |   |  |
| UCI: system.@pam_auth[0].pamservice<br>Opt: pamservice                            | Selects the method which users should be authenticated by. <table border="1"> <tr> <td>login</td> <td>User connecting over console cable.</td> </tr> <tr> <td>sshd</td> <td>User connecting over SSH.</td> </tr> <tr> <td>luci</td> <td>User connecting over web.</td> </tr> </table>  | login      | User connecting over console cable.   | sshd     | User connecting over SSH.  | luci  | User connecting over web.  |
| login   | User connecting over console cable.  |            |   |          |  |   |  |
| sshd  | User connecting over SSH.  |            |   |          |  |   |  |
| luci  | User connecting over web.  |            |   |          |  |   |  |
| UCI: system.@pam_auth[0].pamcontrol<br>Opt: pamcontrol                            | Specifies the authentication behaviour after authentication fails or the connection to TACACS server is broken. <table border="1"> <tr> <td>Sufficient</td> <td>First authenticates against the remote TACACS if password authentication fails, then it tries local database (user defined in package management_users)</td> </tr> <tr> <td>Required</td> <td>If either authentication fails or the TACACS server is not reachable, then the user is not allowed to access the router.</td> </tr> <tr> <td>[success=done<br/>new_authtok_reqd=done<br/>authinfo_unavail=ignore<br/>default=die]</td> <td>Local database is only checked if the TACACS server is not reachable.</td> </tr> </table> | Sufficient | First authenticates against the remote TACACS if password authentication fails, then it tries local database (user defined in package management_users) | Required | If either authentication fails or the TACACS server is not reachable, then the user is not allowed to access the router. | [success=done<br>new_authtok_reqd=done<br>authinfo_unavail=ignore<br>default=die] | Local database is only checked if the TACACS server is not reachable.      |
| Sufficient  | First authenticates against the remote TACACS if password authentication fails, then it tries local database (user defined in package management_users)  |            |   |          |  |   |  |
| Required  | If either authentication fails or the TACACS server is not reachable, then the user is not allowed to access the router.   |            |   |          |  |   |  |
| [success=done<br>new_authtok_reqd=done<br>authinfo_unavail=ignore<br>default=die] | Local database is only checked if the TACACS server is not reachable.  |            |   |          |  |   |  |
| UCI:<br>system.@pam_auth[0].pammodule.auth<br>Opt: pammodule                      | Selects which TACACS module this part of the configuration relates to. <table border="1"> <tr> <td>auth</td> <td>Auth module provides the actual authentication and sets credentials.</td> </tr> <tr> <td>account</td> <td>Account module checks to make sure that access is allowed for the user.</td> </tr> <tr> <td>session</td> <td>Session module performs additional tasks which are needed to allow access.</td> </tr> </table>   | auth       | Auth module provides the actual authentication and sets credentials.  | account  | Account module checks to make sure that access is allowed for the user.  | session   | Session module performs additional tasks which are needed to allow access. |
| auth  | Auth module provides the actual authentication and sets credentials.   |            |   |          |  |   |  |
| account   | Account module checks to make sure that access is allowed for the user.  |            |   |          |  |   |  |
| session   | Session module performs additional tasks which are needed to allow access.   |            |   |          |  |   |  |
| system.@pam_auth[0].type=tacplus<br>Opt: type                                     | Specifies the authentication method.   |            |   |          |  |   |  |

|   |   |
|---|---|
| UCI: system.@pam_auth[0].servers<br>Opt: servers          | Specifies TACACS servers along with port number and password.<br>Port is optional. The default port for TACACS is 49.<br>Multiple servers are entered using a space separator.<br>Syntax:<br><server ip address>[:<port>] <secret><br>Examples:<br>option servers `192.168.0.1 test`<br>option servers `192.168.0.1 test 192.168.2.5:1234 secret` |
| UCI:<br>system.@pam_auth[1].args=service=ppp<br>Opt: args | Additional arguments to pass to TACACS server.  |

Table7: Information table for TACACS authentication

## 5.11 SSH

SSH allows you to access remote machines over text-based shell sessions. SSH uses public key cryptography to create a secure connection. These connections allow you to issue commands remotely via a command line.

The router uses a package called Dropbear to configure the SSH server on the box. You can configure Dropbear using the web interface or through an SSH connection by editing the file stored on: /etc/config\_name/dropbear.

### 5.11.1 Configuration packages used

| Package  | Sections |
|----------|----------|
| dropbear | dropbear |

### 5.11.2 SSH access using the web interface


In the top menu, click **System -> Administration**. The Administration page appears. Scroll down to the SSH Access section.


## SSH Access


Dropbear offers [SSH](#) network shell access and an integrated [SCP](#) server


### Dropbear Instance

Interface  LAN: (no interfaces attached)

LAN1: 

MOBILE1: 

PPPoADSL: 

loopback: 

unspecified

Listen only on the given interface or, if unspecified, on all

Port  Specifies the listening port of this Dropbear instance

Password authentication  Allow SSH password authentication

Allow root logins with password  Allow the root user to login with password

Gateway ports  Allow remote hosts to connect to local SSH forwarded ports

Idle Session Timeout (seconds)  Remote session will be closed after this many seconds of inactivity

Maximum login attempts  SSH connection is dropped once this limit is reached

Figure 11: The SSH access section

| Web Field/UCI/Package Option  | Description   |               |                            |       |                             |
|---|---|---------------|----------------------------|-------|-----------------------------|
| Web: Interface<br>UCI: dropbear.@dropbear[0].Interface<br>Opt: interface  | <p>Listens only on the selected interface. If you check unspecified, it listens on all interfaces. All configured interfaces will be displayed via the web GUI.</p> <table border="1" style="width: 100%;"> <tr> <td>(unspecified)</td> <td>Listens on all interfaces.</td> </tr> <tr> <td>Range</td> <td>Configured interface names.</td> </tr> </table> | (unspecified) | Listens on all interfaces. | Range | Configured interface names. |
| (unspecified)   | Listens on all interfaces.  |               |                            |       |                             |
| Range   | Configured interface names.   |               |                            |       |                             |
| Web: Port<br>UCI: dropbear.@dropbear[0].Port<br>Opt: port   | <p>Specifies the listening port of the Dropbear instance.</p> <table border="1" style="width: 100%;"> <tr> <td>22</td> <td></td> </tr> <tr> <td>Range</td> <td>0-65535</td> </tr> </table>  | 22            |                            | Range | 0-65535                     |
| 22  |   |               |                            |       |                             |
| Range   | 0-65535   |               |                            |       |                             |
| Web: Password authentication<br>UCI:<br>dropbear.@dropbear[0].PasswordAuth<br>Opt: PasswordAuth                 | <p>If enabled, allows SSH password authentication.</p> <table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0             | Disabled.                  | 1     | Enabled.                    |
| 0   | Disabled.   |               |                            |       |                             |
| 1   | Enabled.  |               |                            |       |                             |
| Web: Allow root logins with password<br>UCI:<br>dropbear.@dropbear[0].RootPasswordAuth<br>Opt: RootPasswordAuth | <p>Allows the root user to login with password.</p> <table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0             | Disabled.                  | 1     | Enabled.                    |
| 0   | Disabled.   |               |                            |       |                             |
| 1   | Enabled.  |               |                            |       |                             |
| Web: Gateway ports<br>UCI:<br>dropbear.@dropbear[0].GatewayPorts<br>Opt: GatewayPorts                           | <p>Allows remote hosts to connect to local SSH forwarded ports.</p> <table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0             | Disabled.                  | 1     | Enabled.                    |
| 0   | Disabled.   |               |                            |       |                             |
| 1   | Enabled.  |               |                            |       |                             |

|  |  |             |
|--|--|-------------|
| Web: Idle Session Timeout<br>UCI: dropbear.@dropbear[0].IdleTimeout<br>Opt: IdleTimeout                | Defines the idle period where the remote session will be closed after the allocated number of seconds of inactivity. |             |
|  | 30   | 30 seconds. |
| Web: n/a<br>UCI: dropbear.@dropbear[0].BannerFile<br>Opt: BannerFile                                   | Defines a banner file to be displayed during login.  |             |
|  | /etc/banner  |             |
| Web: Maximum login attempts<br>UCI:<br>dropbear.@dropbear[0].MaxLoginAttempts<br>Opt: MaxLoginAttempts | Specifies maximum login failures before session terminates.  |             |
|  | 10   |             |
|  | 0-infinite   |             |

Table 11: Information table for SSH access settings

## 5.12 Package dropbear using UCI

```

root@VA_router:~# uci show dropbear
dropbear.@dropbear[0]=dropbear
dropbear.@dropbear[0].PasswordAuth=on
dropbear.@dropbear[0].RootPasswordAuth=on
dropbear.@dropbear[0].GatewayPorts=0
dropbear.@dropbear[0].IdleTimeout=30
dropbear.@dropbear[0].Port=22
dropbear.@dropbear[0].MaxLoginAttempts=3
Package dropbear using package options
root@VA_router:~# uci export dropbear
package dropbear
config dropbear'
    option PasswordAuth 'on'
    option RootPasswordAuth 'on'
    option Port '22'
    option GatewayPorts '0'
    option IdleTimeout '30'
    option MaxLoginAttempts '3'

```

## 5.13 Certs and private keys

Certificates are used to prove ownership of a public key. They contain information about the key, its owner's ID, and the digital signature of an individual that has verified the content of the certificate.

In asymmetric cryptography, public keys are announced to the public, and a different private key is kept by the receiver. The public key is used to encrypt the message and the private key is used to decrypt it.

To access certs and private keys, in the top menu, click **System -> Administration**. The Administration page appears. Scroll down to the Certs & Private Keys section.

**Certificates & Private Keys**  
Certificates and private keys used for various services could be uploaded here

IPsec Certificates and Keys  No file chosen

Upload a \*.tar.gz file containing certificates and/or private keys. All the ipsec certs previously uploaded will be deleted when new ones uploaded. Archive structure should match this of /etc/ipsec.d folder. Every file should be in one of 8 subfolders according to it's purpose:  
**private** (private keys) **certs** (entity certs)  
**crts** (revocation lists)  
**cacerts** (CA certs)  
**ocspcerts** (OCSP signer certs)  
**aacerts** (Authorization Authority certs)  
**acerts** (attribute certs)  
**reqs** (PKCS#10 cert requests)  
[More info](#)

OpenVPN Certificates and Keys  No file chosen

Upload a \*.tar.gz file containing certificates and/or private keys. All the openvpn certs previously uploaded will be deleted when new ones uploaded. OpenVPN requires no special folder structure, hence files will be installed into the openvpn folder as they are in archive

VA Certificates and Keys  No file chosen

Upload a \*.tar.gz file containing certificates and/or private keys. All the va certs previously uploaded will be deleted when new ones uploaded. Archive structure should match this of /etc/certs folder which is similar to /etc/ipsec.d folder.

**Figure 12: The certificates & private keys section**

This section allows you to upload any certificates and keys that you may have stored. There is support for IPsec, OpenVPN and VA certificates and keys.

If you have generated your own SSH public keys, you can input them in the SSH Keys section, for SSH public key authentication.

**SSH-Keys**  
Here you can paste public SSH-Keys (one per line) for SSH public-key authentication.

**Figure 13: The SSH-keys box**

## 5.14 Configuring a router's web server

The router's web server is configured in package uhttpd. This file defines the behaviour of the server and default values for certificates generated for SSL operation. uhttpd supports multiple instances, that is, multiple listen ports, each with its own document root and other features, as well as cgi and lua. There are two sections defined:

**Main:** this uHTTPd section contains general server settings.

**Cert:** this section defines the default values for SSL certificates.

## 5.14.1 Configuration packages used

| Package | Sections |
|---------|----------|
| uhttpd  | main     |
|         | cert     |

To configure the router's HTTP server parameters, in the top menu, select **Services -> HTTP Server**. The HTTP Server page has two sections.

|                      |                       |
|----------------------|-----------------------|
| Main Settings        | Server configurations |
| Certificate Settings | SSL certificates.     |

## 5.14.2 Main settings

### HTTP Server

Configuration of the Http Server used for management of the device.

#### Main Settings

Basic configuration of the Http Server.

Listen Address and Port:  Specifies the ports and addresses to listen on for plain HTTP access. If only a port number is given, the server will attempt to serve both IPv4 and IPv6 requests. Use 0.0.0.0:80 to bind at port 80 only on IPv4 interfaces or [::]:80 to serve only IPv6

Secure Listen Address and Port:  Specifies the ports and addresses to listen on for encrypted HTTPS access.

Home path:  Defines the server document root.

Cert file:  PEM certificate used to serve HTTPS connections.

Key file:  PEM private key used to serve HTTPS connections.

CGI prefix:  Defines the prefix for CGI scripts, relative to the document root. CGI support is disabled if this option is missing

Script timeout (s):  Maximum wait time for CGI or Lua requests in seconds. Requested executables are terminated if no output was generated until the timeout expired

Network timeout (s):  Maximum wait time for network activity. Requested executables are terminated and connection is shut down if no network activity occurred for the specified number of seconds

rfc1918 filter:

TLS protocol version:  Min supported TLS version. versions below this will not be supported by the https server

Figure 14: HTTP server settings

| Web Field/UCI/Package Option   | Description   |             |  |          |  |       |                         |
|--|---|-------------|--|----------|--|-------|-------------------------|
| Web: Listen Address and Port<br>UCI: uhttpd.main.listen_http<br>Opt: list listen_http          | Specifies the ports and addresses to listen on for plain HTTP access. If only a port number is given, the server will attempt to serve both IPv4 and IPv6 requests. <table border="1" style="width: 100%; margin-top: 5px;"> <tbody> <tr> <td>0.0.0.0:80</td> <td>Bind at port 80 only on IPv4 interfaces.</td> </tr> <tr> <td>[::]:80</td> <td>Bind at port 80 only on IPv6 interfaces.</td> </tr> <tr> <td>Range</td> <td>IP address and/or port</td> </tr> </tbody> </table> | 0.0.0.0:80  | Bind at port 80 only on IPv4 interfaces. | [::]:80  | Bind at port 80 only on IPv6 interfaces. | Range | IP address and/or port  |
| 0.0.0.0:80   | Bind at port 80 only on IPv4 interfaces.  |             |  |          |  |       |                         |
| [::]:80  | Bind at port 80 only on IPv6 interfaces.  |             |  |          |  |       |                         |
| Range  | IP address and/or port  |             |  |          |  |       |                         |
| Web: Secure Listen Address and Port<br>UCI: uhttpd.main.listen_https<br>Opt: list listen_https | Specifies the ports and address to listen on for encrypted HTTPS access. The format is the same as listen_http. <table border="1" style="width: 100%; margin-top: 5px;"> <tbody> <tr> <td>0.0.0.0:443</td> <td>Bind at port 443 only.</td> </tr> <tr> <td>[::]:443</td> <td></td> </tr> <tr> <td>Range</td> <td>IP address and/or port.</td> </tr> </tbody> </table>  | 0.0.0.0:443 | Bind at port 443 only.                   | [::]:443 |  | Range | IP address and/or port. |
| 0.0.0.0:443  | Bind at port 443 only.  |             |  |          |  |       |                         |
| [::]:443   |   |             |  |          |  |       |                         |
| Range  | IP address and/or port.   |             |  |          |  |       |                         |

|   |   |                                  |           |       |          |     |  |
|---|---|----------------------------------|-----------|-------|----------|-----|--|
| <p>Web: Home path<br/>UCI: uhttpd.main.home<br/>Opt: home</p>                             | <p>Defines the server document root.</p> <table border="1"> <tr><td>/www</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>   | /www                             |           | Range |          |     |  |
| /www  |   |                                  |           |       |          |     |  |
| Range   |   |                                  |           |       |          |     |  |
| <p>Web: Cert file<br/>UCI: uhttpd.main.cert<br/>Opt: cert</p>                             | <p>ASN.1/DER certificate used to serve HTTPS connections. If no listen_https options are given the key options are ignored.</p> <table border="1"> <tr><td>/etc/uhttpd.crt</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>   | /etc/uhttpd.crt                  |           | Range |          |     |  |
| /etc/uhttpd.crt   |   |                                  |           |       |          |     |  |
| Range   |   |                                  |           |       |          |     |  |
| <p>Web: Key file<br/>UCI: uhttpd.main.key<br/>Opt: key</p>                                | <p>ASN.1/DER private key used to serve HTTPS connections. If no listen_https options are given the key options are ignored.</p> <table border="1"> <tr><td>/etc/uhttpd.key</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>   | /etc/uhttpd.key                  |           | Range |          |     |  |
| /etc/uhttpd.key   |   |                                  |           |       |          |     |  |
| Range   |   |                                  |           |       |          |     |  |
| <p>Web: CGI profile<br/>UCI: uhttpd.main.cgi_prefix<br/>Opt: cgi_prefix</p>               | <p>Defines the prefix for CGI scripts, relative to the document root. CGI support is disabled if this option is missing.</p> <table border="1"> <tr><td>/cgi-bin</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>   | /cgi-bin                         |           | Range |          |     |  |
| /cgi-bin  |   |                                  |           |       |          |     |  |
| Range   |   |                                  |           |       |          |     |  |
| <p>Web: N/A<br/>UCI: uhttpd.main.lua_prefix<br/>Opt: lua_prefix</p>                       | <p>Defines the prefix for dispatching requests to the embedded lua interpreter, relative to the document root. Lua support is disabled if this option is missing.</p> <table border="1"> <tr><td>/luci</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>                 | /luci                            |           | Range |          |     |  |
| /luci   |   |                                  |           |       |          |     |  |
| Range   |   |                                  |           |       |          |     |  |
| <p>Web: N/A<br/>UCI: uhttpd.main.lua_handler<br/>Opt: lua_handler</p>                     | <p>Specifies the lua handler script used to initialise the lua runtime on server start.</p> <table border="1"> <tr><td>/usr/lib/lua/luci/cgi/uhttpd.lua</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>  | /usr/lib/lua/luci/cgi/uhttpd.lua |           | Range |          |     |  |
| /usr/lib/lua/luci/cgi/uhttpd.lua  |   |                                  |           |       |          |     |  |
| Range   |   |                                  |           |       |          |     |  |
| <p>Web: Script timeout<br/>UCI: uhttpd.main.script_timeout<br/>Opt: script_timeout</p>    | <p>Sets the maximum wait time for CGI or lua requests in seconds. Requested executables are terminated if no output was generated.</p> <table border="1"> <tr><td>60</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>   | 60                               |           | Range |          |     |  |
| 60  |   |                                  |           |       |          |     |  |
| Range   |   |                                  |           |       |          |     |  |
| <p>Web: Network timeout<br/>UCI: uhttpd.main.network_timeout<br/>Opt: network_timeout</p> | <p>Maximum wait time for network activity. Requested executables are terminated and the connection is shut down if no network activity occurred for the specified number of seconds.</p> <table border="1"> <tr><td>30</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table> | 30                               |           | Range |          |     |  |
| 30  |   |                                  |           |       |          |     |  |
| Range   |   |                                  |           |       |          |     |  |
| <p>Web: rfc 1918 filter<br/>UCI: uhttpd.main.rfc1918_filter<br/>Opt: rfc1918_filter</p>   | <p>Enables option to reject requests from RFC1918 IPs to public server IPs (DNS rebinding counter measure).</p> <table border="1"> <tr><td>0</td><td>Disabled.</td></tr> <tr><td>1</td><td>Enabled.</td></tr> </table>  | 0                                | Disabled. | 1     | Enabled. |     |  |
| 0   | Disabled.   |                                  |           |       |          |     |  |
| 1   | Enabled.  |                                  |           |       |          |     |  |
| <p>Web: TLS protocol version<br/>UCI: uhttpd.main.tls_version<br/>Opt: tls_version</p>    | <p>Defines the minimum supported TLS version for the https server.</p> <table border="1"> <tr><td>1.0</td><td></td></tr> <tr><td>1.1</td><td></td></tr> <tr><td>1.2</td><td></td></tr> </table>   | 1.0                              |           | 1.1   |          | 1.2 |  |
| 1.0   |   |                                  |           |       |          |     |  |
| 1.1   |   |                                  |           |       |          |     |  |
| 1.2   |   |                                  |           |       |          |     |  |
| <p>Web: N/A<br/>UCI: uhttpd.main.realm<br/>Opt: realm</p>                                 | <p>Defines basic authentication realm when prompting the client for credentials (HTTP 400).</p> <table border="1"> <tr><td>OpenWrt</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>   | OpenWrt                          |           | Range |          |     |  |
| OpenWrt   |   |                                  |           |       |          |     |  |
| Range   |   |                                  |           |       |          |     |  |

|  |   |                |           |       |          |
|--|---|----------------|-----------|-------|----------|
| Web: N/A<br>UCI: uhttpd.main.config<br>Opt: config           | Config file in Busybox httpd format for additional settings. Currently only used to specify basic auth areas.<br><table border="1"> <tr> <td>/etc/http.conf</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table> | /etc/http.conf |           | Range |          |
| /etc/http.conf   |   |                |           |       |          |
| Range  |   |                |           |       |          |
| Web: N/A<br>UCI: uhttpd.main.index_page<br>Opt: index_page   | Index file to use for directories, for example, add index.php when using php.<br><table border="1"> <tr> <td></td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   |                |           | Range |          |
|  |   |                |           |       |          |
| Range  |   |                |           |       |          |
| Web: N/A<br>UCI: httpd.main.error_page<br>Opt: error_page    | Virtual URL of file of CGI script to handle 404 requests. Must begin with '/' (forward slash).<br><table border="1"> <tr> <td></td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>                              |                |           | Range |          |
|  |   |                |           |       |          |
| Range  |   |                |           |       |          |
| Web: N/A<br>UCI: uhttpd.main.no_symlinks<br>Opt: no_symlinks | Does not follow symbolic links if enabled.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0              | Disabled. | 1     | Enabled. |
| 0  | Disabled.   |                |           |       |          |
| 1  | Enabled.  |                |           |       |          |
| Web: N/A<br>UCI: uhttpd.main.no_dirlists<br>Opt: no_symlinks | Does not generate directory listings if enabled.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0              | Disabled. | 1     | Enabled. |
| 0  | Disabled.   |                |           |       |          |
| 1  | Enabled.  |                |           |       |          |

Table 12: Information table for http server basic settings

### 5.14.3 HTTP server using command line

Multiple sections of the type uhttpd may exist. The init script will launch one webserver instance per section.

A standard uhttpd configuration is shown below.

#### 5.14.3.1 HTTP Server using UCI

```

root@VA_router:~# uci show uhttpd
uhttpd.main=uhttpd
uhttpd.main.listen_http=0.0.0.0:80
uhttpd.main.listen_https=0.0.0.0:443
uhttpd.main.home=/www
uhttpd.main.rfc1918_filter=1
uhttpd.main.cert=/etc/uhttpd.crt
uhttpd.main.key=/etc/uhttpd.key
uhttpd.main.cgi_prefix=/cgi-bin
uhttpd.main.script_timeout=60
uhttpd.main.network_timeout=30
uhttpd.main.config=/etc/http.conf
uhttpd.main.tls_version=1.0

```



### 5.14.3.2 HTTP server using package options

```
root@VA_router:~# uci export uhttpd

config uhttpd 'main'

    list listen_http '0.0.0.0:80'
    list listen_https '0.0.0.0:443'
    option home '/www'
    option rfc1918_filter '1'
    option cert '/etc/uhttpd.crt'
    option key '/etc/uhttpd.key'
    option cgi_prefix '/cgi-bin'
    option script_timeout '60'
    option network_timeout '30'
    option config '/etc/http.conf'
    option tls_version '1.0'
```

### 5.14.4 HTTPs server certificate settings

To configure HTTPs server certificate settings, in the top menu, select **Services -> HTTP Server**. Scroll down to the Certificate Settings section.

Certificate Settings  
Set parameters for initial certificate generation.

Days: 3650 Validity time of the generated certificates in days.

Bits: 1024 Size of the generated RSA key in bits.

country: IE ISO country code of the certificate issuer.

state: Dublin State of the certificate issuer.

location: Dublin Location/city of the certificate issuer.

commonname: VirtualAccessGW Common name covered by the certificate.

Buttons: Delete, Save & Apply, Save, Reset

Figure 15: HTTP server certificate settings

| Web Field/UCI/Package Option                                 | Description  |
|--|--|
| Web: Days<br>UCI: uhttpd.px5g.days<br>Opt: days              | Validity time of the generated certificates in days.<br>730<br>Range   |
| Web: Bits<br>UCI: uhttpd.px5g.bits<br>Opt: bits              | Size of the generated RSA key in bits.<br>1024<br>Range  |
| Web: Country<br>UCI: uhttpd.px5g.country<br>Opt: country     | ISO code of the certificate issuer.  |
| Web: State<br>UCI: uhttpd.px5g.state<br>Opt: state           | State of the certificate issuer.   |
| Web: Location<br>UCI: uhttpd.px5g.location<br>Opt: location  | Location or city of the certificate user.  |
| Web: Commonname<br>UCI: uhttpd.commonname<br>Opt: commonname | Common name covered by the certificate. For the purposes of secure activation, this must be set to the serial number (Eth0 MAC address) of the device. |

Table 13: Information table for HTTP server certificate settings

### 5.14.5 HTTPs server using UCI

```

root@VA_router:~# uci show uhttpd.px5g
uhttpd.px5g=cert
uhttpd.px5g.days=3650
uhttpd.px5g.bits=1024
uhttpd.px5g.country=IE
uhttpd.px5g.state=Dublin
uhttpd.px5g.location=Dublin
uhttpd.px5g.commonname=00E0C8000000
HTTPs server using package options
root@VA_router:~# uci export uhttpd
package uhttpdconfig 'cert' 'px5g'
    option 'days' '3650'
    option 'bits' '1024'
    option 'state' 'Dublin'

    option 'location' 'Dublin'
    option 'commonname' '00E0C8000000'

```

## 5.15 Basic authentication (httpd conf)

For backward compatibility reasons, uhttpd uses the file `/etc/httpd.conf` to define authentication areas and the associated usernames and passwords. This configuration file is not in UCI format.

Authentication realms are defined in the format `prefix:username:password` with one entry and a line break.

Prefix is the URL part covered by the realm, for example, `cgi-bin` to request basic auth for any CGI program.

**Username** specifies the username a client has to login with.

**Password** defines the secret password required to authenticate.

The password can be either in plain text format, MD5 encoded or in the form `$p$user` where the user refers to an account in `/etc/shadow` or `/etc/passwd`.

If you use `$p$...` format, uhttpd will compare the client provided password against the one stored in the shadow or passwd database.

## 5.16 Securing uhttpd

By default, uhttpd binds to `0.0.0.0` which also includes the WAN port of your router. To bind uhttpd to the LAN port only you have to change the `listen_http` and `listen_https` options to your LAN IP address.

To get your current LAN IP address, enter:

```
uci get network.lan.ipaddr
```

Then modify the configuration appropriately:

```
uci set uhttpd.main.listen_http='192.168.1.1:80'
uci set uhttpd.main.listen_https='192.168.1.1:443'

config 'uhttpd' 'main'
    list listen_http      192.168.1.1:80
    list listen_https     192.168.1.1:443
```

## 5.17 Displaying custom information via login screen

The login screen, by default, shows the hostname of the router in addition to the username and password prompt. However, the router can be configured to show some other basic information if required using a UDS script.

**Note:** this can only be configured via the command line.

### 5.17.1 Configuration packages used

| Package | Sections |
|---------|----------|
| luci    | main     |
| uds     | script   |

### 5.17.2 Configuring login screen custom information

The luci package option `login_page_info_template` is configured with the path to a UDS script that would render the required information on the right side of the login page.

The following example shows how to display serial number and mobile signal strength.

**Note:** this can only be configured via the command line.

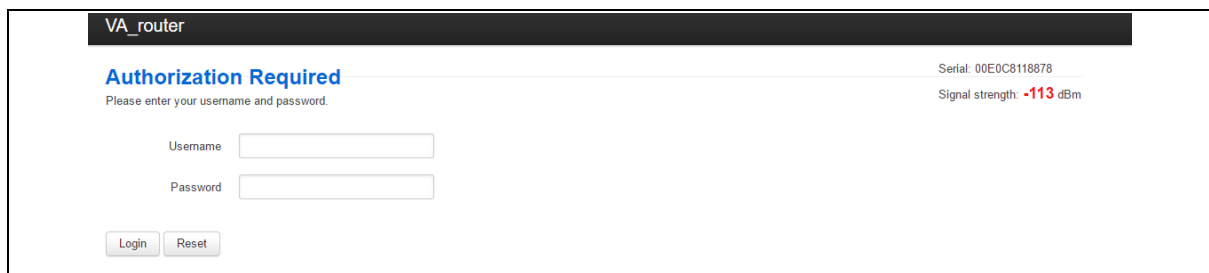


Figure 16: Example login screen displaying serial and signal strength

#### 5.17.2.1 Login screen custom information using UCI

```
root@VA_router:~# uci show luci
luci.main=core
luci.main.login_page_info_template=/tmp/uds/sysauth_template

root@VA_router:~# uci show uds
uds.sysauth_template=script
uds.sysauth_template.enabled=1
uds.sysauth_template.exec_type=none
uds.sysauth_template.fname=sysauth_template.htm
uds.sysauth_template.type=none
uds.sysauth_template.text=Serial: <%=pcdata(luci.version.serial)%><br/> <%
local sig = luci.dispatcher.uci.cursor_state():get("mobile", "3g_1_1",
"sig_dbm") or -113 sig = tonumber(sig) local hue = (sig + 113) * 2 local
hue = math.min(math.max(hue, 0), 120) %> Signal strength: <h3
style="color:hsl(<%=hue%>, 90%, 50%); display:inline;"><%=sig%></h3> dBm
```

### 5.17.2.2 Login screen custom information using package options

```
root@VA_router:~# uci export luci
package luci
config core 'main'
    option login_page_info_template '/tmp/uds/sysauth_template'
root@VA_router:~# uci export uds
package uds
config script 'sysauth_template'
    option enabled '1'
    option exec_type 'none'
    option fname 'sysauth_template.htm'
    option type 'none'
    list text 'Serial: <%=pcdata(luci.version.serial)%><br/>'
    list text '<% local sig =
luci.dispatcher.uci.cursor_state():get("mobile", "3g_1_1", "sig_dbm") or -
113'
    list text 'sig = tonumber(sig)'
    list text 'local hue = (sig + 113) * 2'
    list text 'local hue = math.min(math.max(hue, 0), 120) %>'
    list text 'Signal strength: <h3 style="color:hsl(<%=hue%>, 90%,
50%); display:inline;"><%=sig%></h3> dBm
```

## 6 Router file structure

This section describes the file structure and location of essential directories and files on Virtual Access routers.

Throughout this document, we use information tables to show the different ways to configure the router using the router's web interface and command line interface (CLI).

When showing examples of the command line interface we use the host name 'VA\_router' to indicate the system prompt. For example, the table below displays what the user should see when entering the command to show the current configuration in use on the router:

```
root@VA_router:~# va_config.sh
```

### 6.1 System information

General information about software and configuration used by the router is displayed on the Status page. To view the running configuration file status on the web interface, in the top menu, select **Status -> Overview**. This page also appears immediately after you have logged in.

| System               |                                |
|----------------------|--------------------------------|
| Router Name          | GW0000                         |
| Router Model         | Virtual Access GW0031W-AA0179E |
| Firmware Version     | VIE-16.00.55                   |
| Current Image/Config | image2 / config2               |
| Kernel Version       | 3.2.12                         |
| Local Time           | Fri Aug 5 11:43:52 2016        |
| Uptime               | 0h 10m 8s                      |
| Load Average         | 0.27, 0.35, 0.31               |

**Figure 17: Example of the status page**

System information is also available from the CLI if you enter the following command:

```
root@VA_router:~# va_vars.sh
```

The example below shows the output from the above command.

```

VA_SERIAL:          00E0C8121215
VA_MODEL:           GW0000
VA_ACTIVEIMAGE:     image2
VA_ACTIVECONFIG:    config1
VA_IMAGE1VER:       VIE-16.00.44
VA_IMAGE2VER:       VIE-16.00.44

```

## 6.2 Identify your software version

To check which software version your router is running, in the top menu, browse to **Status -> Overview**.

| Status               |                                |
|----------------------|--------------------------------|
| System               |                                |
| Router Name          | GW0000                         |
| Router Model         | Virtual Access GW0031W-AA0179E |
| Firmware Version     | VIE-16.00.55                   |
| Current Image/Config | image2 / config2               |
| Kernel Version       | 3.2.12                         |
| Local Time           | Fri Aug 5 11:43:52 2016        |
| Uptime               | 0h 10m 8s                      |
| Load Average         | 0.27, 0.35, 0.31               |

**Figure 18: The status page showing a software version prior to 72.002**

| Status               |                          |
|----------------------|--------------------------|
| System               |                          |
| Router Name          | dmvpn                    |
| Router Model         | GW2028                   |
| Firmware Version     | LIS-15.00.72.002rc4      |
| Current Image/Config | image1 / config1         |
| Kernel Version       | 3.2.12                   |
| Local Time           | Thu Jan 26 14:46:03 2017 |
| Uptime               | 0h 39m 37s               |
| Load Average         | 1.02, 0.53, 0.48         |

**Figure 19: The status page showing software version 72.002**

In the Firmware Version row, the first two digits of the firmware version identify the hardware platform, for example LIS-15; while the remaining digits: .00.72.002, show the software version.

## 6.3 Image files

The system allows for two firmware image files:

- image1, and
- image2

Two firmware images are supported to enable the system to rollback to a previous firmware version if the upgrade of one image fails.

The image names (image1, image2) themselves are symbols that point to different partitions in the overall file system. A special image name "altimage" exists which always points to the image that is not running.

The firmware upgrade system always downloads firmware to "altimage".

## 6.4 Directory locations for UCI configuration files

Router configurations files are stored in folders on:

- /etc/factconf,
- /etc/config1, and
- /etc/config2

Multiple configuration files exist in each folder. Each configuration file contains configuration parameters for different areas of functionality in the system.

A symbolic link exists at /etc/config, which always points to one of factconf, config1 or config2 is the active configuration file.

Files that appear to be in /etc/config are actually in /etc/factconf|config1|config2 depending on which configuration is active.

If /etc/config is missing on start-up, for example on first boot, the links and directories are created with configuration files copied from /rom/etc/config/.

At any given time, only one of the configurations is the active configuration. The UCI system tool (Unified Configuration Interface) only acts upon the currently active configuration.

## 6.5 Viewing and changing current configuration

To show the configuration currently running, enter:

```
root@VA_router:~# va_config.sh
```

To show the configuration to run after the next reboot, enter:

```
root@VA_router:~# va_config.sh next
```

To set the configuration to run after the next reboot, enter:

```
root@VA_router:~# va_config.sh -s [factconf|config1|config2|altconfig]
```



## 6.6 Configuration file syntax

The configuration files consist of sections – or packages - that contain one or more config statements. These optional statements define actual values.

Below is an example of a simple configuration file.

```
package 'example'
config 'example' 'test'
    option 'string' 'some value'
    option 'boolean' '1'
    list 'collection' 'first item'
    list 'collection' 'second item'
```

The config 'example' 'test' statement defines the start of a section with the type example and the name test.

| Command  | Target                                | Description   |
|----------|---------------------------------------|---|
| export   | [<config>]                            | Exports the configuration in a machine readable format. It is used internally to evaluate configuration files as shell scripts. |
| import   | [<config>]                            | Imports configuration files in UCI syntax.  |
| add      | <config> <section-type>               | Adds an anonymous section of type-section type to the given configuration.  |
| add_list | <config>.<section>.<option>=<string>  | Adds the given string to an existing list option.   |
| show     | [<config>[.<section>[.<option>]]]     | Shows the given option, section or configuration in compressed notation.  |
| get      | <config>.<section>[.<option>]         | Gets the value of the given option or the type of the given section.  |
| Set      | <config>.<section>[.<option>]=<value> | Sets the value of the given option, or adds a new section with the type set to the given value.                                 |
| delete   | <config>[.<section>[.<option>]]       | Deletes the given section or option.  |

Table 1: Common commands, target and their descriptions

## 6.7 Managing configurations

### 6.7.1 Managing sets of configuration files using directory manipulation

Configurations can also be managed using directory manipulation.

To remove the contents of the current folder, enter:

```
root@VA_router:/etc/config1# rm -f *
```

**Warning: the above command makes irreversible changes.**

To remove the contents of a specific folder regardless of the current folder (config2), enter:

```
root@VA_router:/ # rm -f /etc/config1/*
```

**Warning: the above command makes irreversible changes.**

To copy the contents of one folder into another (config2 into config1), enter:

```
root@VA_router:/etc/config1# cp /etc/config2/* /etc/config1
```

## 6.8 Exporting a configuration file

If you have software versions prior to 72.002, to export a configuration file using the web interface, go to section 6.8.1.

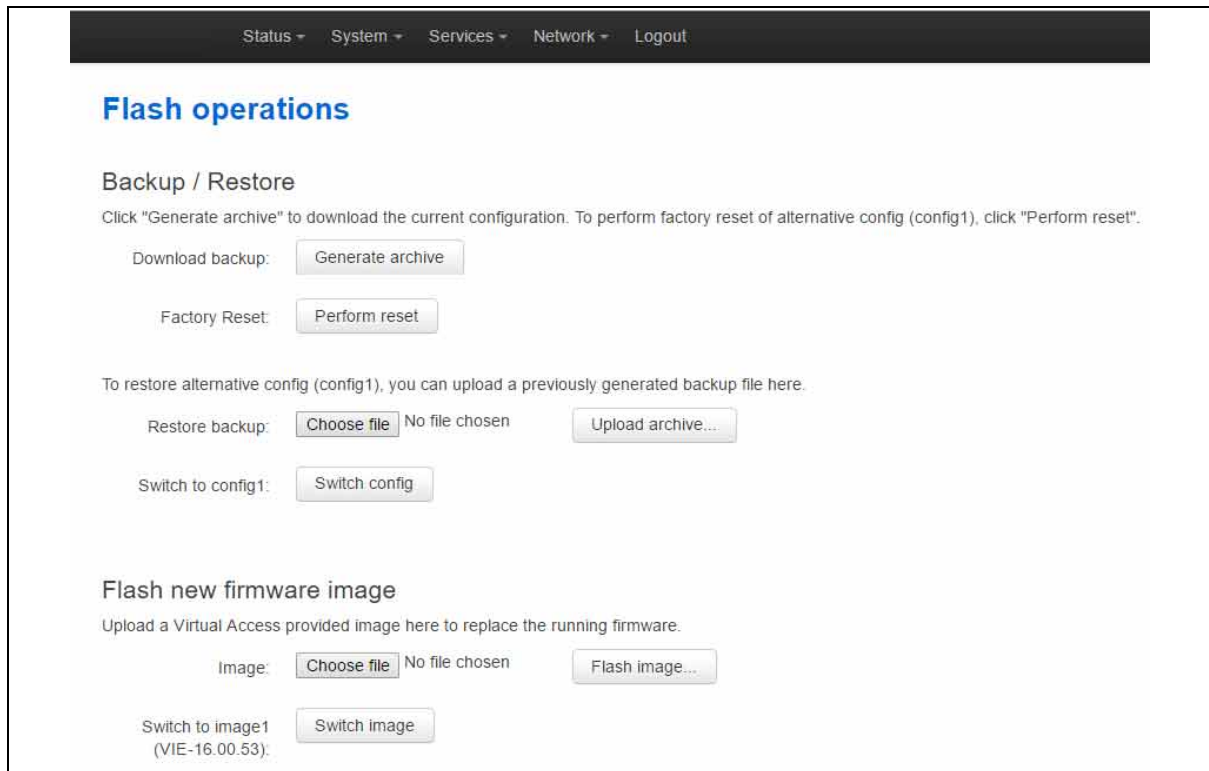
If you have software version 72.002 or above, export a configuration file using the web interface go to section 6.8.2.

To export a configuration file using UCI, for any software version, go to section 6.8.3.

### 6.8.1 Exporting a configuration file using the web interface for software versions pre- 72.002

The current running configuration file may be exported using the web interface.

In the top menu, select **System -> Backup/Flash Firmware**. The Flash operations page appears.



**Figure 20: The flash operations page**

In the Backup/Restore section, select **Generate Archive**.

## 6.8.2 Exporting a configuration file using the web interface for software version 72.002 and above

The current running configuration file may be exported using the web interface.

In the top menu, select **System -> Flash Operations**. The Flash operations page appears.

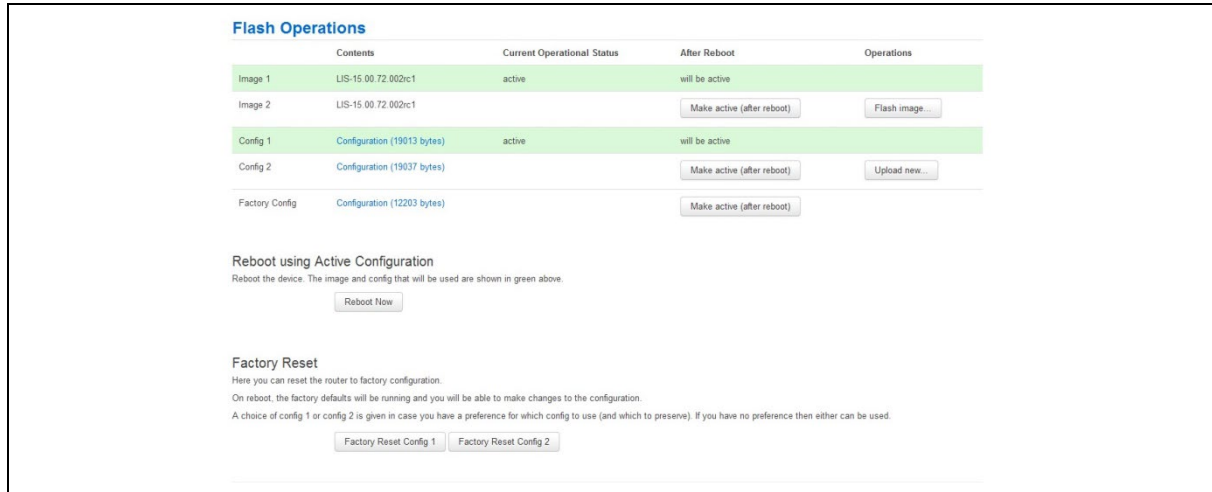


Figure 21: The flash operations page

In the **Flash Operation** section, click the configuration file in the Contents column to download it.

## 6.8.3 Exporting a configuration file using UCI

You can view any configuration file segment using UCI.

To export the running configuration file, enter:

```
root@VA_router:~# uci export
```

To export the factory configuration file, enter:

```
root@VA_router:~# uci -c /etc/factconf/ export
```

To export config1 or config2 configuration file, enter:

```
root@VA_router:~# uci -c /etc/config1/ export
root@VA_router:~# uci -c /etc/config2/ export
```

## 6.9 Importing a configuration file

If you have software versions prior to 72.002, to import a configuration file using the web interface, go to section 6.9.1.

If you have software version 72.002 or above, to import a configuration file using the web interface go to section 6.9.2.

To import a configuration file using UCI, for any software version, go to section 6.9.3.

### 6.9.1 Importing a configuration file using the web interface for software versions pre- 72.002

You can import a configuration file to the alternate configuration segment using the web interface. This will automatically reboot the router into this configuration file.

In the top menu, select **System -> Backup/Flash Firmware**. The Flash operations page appears.

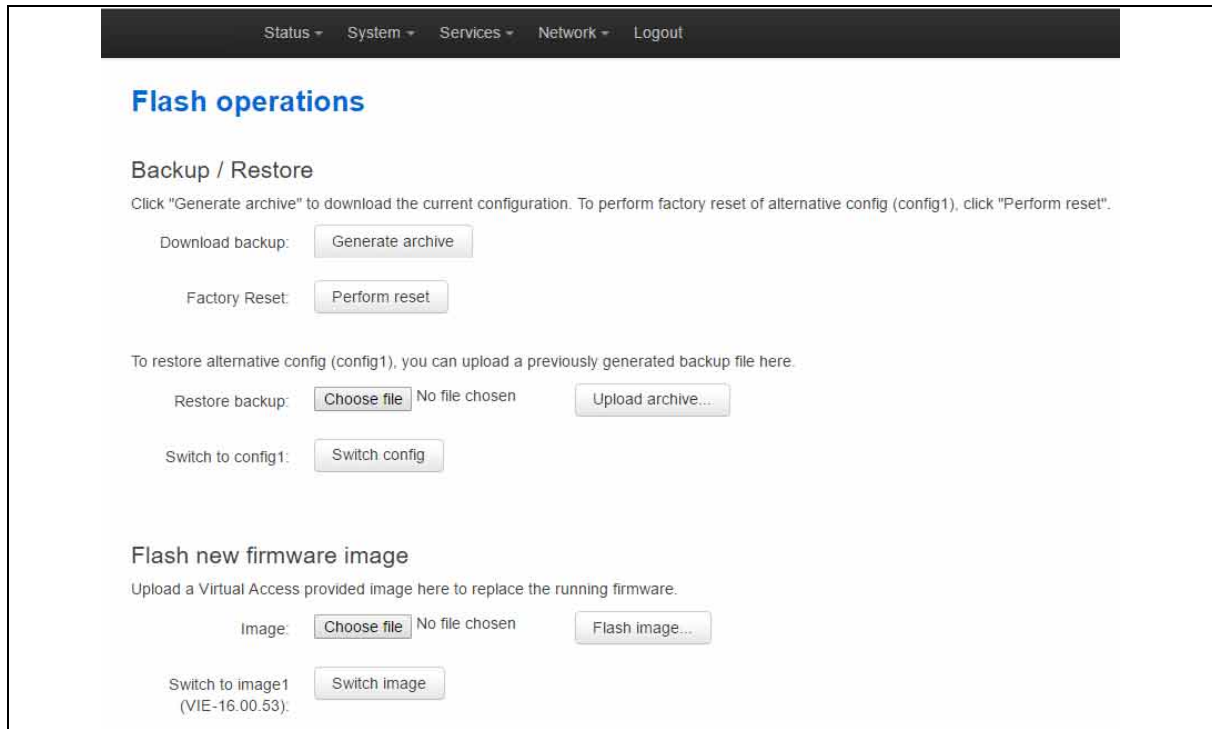


Figure 22: The flash operations page

Under Backup/Restore, choose **Restore Backup: Choose file**. Select the appropriate file and then click **Upload archive**.

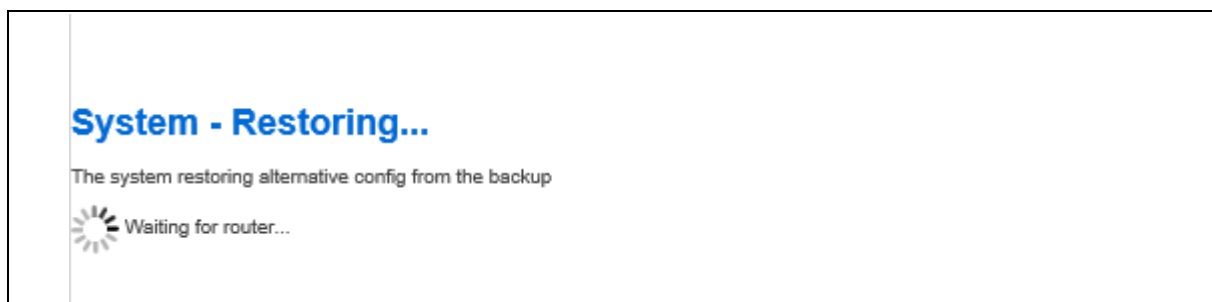


Figure 23: The system – restoring...page

When the 'waiting for router' icon disappears, the upgrade is complete, and the login homepage appears.

## 6.9.2 Importing a configuration file using the web interface for software version 72.002 and above

You can import a configuration file to the alternate configuration segment using the web interface.

In the top menu, select **System -> Flash Operations**. The Flash operations page appears.

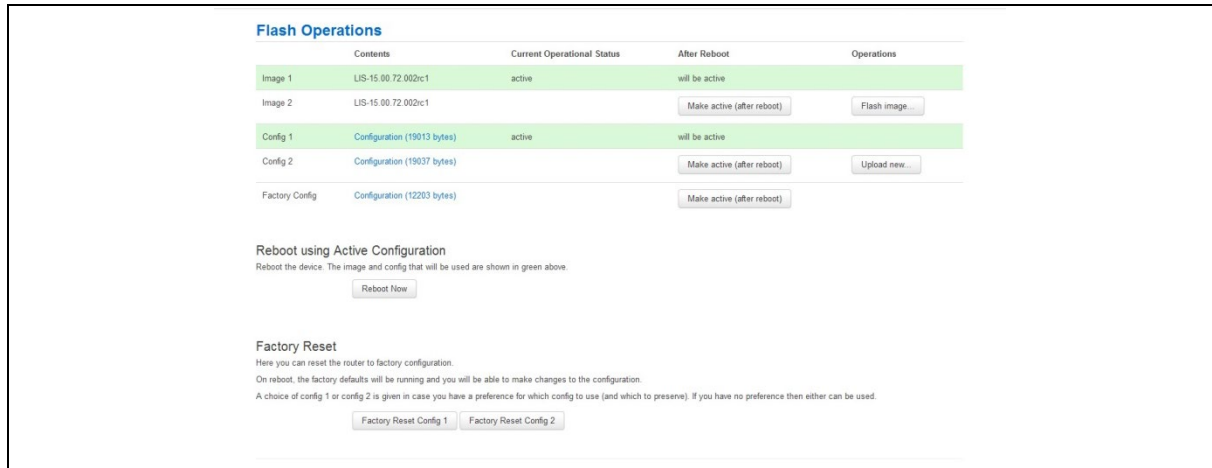


Figure 24: The flash operations page

In the Operations column, click **Upload new**. Select the appropriate file.

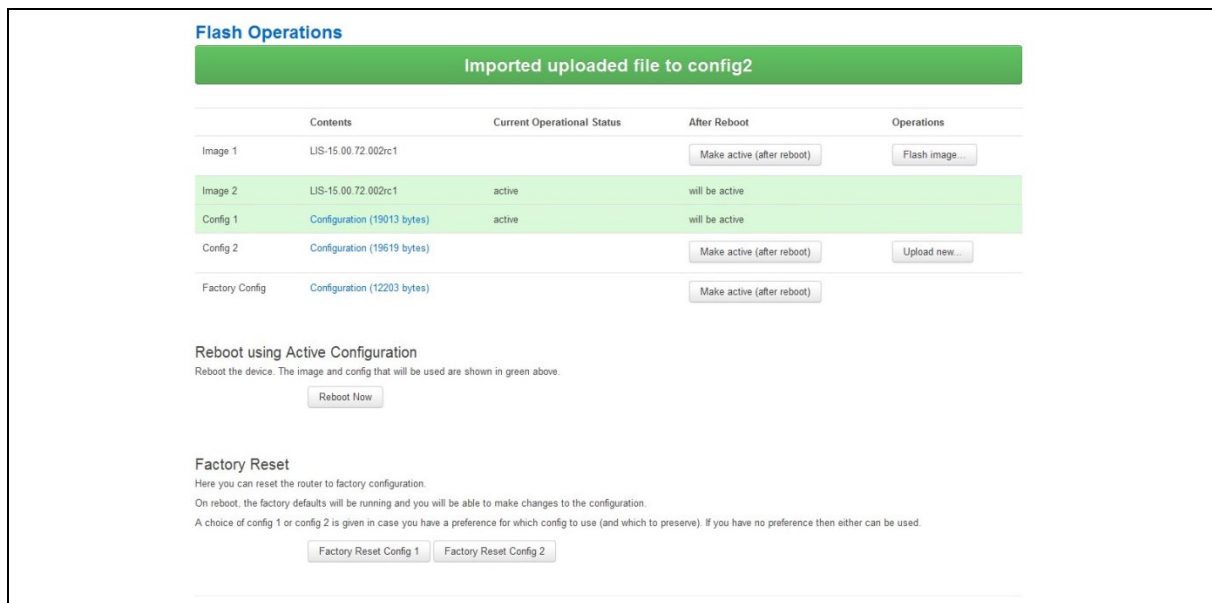


Figure 25: The flash operations succeed upload configuration page

If you select 'Flash image and do not reboot', the router will only run this configuration if you click **OK** to return to the Flash Operations page. There you can manually select **Made Active (after reboot)**. Then click **Reboot Now** in the 'Reboot using Active Configuration' section.

### 6.9.3 Importing a configuration file using UCI

You can import a configuration file to any file segment using UCI.

To import to config1, enter:

```
root@VA_router:~# uci -c /etc/config1/ import  
<paste in config file>  
<CTRL-D>
```

**Note:** it is very important that the config file is in the correct format otherwise it will not import correctly.

## 7 Using the Command Line Interface

This chapter explains how to view Virtual Access routers' log files and edit configuration files using a Command Line Interface (CLI) and the Unified Configuration Interface (UCI) system. Some commands may vary between router models.

### 7.1 Overview of some common commands

Virtual Access routers' system has an SSH server typically running on port 22.

The factconf default password for the root user is **admin**.

To change the factconf default password, enter:

```
root@VA_router:/# uci set system.main.password="*****"  
root@VA_router:/# uci commit system
```

To reboot the system, enter:

```
root@VA_router:/# reboot
```

The system provides a Unix-like command line. Common Unix commands are available such as `ls`, `cd`, `cat`, `top`, `grep`, `tail`, `head`, `more` and `less`.

Typical pipe and redirect operators are also available, such as: `>`, `>>`, `<`, `|`

The system log can be viewed using any of the following commands:

```
root@VA_router:/# logread  
  
root@VA_router:/# logread | tail  
  
root@VA_router:/# logread -f
```

These commands will show the full log, end of the log (`tail`) and continuously (`-f`). Enter **Ctrl-C** to stop the continuous output from `logread -f`.

To view and edit configuration files, the system uses the Unified Configuration Interface (UCI) which is described further on in this chapter. This is the preferred method of editing configuration files. However, you can also view and edit these files using some of the standard Unix tools.

For example, to view a text or configuration file in the system, enter:

```
root@VA_router:/# cat /etc/passwd
```

The command output information shows the following, or similar output.

```
root:x:0:0:root:/root:/bin/ash
daemon:*:1:1:daemon:/var:/bin/false
ftp:*:55:55:ftp:/home/ftp:/bin/false
sftp:*:56:56:sftp:/var:/usr/lib/sftp-server
network:*:101:101:network:/var:/bin/false
nobody:*:65534:65534:nobody:/var:/bin/false
```

To view files in the current folder, enter:

```
root@VA_router:/# ls

bin      etc      lib      opt      sbin     usr
bkrepos  home     linuxrc  proc     sys      var
dev      init     mnt      root     tmp      www
```

For more details add the `-l` argument:

```
root@VA_router:/# ls -l

drwxrwxr-x  2 root    root    642 Jul 16  2012 bin
drwxr-xr-x  5 root    root   1020 Jul  4  01:27 dev
drwxrwxr-x  1 root    root     0 Jul  3  18:41 etc
drwxr-xr-x  1 root    root     0 Jul  9  2012 lib
drwxr-xr-x  2 root    root     3 Jul 16  2012 mnt
drwxr-xr-x  7 root    root     0 Jan  1  1970 overlay
dr-xr-xr-x 58 root    root     0 Jan  1  1970 proc
drwxr-xr-x 16 root    root    223 Jul 16  2012 rom
drwxr-xr-x  1 root    root     0 Jul  3  22:53 root
drwxrwxr-x  2 root    root    612 Jul 16  2012 sbin
drwxr-xr-x 11 root    root     0 Jan  1  1970 sys
drwxrwxrwt 10 root    root    300 Jul  4  01:27 tmp
drwxr-xr-x  1 root    root     0 Jul  3  11:37 usr
lrwxrwxrwx  1 root    root     4 Jul 16  2012 var -> /tmp
drwxr-xr-x  4 root    root    67 Jul 16  2012 www
```



To change the current folder, enter **cd** followed by the desired path:

```
root@VA_router:/# cd /etc/config1
root@VA_router:/etc/config1#
```

**Note:** if the specified directory is actually a link to a directory, the real directory will be shown in the prompt.

To view scheduled jobs, enter:

```
root@VA_router:/# crontab -l

0 * * * * slaupload 00FF5FF92752 TFTP 1 172.16.250.100 69
```

To view currently running processes, enter:

```
root@VA_router:/# ps

PID  Uid      VmSize  Stat  Command
  1  root          356  S    init
  2  root           DW   [keventd]
  3  root          RWN  [ksoftirqd_CPU0]
  4  root          SW   [kswapd]
  5  root          SW   [bdflush]
  6  root          SW   [kupdated]
  8  root          SW   [mtdblockd]
 89  root         344  S    logger -s -p 6 -t
 92  root         356  S    init
 93  root         348  S    syslogd -C 16
 94  root         300  S    klogd
424  root         320  S    wifi up
549  root         364  S    httpd -p 80 -h /www -r VA_router
563  root         336  S    crond -c /etc/crontabs
6712 root         392  S    /usr/sbin/dropbear
6824 root         588  S    /usr/sbin/dropbear
7296 root         444  S    -ash
 374 root         344  R    ps ax
 375 root         400  S    /bin/sh /sbin/hotplug button
 384 root         396  R    /bin/sh /sbin/hotplug button
 385 root           RW   [keventd]
```

To search for a process, enter: `pgrep -fl '<process name or part of name>'`:

```
root@VA_router:/# pgrep -fl 'wifi'

424 root          320 S    wifi up
```

To kill a process, enter the PID:

```
root@VA_router:~# kill 424
```

## 7.2 Using Unified Configuration Interface (UCI)

The system uses Unified Configuration Interface (UCI) for central configuration management. Most common and useful configuration settings can be accessed and configured using the UCI system.

UCI consists of a Command Line Utility (CLI), the files containing the actual configuration data, and scripts that take the configuration data and apply it to the proper parts of the system, such as the networking interfaces. Entering the command `'uci'` on its own will display the list of valid arguments for the command and their format.

```
root@VA_router:/lib/config# uci
```

Usage: `uci [<options>] <command> [<arguments>]`

```
Commands:
export      [<config>]
import      [<config>]
changes     [<config>]
commit      [<config>]
add         <config> <section-type>
add_list    <config>.<section>.<option>=<string>
show        [<config>[.<section>[.<option>]]]
get         <config>.<section>[.<option>]
set         <config>.<section>[.<option>]=<value>
delete      <config>[.<section>[.<option>]]
rename      <config>.<section>[.<option>]=<name>
revert      <config>[.<section>[.<option>]]

Options:
-c <path>   set the search path for config files (default: /etc/config)
-d <str>    set the delimiter for list values in uci show
-f <file>   use <file> as input instead of stdin
-m          when importing, merge data into an existing package
```

```

-n      name unnamed sections on export (default)
-N      don't name unnamed sections
-p <path> add a search path for config change files
-P <path> add a search path for config change files and use as default
-q      quiet mode (don't print error messages)
-s      force strict mode (stop on parser errors, default)

-S      disable strict mode
-X      do not use extended syntax on 'show'

```

The table below describes commands for the UCI command line and some further examples of how to use this utility.

| Command  | Target                                | Description   |
|----------|---------------------------------------|---|
| commit   | [<config>]                            | Writes changes of the given configuration file, or if none is given, all configuration files, to the filesystem. All "uci set", "uci add", "uci rename" and "uci delete" commands are staged into a temporary location and written to flash at once with "uci commit". This is not needed after editing configuration files with a text editor, but for scripts, GUIs and other programs working directly with UCI files. |
| export   | [<config>]                            | Exports the configuration in a UCI syntax and does validation.  |
| import   | [<config>]                            | Imports configuration files in UCI syntax.  |
| changes  | [<config>]                            | Lists staged changes to the given configuration file or if none given, all configuration files.   |
| add      | <config> <section-type>               | Adds an anonymous section of type section-type to the given configuration.  |
| add_list | <config>.<section>.<option>=<string>  | Adds the given string to an existing list option.   |
| show     | [<config>[.<section>[.<option>]]]     | Shows the given option, section or configuration in compressed notation.  |
| get      | <config>.<section>[.<option>]         | Gets the value of the given option or the type of the given section.  |
| set      | <config>.<section>[.<option>]=<value> | Sets the value of the given option, or add a new section with the type set to the given value.  |
| delete   | <config>[.<section>[.<option>]]       | Deletes the given section or option.  |
| rename   | <config>.<section>[.<option>]=<name>  | Renames the given option or section to the given name.  |
| revert   | <config>[.<section>[.<option>]]       | Deletes staged changes to the given option, section or configuration file.  |

**Table 14: Common commands, target and their descriptions**

**Note:** all operations do not act directly on the configuration files. A commit command is required after you have finished your configuration.

```
root@VA_router:~# uci commit
```

### 7.2.1 Using uci commit to avoid router reboot

After changing the port, uhttpd listens on from 80 to 8080 in the file `/etc/config/uhttpd`; save it, then enter:

```
root@VA_router:~# uci commit uhttpd
```

Then enter:

```
root@VA_router:~# /etc/init.d/uhttpd restart
```

For this example, the router does not need to reboot as the changes take effect when the specified process is restarted.

### 7.2.2 Export a configuration

Using the `uci export` command it is possible to view the entire configuration of the router or a specific package. Using this method to view configurations does not show comments that are present in the configuration file:

```
root@VA_router:~# uci export httpd

package 'httpd'
config 'httpd'
option 'port' '80'
option 'home' '/www'
```

### 7.2.3 Show a configuration tree

The configuration tree format displays the full path to each option. This path can then be used to edit a specific option using the `uci set` command.

To show the configuration 'tree' for a given config, enter:

```
root@VA_router:~# uci show network

network.loopback=interface
network.loopback.ifname=lo
network.loopback.proto=static
network.loopback.ipaddr=127.0.0.1
network.loopback.netmask=255.0.0.0
network.lan=interface
network.lan.ifname=eth0
network.lan.proto=dhcp
network.wan=interface
network.wan.username=foo
```

```
network.wan.password=bar
network.wan.proto=3g
network.wan.device=/dev/ttyACM0
network.wan.service=umts
network.wan.auto=0
network.wan.apn=arkessa.com
network.@va_switch[0]=va_switch
network.@va_switch[0].eth0=A B C
network.@va_switch[0].eth1=D
```

It is also possible to display a limited subset of a configuration:

```
root@VA_router:~# uci show network.wan
network.wan=interface
network.wan.username=foo
network.wan.password=bar
network.wan.proto=3g
network.wan.device=/dev/ttyACM0
network.wan.service=umts
network.wan.auto=0
network.wan.apn=hs.vodafone.ie
```

#### 7.2.4 Display just the value of an option

To display a specific value of an individual option within a package, enter:

```
root@VA_router:~# uci get httpd.@httpd[0].port
80
root@VA_router:~#
```

#### 7.2.5 High level image commands

To show the image running currently, enter:

```
root@VA_router:~# vacmd show current image
```

To set the image to run on next reboot, enter:

```
root@VA_router:~# vacmd set next image [image1|image2|altimage]
root@VA_router:~# reboot
```

## 7.2.6 Format of multiple rules

When there are multiple rules next to each other, UCI uses array-like references for them. For example, if there are 8 NTP servers, UCI will let you reference their sections as `timeserver.@timeserver[0]` for the first section; or `timeserver.@timeserver[7]` for the last section.

You can also use negative indexes, such as `timeserver.@timeserver[-1]` '-1' means the last one, and '-2' means the second-to-last one. This is useful when appending new rules to the end of a list.

```
root@VA_router:/# uci show va_eventd
va_eventd.main=va_eventd
va_eventd.main.enabled=yes
va_eventd.main.event_queue_file=/tmp/event_buffer
va_eventd.main.event_queue_size=128K
va_eventd.@conn_tester[0]=conn_tester
va_eventd.@conn_tester[0].name=Pinger
va_eventd.@conn_tester[0].enabled=yes
va_eventd.@conn_tester[0].type=ping
va_eventd.@conn_tester[0].ping_dest_addr=192.168.250.100
va_eventd.@conn_tester[0].ping_success_duration_sec=5
va_eventd.@target[0]=target
va_eventd.@target[0].name=MonitorSyslog
va_eventd.@target[0].enabled=yes
va_eventd.@target[0].type=syslog
va_eventd.@target[0].target_addr=192.168.250.100
va_eventd.@target[0].conn_tester=Pinger
va_eventd.@target[0].suppress_duplicate_forwardings=no
va_eventd.@forwarding[0]=forwarding
va_eventd.@forwarding[0].enabled=yes
va_eventd.@forwarding[0].className=ethernet
va_eventd.@forwarding[0].target=MonitorSyslog
va_eventd.@forwarding[1]=forwarding
va_eventd.@forwarding[1].enabled=yes
va_eventd.@forwarding[1].className=auth
va_eventd.@forwarding[1].target=MonitorSyslog
va_eventd.@forwarding[2]=forwarding
va_eventd.@forwarding[2].enabled=yes
va_eventd.@forwarding[2].className=adsl
```

```

va_eventd.@forwarding[2].target=MonitorSyslog
va_eventd.@forwarding[3]=forwarding
va_eventd.@forwarding[3].enabled=yes
va_eventd.@forwarding[3].className=ppp
va_eventd.@forwarding[3].target=MonitorSyslog

```

## 7.3 Configuration files

The table below lists common package configuration files that can be edited using uci commands. Other configuration files may also be present depending on the specific options available on the Virtual Access router.

| File                   | Description   |
|------------------------|---|
| Management             |   |
| /etc/config/autoload   | Boot up Activation behaviour (typically used in factconf) |
| /etc/config/httpclient | Activator addresses and urls                              |
| /etc/config/monitor    | Monitor details   |
| Basic                  |   |
| /etc/config/dropbear   | SSH server options  |
| /etc/config/dhcp       | Dnsmasq configuration and DHCP settings                   |
| /etc/config/firewall   | NAT, packet filter, port forwarding, etc.                 |
| /etc/config/network    | Switch, interface, L2TP and route configuration           |
| /etc/config/system     | Misc. system settings including syslog                    |
| Other                  |   |
| /etc/config/snmpd      | SNMPd settings  |
| /etc/config/uhttpd     | Web server options (uHTTPd)                               |
| /etc/config/strongswan | IPSec settings  |

## 7.4 Configuration file syntax

The configuration files usually consist of one or more config statements, so-called sections with one or more option statements defining the actual values.

Below is an example of a simple configuration file.

```

package 'example'
config 'example' 'test'
    option 'string' 'some value'
    option 'boolean' '1'
    list 'collection' 'first item'
    list 'collection' 'second item'

```

The config 'example' 'test' statement defines the start of a section with the type example and the name test. There can also be so-called anonymous sections with only a type, but no name identifier. The type is important for the processing programs to decide how to treat the enclosed options.

The option 'string' 'some value' and option 'boolean' '1' lines define simple values within the section.

**Note:** there are no syntactical differences between text and boolean options. Per convention, boolean options may have one of the values '0', 'no', 'off' or 'false' to specify a false value or '1', 'yes', 'on' or 'true' to specify a true value.

In the lines starting with a list keyword, an option with multiple values is defined. All list statements that share the same name collection in our example will be combined into a single list of values with the same order as in the configuration file.

The indentation of the option and list statements is a convention to improve the readability of the configuration file but it is not syntactically required.

Usually you do not need to enclose identifiers or values in quotes. Quotes are only required if the enclosed value contains spaces or tabs. Also it is legal to use double-quotes instead of single-quotes when typing configuration options.

All of the examples below are valid syntax.

```
option example value
option 'example' value
option example "value"
option "example" 'value'
option 'example' "value"
```

In contrast, the following examples are not valid syntax.

```
option 'example" "value'
```

Quotes are unbalanced.

```
option example some value with space
```

Missing quotes around the value.

It is important to note that identifiers and config file names may only contain the characters a-z, A-Z, 0-9 and `_`. However, option values may contain any character, as long they are properly quoted.



## 8 Upgrading router firmware

This chapter describes how to upgrade router firmware. The upgrade process is as follows:

- Firmware is transferred to the device.
- Firmware is checked to ensure there are no corruptions.
- Firmware is saved to persistent storage.
- Data in persistent storage is validated.

To avoid any unrecoverable errors during the process, you must follow several safety steps described in this chapter.

On successful completion of the process, you can restart the device running the new firmware.

### 8.1 Software versions

If you have software versions prior to 72.002, to upgrade firmware using the web interface, go to section 8.1.2.

If you have software version 72.002 or above, to upgrade firmware using the web interface go to section 8.1.3.

To upgrade firmware using CLI, for any software version, go to section 8.2.

#### 8.1.1 Identify your software version

To check which software version your router is running, in the top menu, browse to **Status -> Overview**.

| Status               |                                |
|----------------------|--------------------------------|
| System               |                                |
| Router Name          | GW0000                         |
| Router Model         | Virtual Access GW0031W-AA0179E |
| Firmware Version     | VIE-16.00.55                   |
| Current Image/Config | image2 / config2               |
| Kernel Version       | 3.2.12                         |
| Local Time           | Fri Aug 5 11:43:52 2016        |
| Uptime               | 0h 10m 8s                      |
| Load Average         | 0.27, 0.35, 0.31               |

**Figure 26: The status page showing a software version prior to 72.002**

| Status               |                          |
|----------------------|--------------------------|
| System               |                          |
| Router Name          | dmvpn                    |
| Router Model         | GW2028                   |
| Firmware Version     | LIS-15.00.72.002rc4      |
| Current Image/Config | image1 / config1         |
| Kernel Version       | 3.2.12                   |
| Local Time           | Thu Jan 26 14:46:03 2017 |
| Uptime               | 0h 39m 37s               |
| Load Average         | 1.02, 0.53, 0.48         |

**Figure 27: The status page showing software version 72.002**

In the Firmware Version row, the first two digits of the firmware version identify the hardware platform, for example LIS-15; while the remaining digits: .00.72.002, show the software version.

### 8.1.2 Upgrading router firmware for software versions pre- 72.002

Copy the new firmware issued by Virtual Access to a PC connected to the router.

In the top menu, select **System tab -> Backup/Flash Firmware**. The Flash operations page appears.

Status ▾
System ▾
Services ▾
Network ▾
Logout

## Flash operations

### Backup / Restore

Click "Generate archive" to download the current configuration. To perform factory reset of alternative config (config1), click "Perform reset".

Download backup:

Factory Reset:

To restore alternative config (config1), you can upload a previously generated backup file here.

Restore backup:  No file chosen

Switch to config1:

### Flash new firmware image

Upload a Virtual Access provided image here to replace the running firmware.

Image:  No file chosen

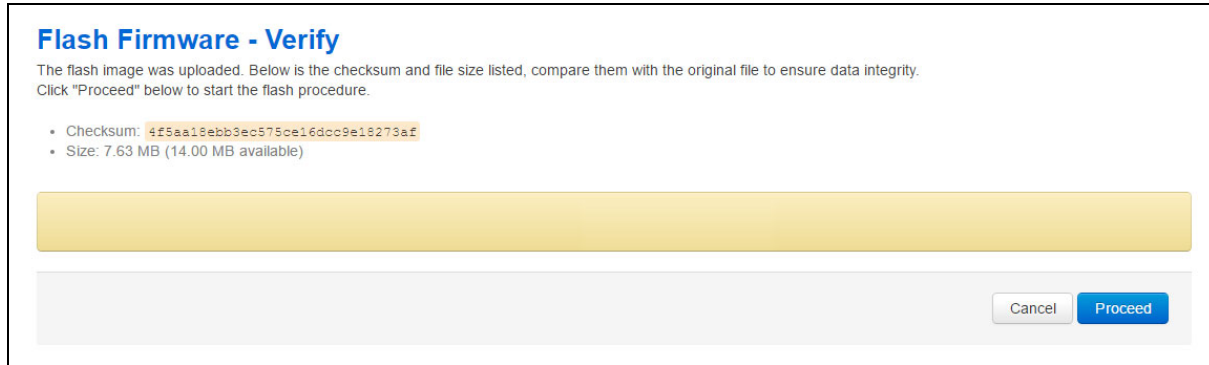
Switch to image2 (VIE-16.00.53):

**Figure 28: The flash operations page**

Under Flash new firmware image, click **Choose File** or **Browse**.

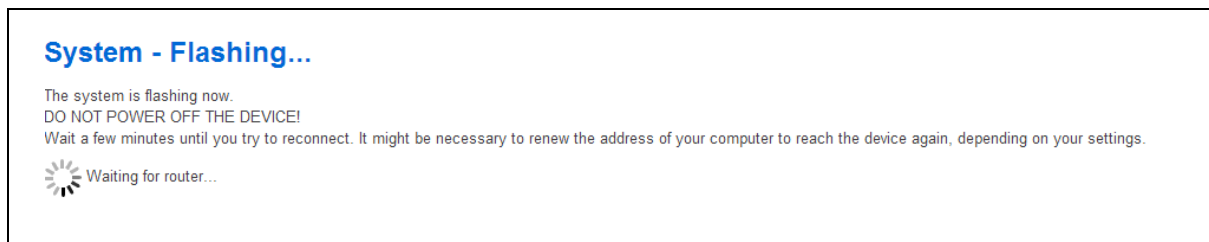
**Note:** the button will vary depending on the browser you are using.

Select the appropriate image and then click **Flash Image**. The Flash Firmware – Verify page appears.



**Figure 29: The flash firmware - verify page**

Click **Proceed**. The System – Flashing... page appears.



**Figure 30: The system – flashing...page**

When the 'waiting for router' icon disappears, the upgrade is complete, and the login homepage appears.

To verify that the router has been upgraded successfully, click **Status** in the top menu. The Firmware Version shows in the system list.

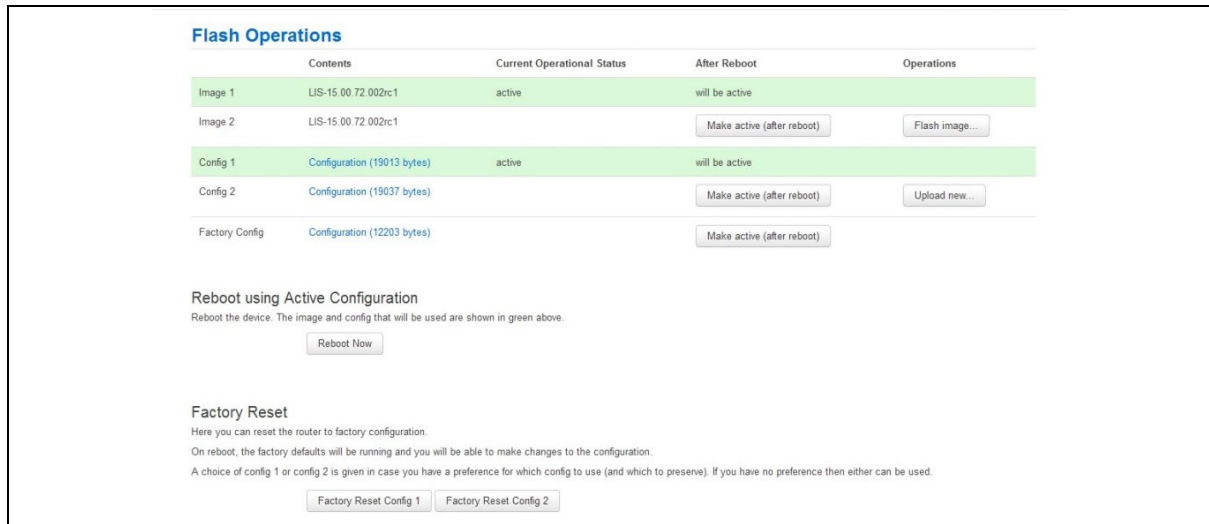
| Status               |                                |
|----------------------|--------------------------------|
| System               |                                |
| Router Name          | GW0000                         |
| Router Model         | Virtual Access GW0031W-AA0179E |
| Firmware Version     | VIE-16.00.55                   |
| Current Image/Config | image2 / config2               |
| Kernel Version       | 3.2.12                         |
| Local Time           | Fri Aug 5 11:43:52 2016        |
| Uptime               | 0h 10m 8s                      |
| Load Average         | 0.27, 0.35, 0.31               |

**Figure 31: The system status list**

### 8.1.3 Upgrading router firmware for software version 72.002 and above

Copy the new firmware issued by Virtual Access to a PC connected to the router.

In the top menu, select **System tab -> Flash operations**. The Flash operations page appears.

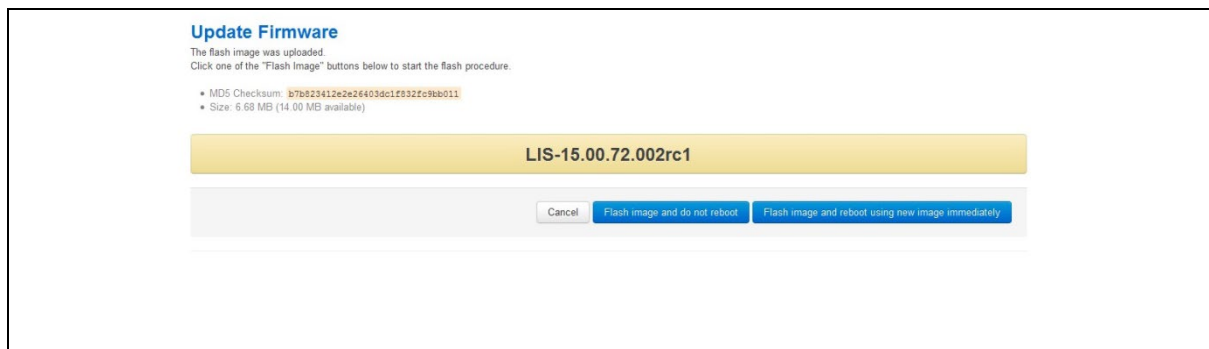


**Figure 32: The flash operations page**

Under Flash Operations, click **Flash Image**. Only the inactive image is available to flash. Select the appropriate image and then wait until image has loaded.

**Note:** this process may take a while depending on the available connection speed.

When the image has loaded, the Update Firmware page appears.



**Figure 33: The flash firmware - verify page**

Click either: **Flash image and do not reboot**, or **Flash image and reboot using new image immediately**. The 'Firmware update is being applied' message appears.

When the firmware update is complete, the Update Firmware page appears. There are various messages, depending on which option you selected, or if any corruptions have occurred.

### 8.1.4 Flash image and do not reboot option

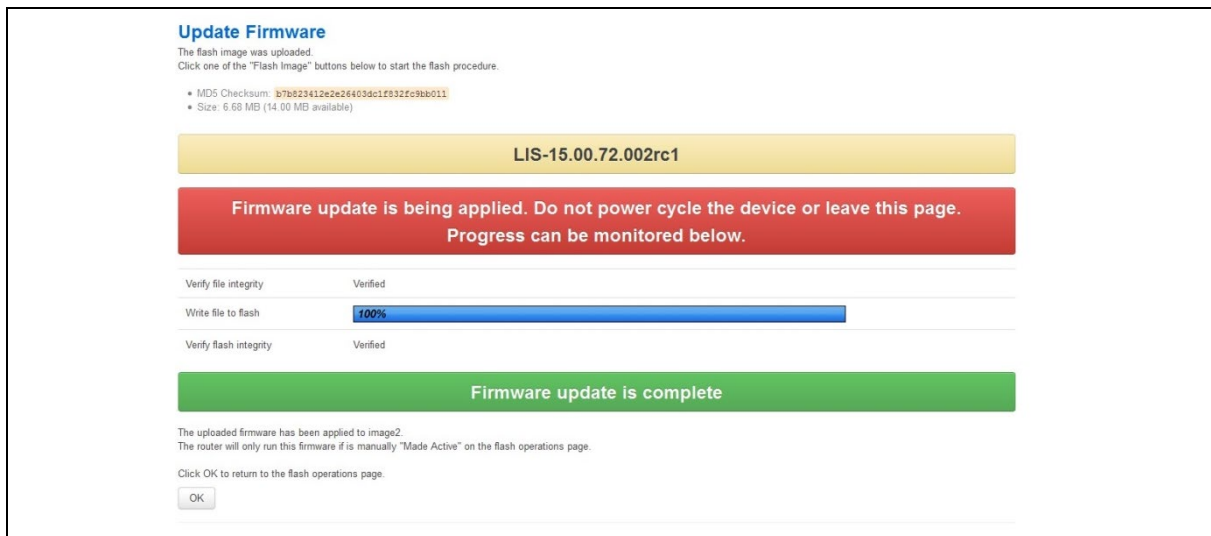


Figure 34: The firmware update page after ‘...do not reboot’ option selected

If you select ‘Flash image and do not reboot’, the router will only run the firmware if you click **OK** to return to the Flash Operations page. There you can manually select **Made Active (after reboot)**. Then click **Reboot Now** in the ‘Reboot using Active Configuration’ section.

### 8.1.5 Update flash image and reboot using new image immediately option

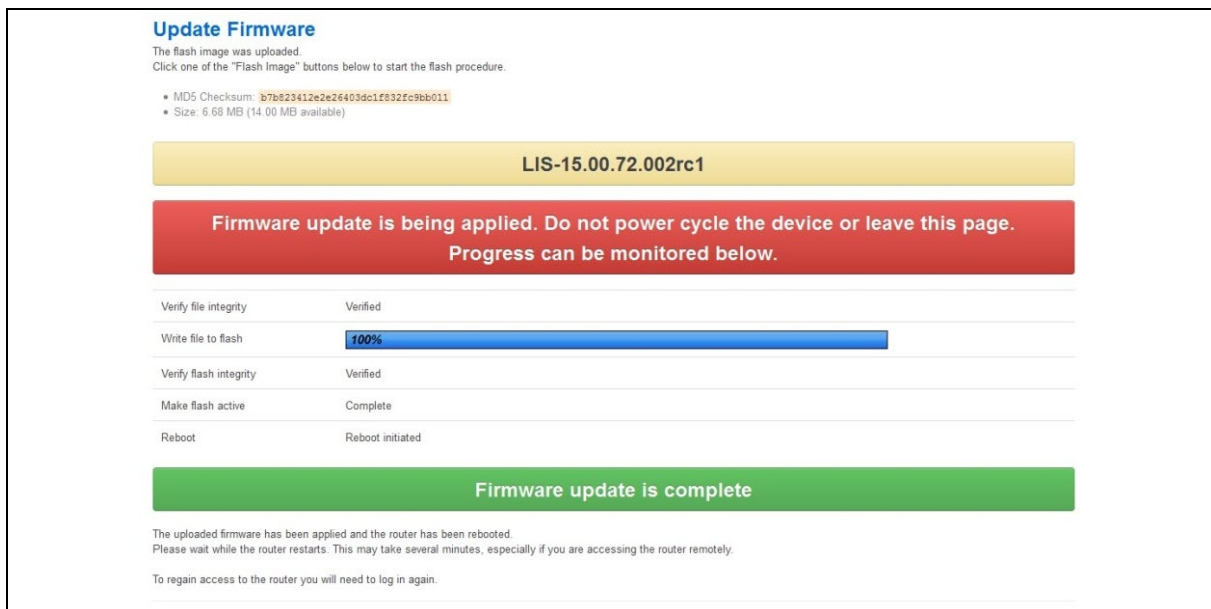


Figure 35: The firmware update page after ‘update flash image and reboot...’ option selected

If you select ‘Update flash image and reboot using new image immediately’ and the overall validation and flashing process has succeeded, the router will reboot immediately. To regain access to the router you must login again. If any part of the processes encounters an error the reboot does **not** occur and a report is given.

## 8.1.6 Possible file corruption

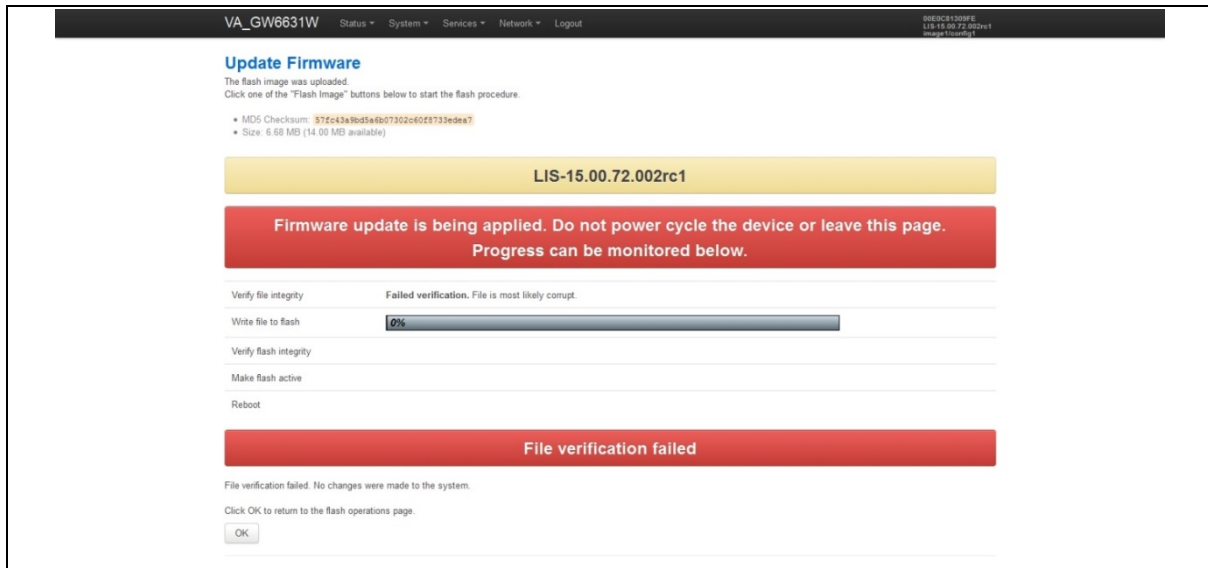


Figure 36: The firmware update failure page

In the unfortunate event that the firmware upgrade fails, the 'Failed verification File is most likely corrupt' or similar message will appear in the Verify file integrity row. No changes will be made to the system and the general message **File verification failed** appears.

## 8.1.7 Verify the firmware has been upgraded successfully

To check the firmware version, in the top menu, browse to **System -> Flash Operations**, or after router reboots, in the top menu, click **Status**. The Firmware Version shows in the system list and also in the right top corner of the menu bar.

| Status               |                                |
|----------------------|--------------------------------|
| System               |                                |
| Router Name          | GW0000                         |
| Router Model         | Virtual Access GW0031W-AA0179E |
| Firmware Version     | VIE-16.00.55                   |
| Current Image/Config | image2 / config2               |
| Kernel Version       | 3.2.12                         |
| Local Time           | Fri Aug 5 11:43:52 2016        |
| Uptime               | 0h 10m 8s                      |
| Load Average         | 0.27, 0.35, 0.31               |

Figure 37: The system status list showing current firmware version

## 8.2 Upgrading firmware using CLI

### 8.2.1 Transfer file to router

To upgrade firmware using CLI, you will need a TFTP server on a connected PC or SCP available.

Open up an SSH or Telnet session to the router.

Enter in the relevant username and password.

To access the temp folder, enter **cd /tmp**

Depending on the router's software version the following TFTP clients are available:

- atftp
- curl

To determine which is available on your router, enter:

```
which curl || which atftp
```

The output shows the available application:

```
/usr/bin/curl
```

#### ATFTP

Inline command usage:

```
atftp -g -r LIS-15.00.72.002.image -l /tmp/LIS-15.00.72.002.image x.x.x.x
```

where x.x.x.x is the IP address of your PC, **-g** is get operation and **-l** / **-r** are local and remote file name to store.

#### CURL

Inline command usage:

```
curl tftp://x.x.x.x/LIS-15.00.72.002.image -o /tmp/LIS-15.00.72.002.image
```

where x.x.x.x is the IP of your PC, **-o** is local file name to store.

#### SCP

Secure Copy (SCP) is a part of Secure Shell (SSH) and enables file transfers to the router using authentication and encryption. It is different to TFTP, which uses UDP, while SCP uses a TCP connection. On Unix machines, SCP is a standard part of the system; on Windows it requires an additional application.

The usage example below is for a Unix machine and therefore assumes the image file is in the current folder.

```
scp LIS-15.00.72.002.image root@x.x.x.x:/tmp/LIS-15.00.72.002.image
```

Where the first argument 'LIS-15.00.72.002.image' in SCP is the source and the second argument 'tmp/LIS-15.00.72.002.image' is the destination path, enter **root** as the username to connect to x.x.x.x IP address.

After you execute the above command you will be asked to provide a root password.

At this stage the output shows the process of copying the software file into destination directory.

```
root@192.168.100.1's password:
LIS-15.00.72.000.image          100% 6812KB  2.2MB/s  00:03
```

## 8.2.2 Image verification before flashing

To verify the integrity of the image, firmware version xx.yy.72.002 and later uses an image-check application.

**Note:** it is the user's responsibility to verify the image before starting to write the image to flash process.

To use the image-check on downloaded image, enter:

```
image-check /tmp/LIS-15.00.72.002.image
```

In the case of any image corruption, an appropriate error message appears:

```
Error: no SquashFS filesystem after CRC'd section - data length 3
Error: read failed, expected at least 3 more bytes
```

or similar.

**Note:** the image is valid only if no error message appears. This process is done automatically during Web UI firmware update.

## 8.2.3 Flashing

When downloaded firmware verification succeeds, the new image can be written to flash.

To write the image into the alternative image, enter:

```
mtd write LIS-15.00.72.002.image altimage
```

**Note:** this is an example, substitute the correct file name.

## 8.2.4 Flash verification after flashing

After the write process has finished, you must complete a post verification of the firmware.

To verify the checksum of downloaded firmware, enter:

```
va_image_csum.sh /tmp/LIS-15.00.72.002.image
```



The checksum of the downloaded binary is shown:

```
08761cd03e33c569873bcc24cf2b7389 7006920 LIS-15.00.72.002 This MD5
```

To verify the checksum of written firmware, enter:

```
va_image_csum.sh alt
```

After a while the checksum will be calculated:

```
Calculating checksum.....
```

```
08761cd03e33c569873bcc24cf2b7389 7006920 LIS-15.00.72.002 This MD5
```

Verify and compare the checksum with the MD5 sum of the downloaded image.

If the checksum of the written firmware in altimage matches the one from the downloaded image in /tmp, the new firmware has been programmed successfully.

### 8.2.5 Setup an alternative image

Provided the programming has succeeded, you can set it as the next image to use after reboot; enter:

```
vacmd set next image altimage
```

To reboot using the new firmware, enter:

```
reboot
```

## 8.3 Firmware recovery

The router has an automatic boot recovery feature that will

- revert the active firmware to the alternate firmware segment on three consecutive failed software restarts.
- Change the boot configuration to factory configuration after ten failed restarts

By design this feature is intended to allow recovery from firmware problems and therefore excludes restarts due to power loss.

## 9 System settings

The system section contains settings that apply to the most basic operation of the system, such as the host name, time zone, logging details, NTP server, language and style.

The host name appears in the top left hand corner of the interface menu bar. It also appears when you open a Telnet or SSH session.

**Note:** this document shows no host name in screen shots. Throughout the document we use the host name 'VA\_router'.

The system configuration contains a logging section for the configuration of a syslog client.

### 9.1 Syslog overview

Most syslog settings appear in the main System Configuration page.

Syslog messages have a timestamp, source facility, priority, and message section. Often the message section begins with an optional tag identifying the usermode program name and process ID responsible for the message.

Messages can be stored locally and also forwarded remotely. Separate filter options apply to each case. At a broad level, you can set the minimum severity level for local and remote targets; only messages with a priority more severe than the configured level will be recorded.

Kernel messages are recorded separately in their own buffer. However, for convenience, these are copied to the system log automatically so that a unified system log is available.

In addition, you can also define filter rules to determine how particular log messages are handled. For example, you may decide that certain debug messages are directed into their own log file, to avoid cluttering up the main system log, and to save bandwidth if delivering to a remote syslog server. You can define filters to be applied to local and remote targets, or both. A filter matches specific log messages and then determines an action for them.

### 9.2 Configuration package used

| Package | Sections       |
|---------|----------------|
| system  | main           |
|         | syslog_fillter |
|         | timeserver     |
| luci    | main           |

## 9.3 Configuring system properties

To set your system properties, select **System -> System**. There are five sections in the System page.

| Section              | Description   |
|----------------------|---|
| General settings     | Configure host name, local time and time zone.  |
| Logging              | Configure a router to log to a server. You can configure a syslog client in this section. |
| Language and style   | Configure the router's web language and style.  |
| Time synchronization | Configure the NTP server in this section.   |
| Audit configuration  | Configures auditing of configuration changes and shell execution.                         |

### 9.3.1 General settings

Figure 38: General settings in system properties

| Web Field/UCI/Package Option   | Description   |
|--|---|
| Web: Local Time  | Sets the local time and syncs with browser. You can manually configure on CLI, using:<br><code>date -s YYYY.MM.DD-hh:mm:ss</code> |
| Web: hostname<br>UCI: system.main.hostname<br>Opt: hostname          | Specifies the hostname for this system.   |
| Web: Timezone<br>UCI: system.main.timezone<br>Opt: timezone          | Specifies the time zone that the date and time should be rendered in by default.  |
| Web: n/a<br>UCI: system.main.timezone<br>Opt: time_save_interval_min | Defines the interval in minutes to store the local time for use on next reboot.<br><input type="text" value="10m"/>               |

Table 15: Information table for general settings section

### 9.3.2 Logging

#### System Properties

General Settings
Logging
Language and Style

---

Log Storage

System log buffer size  kiB

System log buffer size for RAM  kiB

External system log server

External system log server port

External system backup log server

External system backup log server port

Log file location

Rotated log files to keep

Max Age of rotated log files  hours

Custom log hostname

Log output level

Remote log output level

**Figure 39: The logging section in system properties**

| Web Field/UCI/Package Option                                   | Description  |           |             |     |     |  |          |      |   |      |
|--|--|-----------|-------------|-----|-----|--|----------|------|---|------|
| Web: Log storage<br>UCI: system.main.log_type<br>Opt: log_type | Defines the system log storage type. Messages stored in RAM can be seen using <code>logread</code> .<br><b>Note:</b> system log stored in RAM will be lost on reboot. <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <thead> <tr> <th style="width: 15%;">Web value</th> <th style="width: 60%;">Description</th> <th style="width: 25%;">UCI</th> </tr> </thead> <tbody> <tr> <td>RAM</td> <td>Store system log in RAM. Lost on reboot. Viewed using <code>logread</code></td> <td>circular</td> </tr> <tr> <td>File</td> <td>Store system log in flash. Maintained through reboot. Viewed using <code>cat /log file</code></td> <td>file</td> </tr> </tbody> </table> | Web value | Description | UCI | RAM | Store system log in RAM. Lost on reboot. Viewed using <code>logread</code> | circular | File | Store system log in flash. Maintained through reboot. Viewed using <code>cat /log file</code> | file |
| Web value  | Description  | UCI       |             |     |     |  |          |      |   |      |
| RAM  | Store system log in RAM. Lost on reboot. Viewed using <code>logread</code>   | circular  |             |     |     |  |          |      |   |      |
| File   | Store system log in flash. Maintained through reboot. Viewed using <code>cat /log file</code>  | file      |             |     |     |  |          |      |   |      |

|  |   |       |            |              |  |
|--|---|-------|------------|--------------|--|
| <p>Web: System log buffer size<br/>UCI: system.main.log_size<br/>Opt: log_size</p>                               | <p>File log buffer size in KB.<br/><b>Note:</b> when the file reaches the configured size it is copied to the archive file (<code>log_file_name.0</code>).</p> <table border="1" data-bbox="639 286 1289 360"> <tr><td>Range</td><td></td></tr> <tr><td>16</td><td>16 KB</td></tr> </table>   | Range |            | 16           | 16 KB                                    |
| Range  |   |       |            |              |  |
| 16   | 16 KB   |       |            |              |  |
| <p>Web: System log buffer size for RAM<br/>UCI: system.main.log_size_ram<br/>Opt: log_size_ram</p>               | <p>RAM log buffer size in KB.</p> <table border="1" data-bbox="639 394 1289 470"> <tr><td>Range</td><td></td></tr> <tr><td>16</td><td>16 KB</td></tr> </table>  | Range |            | 16           | 16 KB                                    |
| Range  |   |       |            |              |  |
| 16   | 16 KB   |       |            |              |  |
| <p>Web: External system log server<br/>UCI: system.main.log_ip<br/>Opt: log_ip</p>                               | <p>External syslog server IP address. If defined, syslog messages will be sent in addition to local storage.</p> <table border="1" data-bbox="639 555 1289 629"> <tr><td>Range</td><td>IP of FQDN</td></tr> <tr><td>0.0.0.0</td><td></td></tr> </table>   | Range | IP of FQDN | 0.0.0.0      |  |
| Range  | IP of FQDN  |       |            |              |  |
| 0.0.0.0  |   |       |            |              |  |
| <p>Web: External system log server port<br/>UCI: system.main.log_port<br/>Opt: log_port</p>                      | <p>External syslog server port number.</p> <table border="1" data-bbox="639 667 1289 743"> <tr><td>Range</td><td></td></tr> <tr><td>514</td><td></td></tr> </table>   | Range |            | 514          |  |
| Range  |   |       |            |              |  |
| 514  |   |       |            |              |  |
| <p>Web: External system backup log server<br/>UCI: system.main.log_ip_backup<br/>Opt: log_ip_backup</p>          | <p>Backup external syslog server IP address. If defined, syslog messages will be sent here in addition to the main log server.</p> <table border="1" data-bbox="639 833 1289 907"> <tr><td>Range</td><td>IP or FQDN</td></tr> <tr><td>0.0.0.0</td><td></td></tr> </table>   | Range | IP or FQDN | 0.0.0.0      |  |
| Range  | IP or FQDN  |       |            |              |  |
| 0.0.0.0  |   |       |            |              |  |
| <p>Web: External system backup log server port<br/>UCI: system.main.log_port_backup<br/>Opt: log_port_backup</p> | <p>External syslog server port number for use with backup server.</p> <table border="1" data-bbox="639 945 1289 1019"> <tr><td>Range</td><td></td></tr> <tr><td>514</td><td></td></tr> </table>   | Range |            | 514          |  |
| Range  |   |       |            |              |  |
| 514  |   |       |            |              |  |
| <p>Web: Log file location<br/>UCI: system.main.log_file<br/>Opt: log_file</p>                                    | <p>Defines the file path for log storage when log storage is set to 'file'.<br/><b>Note:</b> when the file reaches the configured size it is copied to the archive file (<code>log_file_name.0</code>).</p> <p>Set to: <code>root/syslog.messages</code></p> <table border="1" data-bbox="639 1160 1289 1234"> <tr><td>Range</td><td></td></tr> <tr><td>/root/syslog</td><td></td></tr> </table>  | Range |            | /root/syslog |  |
| Range  |   |       |            |              |  |
| /root/syslog   |   |       |            |              |  |
| <p>Web: Rotated log files to keep<br/>UCI: system.main.log_file_count<br/>Opt: log_file_count</p>                | <p>Defines the file number of archive files for storage in flash when Log Storage is set to 'file'.<br/>When the system log file reaches the configured size it is copied to the archive file (<code>log_file_name.0</code>). Existing archive files are copied to <code>log_file_name.(x+1)</code>.</p> <table border="1" data-bbox="639 1379 1289 1453"> <tr><td>Range</td><td></td></tr> <tr><td>1</td><td>Store 1 archive log file in flash.</td></tr> </table> | Range |            | 1            | Store 1 archive log file in flash.       |
| Range  |   |       |            |              |  |
| 1  | Store 1 archive log file in flash.  |       |            |              |  |
| <p>Web: Max Age of rotated log files<br/>UCI: system.main.log_age<br/>Opt: log_age</p>                           | <p>Defines the maximum duration in hours before archive syslog files are deleted.<br/>Set to <b>0</b> to define no age limit.</p> <table border="1" data-bbox="639 1547 1289 1621"> <tr><td>Range</td><td></td></tr> <tr><td>0</td><td>No age limit</td></tr> </table>  | Range |            | 0            | No age limit                             |
| Range  |   |       |            |              |  |
| 0  | No age limit  |       |            |              |  |
| <p>Web: Custom log hostname<br/>UCI: system.main.log_hostname<br/>Opt: log_hostname</p>                          | <p>Defines a custom host name for syslog messages.<br/>Magic values <code>%hostname</code> (system hostname), <code>%ser</code> (serial), and <code>%mon</code> (Monitor dev_reference) are also recognised.</p> <table border="1" data-bbox="639 1715 1289 1805"> <tr><td>Range</td><td></td></tr> <tr><td>Empty</td><td>Use router hostname for syslog messages.</td></tr> </table>   | Range |            | Empty        | Use router hostname for syslog messages. |
| Range  |   |       |            |              |  |
| Empty  | Use router hostname for syslog messages.  |       |            |              |  |

| <p>Web: Log output level<br/>UCI: system.main.conologlevel<br/>Opt: conologlevel</p>                | <p>Sets the maximum log output level severity for system events. System events are written to the system log. Messages with a lower level or level equal to the configured level are displayed on the console using the logread command, or alternatively written to a flash file, if configured to do so.</p> <table border="1" data-bbox="639 331 1334 750"> <thead> <tr> <th>Web value</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Debug</td> <td>Information useful to developers for debugging the application.</td> <td>8</td> </tr> <tr> <td>Info</td> <td>Normal operational messages that require no action.</td> <td>7</td> </tr> <tr> <td>Notice</td> <td>Events that are unusual, but not error conditions.</td> <td>6</td> </tr> <tr> <td>Warning</td> <td>May indicate that an error will occur if action is not taken.</td> <td>5</td> </tr> <tr> <td>Error</td> <td>Error conditions</td> <td>4</td> </tr> <tr> <td>Critical</td> <td>Critical conditions</td> <td>3</td> </tr> <tr> <td>Alert</td> <td>Should be addressed immediately</td> <td>2</td> </tr> <tr> <td>Emergency</td> <td>System is unusable</td> <td>1</td> </tr> </tbody> </table> | Web value | Description | UCI  | Debug   | Information useful to developers for debugging the application. | 8 | Info | Normal operational messages that require no action. | 7 | Notice | Events that are unusual, but not error conditions. | 6 | Warning | May indicate that an error will occur if action is not taken. | 5 | Error | Error conditions  | 4 | Critical | Critical conditions  | 3 | Alert | Should be addressed immediately  | 2 | Emergency | System is unusable  | 1 |
|---|---|-----------|-------------|------|---------|---|---|------|---|---|--------|--|---|---------|---|---|-------|-------------------|---|----------|----------------------|---|-------|----------------------------------|---|-----------|---------------------|---|
| Web value   | Description   | UCI       |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| Debug   | Information useful to developers for debugging the application.   | 8         |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| Info  | Normal operational messages that require no action.   | 7         |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| Notice  | Events that are unusual, but not error conditions.  | 6         |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| Warning   | May indicate that an error will occur if action is not taken.   | 5         |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| Error   | Error conditions  | 4         |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| Critical  | Critical conditions   | 3         |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| Alert   | Should be addressed immediately   | 2         |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| Emergency   | System is unusable  | 1         |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| <p>Web: Remote log output level<br/>UCI: system.main.remoteloglevel<br/>Opt: remoteloglevel</p>     | <p>Sets the maximum log output level severity for system events sent to remote syslog server.</p> <table border="1" data-bbox="639 813 1334 1234"> <thead> <tr> <th>Web value</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Debug</td> <td>Information useful to developers for debugging the application.</td> <td>8</td> </tr> <tr> <td>Info</td> <td>Normal operational messages that require no action.</td> <td>7</td> </tr> <tr> <td>Notice</td> <td>Events that are unusual, but not error conditions.</td> <td>6</td> </tr> <tr> <td>Warning</td> <td>May indicate that an error will occur if action is not taken.</td> <td>5</td> </tr> <tr> <td>Error</td> <td>Error conditions.</td> <td>4</td> </tr> <tr> <td>Critical</td> <td>Critical conditions.</td> <td>3</td> </tr> <tr> <td>Alert</td> <td>Should be addressed immediately.</td> <td>2</td> </tr> <tr> <td>Emergency</td> <td>System is unusable.</td> <td>1</td> </tr> </tbody> </table>   | Web value | Description | UCI  | Debug   | Information useful to developers for debugging the application. | 8 | Info | Normal operational messages that require no action. | 7 | Notice | Events that are unusual, but not error conditions. | 6 | Warning | May indicate that an error will occur if action is not taken. | 5 | Error | Error conditions. | 4 | Critical | Critical conditions. | 3 | Alert | Should be addressed immediately. | 2 | Emergency | System is unusable. | 1 |
| Web value   | Description   | UCI       |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| Debug   | Information useful to developers for debugging the application.   | 8         |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| Info  | Normal operational messages that require no action.   | 7         |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| Notice  | Events that are unusual, but not error conditions.  | 6         |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| Warning   | May indicate that an error will occur if action is not taken.   | 5         |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| Error   | Error conditions.   | 4         |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| Critical  | Critical conditions.  | 3         |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| Alert   | Should be addressed immediately.  | 2         |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| Emergency   | System is unusable.   | 1         |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| <p>Web: n/a<br/>UCI: system.main.audit_shell<br/>Opt: audit_shell</p>                               | <p>Log every command executed in shell.</p> <table border="1" data-bbox="639 1267 1289 1339"> <tbody> <tr> <td>1</td> <td>Enable</td> </tr> <tr> <td>0</td> <td>Disable</td> </tr> </tbody> </table>  | 1         | Enable      | 0    | Disable |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| 1   | Enable  |           |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| 0   | Disable   |           |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| <p>Web: n/a<br/>UCI: system.main.audit_cfg<br/>Opt: audit_cfg</p>                                   | <p>Log changes made to configuration file through any interface.</p> <table border="1" data-bbox="639 1402 1289 1473"> <tbody> <tr> <td>1</td> <td>Enable</td> </tr> <tr> <td>0</td> <td>Disable</td> </tr> </tbody> </table>   | 1         | Enable      | 0    | Disable |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| 1   | Enable  |           |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| 0   | Disable   |           |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| <p>Web: n/a<br/>UCI: system.main.audit_cfg_hul_interval_h<br/>Opt: audit_cfg_hul_interval_hours</p> | <p>Defines the interval, in hours, at which configuration changes are uploaded to Activator.<br/>Set to <b>0</b> to disable.</p> <table border="1" data-bbox="639 1599 1289 1671"> <tbody> <tr> <td>Range</td> <td></td> </tr> <tr> <td>6</td> <td>6 hours</td> </tr> </tbody> </table>   | Range     |             | 6    | 6 hours |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| Range   |   |           |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| 6   | 6 hours   |           |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| <p>Web: n/a<br/>UCI: system.main.audit_cfg_max_size_kb<br/>Opt: audit_cfg_max_size_kb</p>           | <p>Defines the maximum size audit data can take in flash in 1024 byte units.</p> <table border="1" data-bbox="639 1756 1289 1827"> <tbody> <tr> <td>Range</td> <td></td> </tr> <tr> <td>1024</td> <td>6 hours</td> </tr> </tbody> </table>  | Range     |             | 1024 | 6 hours |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| Range   |   |           |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |
| 1024  | 6 hours   |           |             |      |         |   |   |      |   |   |        |  |   |         |   |   |       |                   |   |          |                      |   |       |                                  |   |           |                     |   |

Table 16: Information table for the logging section

### 9.3.3 Language and style

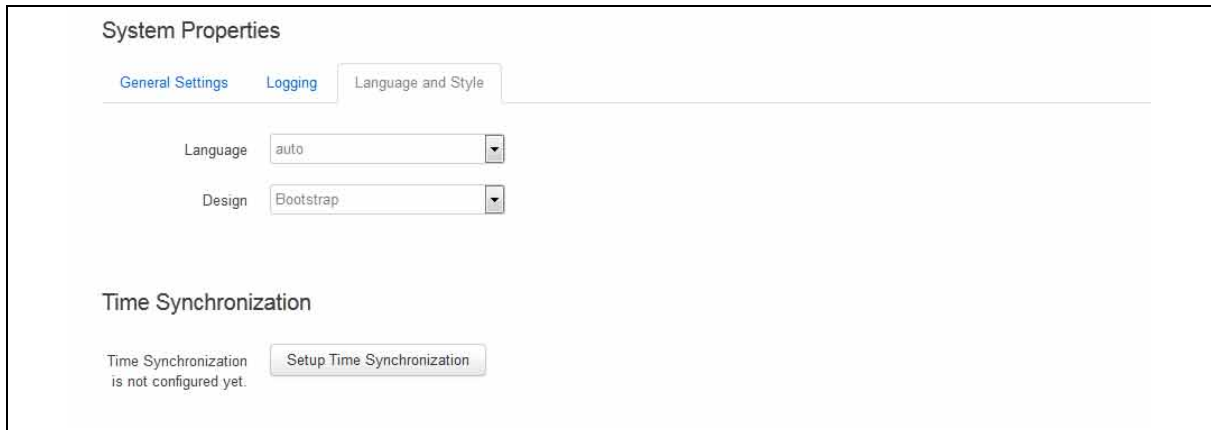


Figure 40: The language and style section in system properties

| Web Field/UCI/Package Option | Description  |      |  |         |  |
|------------------------------|--|------|--|---------|--|
| Language                     | Sets the language to 'auto' or 'English'.<br><table border="1" style="width: 100%;"> <tr> <td>Auto</td> <td></td> </tr> <tr> <td>English</td> <td></td> </tr> </table> | Auto |  | English |  |
| Auto                         |  |      |  |         |  |
| English                      |  |      |  |         |  |
| Design                       | Sets the router's style.   |      |  |         |  |

Table 17: Information table for the language and style page

### 9.3.4 Audit configuration

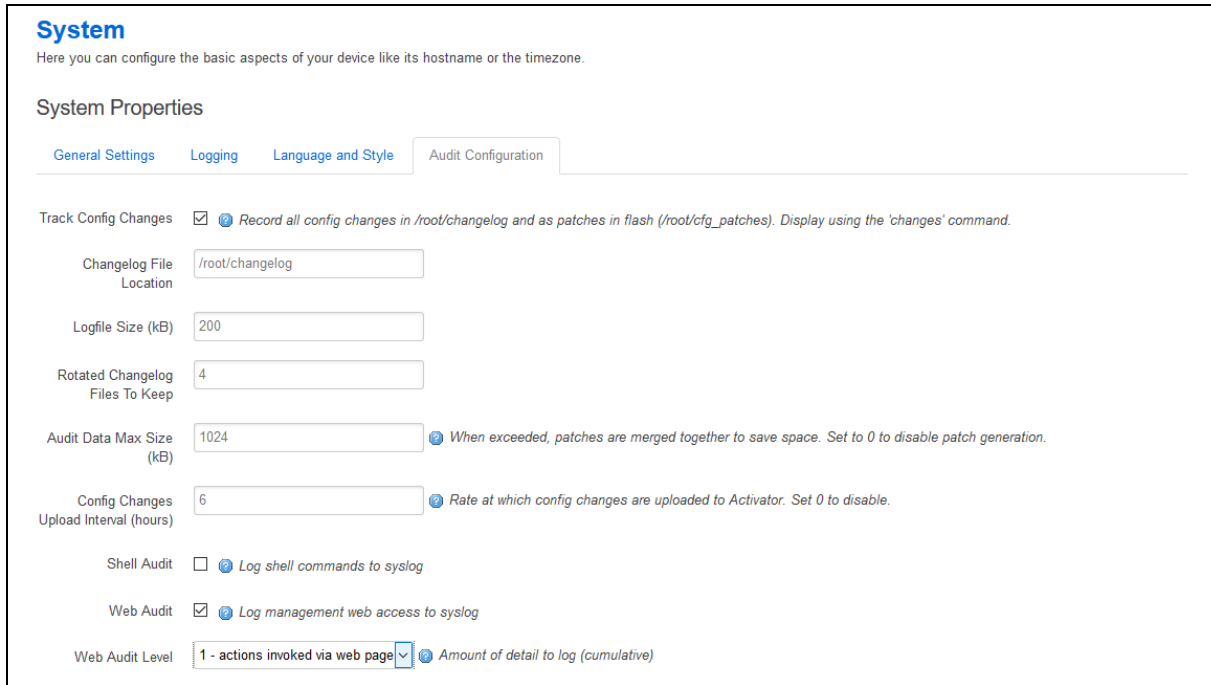


Figure 41: The language and style section in system properties

| Web Field/UCI/Package Option   | Description   |           |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
|--|---|-----------|-------------|-----------------|---|--|---|-----------------------------|--|---|-------------------------------------|--|---|-------------------------------|--|---|
| Web: Track Config Changes<br>UCI: system.main.audit_cfg<br>Opt: audit_cfg  | Any changes made to configuration file through any interface are logged to syslog.<br><table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table>  | 1         | Enabled.    | 0               | Disabled.                               |  |   |                             |  |   |                                     |  |   |                               |  |   |
| 1  | Enabled.  |           |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| 0  | Disabled.   |           |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| Web: Changelog File Location<br>UCI: system.main.audit_cfg_log_file<br>Opt: audit_cfg_log_file                               | Defines the location of the configuration change log<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> <tr> <td>/root/changelog</td> <td></td> </tr> </table>   | Range     |             | /root/changelog |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| Range  |   |           |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| /root/changelog  |   |           |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| Web: Logfile Size (kB)<br>UCI: system.main.audit_cfg_log_size<br>Opt: audit_cfg_log_size                                     | Defines the maximum size of the configuration change log file in kB<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> <tr> <td>200</td> <td>200 kB</td> </tr> </table>  | Range     |             | 200             | 200 kB                                  |  |   |                             |  |   |                                     |  |   |                               |  |   |
| Range  |   |           |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| 200  | 200 kB  |           |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| Web: Rotated Changelog Files to Keep<br>UCI: system.main.audit_cfg_log_count<br>Opt: audit_cfg_log_count                     | Defines the maximum number of configuration change log files to store<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> <tr> <td>4</td> <td>Store 4 changelog files before rotating</td> </tr> </table>   | Range     |             | 4               | Store 4 changelog files before rotating |  |   |                             |  |   |                                     |  |   |                               |  |   |
| Range  |   |           |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| 4  | Store 4 changelog files before rotating   |           |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| Web: Audit Data Max Size (kB)<br>UCI: system.main.audit_cfg_max_size_kb<br>Opt: audit_cfg_max_size_kb                        | Defines the maximum size audit data can take in flash in kB.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> <tr> <td>1024</td> <td></td> </tr> </table>  | Range     |             | 1024            |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| Range  |   |           |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| 1024   |   |           |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| Web: Config Changes Upload Interval<br>UCI:<br>system.main.audit_cfg_hul_interval_hours<br>Opt: audit_cfg_hul_interval_hours | Defines the interval, in hours, at which configuration change messages are uploaded to Activator.<br>Set to <b>0</b> to disable.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> <tr> <td>6</td> <td>6 hours</td> </tr> </table>  | Range     |             | 6               | 6 hours                                 |  |   |                             |  |   |                                     |  |   |                               |  |   |
| Range  |   |           |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| 6  | 6 hours   |           |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| Web: Shell Audit<br>UCI: system.main.audit_shell<br>Opt: audit_shell   | Every command executed in shell is logged to syslog.<br><table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table>  | 1         | Enabled.    | 0               | Disabled.                               |  |   |                             |  |   |                                     |  |   |                               |  |   |
| 1  | Enabled.  |           |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| 0  | Disabled.   |           |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| Web: Web Audit<br>UCI: luci.main.audit_req<br>Opt: audit_req   | Enables logging management web access to syslog.<br><table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table>  | 1         | Enabled.    | 0               | Disabled.                               |  |   |                             |  |   |                                     |  |   |                               |  |   |
| 1  | Enabled.  |           |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| 0  | Disabled.   |           |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| Web: Web Audit Level<br>UCI: luci.main.audit_shell<br>Opt: audit_level   | Defines the type of web operation to be logged to syslog.<br><table border="1"> <thead> <tr> <th>Web value</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>1 – actions invoked via web page</td> <td></td> <td>1</td> </tr> <tr> <td>2 – config and status pages</td> <td></td> <td>2</td> </tr> <tr> <td>3 – config, status and polled pages</td> <td></td> <td>3</td> </tr> <tr> <td>4 – comprehensive URL logging</td> <td></td> <td>4</td> </tr> </tbody> </table> | Web value | Description | UCI             | 1 – actions invoked via web page        |  | 1 | 2 – config and status pages |  | 2 | 3 – config, status and polled pages |  | 3 | 4 – comprehensive URL logging |  | 4 |
| Web value  | Description   | UCI       |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| 1 – actions invoked via web page   |   | 1         |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| 2 – config and status pages  |   | 2         |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| 3 – config, status and polled pages  |   | 3         |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |
| 4 – comprehensive URL logging  |   | 4         |             |                 |   |  |   |                             |  |   |                                     |  |   |                               |  |   |

Table 18: Information table for the audit configuration page

### 9.3.5 Time synchronization

The router time must be synchronized using NTP. The router can act as both an NTP client and an NTP server. It is enabled as an NTP client by default and individual interfaces can be configured to respond to NTP requests.



**Time Synchronization**

NTP update interval

NTP server candidates

- 
- 
- 
- 

Max Round-Trip Time (sec)  ? If NTP round-trip would take longer then this, it won't be regarded for calculation

NTP Server Interface

NTP Server Stratum

NTP Source Combine Limit

**Figure 42: The time synchronization section in system properties**

| Web Field/UCI/Package Option   | Description   |       |                                 |       |            |
|--|---|-------|---------------------------------|-------|------------|
| Web: NTP update interval<br>UCI: system.ntp.interval_hours<br>Opt: interval_hours                      | Specifies interval of NTP requests in hours. Default value set to auto.<br><table border="1"> <tr> <td>Auto</td> <td></td> </tr> <tr> <td>Range</td> <td>auto; 1-23</td> </tr> </table>   | Auto  |                                 | Range | auto; 1-23 |
| Auto   |   |       |                                 |       |            |
| Range  | auto; 1-23  |       |                                 |       |            |
| Web: NTP server candidates<br>UCI: system.ntp.server<br>Opt: list server                               | Defines the list of NTP servers to poll the time from. If the list is empty, the built-in NTP daemon is not started. Multiple servers can be configured and are separated by a space if using UCI. By default all fields are set to 0.0.0.0.  |       |                                 |       |            |
| Web: Max Round-Trip Time (secs)<br>UCI: system.ntp.max_ntp_roundtrip_sec<br>Opt: max_ntp_roundtrip_sec | Defines the maximum time in seconds for an NTP poll. Any polls that take longer than this will be not be used for NTP calculation.<br><table border="1"> <tr> <td>2</td> <td>Two seconds.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 2     | Two seconds.                    | Range |            |
| 2  | Two seconds.  |       |                                 |       |            |
| Range  |   |       |                                 |       |            |
| Web: NTP Server Interface<br>UCI: system.ntp.listen<br>Opt: listen                                     | Defines a list of interfaces that respond to NTP requests. Interfaces should be delimited using space. Example:<br>option listen 'LAN1 LAN2'<br><table border="1"> <tr> <td>Blank</td> <td>Do not respond to NTP requests.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | Blank | Do not respond to NTP requests. | Range |            |
| Blank  | Do not respond to NTP requests.   |       |                                 |       |            |
| Range  |   |       |                                 |       |            |
| Web: NTP Server Stratum<br>UCI: system.ntp.stratum<br>Opt: stratum                                     | Defines how far this NTP server is from the reference clock. For example, an NTP server getting time directly from the reference clock will have a stratum of 1. In general, this should be left blank, which means that the router NTP server will derive the stratum from the NTP dialogue.<br><table border="1"> <tr> <td>Blank</td> <td>NTP server will derive stratum</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | Blank | NTP server will derive stratum  | Range |            |
| Blank  | NTP server will derive stratum  |       |                                 |       |            |
| Range  |   |       |                                 |       |            |
| Web: NTP Source Combine Limit<br>UCI: system.ntp.combinelimit<br>Opt: combinelimit                     | Defines whether to limit sources included in the combining algorithm.<br>When chronyd has multiple sources available for synchronization, it has to select one source as the synchronization source. The measured offsets and frequencies of the system clock relative to the other sources, however, can be combined with the selected source to improve the accuracy of the system clock.<br>The combinelimit directive limits which sources are included in the combining algorithm. Their synchronization distance has to be shorter than the distance of the selected source multiplied by the value of the limit. Also, their measured frequencies have to be close to the frequency of the selected source.<br><table border="1"> <tr> <td>3</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table> | 3     |                                 | Range |            |
| 3  |   |       |                                 |       |            |
| Range  |   |       |                                 |       |            |

Table 19: Information table for time synchronization section

### 9.3.6 Console login banner

To configure a message that is displayed after login via SSH, telnet or console, in the top menu, select **System -> Administration**. Navigate to the Console login banner section.

Console login banner

Here you can specify the banner that is shown prior to logins

This is a test banner

Figure 43: The console login banner in system section

| Web Field/UCI/Package Option   | Description  |
|--|--|
| Web: Console login banner<br>UCI: system.main.banner<br>list: banner | Defines a login banner that is displayed after log in via SSH, telnet or console |
|  |  |
|  | Range  |

Figure 44: Information table for console login banner

### 9.3.7 System reboot

The router can be configured to reboot immediately, or scheduled to reboot a configured time in the future.

In the top menu, select **System -> Reboot**. The System page appears.

Ensure you have saved all your configuration changes before you reboot.

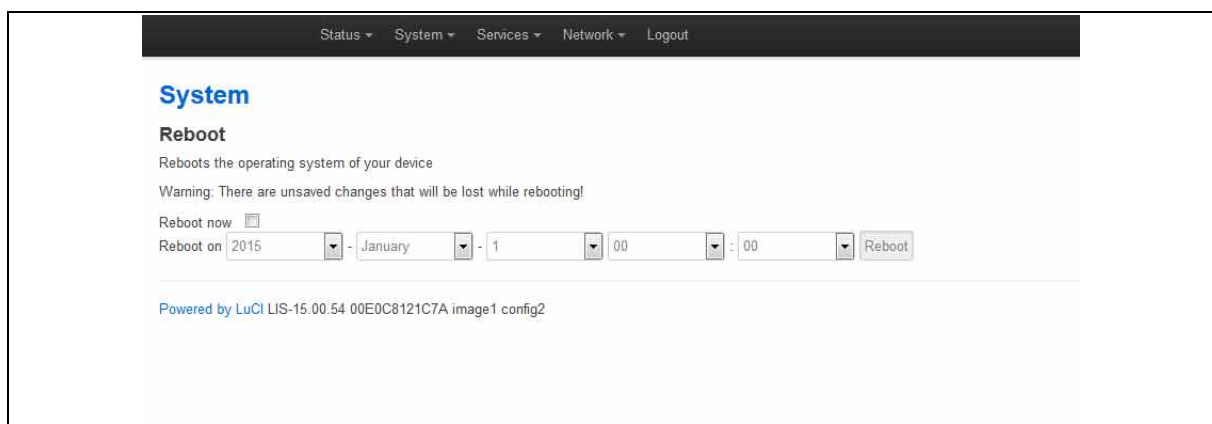


Figure 45: The reboot page

Check the **Reboot now** check box and then click **Reboot**.

## 9.4 System settings using command line

System settings are configured under the system package **/etc/config/system**. There are several configuration sections.

| Section       | Description   |
|---------------|---|
| system        | General system configuration options                |
| timeserver    | Router time and NTP configuration options           |
| syslog_filter | Advanced filter rules (see Advanced filter section) |

### 9.4.1 System settings using UCI

```
root@VA_router:~# uci show system
system.main=system
system.main.hostname=VA_router
system.main.timezone=UTC
system.main.log_ip=1.1.1.1
system.main.log_port=514
system.main.remoteloglevel=8
system.main.log_file=/root/syslog.messages
system.main.log_size=400
system.main.log_type=file
system.main.log_file_count=3
system.main.conloglevel=8
system.main.cronloglevel=8
system.main.banner=This is a test banner
system.ntp.interval_hours=auto
system.ntp.server=0.VA_router.pool.ntp.org 10.10.10.10
system.ntp.combinelimit=3
```

### 9.4.2 System settings using package options

```
root@VA_router:~# uci export system
package 'system'

config 'system' 'main'
    option 'hostname' "VA_router"
    option 'timezone' "UTC"
    option 'log_ip' "1.1.1.1"
    option 'log_port' "514"
    option remoteloglevel '8'
    option log_file '/root/syslog.messages'
    option log_size '400'
    option log_type 'file'
    option log_file_count '3'
    option time_save_interval_min "10"
    option conloglevel '8'
    option cronloglevel '8'
```

```

list banner `This is a test banner`

config 'timeserver' 'ntp'
  option interval_hours 'auto'
  list server "0.VA_router.pool.ntp.org"
  list server '10.10.10.10'
  option listen `LAN1 LAN2`
  option combinelimit `3`

```

## 9.5 System diagnostics

### 9.5.1 System log messages

System log messages comprise of a date, source facility, hostname, severity and message description in the form tag: message.

#### 9.5.1.1 Source facility list:

| Facility | Description                            |
|----------|--|
| auth     | Authorisation/security                 |
| authpriv | Authorisation (private)                |
| cron     | Scheduled jobs                         |
| daemon   | Background daemons                     |
| kern     | Kernel messages                        |
| local0   | hotplug scripts                        |
| security | Same as auth                           |
| syslog   | Internal syslog events                 |
| user     | General user-mode application messages |

**Table 20: Syslog message severity list**

#### 9.5.1.2 Event severity list

The severities are ordered from most severe to least severe.

| Level | Name    | Description               |
|-------|---------|---------------------------|
| 0     | emerg   | System is unusable        |
| 1     | alert   | Immediate action required |
| 2     | crit    | Critical conditions       |
| 3     | error   | Error conditions          |
| 4     | warning | Warning conditions        |
| 5     | notice  | Normal but significant    |
| 6     | info    | Informational             |
| 7     | debug   | Debug-level messages      |
| -     | none    | No priority               |

**Table 21: Syslog message severity list**

### 9.5.1.3 System log messages in RAM

By default, system log messages are stored in the system log in RAM.

To view the system log in RAM, enter:

```
root@VA_router:~# logread
```

Shows the log.

```
root@VA_router:~# logread |tail
```

Shows end of the log.

```
root@VA_router:~# logread | more
```

Shows the log page by page.

```
root@VA_router:~# logread -f
```

Shows the log on an ongoing basis. To stop this option, press **ctrl-c**.

```
root@VA_router:~# logread -f &
```

Shows the log on an ongoing basis while in the background. This allows you to run other commands while still tracing the event logs. To stop this option, type **fg** to view the current jobs, then press **ctrl-c** to kill those jobs.

### 9.5.1.4 System log messages in flash

Since logread is limited by memory size and does not survive a reset, it is beneficial to write system messages to flash memory. To do this, modify the system config under the system package. Set the options '**log\_file**', '**log\_size**', '**log\_type**' and '**log\_file\_count**' as shown below:

```
root@VA_router:~# uci export system
package system
config system 'main'
    option hostname 'VA_router'
    option zonename 'UTC'
    option timezone 'GMT0'
    option conloglevel '8'
    option cronloglevel '8'
    option time_save_interval_hour '10'
    option log_hostname '%serial'
    option log_ip '1.1.1.1'
    option log_port '514'
    option log_file '/root/syslog.messages'
```

```
option log_size '400'  
option log_type 'file'  
option log_file_count '3'
```

The above commands will take effect after a reboot, or by running the console command:

```
root@VA_router:~# /etc/init.d/syslogd restart
```

```
root@VA_router:~# cat /root/syslog.messages
```

Shows all the system events stored in flash.

```
root@VA_router:~# tail /root/syslog.messages
```

Shows end of the events stored flash.

```
root@VA_router:~# tail -f /root/syslog.messages &
```

Shows the log on an ongoing basis. To stop this option, press **ctrl-c**.

## 9.5.2 Kernel messages

To view kernel messages, enter `dmesg`

```
root@VA_router:~# dmesg  
[ 0.000000] Linux version 3.10.12 (info@virtualaccess.com) (gcc version  
4.8.1 20130401 (prerelease) (Linaro GCC 4.8-2013.04) ) #130 PREEMPT 1970-  
01-01T00:00:00Z  
[ 0.000000] SoC: xRX330 rev 1.1  
[ 0.000000] bootconsole [early0] enabled  
[ 0.000000] CPU0 revision is: 00019556 (MIPS 34Kc)  
[ 0.000000] adding memory size:267386880 from DT  
[ 0.000000] MIPS: machine is Virtual Access GW6600V series  
[ 0.000000] Determined physical RAM map:  
[ 0.000000] memory: 0ff00000 @ 00000000 (usable)  
[ 0.000000] User-defined physical RAM map:  
[ 0.000000] memory: 07200000 @ 00000000 (usable)
```

**Note:** kernel messages are also copied to the main system log by default.

### 9.5.3 Syslog process

To check the syslog process is running correctly, enter `pgrep -fl syslogd`

```
root@VA_router:~# pgrep -fl syslogd
5409 /sbin/syslogd -h VARouter -L -R 192.168.14.202:514 -l 7 -r 8 -s 400 -O
/root/syslog.messages -b 3 -C64 -R localhost:2048
```

Changes to the syslog configuration will take effect with a restart of `syslogd`

```
root@VA_router:~# /etc/init.d/syslogd restart
```

### 9.5.4 NTP process

To check the NTP process is running correctly, enter `pgrep -fl chrony`

```
root@VA_router:~# pgrep -fl chrony
2553 /usr/sbin/chronyd -f /etc/chrony.conf
```

Changes to the NTP configuration will take effect with a restart of `chrony`

```
root@VA_router:~# /etc/init.d/chrony restart
```

## 9.6 Advanced filtering of syslog messages

Syslog messages can be filtered against a series of rules that are checked for each message generated. If a match is found, then the specified action is taken. If no match occurs, then the default action is taken, as defined in the main system logging settings.

A message may match multiple filters. They are processed in the order listed. For example, you may wish to record authorisation messages in the main system log, but also make a copy in a separate authorisation log which can span a much longer period of time.

By default, all matching filters will be applied to each message. However, you can mark a filter to indicate that after it matches, no further filter processing should take place.

The filter rules are defined in a free-form text list in the `syslog_filter` configuration section. There are two section types, one for messages to be stored locally, and one for messages delivered remotely.

Configuring advanced filters on the web interface is not currently supported; they must be edited using the command line interface.



## 9.6.1 Advanced filtering using command line

Filters are defined in the `syslog_filter` configuration section of the system package. A set of filters can be either local or remote.

- All messages are matched against both local and remote filter rules, if configured.
- Each local filter matched is executed; if there is no match, then the default local logging action applies.
- Any remote filter matched is executed; if there is no match, then the default remote logging action applies.

```
root@VA_router:~# uci export system
package system
.....
config syslog_filter 'local'
    list text "...line 1..."
    list text "...line 2..."
    list text "...line 3..."
    ...

config syslog_filter 'remote'
    list text "...line 1..."
    list text "...line 2..."
    list text "...line 3..."
    ...
```

Lines defined here are copied to the router runtime file `/var/conf/syslog.conf` which may be reviewed to determine current rules in use.

## 9.6.2 Filter definitions

Each filter ruleset is a series of lines. Each line can be:

- A filter pattern, of the form `facility.[op]severity(pattern) target [~]`
- A blank line, or comment line, starting with hash (`#`).

If a message does not match any of the filter lines for a destination, local or remote, the default action for that destination is taken.

The sections of a filter pattern break down as follows:

| Section  | Description   |
|----------|---|
| facility | Any keyword or comma-separated list of keywords from the source facility list. See the Source Facilities table in section 9.5.1.1.<br>Use the wildcard '*' to match all facilities.   |
| severity | Any keyword from the event severity list (see Event Severity table above). The rule will match all severities more urgent if the message severity level is at least as urgent as this.<br>Use the wildcard '*' to match all facilities. |

|             |   |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
|-------------|---|---------|--|---------|---|---------|--|-----|---|----|-------------------------------|-------------|---|-----------|---------------------------------------|-----------|---|-----------|--|
| op          | <p>Defines an optional severity condition.</p> <table border="1" data-bbox="456 226 1370 367"> <tr> <td>(empty)</td> <td>match listed severity, and also anything more severe</td> </tr> <tr> <td>!</td> <td>match on less urgent severities than that listed</td> </tr> <tr> <td>=</td> <td>severity must match exactly</td> </tr> <tr> <td>!=</td> <td>match any severity other than the listed severity</td> </tr> </table> <p>Examples:<br/> *.debug matches all messages of debug severity and greater (i.e. debug, info, warning, etc).<br/> *.=debug matches all debug messages.</p>   | (empty) | match listed severity, and also anything more severe                     | !       | match on less urgent severities than that listed      | =       | severity must match exactly  | !=  | match any severity other than the listed severity   |    |                               |             |   |           |                                       |           |   |           |  |
| (empty)     | match listed severity, and also anything more severe  |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| !           | match on less urgent severities than that listed  |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| =           | severity must match exactly   |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| !=          | match any severity other than the listed severity   |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| pattern     | <p>Defines an optional pattern to match against the message text. The pattern is used to restrict the number of log messages matching this filter.</p> <p>The pattern syntax is a simple case-insensitive regular expression, using these characters:</p> <table border="1" data-bbox="456 618 1353 792"> <tr> <td>*</td> <td>Matches zero or more characters.</td> </tr> <tr> <td>?</td> <td>Matches any single character (use this for spaces).</td> </tr> <tr> <td>!</td> <td>Matches anything not matching the following pattern.</td> </tr> <tr> <td>^</td> <td>Matches the start of a message.</td> </tr> <tr> <td>\$</td> <td>Matches the end of a message.</td> </tr> </table> <p>Examples:</p> <table border="1" data-bbox="456 826 1388 969"> <tr> <td>(firewall:)</td> <td>Match any message containing the string 'firewall:'</td> </tr> <tr> <td>(up*eth1)</td> <td>Match any UP message referencing eth1</td> </tr> <tr> <td>(!mobile)</td> <td>Match only messages that do not include the string 'mobile'</td> </tr> <tr> <td>(^mobile)</td> <td>Match only messages beginning with the string 'mobile'</td> </tr> </table> | *       | Matches zero or more characters.   | ?       | Matches any single character (use this for spaces).   | !       | Matches anything not matching the following pattern.   | ^   | Matches the start of a message.   | \$ | Matches the end of a message. | (firewall:) | Match any message containing the string 'firewall:' | (up*eth1) | Match any UP message referencing eth1 | (!mobile) | Match only messages that do not include the string 'mobile' | (^mobile) | Match only messages beginning with the string 'mobile' |
| *           | Matches zero or more characters.  |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| ?           | Matches any single character (use this for spaces).   |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| !           | Matches anything not matching the following pattern.  |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| ^           | Matches the start of a message.   |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| \$          | Matches the end of a message.   |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| (firewall:) | Match any message containing the string 'firewall:'   |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| (up*eth1)   | Match any UP message referencing eth1   |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| (!mobile)   | Match only messages that do not include the string 'mobile'   |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| (^mobile)   | Match only messages beginning with the string 'mobile'  |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| target      | <p>Defines what to do with the log message when a match occurs. It is optional for remote filters. It can be the name of a disk file, or one of the special target keywords listed below.</p> <table border="1" data-bbox="456 1055 1353 1252"> <tr> <td>default</td> <td>Do whatever the default action is, as if not the filter rule is matched.</td> </tr> <tr> <td>ignore</td> <td>Never log this message (useful for remote filtering).</td> </tr> <tr> <td>console</td> <td>Log this message to the console. To view the console use <code>cat /proc/conlog</code> For GW6600/GW6600V Series routers only.</td> </tr> <tr> <td>mem</td> <td>Log this message to the memory buffer (logread), if configured.<br/><b>Note:</b> logread is not stored through reboot.</td> </tr> </table>  | default | Do whatever the default action is, as if not the filter rule is matched. | ignore  | Never log this message (useful for remote filtering). | console | Log this message to the console. To view the console use <code>cat /proc/conlog</code> For GW6600/GW6600V Series routers only. | mem | Log this message to the memory buffer (logread), if configured.<br><b>Note:</b> logread is not stored through reboot. |    |                               |             |   |           |                                       |           |   |           |  |
| default     | Do whatever the default action is, as if not the filter rule is matched.  |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| ignore      | Never log this message (useful for remote filtering).   |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| console     | Log this message to the console. To view the console use <code>cat /proc/conlog</code> For GW6600/GW6600V Series routers only.  |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| mem         | Log this message to the memory buffer (logread), if configured.<br><b>Note:</b> logread is not stored through reboot.   |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| ~           | <p>Optional flag to indicate no further filters should be checked, if this filter matches. This prevents later filters from acting on the same message. For convenience this is automatically implied when a target of ignore is used. A space must be present before the ~ character.</p> <table border="1" data-bbox="456 1368 1353 1433"> <tr> <td>~</td> <td>No further filters should be checked after a match.</td> </tr> <tr> <td>(empty)</td> <td>Continue checking other filters after a match.</td> </tr> </table>  | ~       | No further filters should be checked after a match.                      | (empty) | Continue checking other filters after a match.        |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| ~           | No further filters should be checked after a match.   |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |
| (empty)     | Continue checking other filters after a match.  |         |  |         |   |         |  |     |   |    |                               |             |   |           |                                       |           |   |           |  |

Table 22: Filter syntax definitions

## 9.6.3 Filter examples

### 9.6.3.1 Example 1

Log all debug messages to memory buffer. Do not log anywhere else locally.

Log all authorisation facility messages to filepath 'var/log/auth'. Do not log anywhere else locally.

Log all ipsec messages to filepath 'va/log/ipsec'. Do not log anywhere else locally.

For everything else, apply default local logging.

No remote filter rules defined, so apply default remote logging to all messages.

```

config syslog_filter 'local'
    list text '*.debug mem ~'
    list text 'auth,authpriv.* /var/log/auth ~'
    list text '*.*(ipsec:) /var/log/ipsec ~'

```

### 9.6.3.2 Example 2

As Example 1 but in addition to specified local files, copy auth, authpriv and ipsec to local default log.

```

config syslog_filter 'local'
    list text '*.debug mem ~'
    list text 'auth,authpriv.* /var/log/auth'
    list text '*.*(ipsec:) /var/log/ipsec'
    list text '*.* default'

```

### 9.6.3.3 Example 3

As in Example 2, except **do not** send any auth or auth priv messages remotely.

```

config syslog_filter 'local'
    list text '*.debug mem ~'
    list text 'auth,authpriv.* /var/log/auth'
    list text '*.*(ipsec:) /var/log/ipsec'
    list text '*.* default'

config syslog_filter 'remote'
    list text 'auth,authpriv.* ignore'

```

### 9.6.3.4 Example 4

As in Example 3, except **only** send auth or auth priv messages remotely.

```

config syslog_filter 'local'
    list text '*.debug mem ~'
    list text 'auth,authpriv.* /var/log/auth'
    list text '*.*(ipsec:) /var/log/ipsec'
    list text '*.* default'

config syslog_filter 'remote'
    list text 'auth,authpriv.* ~'
    list text '*.* ignore'

```

## 9.6.4 Filter diagnostics

To view configured filters, enter `cat /var/conf/syslog.conf`

```
root@VA_router:~# cat /var/conf/syslog.conf
[local]
auth,authpriv.* /var/log/auth
*.*(ipsec:)      /var/log/ipsec
*.*              default

[remote]
auth,authpriv.info
*.* ignore
```

## 10 Configuring an Ethernet interface

This chapter describes how to configure an Ethernet interface including configuring the interface as a DHCP server, adding the interface to a firewall zone, mapping the physical switch ports and defining loopback interface.

### 10.1 Configuration packages used

| Package  | Sections  |
|----------|-----------|
| network  | interface |
|          | route     |
|          | va_switch |
|          | alias     |
| firewall | zone      |
| dhcp     | dhcp      |

### 10.2 Configuring an Ethernet interface using the web interface

To create and edit interfaces via the web interface, in the top menu, click **Network -> Interfaces**. The Interfaces overview page appears.

The screenshot displays the Mikrotik WinBox 'Interfaces' overview page. At the top, there is a navigation bar with 'Status', 'System', 'Services', 'Network', and 'Logout' menus, along with an 'AUTO REFRESH ON' indicator. The main content area is titled 'Interfaces' and 'Interface Overview'. It features a table with columns for 'Network' and 'Status'. The table lists several interfaces: 3G\_S1\_VODA, 3g-3g\_s1\_voda, LAN (eth0), LAN1 (eth1), LOOPBACK (lo), WAN (3g-wan), WAN1 (3g-wan1), and WAN2 (3g-wan2). Each interface entry shows its status (e.g., 'Up') and associated statistics like RX/TX bytes and packets. To the right of the table, there are 'Actions' buttons for each interface: 'Connect', 'Stop', 'Edit', and 'Delete'. Below the table, there is an 'Add new interface...' button. The 'Port Map' section allows mapping device ports to ethernet interfaces, with input fields for eth0 (A) and eth1 (B). The 'ATM Bridges' section provides information about ATM bridges and an 'Add' button. At the bottom right, there are 'Save & Apply', 'Save', and 'Reset' buttons.

Figure 46: The interfaces overview page

There are three sections in the Interfaces page.

| Section            | Description  |
|--------------------|--|
| Interface Overview | Shows existing interfaces and their status. You can create new, and edit existing interfaces here.   |
| Port Map           | In this section you can map device ports to Ethernet interfaces. Ports are marked with capital letters starting with 'A'. Type in space-separated port character in the port map fields. |
| ATM Bridges        | ATM bridges expose encapsulated Ethernet in AAL5 connections as virtual Linux network interfaces, which can be used in conjunction with DHCP or PPP to dial into the provider network.   |

### 10.2.1 Interface overview: editing an existing interface

To edit an existing interface, from the interface tabs at the top of the page, select the interface you wish to configure. Alternatively, click **Edit** in the interface's row.

### 10.2.2 Interface overview: creating a new interface

To create a new interface, in the Interface Overview section, click **Add new interface**. The Create Interface page appears.

Figure 47: The create interface page

| Web Field/UCI/Package Option  | Description  |          |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
|---|--|----------|-------------|--------|---|--|--------|-------------|---|------|-----------|-------------|------|------------------------|---------------------------|--|----------------|-------------------------------------|--|-----|--|-----|-----|-----|-----|------|-----------------------------|------|--------|----------------------------|--------|-----|-------------------------|-----|------|------------------------------------|------|-------|-------------------|-------|---------|--------------|-------|---------------------|---|----|-----------------|---------------|----------|
| Web: Name of the new interface<br>UCI: network.<if name><br>Opt: config interface         | Assigns a logical name to the interface. The network interface section will assign this name (<if name>).<br>Type the name of the new interface.<br>Allowed characters are A-Z, a-z, 0-9 and _   |          |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Web: Protocol of the new interface<br>UCI: network.<if name>.proto<br>Opt: proto          | Specifies what protocol the interface will operate on. Select <b>Static</b> . <table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Static</td> <td>Static configuration with fixed address and netmask.</td> <td>static</td> </tr> <tr> <td>DHCP Client</td> <td>Address and netmask are assigned by DHCP.</td> <td>dhcp</td> </tr> <tr> <td>Unmanaged</td> <td>Unspecified</td> <td>none</td> </tr> <tr> <td>IPv6-in-IPv4 (RFC4213)</td> <td>Used with tunnel brokers.</td> <td></td> </tr> <tr> <td>IPv6-over-IPv4</td> <td>Stateless IPv6 over IPv4 transport.</td> <td></td> </tr> <tr> <td>GRE</td> <td>Generic Routing Encapsulation protocol</td> <td>gre</td> </tr> <tr> <td>IOT</td> <td>IOT</td> <td>iot</td> </tr> <tr> <td>L2TP</td> <td>Layer 2 Tunnelling Protocol</td> <td>l2tp</td> </tr> <tr> <td>L2TPv3</td> <td>L2TPv3 Tunnelling Protocol</td> <td>l2tpv3</td> </tr> <tr> <td>PPP</td> <td>Point to Point Protocol</td> <td>ppp</td> </tr> <tr> <td>PPtP</td> <td>Point to Point Tunnelling Protocol</td> <td>pptp</td> </tr> <tr> <td>PPPoE</td> <td>PPP over Ethernet</td> <td>pppoe</td> </tr> <tr> <td>PPPoATM</td> <td>PPP over ATM</td> <td>pppoa</td> </tr> <tr> <td>LTE/UMTS/GPRS/EV-DO</td> <td>CDMA, UMTS or GPRS connection using an AT-style 3G modem.</td> <td>3g</td> </tr> <tr> <td>PPP(PSTN-Modem)</td> <td>PPP v90 modem</td> <td>pppmodem</td> </tr> </tbody> </table> | Web      | Description | UCI    | Static  | Static configuration with fixed address and netmask. | static | DHCP Client | Address and netmask are assigned by DHCP. | dhcp | Unmanaged | Unspecified | none | IPv6-in-IPv4 (RFC4213) | Used with tunnel brokers. |  | IPv6-over-IPv4 | Stateless IPv6 over IPv4 transport. |  | GRE | Generic Routing Encapsulation protocol | gre | IOT | IOT | iot | L2TP | Layer 2 Tunnelling Protocol | l2tp | L2TPv3 | L2TPv3 Tunnelling Protocol | l2tpv3 | PPP | Point to Point Protocol | ppp | PPtP | Point to Point Tunnelling Protocol | pptp | PPPoE | PPP over Ethernet | pppoe | PPPoATM | PPP over ATM | pppoa | LTE/UMTS/GPRS/EV-DO | CDMA, UMTS or GPRS connection using an AT-style 3G modem. | 3g | PPP(PSTN-Modem) | PPP v90 modem | pppmodem |
| Web   | Description  | UCI      |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Static  | Static configuration with fixed address and netmask.   | static   |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| DHCP Client   | Address and netmask are assigned by DHCP.  | dhcp     |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Unmanaged   | Unspecified  | none     |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| IPv6-in-IPv4 (RFC4213)  | Used with tunnel brokers.  |          |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| IPv6-over-IPv4  | Stateless IPv6 over IPv4 transport.  |          |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| GRE   | Generic Routing Encapsulation protocol   | gre      |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| IOT   | IOT  | iot      |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| L2TP  | Layer 2 Tunnelling Protocol  | l2tp     |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| L2TPv3  | L2TPv3 Tunnelling Protocol   | l2tpv3   |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| PPP   | Point to Point Protocol  | ppp      |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| PPtP  | Point to Point Tunnelling Protocol   | pptp     |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| PPPoE   | PPP over Ethernet  | pppoe    |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| PPPoATM   | PPP over ATM   | pppoa    |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| LTE/UMTS/GPRS/EV-DO   | CDMA, UMTS or GPRS connection using an AT-style 3G modem.  | 3g       |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| PPP(PSTN-Modem)   | PPP v90 modem  | pppmodem |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Web: Create a bridge over multiple interfaces<br>UCI: network.<if name>.type<br>Opt: type | If you select this option, then the new logical interface created will act as a bridging interface between the chosen existing physical interfaces. <table border="1"> <tbody> <tr> <td>Empty</td> <td></td> </tr> <tr> <td>Bridge</td> <td>Configures a bridge over multiple interfaces.</td> </tr> </tbody> </table>   | Empty    |             | Bridge | Configures a bridge over multiple interfaces. |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Empty   |  |          |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Bridge  | Configures a bridge over multiple interfaces.  |          |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Web: Cover the following interface<br>UCI: network.<if name>.ifname<br>Opt: ifname        | Physical interface name to assign to this logical interface. If creating a bridge over multiple interfaces select two interfaces to bridge. When using UCI the interface names should be separated by a space e.g. option ifname 'eth2 eth3'   |          |             |        |   |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |

**Table 23: Information table for the create new interface page**

Click **Submit**. The Interface configuration page appears. There are three sections:

| Section              | Description  |
|----------------------|--|
| Common Configuration | Configure the interface settings such as protocol, IP address, gateway, netmask, custom DNS servers, MTU and firewall configuration. |
| IP-Aliases           | Assigning multiple IP addresses to the interface.  |
| DHCP Server          | Configuring DHCP server settings for this interface.   |

### 10.2.3 Interface overview: common configuration


The common configuration section has four sub-sections:

| Section           | Description   |
|-------------------|---|
| General Setup     | Configure the basic interface settings such as protocol, IP address, gateway, netmask, custom DNS servers.  |
| Advanced Settings | 'Bring up on boot', 'Monitor interface state', Override MAC address, Override MTU and 'Use gateway metric'. |
| Physical Settings | Bridge interfaces, VLAN PCP to SKB priority mapping.  |
| Firewall settings | Assign a firewall zone to the interface.  |

#### 10.2.3.1 Common configuration: general setup

### Common Configuration

General Setup
Advanced Settings
Physical Settings
Firewall Settings

Status  **MAC Address:** 00:E0:C8:D3:18:20

RX: 0.00 B (0 Pkts.)

TX: 0.00 B (0 Pkts.)


Protocol Static address ▼

IPv4 address

IPv4 netmask

IPv4 gateway

IPv4 broadcast

Use custom DNS servers  

Accept router advertisements

Send router solicitations

IPv6 address

IPv6 gateway

**Figure 48: The Ethernet connection common configuration settings page**

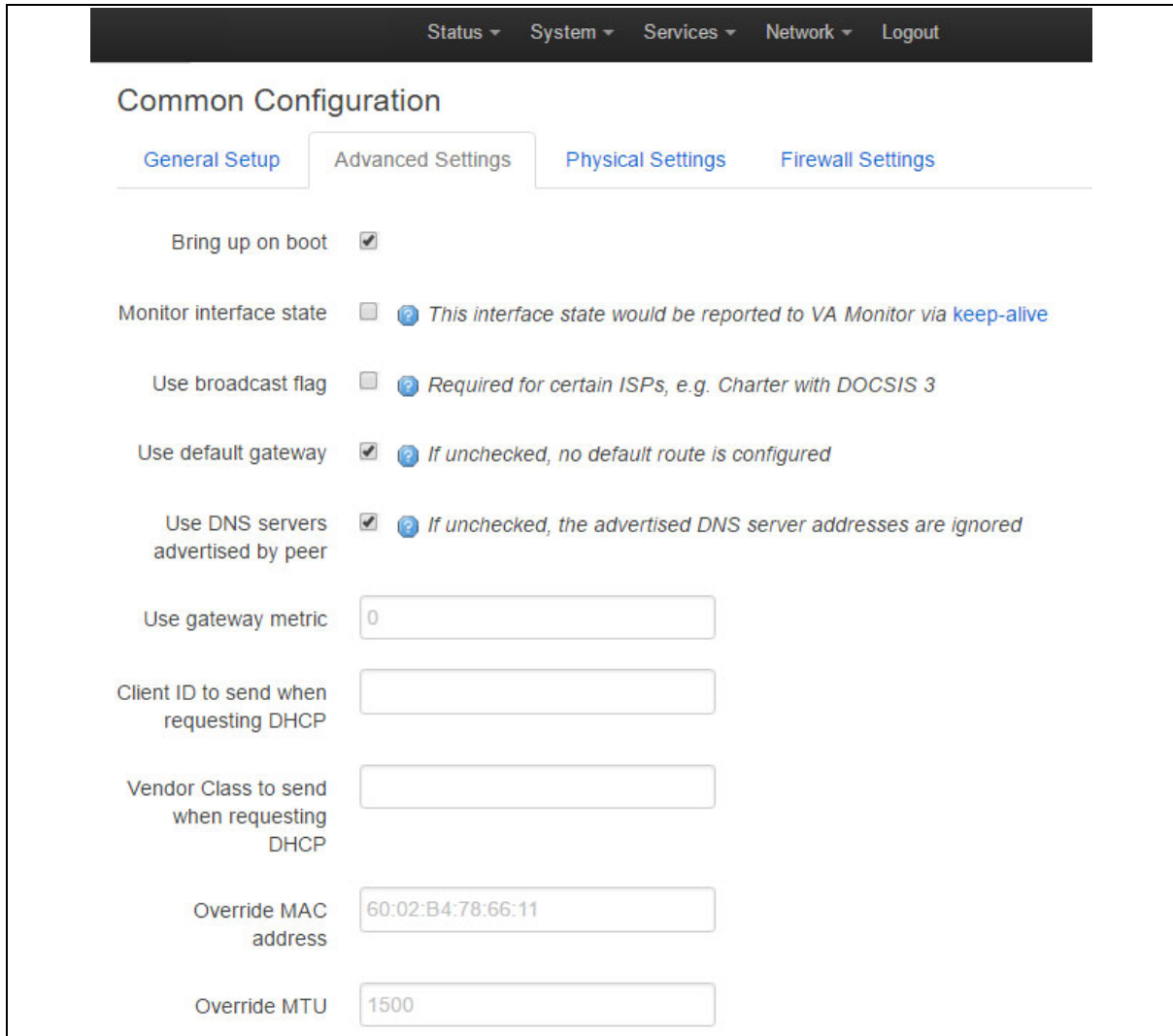


| Web Field/UCI/Package Option  | Description  |          |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
|---|--|----------|-------------|-----|--------|--|--------|-------------|---|------|-----------|--------------|------|------------------------|---------------------------|--|----------------|-------------------------------------|--|-----|---|-----|-----|-----|-----|------|-----------------------------|------|--------|----------------------------|--------|-----|-------------------------|-----|------|------------------------------------|------|-------|-------------------|-------|---------|--------------|-------|---------------------|---|----|-----------------|---------------|----------|
| Web: Status   | Shows the current status of the interface.   |          |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Web: Protocol<br>UCI: network.<if name>.proto<br>Opt: proto                             | <p>Protocol type. The interface protocol may be one of the options shown below. The protocol selected in the previous step will be displayed as default but can be changed if required.</p> <table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Static</td> <td>Static configuration with fixed address and netmask.</td> <td>static</td> </tr> <tr> <td>DHCP Client</td> <td>Address and netmask are assigned by DHCP.</td> <td>dhcp</td> </tr> <tr> <td>Unmanaged</td> <td>Unspecified.</td> <td>none</td> </tr> <tr> <td>IPv6-in-IPv4 (RFC4213)</td> <td>Used with tunnel brokers.</td> <td></td> </tr> <tr> <td>IPv6-over-IPv4</td> <td>Stateless IPv6 over IPv4 transport.</td> <td></td> </tr> <tr> <td>GRE</td> <td>Generic Routing Encapsulation protocol.</td> <td>gre</td> </tr> <tr> <td>IOT</td> <td>IOT</td> <td>iot</td> </tr> <tr> <td>L2TP</td> <td>Layer 2 Tunnelling Protocol</td> <td>l2tp</td> </tr> <tr> <td>L2TPv3</td> <td>L2TPv3 Tunnelling Protocol</td> <td>l2tpv3</td> </tr> <tr> <td>PPP</td> <td>Point to Point Protocol</td> <td>ppp</td> </tr> <tr> <td>PPTP</td> <td>Point to Point Tunnelling Protocol</td> <td>pptp</td> </tr> <tr> <td>PPPoE</td> <td>PPP over Ethernet</td> <td>pppoe</td> </tr> <tr> <td>PPPoATM</td> <td>PPP over ATM</td> <td>pppoa</td> </tr> <tr> <td>LTE/UMTS/GPRS/EV-DO</td> <td>CDMA, UMTS or GPRS connection using an AT-style 3G modem.</td> <td>3g</td> </tr> <tr> <td>PPP(PSTN-Modem)</td> <td>PPP v90 modem</td> <td>pppmodem</td> </tr> </tbody> </table> | Web      | Description | UCI | Static | Static configuration with fixed address and netmask. | static | DHCP Client | Address and netmask are assigned by DHCP. | dhcp | Unmanaged | Unspecified. | none | IPv6-in-IPv4 (RFC4213) | Used with tunnel brokers. |  | IPv6-over-IPv4 | Stateless IPv6 over IPv4 transport. |  | GRE | Generic Routing Encapsulation protocol. | gre | IOT | IOT | iot | L2TP | Layer 2 Tunnelling Protocol | l2tp | L2TPv3 | L2TPv3 Tunnelling Protocol | l2tpv3 | PPP | Point to Point Protocol | ppp | PPTP | Point to Point Tunnelling Protocol | pptp | PPPoE | PPP over Ethernet | pppoe | PPPoATM | PPP over ATM | pppoa | LTE/UMTS/GPRS/EV-DO | CDMA, UMTS or GPRS connection using an AT-style 3G modem. | 3g | PPP(PSTN-Modem) | PPP v90 modem | pppmodem |
| Web   | Description  | UCI      |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Static  | Static configuration with fixed address and netmask.   | static   |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| DHCP Client   | Address and netmask are assigned by DHCP.  | dhcp     |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Unmanaged   | Unspecified.   | none     |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| IPv6-in-IPv4 (RFC4213)  | Used with tunnel brokers.  |          |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| IPv6-over-IPv4  | Stateless IPv6 over IPv4 transport.  |          |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| GRE   | Generic Routing Encapsulation protocol.  | gre      |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| IOT   | IOT  | iot      |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| L2TP  | Layer 2 Tunnelling Protocol  | l2tp     |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| L2TPv3  | L2TPv3 Tunnelling Protocol   | l2tpv3   |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| PPP   | Point to Point Protocol  | ppp      |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| PPTP  | Point to Point Tunnelling Protocol   | pptp     |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| PPPoE   | PPP over Ethernet  | pppoe    |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| PPPoATM   | PPP over ATM   | pppoa    |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| LTE/UMTS/GPRS/EV-DO   | CDMA, UMTS or GPRS connection using an AT-style 3G modem.  | 3g       |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| PPP(PSTN-Modem)   | PPP v90 modem  | pppmodem |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Web: IPv4 address<br>UCI: network.<if name>.ipaddr<br>Opt: ipaddr                       | The IPv4 address of the interface. This is optional if an IPv6 address is provided.  |          |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Web: IPv4 netmask<br>UCI: network.<if name>.netmask<br>Opt: netmask                     | Subnet mask to be applied to the IP address of this interface.   |          |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Web: IPv4 gateway<br>UCI: network.<if name>.gateway<br>Opt: gateway                     | IPv4 default gateway to assign to this interface (optional).   |          |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Web: IPv4 broadcast<br>UCI: network.<if name>.broadcast<br>Opt: broadcast               | Broadcast address. This is automatically generated if no broadcast address is specified.   |          |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Web: Use custom DNS servers<br>UCI: network.<if name>.dns<br>Opt: list dns              | List of DNS server IP addresses (optional). Multiple DNS Servers are separated by a space if using UCI.  |          |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Web: Accept router advertisements<br>UCI: network.<if name>.accept_ra<br>Opt: accept_ra | Specifies whether to accept IPv6 Router Advertisements on this interface (optional).<br><b>Note:</b> default is <b>1</b> if protocol is set to DHCP, otherwise defaults to <b>0</b> .  |          |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Web: Send router solicitations<br>UCI: network.<if name>.send_rs<br>Opt: send_rs        | Specifies whether to send Router Solicitations on this interface (optional).<br><b>Note:</b> defaults to <b>1</b> for static protocol, otherwise defaults to <b>0</b> .  |          |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Web: IPv6 address<br>UCI: network.<if name>.ip6addr<br>Opt: ip6addr                     | The IPv6 IP address of the interface. Optional if an IPv4 address is provided.<br>CIDR notation for the IPv6 address is required.  |          |             |     |        |  |        |             |   |      |           |              |      |                        |                           |  |                |                                     |  |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |

|   |   |
|---|---|
| Web: IPv6 gateway<br>UCI: network.<if name>.ip6gw<br>Opt: ip6gw | Assign given IPv6 default gateway to this interface (optional). |
|---|---|

**Table 24: Information table for LAN interface common configuration settings**

**10.2.3.2 Common configuration: advanced settings**



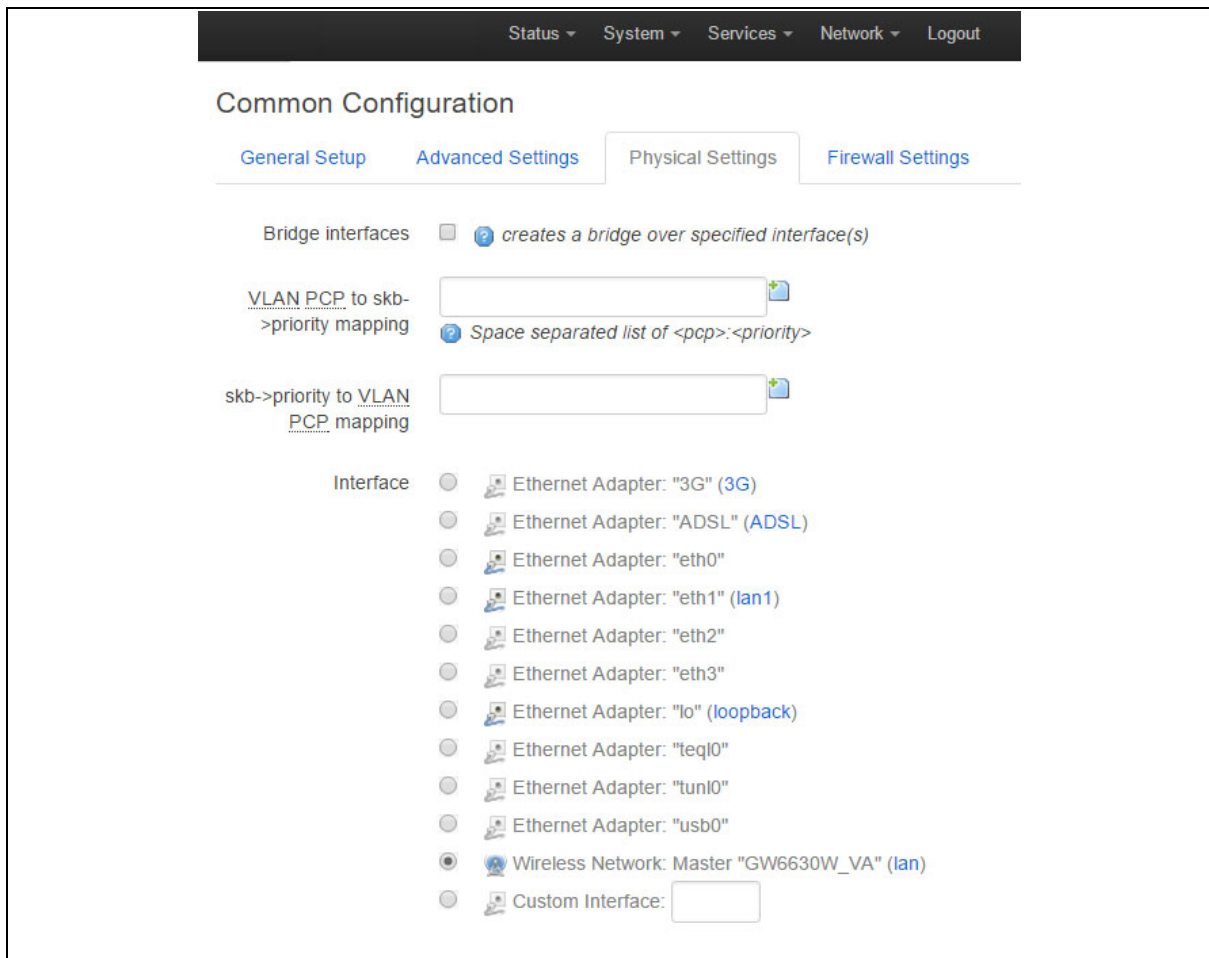
**Figure 49: The Ethernet connection advanced settings page**

| Web Field/UCI/Package Option   | Description   |      |            |   |          |
|--|---|------|------------|---|----------|
| Web: Bring up on boot<br>UCI: network.<if name>.auto<br>Opt: auto                  | Enables the interface to connect automatically on boot up.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>          | 0    | Disabled.  | 1 | Enabled. |
| 0  | Disabled.   |      |            |   |          |
| 1  | Enabled.  |      |            |   |          |
| Web: Monitor interface state<br>UCI: network.<if name>.monitored<br>Opt: monitored | Enabled if status of interface is presented on Monitoring platform.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0    | Disabled.  | 1 | Enabled. |
| 0  | Disabled.   |      |            |   |          |
| 1  | Enabled.  |      |            |   |          |
| Web: Override MAC address<br>UCI: network.<if name>.macaddr<br>Opt: macaddr        | Override the MAC address assigned to this interface. Must be in the form: hh:hh:hh:hh:hh:hh, where h is a hexadecimal number.   |      |            |   |          |
| Web: Override MTU<br>UCI: network.<if name>.mtu<br>Opt: mtu                        | Defines the value to override the default MTU on this interface.<br><table border="1"> <tr> <td>1500</td> <td>1500 bytes</td> </tr> </table>  | 1500 | 1500 bytes |   |          |
| 1500   | 1500 bytes  |      |            |   |          |

|   |   |       |                               |       |                   |     |                  |      |               |      |               |
|---|---|-------|-------------------------------|-------|-------------------|-----|------------------|------|---------------|------|---------------|
| <p>Web: Use gateway metric<br/>UCI: network.&lt;if name&gt;.metric<br/>Opt: metric</p>                | <p>Specifies the default route metric to use for this interface (optional).</p> <table border="1"> <tr> <td>0</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 0     |                               | Range |                   |     |                  |      |               |      |               |
| 0   |   |       |                               |       |                   |     |                  |      |               |      |               |
| Range   |   |       |                               |       |                   |     |                  |      |               |      |               |
| <p>Web: Dependant Interfaces<br/>UCI: network[..x..].dependants<br/>Opt: dependants</p>               | <p>Lists interfaces that are dependant on this parent interface. Dependant interfaces will go down when parent interface is down and will start or restart when parent interface starts. Separate multiple interfaces by a space when using UCI. Example: <code>option dependants 'PPPADSL MOBILE'</code><br/>This replaces the following previous options in child interfaces.</p> <table border="1"> <tr> <td>gre</td> <td>option local_interface</td> </tr> <tr> <td>lt2p</td> <td>option src_ipaddr</td> </tr> <tr> <td>iot</td> <td>option wan1 wan2</td> </tr> <tr> <td>6in4</td> <td>option ipaddr</td> </tr> <tr> <td>6to4</td> <td>option ipaddr</td> </tr> </table> | gre   | option local_interface        | lt2p  | option src_ipaddr | iot | option wan1 wan2 | 6in4 | option ipaddr | 6to4 | option ipaddr |
| gre   | option local_interface  |       |                               |       |                   |     |                  |      |               |      |               |
| lt2p  | option src_ipaddr   |       |                               |       |                   |     |                  |      |               |      |               |
| iot   | option wan1 wan2  |       |                               |       |                   |     |                  |      |               |      |               |
| 6in4  | option ipaddr   |       |                               |       |                   |     |                  |      |               |      |               |
| 6to4  | option ipaddr   |       |                               |       |                   |     |                  |      |               |      |               |
| <p>Web: SNMP Alias ifindex<br/>UCI: network[..x..].snmp_alias_ifindex<br/>Opt: snmp_alias_ifindex</p> | <p>Defines a static SNMP interface alias index for this interface, that can be polled via the SNMP interface index (<code>snmp_alias_ifindex+1000</code>). See 'Configuring SNMP' section for more information.</p> <table border="1"> <tr> <td>Blank</td> <td>No SNMP interface alias index</td> </tr> <tr> <td>Range</td> <td>0 - 4294966295</td> </tr> </table>  | Blank | No SNMP interface alias index | Range | 0 - 4294966295    |     |                  |      |               |      |               |
| Blank   | No SNMP interface alias index   |       |                               |       |                   |     |                  |      |               |      |               |
| Range   | 0 - 4294966295  |       |                               |       |                   |     |                  |      |               |      |               |

**Table 25: Information table for common configuration advanced settings**

### 10.2.3.3 Common configuration: physical settings



**Figure 50: The common configuration physical settings page**

| Web Field/UCI/Package Option   | Description   |       |           |        |   |
|--|---|-------|-----------|--------|---|
| Web: Bridge interfaces<br>UCI: network.<if name>.type<br>Opt: type   | Sets the interface to bridge over a specified interface(s). The physical interfaces can be selected from the list and are defined in network.<if name>.ifname.<br><table border="1"> <tr> <td>Empty</td> <td></td> </tr> <tr> <td>Bridge</td> <td>Configures a bridge over multiple interfaces.</td> </tr> </table> | Empty |           | Bridge | Configures a bridge over multiple interfaces. |
| Empty  |   |       |           |        |   |
| Bridge   | Configures a bridge over multiple interfaces.   |       |           |        |   |
| Web: Enable STP<br>UCI: network.<if name>.stp<br>Opt: stp  | Enable Spanning Tree Protocol. This option is only available when the Bridge Interfaces option is selected.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0     | Disabled. | 1      | Enabled.                                      |
| 0  | Disabled.   |       |           |        |   |
| 1  | Enabled.  |       |           |        |   |
| Web: VLAN PCP to skb>priority mapping<br>UCI: network.<if name>.vlan_qos_map_ingress<br>Opt: list vlan_qos_map_ingress | VLAN priority code point to socket buffer mapping. Multiple priority mappings are entered with a space between them when using UCI.<br>Example: network.<if name>. vlan_qos_map_ingress =1:2 2:1  |       |           |        |   |
| Web: skb priority to >VLAN PCP mapping<br>UCI: network.<if name>.vlan_qos_map_egress<br>Opt: list vlan_qos_map_egress  | Socket buffer to VLAN priority code point mapping. Multiple priority mappings are entered with a space between them when using UCI.<br>Example: network.<if name>. vlan_qos_map_egress =1:2 2:1   |       |           |        |   |
| Web: Interface<br>UCI: network.<if name>.ifname<br>Opt: ifname   | Physical interface to assign the logical interface to. If mapping multiple interfaces for bridging the interface names are separated by a space when using UCI and package options.<br>Example: option ifname 'eth2 eth3' or network.<if name>.ifname=eth2 eth 3  |       |           |        |   |

Table 26: Information table for physical settings page

#### 10.2.3.4 Loopback interfaces

Loopback interfaces are defined in exactly the same way as Ethernet interfaces. For more information, read the section above.

**Note:** there is no software limitation as to how many loopback interfaces can exist on the router.

#### 10.2.3.5 Common configuration: firewall settings

Use this section to select the firewall zone you want to assign to this interface.

Select **unspecified** to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

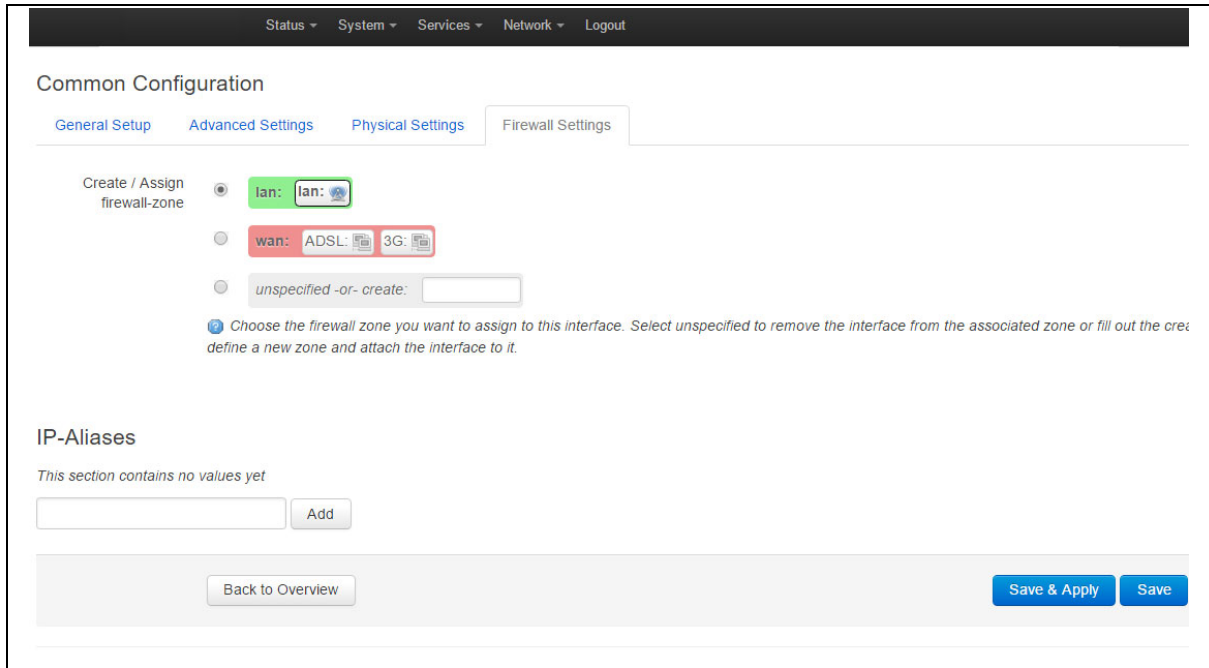


Figure 51: GRE firewall settings

## 10.2.4 Interface overview: IP-aliases

IP-aliasing means associating more than one IP address to a network interface. You can assign multiple aliases.

### 10.2.4.1 IP-alias packages

| Package | Sections |
|---------|----------|
| Network | alias    |

### 10.2.4.2 IP-alias using the web

To use IP-aliases, enter a name for the alias and click **Add**. This name will be assigned to the alias section for this IP-alias. In this example, we use the name 'ethalias1'.

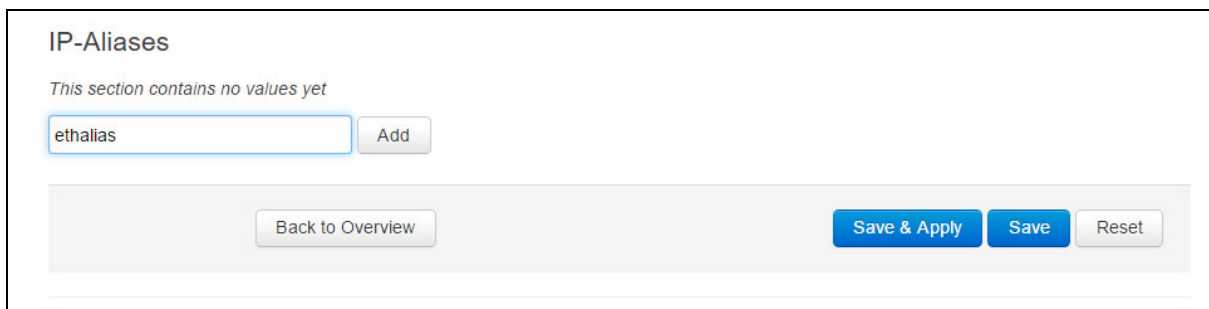


Figure 52: The IP-Aliases section

| Web Field/UCI/Package Option  | Description                                    |
|---|--|
| UCI: network.<alias name>=ifname<br>Opt: config interface `aliasname` | Assigns the alias name.                        |
| UCI: network.<alias name>.interface<br>Opt: interface                 | This maps the IP-Alias to the interface.       |
| UCI: network.<alias name>.proto<br>Opt: proto                         | This maps the interface protocol to the alias. |

**Table 27: Information table for IP-Aliases name assignment**

After you have clicked Add, the IP-Aliases configuration options page appears. The IP-Alias page is divided into two sub sections: general setup and advanced.

### 10.2.4.3 IP-aliases: general setup

**Figure 53: The IP-Aliases general setup section**

| Web Field/UCI/Package Option   | Description                              |
|--|--|
| Web: IPv4-Address<br>UCI: network.<alias name>.ipaddr<br>Opt: ipaddr   | Defines the IP address for the IP-alias. |
| Web: IPv4-Netmask<br>UCI: network.<alias name>.netmask<br>Opt: netmask | Defines the netmask for the IP-alias.    |
| Web: IPv4-Gateway<br>UCI: network.<alias name>.gateway<br>Opt: gateway | Defines the gateway for the IP-alias.    |

**Table 28: Information table for IP-Alias general setup page**

### 10.2.4.4 IP-aliases: advanced settings

Figure 54: The IP-Aliases advanced settings section

| Web Field/UCI/Package Option   | Description  |
|--|--|
| Web: IPv4-Broadcast<br>UCI: network.<alias name>.bcast<br>Opt: bcast | Defines the IP broadcast address for the IP-alias. |
| Web: DNS-Server<br>UCI: network.<alias name>.dns<br>Opt: dns         | Defines the DNS server for the IP-alias.           |

Table 29: Information table for IP-Alias advanced settings page

## 10.2.5 Interface overview: DHCP server

**Note:** this option is only available for interfaces with a static IP address.

### 10.2.5.1 DHCP server: packages

| Package | Sections |
|---------|----------|
| dhcp    | dhcp     |

To assign a DHCP Server to the interface, click **Setup DHCP Server**.

Figure 55: The DHCP Server settings section

The DHCP Server configuration options appear. The DHCP Server is divided into two sub-sections: General Setup and Advanced Settings.

### 10.2.5.2 DHCP server: general setup

#### DHCP Server

General Setup
Advanced Settings

Ignore interface  [Disable DHCP for this interface.](#)

Mode DHCPv4 [Mode of operation](#)

Start 100 [Lowest leased address as offset from the network address.](#)

Limit 150 [Maximum number of leased addresses.](#)

Leasetime 12h [Expiry time of leased addresses, minimum is 2 Minutes \(2m\).](#)

Figure 56: The DHCP server general setup section

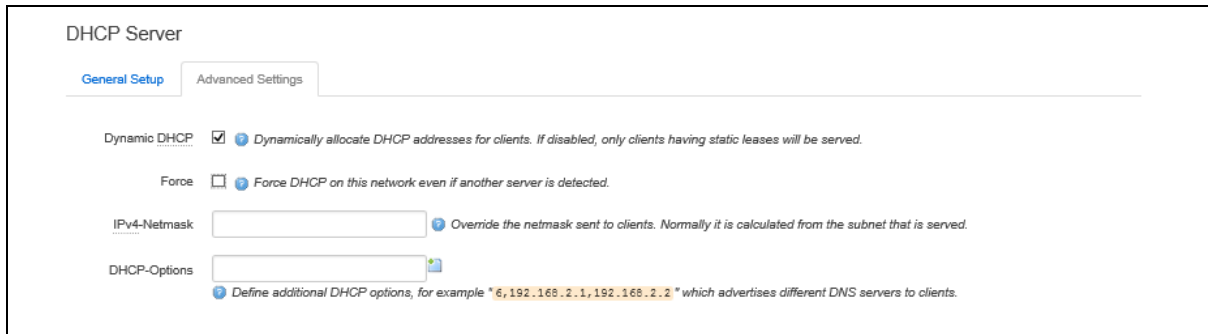
| Web Field/UCI/Package Option                                      | Description  |           |             |       |          |               |      |        |               |           |                            |         |         |                          |                          |         |
|---|--|-----------|-------------|-------|----------|---------------|------|--------|---------------|-----------|----------------------------|---------|---------|--------------------------|--------------------------|---------|
| Web: Ignore interface<br>UCI: dhcp.@dhcp[x].ignore<br>Opt: ignore | Defines whether the DHCP pool should be enabled for this interface. If not specified for the DHCP pool then default is disabled i.e. dhcp pool enabled. <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%; text-align: center;">0</td> <td>Disabled.</td> </tr> <tr> <td style="text-align: center;">1</td> <td>Enabled.</td> </tr> </table>   | 0         | Disabled.   | 1     | Enabled. |               |      |        |               |           |                            |         |         |                          |                          |         |
| 0   | Disabled.  |           |             |       |          |               |      |        |               |           |                            |         |         |                          |                          |         |
| 1   | Enabled.   |           |             |       |          |               |      |        |               |           |                            |         |         |                          |                          |         |
| Web: Mode<br>UCI: dhcp.@dhcp[x].mode<br>Opt: mode                 | Defines whether the DHCP pool should be enabled for this interface. If not specified for the DHCP pool then default is disabled i.e. dhcp pool enabled. <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>DHCPv4</td> <td>DHCP for IPv4</td> <td>ipv4</td> </tr> <tr> <td>DHCPv6</td> <td>DHCP for IPv6</td> <td>ipv6_dhcp</td> </tr> <tr> <td>IPv6 Router Advertisements</td> <td>IPv6 RA</td> <td>ipv6_ra</td> </tr> <tr> <td>DHCPv6 Prefix Delegation</td> <td>DHCPv6 prefix delegation</td> <td>ipv6_pd</td> </tr> </tbody> </table>  | Web       | Description | UCI   | DHCPv4   | DHCP for IPv4 | ipv4 | DHCPv6 | DHCP for IPv6 | ipv6_dhcp | IPv6 Router Advertisements | IPv6 RA | ipv6_ra | DHCPv6 Prefix Delegation | DHCPv6 prefix delegation | ipv6_pd |
| Web   | Description  | UCI       |             |       |          |               |      |        |               |           |                            |         |         |                          |                          |         |
| DHCPv4  | DHCP for IPv4  | ipv4      |             |       |          |               |      |        |               |           |                            |         |         |                          |                          |         |
| DHCPv6  | DHCP for IPv6  | ipv6_dhcp |             |       |          |               |      |        |               |           |                            |         |         |                          |                          |         |
| IPv6 Router Advertisements  | IPv6 RA  | ipv6_ra   |             |       |          |               |      |        |               |           |                            |         |         |                          |                          |         |
| DHCPv6 Prefix Delegation  | DHCPv6 prefix delegation   | ipv6_pd   |             |       |          |               |      |        |               |           |                            |         |         |                          |                          |         |
| Web: Start<br>UCI: dhcp.@dhcp[x].start<br>Opt: start              | Defines the offset from the network address for the start of the DHCP pool.<br>Example: for network address 192.168.100.10/24, start=100, DHCP allocation pool will start at 192.168.100.100.<br>For subnets greater than /24, it may be greater than 255 to span subnets. Alternatively, specify in IP address notation using the wildcard '0' where the octet is required to inherit bits from the interface IP address.<br>Example: to define a DHCP scope starting from 10.1.20.0 on an interface with 10.1.0.0/16 address, set start to 0.0.20.1100 <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <tr> <td style="width: 10%; text-align: center;">100</td> <td></td> </tr> <tr> <td style="text-align: center;">Range</td> <td></td> </tr> </table> | 100       |             | Range |          |               |      |        |               |           |                            |         |         |                          |                          |         |
| 100   |  |           |             |       |          |               |      |        |               |           |                            |         |         |                          |                          |         |
| Range   |  |           |             |       |          |               |      |        |               |           |                            |         |         |                          |                          |         |
| Web: Limit<br>UCI: dhcp.@dhcp[x].limit<br>Opt: limit              | Defines the size of the address pool.<br>Example: for network address 192.168.100.10/24, start=100, limit=150, DHCP allocation pool will be .100 to .249 <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <tr> <td style="width: 10%; text-align: center;">150</td> <td></td> </tr> <tr> <td style="text-align: center;">Range</td> <td>0 - 255</td> </tr> </table>  | 150       |             | Range | 0 - 255  |               |      |        |               |           |                            |         |         |                          |                          |         |
| 150   |  |           |             |       |          |               |      |        |               |           |                            |         |         |                          |                          |         |
| Range   | 0 - 255  |           |             |       |          |               |      |        |               |           |                            |         |         |                          |                          |         |
| Web: Leasetime<br>UCI: dhcp.@dhcp[x].leasetime<br>Opt: leasetime  | Defines the lease time of addresses handed out to clients, for example 12h or 30m. <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <tr> <td style="width: 10%; text-align: center;">12h</td> <td>12 hours</td> </tr> <tr> <td style="text-align: center;">Range</td> <td></td> </tr> </table>   | 12h       | 12 hours    | Range |          |               |      |        |               |           |                            |         |         |                          |                          |         |
| 12h   | 12 hours   |           |             |       |          |               |      |        |               |           |                            |         |         |                          |                          |         |
| Range   |  |           |             |       |          |               |      |        |               |           |                            |         |         |                          |                          |         |



|  |   |     |  |       |  |
|--|---|-----|--|-------|--|
| Web: n/a<br>UCI: dhcp.@dhcp[x].interface<br>Opt: interface | Defines the interface that is served by this DHCP pool. This must be one of the configured interfaces.<br>When configured through the web UI this will be automatically populated with the interface name |     |  |       |  |
|  | <table border="1"> <tr> <td>lan</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | lan |  | Range |  |
| lan  |   |     |  |       |  |
| Range  |   |     |  |       |  |

**Table 30: Information table for DHCP server general setup page**

### 10.2.5.3 DHCP server: advanced settings



**Figure 57: The DHCP server advanced settings section**

| Web Field/UCI/Package Option   | Description   |   |                                    |        |   |
|--|---|---|------------------------------------|--------|---|
| Web: Dynamic DHCP<br>UCI: dhcp.@dhcp[x].dynamicdhcp<br>Opt: dynamicdhcp      | Defines whether to dynamically allocate DHCP leases. <table border="1"> <tr> <td>1</td> <td>Dynamically allocate leases.</td> </tr> <tr> <td>0</td> <td>Use /etc/ethers file for serving DHCP leases.</td> </tr> </table>   | 1 | Dynamically allocate leases.       | 0      | Use /etc/ethers file for serving DHCP leases. |
| 1  | Dynamically allocate leases.  |   |                                    |        |   |
| 0  | Use /etc/ethers file for serving DHCP leases.   |   |                                    |        |   |
| Web: Force<br>UCI: dhcp.@dhcp[x].force<br>Opt: force                         | Forces DHCP serving on the specified interface even if another DHCP server is detected on the same network segment. <table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0 | Disabled.                          | 1      | Enabled.                                      |
| 0  | Disabled.   |   |                                    |        |   |
| 1  | Enabled.  |   |                                    |        |   |
| Web: IPv4-Netmask<br>UCI: dhcp.@dhcp[x].netmask<br>Opt: netmask              | Defines a netmask sent to clients that overrides the netmask as calculated from the interface subnet. <table border="1"> <tr> <td></td> <td>Use netmask from interface subnet.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  |   | Use netmask from interface subnet. | Range  |   |
|  | Use netmask from interface subnet.  |   |                                    |        |   |
| Range  |   |   |                                    |        |   |
| Web: DHCP-Options<br>UCI: dhcp.@dhcp[x].dhcp_option<br>Opt: list dhcp_option | Defines additional options to be added for this dhcp pool.<br>For example with 'list dhcp_option 26,1470' or 'list dhcp_option mtu, 1470' you can assign a specific MTU per DHCP pool. Your client must accept the MTU option for this to work. Options that contain multiple values should be separated by a comma.<br>Example: list dhcp_option 6,192.168.2.1,192.168.2.2 <table border="1"> <tr> <td></td> <td>No options defined.</td> </tr> <tr> <td>Syntax</td> <td>Option_number, option_value</td> </tr> </table> |   | No options defined.                | Syntax | Option_number, option_value                   |
|  | No options defined.   |   |                                    |        |   |
| Syntax   | Option_number, option_value   |   |                                    |        |   |
| Web: n/a<br>UCI: dhcp.@dhcp[x].networkid<br>Opt: networkid                   | Assigns a network-id to all clients that obtain an IP address from this pool. <table border="1"> <tr> <td></td> <td>Use network from interface subnet.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  |   | Use network from interface subnet. | Range  |   |
|  | Use network from interface subnet.  |   |                                    |        |   |
| Range  |   |   |                                    |        |   |

**Table 31: Information table for DHCP advanced settings page**

For more advanced configuration on the DHCP server, read 'DHCP server and DNS configuration section.

## 10.3 Interface configuration using command line

The configuration files are stored at **/etc/config/network**, **/etc/config/firewall** and **/etc/config/dhcp**.

### 10.3.1 Interface configuration using UCI

```
root@VA_router:~# uci show network
...
network.newinterface=interface
network.newinterface.proto=static
network.newinterface.ifname=eth0
network.newinterface.monitored=0
network.newinterface.ipaddr=2.2.2.2
network.newinterface.netmask=255.255.255.0
network.newinterface.gateway=2.2.2.10
network.newinterface.broadcast=2.2.2.255
network.newinterface.vlan_qos_map_ingress=1:2 2:1
network.ethalias1=alias
network.ethalias1.proto=static
network.ethalias1.interface=newinterface
network.ethalias1.ipaddr=10.10.10.1
network.ethalias1.netmask=255.255.255.0
network.ethalias1.gateway=10.10.10.10
network.ethalias1.bcast=10.10.10.255
network.ethalias1.dns=8.8.8.8

root@VA_router:~# uci show firewall
...
firewall.@zone[0]=zone
firewall.@zone[0].name=lan
firewall.@zone[0].input=ACCEPT
firewall.@zone[0].output=ACCEPT
firewall.@zone[0].forward=ACCEPT
firewall.@zone[0].network=lan newinterface

root@VA_router:~# uci show dhcp
...
```

```
dhcp.@dhcp[0]=dhcp
dhcp.@dhcp[0].interface=newinterface
dhcp.@dhcp[0].mode=ipv4
dhcp.@dhcp[0].start=100
dhcp.@dhcp[0].limit=150
dhcp.@dhcp[0].leasetime=12h
```

To change any of the above values use `uci set` command.

### 10.3.2 Interface configuration using package options

```
root@VA_router:~# uci export network
package network
.....
config interface 'newinterface'
    option proto 'static'
    option ifname 'eth0'
    option monitored '0'
    option ipaddr '2.2.2.2'
    option netmask '255.255.255.0'
    option gateway '2.2.2.10'
    option broadcast '2.2.2.255'
    list vlan_qos_map_ingress '1:2'
    list vlan_qos_map_ingress '2:1'

config alias 'ethalias1'
    option proto 'static'
    option interface 'newinterface'
    option ipaddr '10.10.10.1'
    option netmask '255.255.255.0'
    option gateway '10.10.10.10'
    option bcast '10.10.10.255'
    option dns '8.8.8.8'

root@VA_router:~# uci export firewall
package firewall
config zone
    option name 'lan'
```

```

option input 'ACCEPT'
option output 'ACCEPT'
option forward 'ACCEPT'
option network 'lan newinterface'

root@VA_router:~# uci export dhcp
package dhcp
.....
config dhcp
    option interface 'newinterface'
    option mode 'ipv4'
    option start '100'
    option leasetime '12h'
    option limit '150'

```

To change any of the above values use `uci set` command.

### 10.3.3 Loopback interfaces

Loopback interfaces are defined in exactly the same way as Ethernet interfaces. Read the section above.

**Note:** there is no software limitation as to how many loopback interfaces can exist on the router.

An example showing a partial uci export of a loopback interface configuration is shown below.

```

root@VA_router:~# uci export network
.....
config interface 'loopback'
    option proto 'static'
    option ifname 'lo'
    option ipaddr '127.0.0.1'
    option netmask '255.0.0.0'

```

**Note:** we highly recommend you **do not** un-assign the 127.0.0.1 IP address from the loopback interface as this action will cause issues with the syslog mechanism and all internal logs will be routed outside the router.

If you must assign an alternative IP address to a loopback interface then you should create the alias of the loopback interface as shown below.

```

Config alias 'loopback_alt'
option interface 'loopback'

```

```
option proto 'static'
option ipaddr '10.1.1.10'
option netmask '255.255.255.0'
```

## 10.4 Configuring port maps

## 10.5 Port map packages

| Package | Sections  |
|---------|-----------|
| Network | va_switch |

### 10.5.1 Configuring port map using the web interface

The new logical Ethernet interface needs to be mapped to a physical switch port. To configure the Ethernet switch physical port to logical interface mappings, go to the Port Map section at **Network -> Interfaces**.

**Port Map**  
Map device ports to ethernet interfaces. Ports are marked with capital letters starting with 'A'. Type in space separated port numbers to fields below

eth0

eth1

eth2

eth3

**Figure 58: The Interface port map section**

| Web Field/UCI/Package Option                              | Description  |   |                                |   |                                |   |                                |   |                                |
|---|--|---|--------------------------------|---|--------------------------------|---|--------------------------------|---|--------------------------------|
| Web: eth0<br>UCI: network.@va_switch[0].eth0<br>Opt: eth0 | Defines eth0 physical switch port mapping. Must be entered in upper case.<br><table border="1"> <tr> <td>A</td> <td>Eth0 assigned to switch port A</td> </tr> <tr> <td>B</td> <td>Eth0 assigned to switch port B</td> </tr> <tr> <td>C</td> <td>Eth0 assigned to switch port C</td> </tr> <tr> <td>D</td> <td>Eth0 assigned to switch port C</td> </tr> </table> | A | Eth0 assigned to switch port A | B | Eth0 assigned to switch port B | C | Eth0 assigned to switch port C | D | Eth0 assigned to switch port C |
| A   | Eth0 assigned to switch port A   |   |                                |   |                                |   |                                |   |                                |
| B   | Eth0 assigned to switch port B   |   |                                |   |                                |   |                                |   |                                |
| C   | Eth0 assigned to switch port C   |   |                                |   |                                |   |                                |   |                                |
| D   | Eth0 assigned to switch port C   |   |                                |   |                                |   |                                |   |                                |
| Web: eth1<br>UCI: network.@va_switch[0].eth1<br>Opt: eth1 | Defines eth1 physical switch port mapping. Must be entered in upper case.<br><table border="1"> <tr> <td>A</td> <td>Eth1 assigned to switch port A</td> </tr> <tr> <td>B</td> <td>Eth1 assigned to switch port B</td> </tr> <tr> <td>C</td> <td>Eth1 assigned to switch port C</td> </tr> <tr> <td>D</td> <td>Eth1 assigned to switch port C</td> </tr> </table> | A | Eth1 assigned to switch port A | B | Eth1 assigned to switch port B | C | Eth1 assigned to switch port C | D | Eth1 assigned to switch port C |
| A   | Eth1 assigned to switch port A   |   |                                |   |                                |   |                                |   |                                |
| B   | Eth1 assigned to switch port B   |   |                                |   |                                |   |                                |   |                                |
| C   | Eth1 assigned to switch port C   |   |                                |   |                                |   |                                |   |                                |
| D   | Eth1 assigned to switch port C   |   |                                |   |                                |   |                                |   |                                |
| Web: eth2<br>UCI: network.@va_switch[0].eth2<br>Opt: eth2 | Defines eth0 physical switch port mapping. Must be entered in upper case.<br><table border="1"> <tr> <td>A</td> <td>Eth2 assigned to switch port A</td> </tr> <tr> <td>B</td> <td>Eth2 assigned to switch port B</td> </tr> <tr> <td>C</td> <td>Eth2 assigned to switch port C</td> </tr> <tr> <td>D</td> <td>Eth2 assigned to switch port C</td> </tr> </table> | A | Eth2 assigned to switch port A | B | Eth2 assigned to switch port B | C | Eth2 assigned to switch port C | D | Eth2 assigned to switch port C |
| A   | Eth2 assigned to switch port A   |   |                                |   |                                |   |                                |   |                                |
| B   | Eth2 assigned to switch port B   |   |                                |   |                                |   |                                |   |                                |
| C   | Eth2 assigned to switch port C   |   |                                |   |                                |   |                                |   |                                |
| D   | Eth2 assigned to switch port C   |   |                                |   |                                |   |                                |   |                                |
| Web: eth3<br>UCI: network.@va_switch[0].eth3<br>Opt: eth3 | Defines eth0 physical switch port mapping. Must be entered in upper case.<br><table border="1"> <tr> <td>A</td> <td>Eth3 assigned to switch port A</td> </tr> <tr> <td>B</td> <td>Eth3 assigned to switch port B</td> </tr> <tr> <td>C</td> <td>Eth3 assigned to switch port C</td> </tr> <tr> <td>D</td> <td>Eth3 assigned to switch port C</td> </tr> </table> | A | Eth3 assigned to switch port A | B | Eth3 assigned to switch port B | C | Eth3 assigned to switch port C | D | Eth3 assigned to switch port C |
| A   | Eth3 assigned to switch port A   |   |                                |   |                                |   |                                |   |                                |
| B   | Eth3 assigned to switch port B   |   |                                |   |                                |   |                                |   |                                |
| C   | Eth3 assigned to switch port C   |   |                                |   |                                |   |                                |   |                                |
| D   | Eth3 assigned to switch port C   |   |                                |   |                                |   |                                |   |                                |

Table 32: Information table for interface port map page

## 10.5.2 Configuring port maps using UCI

The configuration files are stored on **/etc/config/network**

```
root@VA_router:~# uci show network
.....
network.@va_switch[0]=va_switch
network.@va_switch[0].eth0=A
network.@va_switch[0].eth1=B
network.@va_switch[0].eth2=C
network.@va_switch[0].eth3=D
```

To change any of the above values use `uci set` command.

## 10.5.3 Configuring port map using package options

The configuration files are stored on **/etc/config/network**

```
root@VA_router:~# uci export network
....
config va_switch
    option eth0 'A'
```

```
option eth1 'B'
option eth2 'C'
option eth3 'D'
```

To change any of the above values use `uci set` command.

## 10.5.4 ATM bridges

The ATM bridges section is not used when configuring an Ethernet interface.

## 10.6 Interface diagnostics

### 10.6.1 Interfaces status

To show the current running interfaces, enter:

```
root@VA_router:~# ifconfig
3g-CDMA  Link encap:Point-to-Point Protocol
        inet addr:10.33.152.100  P-t-P:178.72.0.237  Mask:255.255.255.255
        UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1400  Metric:1
        RX packets:6 errors:0 dropped:0 overruns:0 frame:0
        TX packets:23 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:3
        RX bytes:428 (428.0 B)  TX bytes:2986 (2.9 KiB)

eth0     Link encap:Ethernet  HWaddr 00:E0:C8:12:12:15
        inet addr:192.168.100.1  Bcast:192.168.100.255
Mask:255.255.255.0
        inet6 addr: fe80::2e0:c8ff:fe12:1215/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:6645 errors:0 dropped:0 overruns:0 frame:0
        TX packets:523 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:569453 (556.1 KiB)  TX bytes:77306 (75.4 KiB)

lo       Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:385585 errors:0 dropped:0 overruns:0 frame:0
        TX packets:385585 errors:0 dropped:0 overruns:0 carrier:0
```

```
collisions:0 txqueuelen:0
RX bytes:43205140 (41.2 MiB) TX bytes:43205140 (41.2 MiB)
```

To display a specific interface, enter:

```
root@VA_router:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:E0:C8:12:12:15
          inet addr:192.168.100.1  Bcast:192.168.100.255
Mask:255.255.255.0
          inet6 addr: fe80::2e0:c8ff:fe12:1215/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7710 errors:0 dropped:0 overruns:0 frame:0
          TX packets:535 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:647933 (632.7 KiB)  TX bytes:80978 (79.0 KiB)
```

## 10.6.2 ARP table status

To show the current ARP table of the router, enter:

```
root@GW7314:~# arp
? (10.67.253.141) at 30:30:41:30:43:36 [ether] on eth8
? (10.47.48.1) at 0a:44:b2:06 [ether] on gre-gre1
```

## 10.6.3 Route status

To show the current routing status, enter:

```
root@VA_router:~# route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
192.168.100.0    *                255.255.255.0   U        0      0      0 eth0
```

**Note:** a route will only be displayed in the routing table when the interface is up.



# 11 Configuring VLAN

## 11.1 Maximum number of VLANs supported

Virtual Access' routers support up to 4095 VLANs.

## 11.2 Configuration package used

| Package | Sections |
|---------|----------|
| Network |          |

## 11.3 Configuring VLAN using the web interface

### 11.3.1 Create a VLAN interface

To configure VLAN using the web interface, in the top menu, select **Network -> Interfaces**.

Click **Add** new interface. The Create Interface page appears.

**Figure 59: The create interface page**

| Web Field/UCI/Package Option  | Description   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
|---|---|--------|-------------|--------|--|-------------|---|-----------|-------------|------------------------|---------------------------|----------------|-------------------------------------|-----|--|-----|--|------|-----------------------------|-----|-------------------------|-------|-------------------|---------|--------------|---------------------|---|
| Web: Name of the new interface<br>UCI: network.vlan1=interface<br>Opt: interface      | Type the name of the new interface. For example, VLAN1.   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| Web: Protocol of the new interface<br>UCI: network.vlan_test.proto<br>Opt: proto      | <p>Protocol type. Select <b>Static</b>.</p> <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Static</td> <td>Static configuration with fixed address and netmask.</td> </tr> <tr> <td>DHCP Client</td> <td>Address and netmask are assigned by DHCP.</td> </tr> <tr> <td>Unmanaged</td> <td>Unspecified</td> </tr> <tr> <td>IPv6-in-IPv4 (RFC4213)</td> <td>Used with tunnel brokers.</td> </tr> <tr> <td>IPv6-over-IPv4</td> <td>Stateless IPv6 over IPv4 transport.</td> </tr> <tr> <td>GRE</td> <td>Generic Routing Encapsulation protocol</td> </tr> <tr> <td>IOT</td> <td></td> </tr> <tr> <td>L2TP</td> <td>Layer 2 Tunnelling Protocol</td> </tr> <tr> <td>PPP</td> <td>Point to Point Protocol</td> </tr> <tr> <td>PPPoE</td> <td>PPP over Ethernet</td> </tr> <tr> <td>PPPoATM</td> <td>PPP over ATM</td> </tr> <tr> <td>LTE/UMTS/GPRS/EV-DO</td> <td>CDMA, UMTS or GPRS connection using an AT-style 3G modem.</td> </tr> </tbody> </table> | Option | Description | Static | Static configuration with fixed address and netmask. | DHCP Client | Address and netmask are assigned by DHCP. | Unmanaged | Unspecified | IPv6-in-IPv4 (RFC4213) | Used with tunnel brokers. | IPv6-over-IPv4 | Stateless IPv6 over IPv4 transport. | GRE | Generic Routing Encapsulation protocol | IOT |  | L2TP | Layer 2 Tunnelling Protocol | PPP | Point to Point Protocol | PPPoE | PPP over Ethernet | PPPoATM | PPP over ATM | LTE/UMTS/GPRS/EV-DO | CDMA, UMTS or GPRS connection using an AT-style 3G modem. |
| Option  | Description   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| Static  | Static configuration with fixed address and netmask.  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| DHCP Client   | Address and netmask are assigned by DHCP.   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| Unmanaged   | Unspecified   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| IPv6-in-IPv4 (RFC4213)  | Used with tunnel brokers.   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| IPv6-over-IPv4  | Stateless IPv6 over IPv4 transport.   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| GRE   | Generic Routing Encapsulation protocol  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| IOT   |   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| L2TP  | Layer 2 Tunnelling Protocol   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| PPP   | Point to Point Protocol   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| PPPoE   | PPP over Ethernet   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| PPPoATM   | PPP over ATM  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| LTE/UMTS/GPRS/EV-DO   | CDMA, UMTS or GPRS connection using an AT-style 3G modem.   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| Web: Create a bridge over multiple interfaces<br>UCI: network.vlan1.type<br>Opt: type | Create a bridge over multiple interfaces.   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| Web: Cover the following interface<br>UCI: network.vlan1.ifname<br>Opt: ifname        | <p>Check the <b>Custom Interface</b> radio button.</p> <p>Enter a name, for example eth0.100. This will assign VLAN 100 to the eth0 interface.</p>  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |

**Table 33: Information table for the create interface page**

Click **Submit**. The Interfaces page for VLAN1 appears.

## 11.3.2 General setup: VLAN

The screenshot displays the configuration page for the VLAN 1 interface. At the top, there are navigation tabs for WAN, VLAN1 (selected), VLAN2, and LAN. Below this, the 'Interfaces - VLAN1' title is followed by a brief instruction on configuring network interfaces. The 'Common Configuration' section is active, with sub-tabs for General Setup, Advanced Settings, Physical Settings, and Firewall Settings. In the 'General Setup' tab, the 'Protocol' is set to 'Static address'. The 'IPv4 address' field contains '172.16.100.1' and the 'IPv4 netmask' is '255.255.255.0'. Other fields for gateway, broadcast, and custom DNS servers are currently empty. A status block for 'eth0.1' provides system information: Uptime: 0h 4m 41s, MAC Address: 00 E0:C8:10:10:50, RX: 0.00 B (0 Pkts.), TX: 252.00 B (6 Pkts.), and IPv4: 172.16.100.1/24.

Figure 60: The VLAN 1 interface page

| Web Field/UCI/Package Option                                    | Description  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
|---|--|--------|-------------|--------|--|-------------|---|-----------|-------------|------------------------|---------------------------|----------------|-------------------------------------|-----|--|-----|--|------|-----------------------------|-----|-------------------------|-------|-------------------|---------|--------------|---------------------|---|
| Web: Protocol<br>UCI: network.VLAN1.proto<br>Opt: proto         | Protocol type. <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Static</td> <td>Static configuration with fixed address and netmask.</td> </tr> <tr> <td>DHCP Client</td> <td>Address and netmask are assigned by DHCP.</td> </tr> <tr> <td>Unmanaged</td> <td>Unspecified</td> </tr> <tr> <td>IPv6-in-IPv4 (RFC4213)</td> <td>Used with tunnel brokers.</td> </tr> <tr> <td>IPv6-over-IPv4</td> <td>Stateless IPv6 over IPv4 transport.</td> </tr> <tr> <td>GRE</td> <td>Generic Routing Encapsulation protocol</td> </tr> <tr> <td>IOT</td> <td></td> </tr> <tr> <td>L2TP</td> <td>Layer 2 Tunnelling Protocol</td> </tr> <tr> <td>PPP</td> <td>Point to Point Protocol</td> </tr> <tr> <td>PPPoE</td> <td>PPP over Ethernet</td> </tr> <tr> <td>PPPoATM</td> <td>PPP over ATM</td> </tr> <tr> <td>LTE/UMTS/GPRS/EV-DO</td> <td>CDMA, UMTS or GPRS connection using an AT-style 3G modem.</td> </tr> </tbody> </table> | Option | Description | Static | Static configuration with fixed address and netmask. | DHCP Client | Address and netmask are assigned by DHCP. | Unmanaged | Unspecified | IPv6-in-IPv4 (RFC4213) | Used with tunnel brokers. | IPv6-over-IPv4 | Stateless IPv6 over IPv4 transport. | GRE | Generic Routing Encapsulation protocol | IOT |  | L2TP | Layer 2 Tunnelling Protocol | PPP | Point to Point Protocol | PPPoE | PPP over Ethernet | PPPoATM | PPP over ATM | LTE/UMTS/GPRS/EV-DO | CDMA, UMTS or GPRS connection using an AT-style 3G modem. |
| Option  | Description  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| Static  | Static configuration with fixed address and netmask.   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| DHCP Client   | Address and netmask are assigned by DHCP.  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| Unmanaged   | Unspecified  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| IPv6-in-IPv4 (RFC4213)  | Used with tunnel brokers.  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| IPv6-over-IPv4  | Stateless IPv6 over IPv4 transport.  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| GRE   | Generic Routing Encapsulation protocol   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| IOT   |  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| L2TP  | Layer 2 Tunnelling Protocol  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| PPP   | Point to Point Protocol  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| PPPoE   | PPP over Ethernet  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| PPPoATM   | PPP over ATM   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| LTE/UMTS/GPRS/EV-DO   | CDMA, UMTS or GPRS connection using an AT-style 3G modem.  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| Web: IPv4 address<br>UCI: network.VLAN1.ipaddr<br>Opt: ipaddr   | The IPv4 address of the interface. This is optional if an IPv6 address is provided.  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| Web: IPv4 netmask<br>UCI: network.VLAN1.netmask<br>Opt: netmask | Subnet mask to be applied to the IP address of this interface.   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |

|   |  |
|---|--|
| Web: IPv4 gateway<br>UCI: network.VLAN1.gateway<br>Opt: gateway   | IPv4 default gateway to assign to this interface (optional). |
| Web: Use custom DNS servers<br>UCI: network.VLAN1.dns<br>Opt: dns | List of DNS server IP addresses (optional).                  |

Table 34: Information table for VLAN general settings

### 11.3.3 Firewall settings: VLAN

Use this section to select the firewall zone you want to assign to the VLAN interface.

Select **unspecified** to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

Figure 61: Firewall settings page

When you have added all the VLAN interfaces you require, click **Save & Apply**.

## 11.4 Viewing VLAN interface settings

To view the new VLAN interface settings, in the top menu, select **Network -> Interfaces**. The Interfaces Overview page appears.

The example below shows two VLAN interfaces configured.

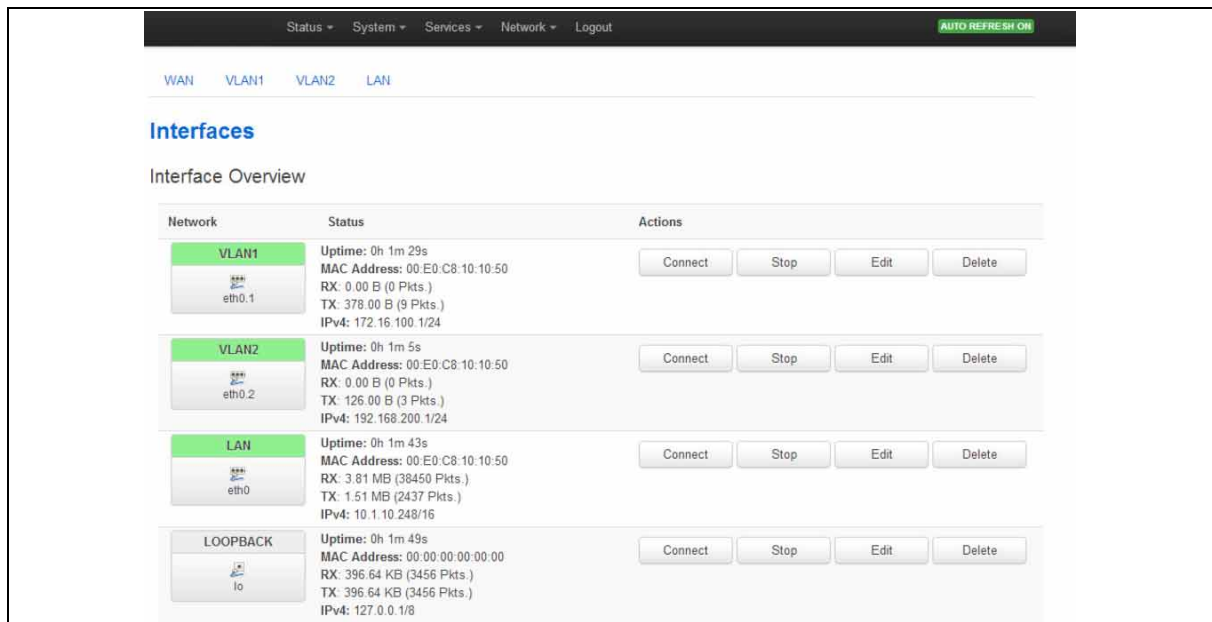


Figure 62: The interface overview page showing two VLAN interfaces

## 11.5 Configuring VLAN using the UCI interface

You can configure VLANs through CLI. The VLAN configuration file is stored on: **/etc/config/network**

```
# uci export network
package network
config interface 'vlan100'
    option proto 'static'
    option ifname 'eth0.100'
    option monitored '0'
    option ipaddr '192.168.100.1'
    option netmask '255.255.255.0'
    option gateway '192.168.100.10'
    option broadcast '192.168.100.255'
    option dns '8.8.8.8'
```

Modify these settings by running `uci set <parameter> command`.

When specifying the ifname ensure that it is written in dotted mode, that is, eth1.100 where eth1 is the physical interface assigned to VLAN tag 100.

**Note:** VLAN1 is, by default, the native VLAN and will not be tagged.

## 12 Configuring Power over Ethernet

Power over Ethernet (PoE) is available on supported hardware models. Current hardware models supporting PoE are GW2300 Series routers.

### 12.1 PoE overview

There is a total power limit of 120W, with each port supplying up to 30W at between 52V and 57V DC. Each port supports 802.3 at Type 2 (PoE+) and device classes 0 – 4 are supported by default.

You can configure individual Ethernet ports to deliver or not deliver power.

### 12.2 Configuration package used

| Package | Sections   |
|---------|--|
| vapoe   | config port A<br>config port B<br>config port C<br>config port D |

### 12.3 Configuring PoE

#### 12.3.1 Configuring PoE using the web UI

To configure PoE, select **Services -> PoE**. Select to enable or disable an individual port

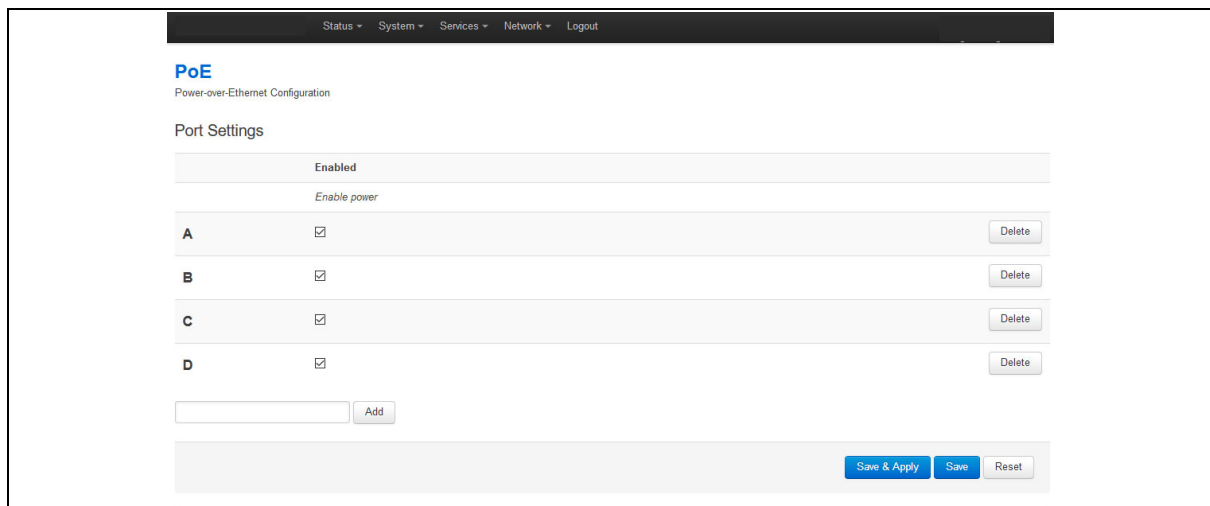


Figure 63: The network interface page

| Web Field/UCI/Package Option                               | Description   |   |                    |   |                     |
|--|---|---|--------------------|---|---------------------|
| Web: Enable power A<br>UCI: vapoe.A.enabled<br>Opt:enabled | Defines whether to enable PoE power on Ethernet port A.<br><table border="1"> <tr> <td>1</td> <td>Enables PoE power.</td> </tr> <tr> <td>0</td> <td>Disables PoE power.</td> </tr> </table> | 1 | Enables PoE power. | 0 | Disables PoE power. |
| 1  | Enables PoE power.  |   |                    |   |                     |
| 0  | Disables PoE power.   |   |                    |   |                     |
| Web: Enable power B<br>UCI: vapoe.B.enabled<br>Opt:enabled | Defines whether to enable PoE power on Ethernet port B.<br><table border="1"> <tr> <td>1</td> <td>Enables PoE power.</td> </tr> <tr> <td>0</td> <td>Disables PoE power.</td> </tr> </table> | 1 | Enables PoE power. | 0 | Disables PoE power. |
| 1  | Enables PoE power.  |   |                    |   |                     |
| 0  | Disables PoE power.   |   |                    |   |                     |
| Web: Enable power C<br>UCI: vapoe.C.enabled<br>Opt:enabled | Defines whether to enable PoE power on Ethernet port C.<br><table border="1"> <tr> <td>1</td> <td>Enables PoE power.</td> </tr> <tr> <td>0</td> <td>Disables PoE power.</td> </tr> </table> | 1 | Enables PoE power. | 0 | Disables PoE power. |
| 1  | Enables PoE power.  |   |                    |   |                     |
| 0  | Disables PoE power.   |   |                    |   |                     |
| Web: Enable power D<br>UCI: vapoe.D.enabled<br>Opt:enabled | Defines whether to enable PoE power on Ethernet port D.<br><table border="1"> <tr> <td>1</td> <td>Enables PoE power.</td> </tr> <tr> <td>0</td> <td>Disables PoE power.</td> </tr> </table> | 1 | Enables PoE power. | 0 | Disables PoE power. |
| 1  | Enables PoE power.  |   |                    |   |                     |
| 0  | Disables PoE power.   |   |                    |   |                     |

Table 35: Information table for PoE configuration

## 12.3.2 Configuring PoE using the command line

You can configure PoE using the port configuration section in the `vapoe` package `/etc/config/vapoe`.

The port section must be named A, B, C or D corresponding to the required Ethernet port

### 12.3.2.1 PoE using UCI

```
root@VA_router:~# uci show vapoe
vapoe.port=A
vapoe.A.enabled=1
vapoe.port=B
vapoe.B.enabled=1
vapoe.port=C
vapoe.C.enabled=1
vapoe.port=D
vapoe.D.enabled=1
```

### 12.3.2.2 PoE using package options

```
root@VA_router:~# uci export vapoe
package vapoe

config port 'A'
    option enabled 1

config port 'B'
    option enabled 1

config port 'C'
```

```
option enabled 1

config port 'D'
option enabled 1
```

## 12.4 Restarting a PoE port

### 12.4.1 Restarting a PoE port via the web interface

You can start PoE on an individual Ethernet port by:

- Disabling the **Enable power** configuration for the port.
- Enabling the **Enable power** configuration for the port.
- Selecting **Save and Apply**.

### 12.4.2 Restarting a PoE port via command line

To restart PoE using the command line, enter:

```
root@VA_router:~# /etc/init.d/vapoe restart
```

## 12.5 PoE diagnostics

### 12.5.1 PoE status

To see the PoE status, select **Status -> PoE**. The Status interface consists of detection status, class detected, power status, voltage and current measurements.

#### 12.5.1.1 PoE status via the web

| Port | Detection | Class   | Powered | Power OK | Voltage  | Current |
|------|-----------|---------|---------|----------|----------|---------|
| A    | Open      | Unknown | -       | -        | 0 V      | 0 mA    |
| B    | OK        | 1       | ✔       | ✔        | 54.566 V | 28 mA   |
| C    | Open      | Unknown | -       | -        | 0 V      | 0 mA    |
| D    | Open      | Unknown | -       | -        | 0 V      | 0 mA    |

Figure 64: The PoE status page



### 12.5.1.2 PoE status via command line

To view PoE status using the command line, enter:

```
root@VA_router:~# /etc/init.d/vapoe status
in1_class:Unknown
in1_curr:0
in1_detect:High Res
in1_enable:1
in1_good:0
in1_label:C
in1_mode:3
in1_power:0
in1_volt:0
in2_class:Unknown
in2_curr:0
in2_detect:Open
in2_enable:1
in2_good:0
in2_label:D
in2_mode:3
in2_power:0
in2_volt:0
in3_class:Unknown
in3_curr:0
in3_detect:Open
in3_enable:1
in3_good:0
in3_label:A
in3_mode:3
in3_power:0
```

## 13 Configuring AC power sense

AC to DC power adapters can store enough power to supply the router for a short period of time after the main AC supply has failed, so AC power sense allows the router to smoothly power down on supply failure. You can configure the time delay between sensed power failure and initiation of power down, so that very short power dropouts do not trigger an unnecessary shutdown.

Routers for AC power sense applications are supplied with a power lead with 3 connectors:

- A 12V signal that goes low as soon as AC power is lost and returns high when it is restored,
- A 12V main power connection, and
- Ground.

### 13.1 Configuration packages used

| Package     | Sections |
|-------------|----------|
| vapowermond | main     |

### 13.2 Configuring vapowermond using the web interface

You can configure the Vapowermond package using the web interface. In the top menu, click **Services -> Power Monitor**. The basic settings page appears.

The screenshot shows the 'Power Monitor' configuration page. The page has a title 'Power Monitor' and a subtitle 'Power Monitor Configuration'. Below the title, there is a 'Settings' section with two tabs: 'Basic' and 'Advanced'. The 'Basic' tab is selected. In the top right corner of the settings area, there is a 'Delete' button. The configuration options are as follows:

- Enable:** A checkbox labeled 'Enable' is checked, with a link 'Enable Power Monitor' next to it.
- AC Timeout:** A text input field contains the value '30'. A help icon and text 'Time in minutes from AC POWER OFF to board power down, set to 0 to disable the timer' are to the right.
- Enable Scripts:** A checkbox labeled 'Enable Scripts' is checked, with a link 'Execute scripts upon detection of power loss/restoration' next to it.
- Voltage On Script:** A text input field contains the path '/usr/bin/powermon\_voltage\_on.sh'. A help icon and text 'Script to execute on detection of power on' are to the right.
- Voltage Off Script:** A text input field contains the path '/usr/bin/powermon\_voltage\_off.sh'. A help icon and text 'Script to execute on detection of power off' are to the right.
- Message Prefix:** A text input field contains the value 'ACPower'. A help icon and text 'Syslog message prefix for messages PowerGood and PowerGone' are to the right.

At the bottom left of the settings area, there is an 'Add' button. At the bottom right, there are three buttons: 'Save & Apply', 'Save', and 'Reset'.

Figure 65: Power monitor basic settings page

### 13.2.1 Power monitor basic settings

| Web field/UCI/Package Option   | Description   |    |          |       |            |
|--|---|----|----------|-------|------------|
| Web field: Enable<br>UCI: vapowermond.main.enabled<br>Opt: enabled   | Enables vapowermond package on a router.<br><table border="1"> <tr> <td>0</td> <td></td> </tr> <tr> <td>Range</td> <td>0-1</td> </tr> </table>  | 0  |          | Range | 0-1        |
| 0  |   |    |          |       |            |
| Range  | 0-1   |    |          |       |            |
| Web field: Ignition Timeout<br>UCI: vapowermond.main.timeout<br>Opt: timeout   | Time in minutes from ignition power off to router power down. Set to <b>0</b> to disable the timer.<br><table border="1"> <tr> <td>30</td> <td></td> </tr> <tr> <td>Range</td> <td>0-infinite</td> </tr> </table> | 30 |          | Range | 0-infinite |
| 30   |   |    |          |       |            |
| Range  | 0-infinite  |    |          |       |            |
| Web field: Enable Scripts<br>UCI:<br>vapowermond.main.voltage_sense_scripts_enable<br>Opt:voltage_sense_scripts_enable | Execute scripts upon detection of power loss/restoration.<br><table border="1"> <tr> <td>0</td> <td>Disabled</td> </tr> <tr> <td>Range</td> <td>0-1</td> </tr> </table>   | 0  | Disabled | Range | 0-1        |
| 0  | Disabled  |    |          |       |            |
| Range  | 0-1   |    |          |       |            |
| Web field: Voltage On Script<br>UCI: vapowermond.main.voltage_on_script<br>Opt: voltage_on_script                      | Script to execute on detection of power on.<br>/usr/bin/powermon_voltage_on.sh  |    |          |       |            |
| Web field: Voltage Off Script<br>UCI: vapowermond.main.voltage_off_script<br>Opt: voltage_off_script                   | Script to execute on detection of power off.<br>/usr/bin/powermon_voltage_off.sh  |    |          |       |            |
| Web field: Message Prefix<br>UCI: vapowermond.main.voltage_msg<br>Opt: voltage_msg                                     | Syslog message prefix for messages IgnitionPowerOn, IgnitionPowerOff.   |    |          |       |            |

Table 36: Information table for power monitor basic settings

### 13.2.2 Power monitor advanced settings

Click the **Advance** tab to access advanced settings.

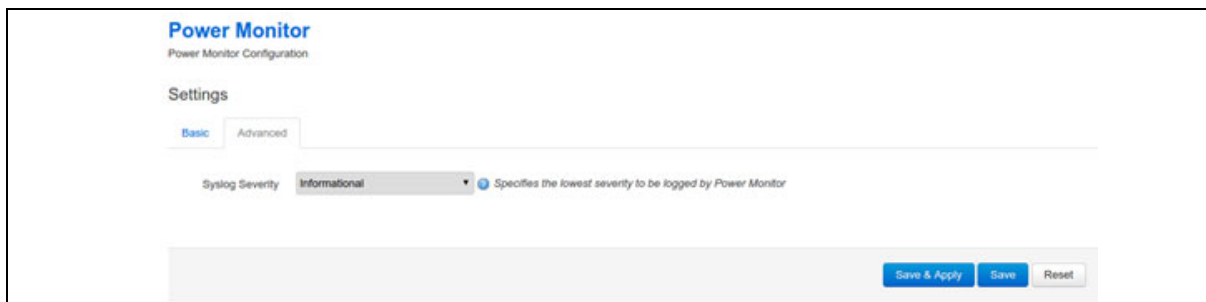


Figure 66: Power monitor advanced settings page

| Web field/UCI/Package Option  | Description  |               |
|---|--|---------------|
| Web field: Syslog Severity<br>UCI: vapowermond.main.log_severity<br>Opt: log_severity | Specifies the lowest severity to be logged by Power Monitor. |               |
|   | 0  | Emergency     |
|   | 1  | Alert         |
|   | 2  | Critical      |
|   | 3  | Error         |
|   | 4  | Warning       |
|   | 5  | Notice        |
|   | 6  | Informational |
|   | 7  | Debug         |

Table 37: Information table for power monitor advanced settings

## 13.3 Configuring vapowermond using the command line

### 13.3.1 UCI

```
root@VA_router:~# uci show vapowermond
vapowermond.main=vapowermond
vapowermond.main.enabled=1
vapowermond.main.timeout=30
vapowermond.main.voltage_sense_scripts_enable=0
vapowermond.main.voltage_on_script=/usr/bin/powermon_voltage_on.sh
vapowermond.main.voltage_off_script=/usr/bin/powermon_voltage_off.sh
vapowermond.main.voltage_msg=powermon
vapowermond.main.log_severity=5
```

### 13.3.2 Package options

```
root@VA_router:~# uci export vapowermond
package vapowermond

config vapowermond 'main'
    option enabled '1'
    option timeout '30'
    option voltage_sense_scripts_enable '0'
    option voltage_on_script '/usr/bin/powermon_voltage_on.sh'
    option voltage_off_script '/usr/bin/powermon_voltage_off.sh'
    option voltage_msg 'powermon'
    option log_severity '5'
```

## 13.4 AC power sense diagnostics

### 13.4.1 Monitoring Vapowermond status using the command line interface

To view status information about the current ignition sense state, enter:

```
root@VA_router:~# cat /sys/devices/platform/gpio-keys-polled/power  
0
```

**1** for power failure

**0** for power good

## 14 Configuring a WiFi connection

This chapter explains how to configure WiFi on a Virtual Access router using the web interface or via UCI.

WiFi can act as an Access Point (AP) to another device in the network or it can act as a client to an existing AP.

You can configure WiFi in two different ways:

- on a new interface, or
- on an existing interface

### 14.1 Configuration packages used

| Package  | Sections                  |
|----------|---------------------------|
| network  | wlan_ap<br>wlan_client    |
| wireless | wifi-device<br>wifi-iface |

### 14.2 Configuring a WiFi interface using the web interface

To create a new WiFi interface via the web interface, in the top menu, click **Network -> Wifi**. The Wireless overview page appears.

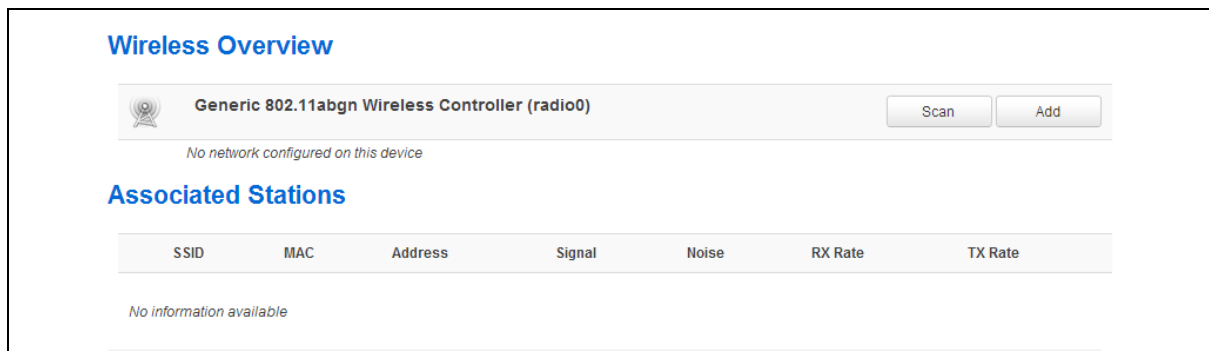


Figure 67: The wireless overview page

Click **Add** to create a new WiFi interface. The Wireless Network configuration page appears. The Wireless Network configuration page consists of two sections:

| Section                 | Description   |
|-------------------------|---|
| Device Configuration    | Configure physical wireless radio settings such as channel and transmit power settings, HT mode, country code, distance optimisation, fragmentation threshold and RTS/CTS threshold. The settings are shared among all defined wireless networks. |
| Interface Configuration | Configure network interface settings: interface name, mode, network settings, security and filtering.   |

#### 14.2.1 Wireless network: device configuration

The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection, which is shared among all defined wireless

networks if the radio hardware is multi-SSID capable. There are two sections within the Device Configuration section.

| Section           | Description  |
|-------------------|--|
| General Setup     | Channel and transmit power settings.   |
| Advanced Settings | HT mode, country code, distance optimisation, fragmentation threshold and RTS/CTS threshold. |

### 14.2.1.1 Device configuration: general setup

The screenshot shows the 'Device Configuration' page with the 'General Setup' tab selected. The status indicates that the wireless network is disabled. The SSID is 'OpenWrt' and the mode is 'Master'. The channel is set to '4 (2.427 GHz)' and the transmit power is '20 dBm (100 mW)'.

Figure 68: The device configuration general setup section

| Web Field/UCI/Package Option  | Description   |       |                            |               |                           |
|---|---|-------|----------------------------|---------------|---------------------------|
| Web: Wireless network<br>UCI: wireless.radio0.disabled<br>Opt: disanabled | Enables or disables a wireless interface.<br><table border="1"> <tr> <td>1</td> <td>Disables a WiFi interface.</td> </tr> <tr> <td>0</td> <td>Enables a WiFi interface.</td> </tr> </table> | 1     | Disables a WiFi interface. | 0             | Enables a WiFi interface. |
| 1   | Disables a WiFi interface.  |       |                            |               |                           |
| 0   | Enables a WiFi interface.   |       |                            |               |                           |
| Web: Channel<br>UCI: wireless.radio0.channel<br>Opt: channel              | Select the channel you require.<br><table border="1"> <tr> <td>Range</td> <td>1-11</td> </tr> <tr> <td>11 (2.462GHz)</td> <td></td> </tr> </table>  | Range | 1-11                       | 11 (2.462GHz) |                           |
| Range   | 1-11  |       |                            |               |                           |
| 11 (2.462GHz)   |   |       |                            |               |                           |
| Web: Transmit power<br>UCI: wireless.radio0.txpower<br>Opt: txpower       | Select the transmit power range range you require.<br><table border="1"> <tr> <td>Range</td> <td>0dBm(1mW)-17dBm(50mW)</td> </tr> <tr> <td>17dBm(50mW)</td> <td></td> </tr> </table>        | Range | 0dBm(1mW)-17dBm(50mW)      | 17dBm(50mW)   |                           |
| Range   | 0dBm(1mW)-17dBm(50mW)   |       |                            |               |                           |
| 17dBm(50mW)   |   |       |                            |               |                           |

Table 38: Information table for the device configuration section

### 14.2.1.2 Device configuration: advanced settings

**Device Configuration**

General Setup
Advanced Settings

---

Mode

HT mode

Country Code  Use ISO/IEC 3166 alpha2 country codes.

Distance Optimization  Distance to farthest network member in meters.

Fragmentation Threshold

RTS/CTS Threshold

**Figure 69: The device configuration advanced settings section**

| Web Field/UCI/Package Option   | Description   |        |                                       |                         |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
|--|---|--------|---------------------------------------|-------------------------|---|-------------------------|---------------------------------------|---------|--------------------------------------|---------|--------------------------------------|-----------|--------------------------------------|-----------|--------------------------------------|
| Web: Mode<br>UCI: wireless.radio0.hwmode<br>Opt: hwmode                      | Mode options. <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Auto</td> <td>Wireless protocl negotiate with supplicat device.</td> </tr> <tr> <td>802.11b</td> <td>Select the wireless protocol to use.</td> </tr> <tr> <td>802.11g</td> <td>Select the wireless protocol to use.</td> </tr> <tr> <td>802.11a</td> <td>Select the wireless protocol to use.</td> </tr> <tr> <td>802.11g+n</td> <td>Select the wireless protocol to use.</td> </tr> <tr> <td>802.11a+n</td> <td>Select the wireless protocol to use.</td> </tr> </tbody> </table> | Option | Description                           | Auto                    | Wireless protocl negotiate with supplicat device. | 802.11b                 | Select the wireless protocol to use.  | 802.11g | Select the wireless protocol to use. | 802.11a | Select the wireless protocol to use. | 802.11g+n | Select the wireless protocol to use. | 802.11a+n | Select the wireless protocol to use. |
| Option   | Description   |        |                                       |                         |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| Auto   | Wireless protocl negotiate with supplicat device.   |        |                                       |                         |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| 802.11b  | Select the wireless protocol to use.  |        |                                       |                         |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| 802.11g  | Select the wireless protocol to use.  |        |                                       |                         |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| 802.11a  | Select the wireless protocol to use.  |        |                                       |                         |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| 802.11g+n  | Select the wireless protocol to use.  |        |                                       |                         |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| 802.11a+n  | Select the wireless protocol to use.  |        |                                       |                         |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| Web: HT mode<br>UCI: wireless.radio0.htmode<br>Opt: country                  | HT mode options. <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td>20MHz</td> <td>Specifies the channel width in 802.11</td> </tr> <tr> <td>40MHz 2nd channel below</td> <td>Specifies the channel width in 802.11</td> </tr> <tr> <td>40MHz 2nd channel above</td> <td>Specifies the channel width in 802.11</td> </tr> </tbody> </table>  | 20MHz  | Specifies the channel width in 802.11 | 40MHz 2nd channel below | Specifies the channel width in 802.11             | 40MHz 2nd channel above | Specifies the channel width in 802.11 |         |                                      |         |                                      |           |                                      |           |                                      |
| 20MHz  | Specifies the channel width in 802.11   |        |                                       |                         |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| 40MHz 2nd channel below  | Specifies the channel width in 802.11   |        |                                       |                         |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| 40MHz 2nd channel above  | Specifies the channel width in 802.11   |        |                                       |                         |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| Web: Country Code<br>UCI: wireless.radio0.country<br>Opt: country            | Sets the country code. Use ISO/1EC 3166 alpha2 country codes.   |        |                                       |                         |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| Web: Distance Optimization<br>UCI: wireless.radio0.distance<br>Opt: distance | Defines the distance between the AP and the furthest client in meters <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td>15</td> <td>15 meters</td> </tr> <tr> <td>Range</td> <td></td> </tr> </tbody> </table>  | 15     | 15 meters                             | Range                   |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| 15   | 15 meters   |        |                                       |                         |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| Range  |   |        |                                       |                         |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| Web: Fragmentation Threshold<br>UCI: wireless.radio0.frag<br>Opt: frag       | Defines the fragmentation threshold. <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td>None</td> <td>Routers defaults applied.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </tbody> </table>   | None   | Routers defaults applied.             | Range                   |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| None   | Routers defaults applied.   |        |                                       |                         |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| Range  |   |        |                                       |                         |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| Web: RTS/CTS Threshold<br>UCI: wireless.radio0.rts<br>Opt: rts               | Defines the RTS/CTS threshold. <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td>None</td> <td>Router defaults applied.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </tbody> </table>  | None   | Router defaults applied.              | Range                   |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| None   | Router defaults applied.  |        |                                       |                         |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |
| Range  |   |        |                                       |                         |   |                         |                                       |         |                                      |         |                                      |           |                                      |           |                                      |

**Table 39: Information table for device configuration advanced settings**



## 14.2.2 Wireless network: interface configuration

The interface configuration section is used to configure the network and security settings. It has three sub-sections.

| Section           | Description                                   |
|-------------------|---|
| General Setup     | Identification, network and mode settings.    |
| Wireless Security | Encryption, cipher and key security settings. |
| MAC Filter        | MAC address filter settings.                  |

### 14.2.2.1 Interface configuration: general setup

Use this section to configure the interface name, mode and network settings. Differing web options may be presented depending on the mode selected.

The screenshot shows the 'Interface Configuration' web page with the 'General Setup' tab selected. The 'ESSID' field contains 'OpenWrt'. The 'Mode' dropdown is set to 'Access Point'. Under the 'Network' section, there are radio buttons for '3G', 'ADSL', 'Test\_BC', 'Tunnel1', 'lan', 'lan2', 'lan3', 'lan4', 'loopback', and 'unspecified -or- create:'. Below the radio buttons, there is a text input field for 'unspecified -or- create:'. A blue information icon is followed by the text: 'Choose the network you want to attach to this wireless interface. Select unspecified to not attach any network or fill out the create field to define a new network.' At the bottom left, there is a 'Hide ESSID' checkbox. At the bottom right, there are three buttons: 'Save & Apply', 'Save', and 'Reset'.

Figure 70: The interface configuration general setup section

| Web Field/UCI/Package Option  | Description  |           |          |              |           |        |     |        |       |         |      |                         |        |         |         |                    |        |              |         |
|---|--|-----------|----------|--------------|-----------|--------|-----|--------|-------|---------|------|-------------------------|--------|---------|---------|--------------------|--------|--------------|---------|
| Web: ESSID<br>UCI: wireless.@wifi-iface[0]..ssid<br>Opt: ssid         | Extended Service Set Identification. Type the name of the wireless local area network.   |           |          |              |           |        |     |        |       |         |      |                         |        |         |         |                    |        |              |         |
| Web: Mode<br>UCI: wireless.@wifi-iface[0].mode<br>Opt: mode           | Mode type. For AP mode, select <b>Access Point</b> . <table border="1"> <tr> <td>Web value</td> <td>UCI</td> </tr> <tr> <td>Access Point</td> <td>ap</td> </tr> <tr> <td>Client</td> <td>sta</td> </tr> <tr> <td>Ad-Hoc</td> <td>adhoc</td> </tr> <tr> <td>802.11s</td> <td>mesh</td> </tr> <tr> <td>Pseudo Ad-Hoc (ah demo)</td> <td>ahdemo</td> </tr> <tr> <td>Monitor</td> <td>monitor</td> </tr> <tr> <td>Access Point (WDS)</td> <td>ap-wds</td> </tr> <tr> <td>Client (WDS)</td> <td>sta-wds</td> </tr> </table> | Web value | UCI      | Access Point | ap        | Client | sta | Ad-Hoc | adhoc | 802.11s | mesh | Pseudo Ad-Hoc (ah demo) | ahdemo | Monitor | monitor | Access Point (WDS) | ap-wds | Client (WDS) | sta-wds |
| Web value   | UCI  |           |          |              |           |        |     |        |       |         |      |                         |        |         |         |                    |        |              |         |
| Access Point  | ap   |           |          |              |           |        |     |        |       |         |      |                         |        |         |         |                    |        |              |         |
| Client  | sta  |           |          |              |           |        |     |        |       |         |      |                         |        |         |         |                    |        |              |         |
| Ad-Hoc  | adhoc  |           |          |              |           |        |     |        |       |         |      |                         |        |         |         |                    |        |              |         |
| 802.11s   | mesh   |           |          |              |           |        |     |        |       |         |      |                         |        |         |         |                    |        |              |         |
| Pseudo Ad-Hoc (ah demo)   | ahdemo   |           |          |              |           |        |     |        |       |         |      |                         |        |         |         |                    |        |              |         |
| Monitor   | monitor  |           |          |              |           |        |     |        |       |         |      |                         |        |         |         |                    |        |              |         |
| Access Point (WDS)  | ap-wds   |           |          |              |           |        |     |        |       |         |      |                         |        |         |         |                    |        |              |         |
| Client (WDS)  | sta-wds  |           |          |              |           |        |     |        |       |         |      |                         |        |         |         |                    |        |              |         |
| Web: Mode<br>UCI: wireless.@wifi-iface[0].bssid<br>Opt: bssid         | Defines the BSSID value. Only displayed if using client, ad-hoc or client (wds) modes.   |           |          |              |           |        |     |        |       |         |      |                         |        |         |         |                    |        |              |         |
| Web: Network<br>UCI: wireless.@wifi-iface[0].network<br>Opt: network  | The network the wireless interface is attached to. If using an existing interface select the appropriate network.<br>Select <b>unspecified</b> to not attach to any network or fill out the <b>create</b> field to define a new network.   |           |          |              |           |        |     |        |       |         |      |                         |        |         |         |                    |        |              |         |
| Web: Hide ESSID<br>UCI: wireless.@wifi-iface[0].hidden<br>Opt: hidden | Hides the SSID when enabled. Only displayed if using access point or access point (wds) modes. <table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table>  | 1         | Enabled. | 0            | Disabled. |        |     |        |       |         |      |                         |        |         |         |                    |        |              |         |
| 1   | Enabled.   |           |          |              |           |        |     |        |       |         |      |                         |        |         |         |                    |        |              |         |
| 0   | Disabled.  |           |          |              |           |        |     |        |       |         |      |                         |        |         |         |                    |        |              |         |

**Table 40: Information table for the interface configuration general setup section**

#### 14.2.2.2 Interface configuration: wireless security

Use this section to configure encryption, cipher and create a security key. Differing options will be defined depending on the encryption selected.

The screenshot shows the 'Interface Configuration' page with the 'Wireless Security' tab selected. The 'Encryption' dropdown is set to 'WPA2-PSK', the 'Cipher' dropdown is set to 'auto', and the 'Key' field contains a masked password. At the bottom right, there are three buttons: 'Save & Apply' (blue), 'Save' (blue), and 'Reset' (grey).

**Figure 71: The wireless security section**

| Web Field/UCI/Package Option  | Description  |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
|---|--|-----------|-----------|---------------|------|------------------|----------|----------------|------------|---------------------|-----------|----------|------|-----------------------------|-----------|---------|-----|----------|------|
| Web: Encryption<br>UCI: wireless.@wifi-iface[0].encryption<br>Opt: encryption                     | Method of encryption. <table border="1"> <thead> <tr> <th>Web value</th> <th>UCI value</th> </tr> </thead> <tbody> <tr> <td>No encryption</td> <td>none</td> </tr> <tr> <td>WEP Open System</td> <td>wep-open</td> </tr> <tr> <td>WEP Shared Key</td> <td>wep-shared</td> </tr> <tr> <td>WPA-PSK</td> <td>psk</td> </tr> <tr> <td>WPA2-PSK</td> <td>psk2</td> </tr> <tr> <td>WPA-PSK/WPA2-PSK Mixed Mode</td> <td>psk-mixed</td> </tr> <tr> <td>WPA-EAP</td> <td>wpa</td> </tr> <tr> <td>WPA2-WAP</td> <td>wpa2</td> </tr> </tbody> </table> | Web value | UCI value | No encryption | none | WEP Open System  | wep-open | WEP Shared Key | wep-shared | WPA-PSK             | psk       | WPA2-PSK | psk2 | WPA-PSK/WPA2-PSK Mixed Mode | psk-mixed | WPA-EAP | wpa | WPA2-WAP | wpa2 |
| Web value   | UCI value  |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| No encryption   | none   |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| WEP Open System   | wep-open   |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| WEP Shared Key  | wep-shared   |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| WPA-PSK   | psk  |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| WPA2-PSK  | psk2   |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| WPA-PSK/WPA2-PSK Mixed Mode   | psk-mixed  |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| WPA-EAP   | wpa  |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| WPA2-WAP  | wpa2   |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| Web: Cipher<br>UCI: wireless.@wifi-iface[0].cipher=<br>Opt: cipher                                | Cipher type. Only displayed if WPA encryption modes are selected. <table border="1"> <thead> <tr> <th>Web value</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Auto</td> <td>auto</td> </tr> <tr> <td>Force CCMP (AES)</td> <td>ccmp</td> </tr> <tr> <td>Force TKIP</td> <td>tkip</td> </tr> <tr> <td>Force TKIP and CCMP</td> <td>tkip+ccmp</td> </tr> </tbody> </table>   | Web value | UCI       | Auto          | auto | Force CCMP (AES) | ccmp     | Force TKIP     | tkip       | Force TKIP and CCMP | tkip+ccmp |          |      |                             |           |         |     |          |      |
| Web value   | UCI  |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| Auto  | auto   |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| Force CCMP (AES)  | ccmp   |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| Force TKIP  | tkip   |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| Force TKIP and CCMP   | tkip+ccmp  |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| Web: Key<br>UCI: wireless.@wifi-iface[0].key<br>Opt: key  | Specifies the wireless key authentication phrase.  |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| Web: Key #1<br>UCI: wireless.@wifi-iface[0].key1<br>Opt: key1                                     | Specifies the first wireless key authentication phrase.  |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| Web: Key #2<br>UCI: wireless.@wifi-iface[0].key2<br>Opt: key2                                     | Specifies the second wireless key authentication phrase.   |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| Web: Key #3<br>UCI: wireless.@wifi-iface[0].key3<br>Opt: key3                                     | Specifies the third wireless key authentication phrase.  |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| Web: Key #4<br>UCI: wireless.@wifi-iface[0].key4<br>Opt: key4                                     | Specifies the fourth wireless key authentication phrase.   |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| Web: Radius Authentication-Server<br>UCI: wireless.@wifi-iface[0].auth_server<br>Opt: auth_server | Defines the radius server for EAP authentication.  |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| Web: Radius Authentication-Port<br>UCI: wireless.@wifi-iface[0].auth_port<br>Opt: auth_port       | Defines the radius server port for EAP authentication.   |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| Web: Radius Authentication-Secret<br>UCI: wireless.@wifi-iface[0].auth_secret<br>Opt: auth_secret | Defines the radius server secret for EAP authentication.   |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| Web: Radius Accounting-Server<br>UCI: wireless.@wifi-iface[0].acct_server<br>Opt: acct_server     | Defines the radius server for EAP accounting.  |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| Web: Radius Accounting -Port<br>UCI: wireless.@wifi-iface[0].acct_port<br>Opt: acct_port          | Defines the radius port for EAP accounting.  |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |
| Web: Radius Accounting -Secret<br>UCI: wireless.@wifi-iface[0].acct_secret<br>Opt: acct_secret    | Defines the radius secret for EAP accounting.  |           |           |               |      |                  |          |                |            |                     |           |          |      |                             |           |         |     |          |      |

|   |  |
|---|--|
| Web: NAS ID<br>UCI: wireless.@wifi-iface[0].nasid<br>Opt: nasid | Defines the NAS ID for the wireless interface. |
|---|--|

Table 41: Information table for the interface configuration wireless security section

### 14.2.2.3 Interface configuration: MAC filter

The screenshot shows the 'Interface Configuration' page with three tabs: 'General Setup', 'Wireless Security', and 'MAC-Filter'. The 'MAC-Filter' tab is active. Underneath, there is a 'MAC-Address Filter' dropdown menu currently set to 'disable'. At the bottom right, there are three buttons: 'Save & Apply' (blue), 'Save' (blue), and 'Reset' (grey).

Figure 72: The MAC filter section

| Web Field/UCI/Package Option  | Description   |         |             |     |         |                              |         |                   |   |       |                         |   |      |
|---|---|---------|-------------|-----|---------|------------------------------|---------|-------------------|---|-------|-------------------------|---|------|
| Web: MAC-Address Filter<br>UCI: wireless.@wifi-iface[0].macfilter<br>Opt: macfilter | MAC address filtering process. <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Disable</td> <td>Disables MAC Address filter.</td> <td>disable</td> </tr> <tr> <td>Allow listed only</td> <td>Allows only the MAC address listed in the text field.</td> <td>allow</td> </tr> <tr> <td>Allow all except listed</td> <td>Allows everything but the MAC address listed in the text field.</td> <td>deny</td> </tr> </tbody> </table> | Option  | Description | UCI | Disable | Disables MAC Address filter. | disable | Allow listed only | Allows only the MAC address listed in the text field. | allow | Allow all except listed | Allows everything but the MAC address listed in the text field. | deny |
| Option  | Description   | UCI     |             |     |         |                              |         |                   |   |       |                         |   |      |
| Disable   | Disables MAC Address filter.  | disable |             |     |         |                              |         |                   |   |       |                         |   |      |
| Allow listed only   | Allows only the MAC address listed in the text field.   | allow   |             |     |         |                              |         |                   |   |       |                         |   |      |
| Allow all except listed   | Allows everything but the MAC address listed in the text field.   | deny    |             |     |         |                              |         |                   |   |       |                         |   |      |
| Web: MAC -List<br>UCI: wireless.@wifi-iface[0].maclist<br>Opt: list maclist         | Defines the MAC addresses to use. Multiple MAC address should be separated by a space if using UCI. MAC must be in the format hh:hh:hh:hh:hh:hh   |         |             |     |         |                              |         |                   |   |       |                         |   |      |

Table 42: Information table for interface configuration MAC filter section

## 14.3 Configuring WiFi in AP mode

AP mode is when the router's WiFi is used as an access point to one of the router's other interfaces. For example, if a router is connected to the internet via 3G, the WiFi on the router can be used as an access point for other devices to connect to the router and use its 3G internet connection.

### 14.3.1 AP mode on a new interface

Configure the WiFi network in AP mode as described in the above section 'Configuring a WiFi interface', selecting a new interface for the wireless network in the Interface Configuration section.

Next, in the top menu, select **Network -> Interfaces**. The Interface Overview page appears.

In the Interface Overview page, click **Edit** on the newly created WiFi interface. Then configure the interface by following instructions in the chapter 'Configuring an Ethernet interface'. When you have completed those steps, continue with the section below.

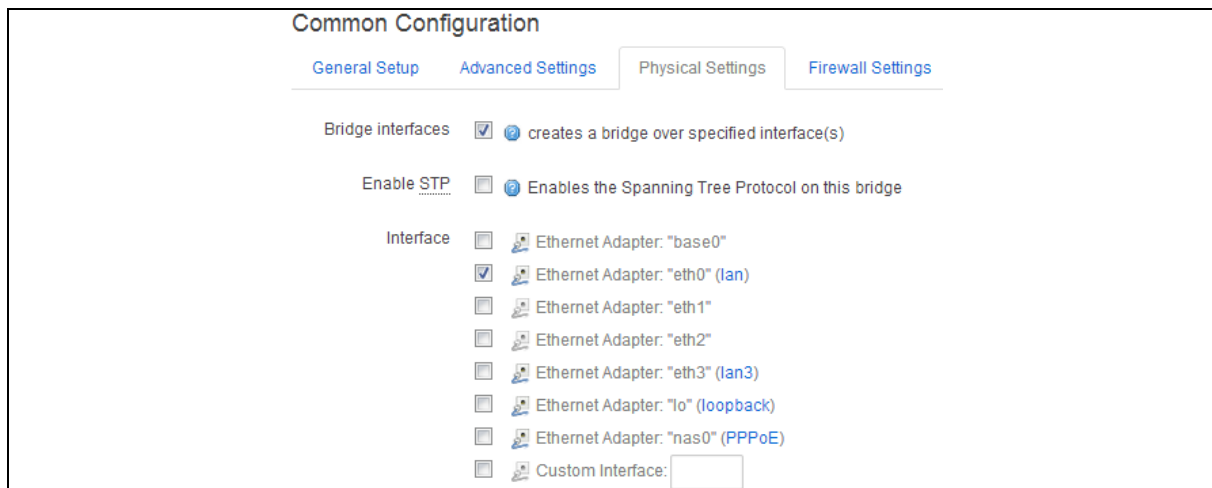
### 14.3.2 AP mode on an existing Ethernet interface

Configure the WiFi network in AP mode as described in the above section 'Configuring a WiFi interface'.

Next, in the top menu, select **Network -> Interfaces**. The Interface Overview page appears.

In the Interface Overview page, click **Edit** on the Ethernet interface that will be bridged into the router's WiFi AP. The Common Configuration page appears. It has four sections.

This configuration only uses the Physical Settings section. Click the **Physical Settings** tab.



**Figure 73: The physical settings section in the common configuration page**

| Web Field/UCI/Package Option                                 | Description  |       |           |        |   |
|--|--|-------|-----------|--------|---|
| Web: Bridge Interfaces<br>UCI: network.lan.type<br>Opt: Type | Creates a bridge over the specified interface.<br><table border="1"> <tr> <td>Empty</td> <td></td> </tr> <tr> <td>Bridge</td> <td>Configures a bridge over multiple interfaces.</td> </tr> </table>  | Empty |           | Bridge | Configures a bridge over multiple interfaces. |
| Empty  |  |       |           |        |   |
| Bridge   | Configures a bridge over multiple interfaces.  |       |           |        |   |
| Web: Enable STP<br>UCI: network.lan.stp<br>Opt: stp          | Enables the Spanning Tree Protocol on this bridge.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0     | Disabled. | 1      | Enabled.                                      |
| 0  | Disabled.  |       |           |        |   |
| 1  | Enabled.   |       |           |        |   |
| Web: Interface<br>UCI: network.lan.ifname<br>Opt: ifname     | Select the physical interfaces to bridge. If mapping multiple interfaces for bridging, the interface names are separated by a space when using UCI and package options.<br>Example:<br>option ifname 'eth2 eth3' or network.<ifname>.ifname=eth2 eth 3 |       |           |        |   |

**Table 43: Information table for the physical section on the common configuration page**

## 14.4 Configuring WiFi using UCI

The configuration files are stored on:

- Network file /etc/config/network
- Wireless file /etc/config/wireless

### 14.4.1 AP modem on a new Ethernet interface using package options

```
root@VA_router:~# uci export network
package network
config interface 'newwifilan'
    option proto 'static'
    option ipaddr '192.168.111.1'
    option netmask '255.255.255.0'
root@VA_router:~# uci export wireless
package wireless
config wifi-device 'radio0'
    option type 'mac80211'
    option channel '11'
    option phy 'phy0'
    option hwmode '11ng'
    option htmode 'HT20'

list ht_capab 'SHORT-GI-40'
    list ht_capab 'TX-STBC'
    list ht_capab 'RX-STBC1'
    list ht_capab 'DSSS_CCK-40'
    option txpower '17'
    option country 'US'

config wifi-iface
    option device 'radio0'
    option mode 'ap'
    option disabled '1'
    option ssid 'Test_AP'
    option network 'newwifilan'
    option encryption 'psk'
    option key 'secretkey'
```

### 14.4.2 AP modem on a new Ethernet interface using UCI

```
root@VA_router:~# uci show network
network.newlan=interface
network.newlan.proto=static
network.newlan.ipaddr=192.168.111.1
network.newlan.netmask=255.255.255.0
root@VA_router:~# uci show wireless
wireless.radio0=wifi-device
wireless.radio0.type=mac80211
wireless.radio0.channel=11
wireless.radio0.phy=phy0
wireless.radio0.hwmode=11ng
wireless.radio0.htmode=HT20
wireless.radio0.ht_capab=SHORT-GI-40 TX-STBC RX-STBC1 DSSS_CCK-40
wireless.radio0.txpower=17
wireless.radio0.country=US
wireless.@wifi-iface[0]=wifi-iface
wireless.@wifi-iface[0].device=radio0
wireless.@wifi-iface[0].mode=ap
wireless.@wifi-iface[0].disabled=1
wireless.@wifi-iface[0].ssid=Test_AP
wireless.@wifi-iface[0].network=newlan
wireless.@wifi-iface[0].encryption=psk
wireless.@wifi-iface[0].key=secretkey
```

### 14.4.3 AP mode on an existing Ethernet interface using packages options

```
root@VA_router:~# uci export network
package network
config interface 'lan'
    option ifname 'eth0'
    option proto 'static'
    option ipaddr '192.168.100.1'
    option netmask '255.255.255.0'
    option type 'bridge'
root@VA_router:~# uci export wireless
package wireless
```

```
config wifi-device 'radio0'
    option type 'mac80211'
    option channel '11'
    option phy 'phy0'
    option hwmode '11ng'
    option htmode 'HT20'
    list ht_capab 'SHORT-GI-40'
    list ht_capab 'TX-STBC'
    list ht_capab 'RX-STBC1'
    list ht_capab 'DSSS_CCK-40'
    option txpower '17'
    option country 'US'

config wifi-iface
    option device 'radio0'
    option mode 'ap'
    option disabled '1'
    option ssid 'Test_AP'
    option network 'lan'
    option encryption 'psk'
    option key 'secretkey'
```

#### 14.4.4 AP mode on an existing Ethernet interface using UCI

```
root@VA_router:~# uci show network
network.lan=interface
network.lan.ifname=eth0
network.lan.proto=static
network.lan.ipaddr=192.168.6.1
network.lan.netmask=255.255.255.0
network.lan.type=bridge
root@VA_router:~# uci show wireless
wireless.radio0=wifi-device
wireless.radio0.type=mac80211
wireless.radio0.channel=11
wireless.radio0.phy=phy0
wireless.radio0.hwmode=11ng
```



```
wireless.radio0.htmode=HT20
wireless.radio0.ht_capab=SHORT-GI-40 TX-STBC RX-STBC1 DSSS_CCK-40
wireless.radio0.txpower=17
wireless.radio0.country=US
wireless.@wifi-iface[0]=wifi-iface
wireless.@wifi-iface[0].device=radio0
wireless.@wifi-iface[0].mode=ap
wireless.@wifi-iface[0].disabled=1
wireless.@wifi-iface[0].ssid=Test_AP
wireless.@wifi-iface[0].network=lan
wireless.@wifi-iface[0].encryption=psk
wireless.@wifi-iface[0].key=secretkey
```

## 14.5 Creating a WiFi interface in client mode using the web interface

A WiFi network in Client mode receives a wireless network from another WiFi AP.

Configure the Wifi network in Client mode as described in the above section 'Configuring a WiFi interface', selecting a new interface for the Wireless Network in the Interface Configuration section. For the examples below the new WiFi interface will be called 'newwifiClient'

Example:

```
wireless.@wifi-iface[0].network=newwifiClient
wireless.@wifi-iface[0].mode=sta
```

In the top menu, select **Network -> Interfaces**. The Interfaces Overview page appears. Click **Edit** in the newly created WiFi Client interface. The Common Configuration page appears.

**Interfaces - WCLIENT**

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

**Common Configuration**

General Setup

Status: Unknown "VA-Wireless" MAC Address: 00:00:00:00:00:00  
RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)

Protocol: DHCP client

Really switch protocol?

IP-Aliases

This section contains no values yet

Figure 74: The client interface page

| Web Field/UCI/Package Option                                     | Description  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
|--|--|--------|-------------|--------|--|-------------|---|-----------|-------------|------------------------|---------------------------|----------------|-------------------------------------|-----|--|-----|--|------|-----------------------------|-----|-------------------------|-------|-------------------|---------|--------------|---------------------|---|
| Web: Protocol<br>UCI: network. newwifiClient.proto<br>Opt: proto | Specifies what protocol the interface will operate on. Select <b>DHCP Client</b> . <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Static</td> <td>Static configuration with fixed address and netmask.</td> </tr> <tr> <td>DHCP Client</td> <td>Address and netmask are assigned by DHCP.</td> </tr> <tr> <td>Unmanaged</td> <td>Unspecified</td> </tr> <tr> <td>IPv6-in-IPv4 (RFC4213)</td> <td>Used with tunnel brokers.</td> </tr> <tr> <td>IPv6-over-IPv4</td> <td>Stateless IPv6 over IPv4 transport.</td> </tr> <tr> <td>GRE</td> <td>Generic Routing Encapsulation protocol</td> </tr> <tr> <td>IOT</td> <td></td> </tr> <tr> <td>L2TP</td> <td>Layer 2 Tunnelling Protocol</td> </tr> <tr> <td>PPP</td> <td>Point to Point Protocol</td> </tr> <tr> <td>PPPoE</td> <td>PPP over Ethernet</td> </tr> <tr> <td>PPPoATM</td> <td>PPP over ATM</td> </tr> <tr> <td>LTE/UMTS/GPRS/EV-DO</td> <td>CDMA, UMTS or GPRS connection using an AT-style 3G modem.</td> </tr> </tbody> </table> | Option | Description | Static | Static configuration with fixed address and netmask. | DHCP Client | Address and netmask are assigned by DHCP. | Unmanaged | Unspecified | IPv6-in-IPv4 (RFC4213) | Used with tunnel brokers. | IPv6-over-IPv4 | Stateless IPv6 over IPv4 transport. | GRE | Generic Routing Encapsulation protocol | IOT |  | L2TP | Layer 2 Tunnelling Protocol | PPP | Point to Point Protocol | PPPoE | PPP over Ethernet | PPPoATM | PPP over ATM | LTE/UMTS/GPRS/EV-DO | CDMA, UMTS or GPRS connection using an AT-style 3G modem. |
| Option   | Description  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| Static   | Static configuration with fixed address and netmask.   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| DHCP Client  | Address and netmask are assigned by DHCP.  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| Unmanaged  | Unspecified  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| IPv6-in-IPv4 (RFC4213)   | Used with tunnel brokers.  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| IPv6-over-IPv4   | Stateless IPv6 over IPv4 transport.  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| GRE  | Generic Routing Encapsulation protocol   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| IOT  |  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| L2TP   | Layer 2 Tunnelling Protocol  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| PPP  | Point to Point Protocol  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| PPPoE  | PPP over Ethernet  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| PPPoATM  | PPP over ATM   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| LTE/UMTS/GPRS/EV-DO  | CDMA, UMTS or GPRS connection using an AT-style 3G modem.  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |

**Table 44: Information table for interfaces WClient page**

When you have clicked **Save and Apply**, the router will restart the network package. It may take up to one minute for connectivity to the router to be restored.

## 14.6 Configuring WiFi in client mode using command line

The configuration files are stored on:

- Network file /etc/config/network
- Wireless file /etc/config/wireless

### 14.6.1 Client modem using package options

```

root@VA_router:~# uci export network
package network
config interface 'newwifiClient'
    option proto 'dhcp'
root@VA_router:~# uci export wireless
package wireless
config wifi-device 'radio0'
    option type 'mac80211'
    option channel '11'
    option phy 'phy0'
    option hwmode '11ng'
    option htmode 'HT20'
    list ht_capab 'SHORT-GI-40'

```

```

list ht_capab 'TX-STBC'
list ht_capab 'RX-STBC1'
list ht_capab 'DSSS_CCK-40'
option txpower '17'
option country 'US'

config wifi-iface
    option device 'radio0'
    option ssid 'Remote-AP'
    option mode 'sta'
    option network ' newwifiClient '
    option encryption 'psk2'
    option key 'testtest'

```

## 14.6.2 Client modem using UCI

```

root@VA_router:~# uci show network
network.new=interface
network.WCLIENT.proto=dhcp

```

### 14.6.2.1 uci show wireless

```

root@VA_router:~# uci show wireless
wireless.radio0=wifi-device
wireless.radio0.type=mac80211
wireless.radio0.channel=11
wireless.radio0.phy=phy0
wireless.radio0.hwmode=11ng
wireless.radio0.htmode=HT20
wireless.radio0.ht_capab=SHORT-GI-40 TX-STBC RX-STBC1 DSSS_CCK-40
wireless.radio0.txpower=17
wireless.radio0.country=US
wireless.@wifi-iface[0]=wifi-iface
wireless.@wifi-iface[0].device=radio0
wireless.@wifi-iface[0].ssid=Remote-AP
wireless.@wifi-iface[0].mode=sta
wireless.@wifi-iface[0].network= newwifiClient
wireless.@wifi-iface[0].encryption=psk2
wireless.@wifi-iface[0].key=testtest

```

## 15 Configuring an xDSL interface

The GW2300, GW6600V and GW7600V router series support both VDSL and ADSL connections, allowing a single configuration to automatically connect to either a VDSL, or ADSL, headend, providing flexibility of deployment to customers using either kind of link.

The router has a single xDSL interface, which can run in either VDSL or ADSL mode. Only one mode is supported at a time, though the router can switch between them by dynamically reloading the firmware.

### 15.1 xDSL overview

VDSL interfaces can run in PTM (Packet Transfer Mode) or ATM (Asynchronous Transfer Mode). PTM is similar to bridged Ethernet directly on the wire, while ATM on VDSL behaves as it does over ADSL. ADSL interfaces on the GW6600V also support PTM mode.

This chapter describes how to configure VDSL PTM connections and ADSL ATM connections as these are the standard connection types.

When you configure PTM mode, a `ptm0` interface is created at startup, similar to `nas0` on ADSL. This interface accepts Ethernet-formatted frames for transmission over VDSL. You can create sub-interfaces with different VLANs to allow multiple logical connections over a single PTM link.

If the DSL device is configured in auto-detect mode, two different upper level interfaces may be defined. When VDSL is negotiated, the VDSL-compatible interface is activated; if ADSL is negotiated, then the ADSL-compatible interface is activated.

### 15.2 xDSL connection options on your router

This chapter describes configuration for the two main types of VDSL service on your router:

- PTM encapsulation PPPoE connection
- PTM encapsulation bridged connection

In addition it describes configuration for the three main types of ADSL service:

- ATM encapsulation PPPoA connection
- ATM encapsulation PPPoAoE connection
- ATM encapsulation bridged connection

Configuration consists of two main steps:

- Configuration of the low-level DSL device
- Configuration of the higher layer interface, or interfaces, that use the low-level DSL device

## 15.3 Configuration package used

| Package | Sections                               |
|---------|--|
| network | xdsl-device<br>interface<br>atm-bridge |

## 15.4 Configuring a DSL device

### 15.4.1 Configuring a DSL device using the web UI

The first step in configuring a DSL connection is to configure the low-level DSL device. This populates the xsdl-device configuration section.

The DSL device configuration specifies the DSL mode and relevant options. In general it can be configured in default auto-detect mode, however it can also be configured to operate explicitly in ADSL or VDSL mode.

By default, the router negotiation order is VDSL followed by ADSL. When the line connection is successful, to avoid unnecessary delay, that line mode will be tried first on the next connection attempt.

The web UI automatically configures an xsdl-device configuration section named dsl0.

To configure a DSL device select **Network -> xDSL**. The xDSL interface appears, displaying the configuration parameters. If a DSL link is currently established, you will also see details about the connection status at the top of the page.

**xDSL**  
Configuration of xDSL.

|        |                      |  |
|--------|----------------------|--|
| Status | Chipset              | Lantiq-VRX300 v7.8.0.9.0.1 (ADSL mode)               |
|        | Front End            | Hybrid Type A: Worldwide (POTS)                      |
|        | State                | UP (0x801, showtime TC sync)                         |
|        | Mode                 | ADSL G.992.5 Annex A                                 |
|        | VDSL Profile         | -  |
|        | DSLAM Vector Support | -  |
|        | Vectoring Active     | -  |
|        | ATU-C Info           | Broadcom   |
|        | ATU-R Info           | Virtual Access (Infineon) v7.8.1.5.0.7, 00E0C812D123 |
|        | Data Rate            | 16.546 Mb/s / 765 Kb/s                               |
|        | Max Rate             | 16.516 Mb/s / 1.065 Mb/s                             |
|        | Line Attenuation     | 22.3 dB / 9.5 dB                                     |
|        | Signal Attenuation   | 22.3 dB / 9.5 dB                                     |
|        | Noise Margin         | 6 dB / 15.2 dB                                       |
|        | Transmit Power       | 17.5 dB / 12 dB                                      |
|        | Interleave Depth     | 192 / 8  |
|        | Last Error           | Comms problem (protocol): timeout, fwcode=65         |
|        | Previous Error       | Comms problem (protocol): timeout, fwcode=315        |
|        | Uptime               | 11724 seconds  |

Enabled

DSL line mode

VDSL Encapsulation mode

VDSL Annex

VDSL Vectoring

ADSL Encapsulation mode

ADSL Annex

Handshake Tone Groups

Figure 75: The xDSL configuration page

| Web Field/UCI/Package Option  | Description   |          |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
|---|---|----------|-------------|-----|-------------------|----------------------------|--------|-------------------|----------------------------|----------|--------------|------------------|------|--------------|-----------------|---|---------------|--|---|----------------|---------|-----|-----------------|--------|----|-----------------|------|------|-----------------|---------|-----|-----------------|------|----|-----------------|------|------|-----------------|----------|---|-----------------|---------|-----|-----------------|--------|----|-----------------|-----------|-------|-------------|------|-----|
| Web: Enabled<br>UCI: network.dsl0.enabled<br>Opt: enabled                               | Enables a DSL device.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0        | Disabled.   | 1   | Enabled.          |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| 0   | Disabled.   |          |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| 1   | Enabled.  |          |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Web: DSL line mode<br>UCI: network.dsl0.line_mode<br>Opt: line_mode                     | Defines the DSL line mode. Select <b>Auto</b> .<br><table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Auto</td> <td>Automatically detect mode</td> <td>auto</td> </tr> <tr> <td>VDSL</td> <td>VDSL mode</td> <td>vdsl</td> </tr> <tr> <td>ADSL</td> <td>ADSL mode</td> <td>adsl</td> </tr> </tbody> </table>  | Web      | Description | UCI | Auto              | Automatically detect mode  | auto   | VDSL              | VDSL mode                  | vdsl     | ADSL         | ADSL mode        | adsl |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Web   | Description   | UCI      |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Auto  | Automatically detect mode   | auto     |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| VDSL  | VDSL mode   | vdsl     |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| ADSL  | ADSL mode   | adsl     |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Web: VDSL Encapsulation mode<br>UCI: network.dsl0.vdsl_xfer_mode<br>Opt: vdsl_xfer_mode | Defines the VDSL encapsulation mode. Select <b>PTM/EFM</b> .<br><table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>PTM/EFM</td> <td>Packet transfer mode</td> <td>ptm</td> </tr> <tr> <td>ATM</td> <td>Asynchronous transfer mode</td> <td>atm</td> </tr> </tbody> </table>   | Web      | Description | UCI | PTM/EFM           | Packet transfer mode       | ptm    | ATM               | Asynchronous transfer mode | atm      |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Web   | Description   | UCI      |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| PTM/EFM   | Packet transfer mode  | ptm      |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| ATM   | Asynchronous transfer mode  | atm      |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Web: VDSL Annex<br>UCI: network.dsl0.vdsl_annex<br>Opt: vdsl_annex                      | Defines the VDSL annex. Select <b>Auto</b> .<br><table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Auto</td> <td>Automatically detect</td> <td>auto</td> </tr> <tr> <td>Annex A</td> <td>Annex A - North America</td> <td>a</td> </tr> <tr> <td>Annex B</td> <td>Annex B - Europe</td> <td>b</td> </tr> <tr> <td>Annex C</td> <td>Annex C - Japan</td> <td>c</td> </tr> </tbody> </table>   | Web      | Description | UCI | Auto              | Automatically detect       | auto   | Annex A           | Annex A - North America    | a        | Annex B      | Annex B - Europe | b    | Annex C      | Annex C - Japan | c |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Web   | Description   | UCI      |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Auto  | Automatically detect  | auto     |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Annex A   | Annex A - North America   | a        |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Annex B   | Annex B - Europe  | b        |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Annex C   | Annex C - Japan   | c        |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Web: VDSL Vectoring<br>UCI: network.dsl0.vdsl_vectoring<br>Opt: vdsl_vectoring          | Defines the VDSL vectoring.<br>VDSL vectoring is a VDSL feature that improves performance when multiple VDSL connections share a single cable bundle.<br>Select <b>Normal</b> .<br><table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Normal</td> <td>G.993.5</td> <td>normal</td> </tr> <tr> <td>Friendly</td> <td>Annex Y G.993.2</td> <td>friendly</td> </tr> <tr> <td>Off</td> <td>Off</td> <td>off</td> </tr> </tbody> </table>  | Web      | Description | UCI | Normal            | G.993.5                    | normal | Friendly          | Annex Y G.993.2            | friendly | Off          | Off              | off  |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Web   | Description   | UCI      |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Normal  | G.993.5   | normal   |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Friendly  | Annex Y G.993.2   | friendly |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Off   | Off   | off      |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Web: ADSL Encapsulation mode<br>UCI: network.dsl0.adsl_xfer_mode<br>Opt: adsl_xfer_mode | Defines the ADSL encapsulation mode. Select <b>ATM</b> .<br><table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>ATM</td> <td>Asynchronous transfer mode</td> <td>atm</td> </tr> <tr> <td>PTM/EFM</td> <td>Packet transfer mode</td> <td>ptm</td> </tr> </tbody> </table>   | Web      | Description | UCI | ATM               | Asynchronous transfer mode | atm    | PTM/EFM           | Packet transfer mode       | ptm      |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Web   | Description   | UCI      |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| ATM   | Asynchronous transfer mode  | atm      |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| PTM/EFM   | Packet transfer mode  | ptm      |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Web: ADSL Annex<br>UCI: network.dsl0.adsl_annex<br>Opt: adsl_annex                      | Defines the ADSL annex.<br><table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Annex A+L+M (all)</td> <td></td> <td>a</td> </tr> <tr> <td>Annex B + J (all)</td> <td></td> <td>bj</td> </tr> <tr> <td>Annex B only</td> <td></td> <td>b</td> </tr> <tr> <td>Annex J only</td> <td></td> <td>j</td> </tr> <tr> <td>Annex M (all)</td> <td></td> <td>m</td> </tr> <tr> <td>Annex A G992.5</td> <td>ADSL 2+</td> <td>a2p</td> </tr> <tr> <td>Annex A G.992.3</td> <td>ADSL 2</td> <td>a2</td> </tr> <tr> <td>Annex A G.992.1</td> <td>ADSL</td> <td>admt</td> </tr> <tr> <td>Annex B G.992.5</td> <td>ADSL 2+</td> <td>b2p</td> </tr> <tr> <td>Annex B G.992.3</td> <td>ADSL</td> <td>b2</td> </tr> <tr> <td>Annex B G.992.1</td> <td>ADSL</td> <td>bdmt</td> </tr> <tr> <td>Annex L G.992.3</td> <td>READSL 2</td> <td>l</td> </tr> <tr> <td>Annex M G.992.5</td> <td>ADSL 2+</td> <td>m2p</td> </tr> <tr> <td>Annex M G.992.3</td> <td>ADSL 2</td> <td>m2</td> </tr> <tr> <td>Annex A G.992.2</td> <td>ADSL Lite</td> <td>alite</td> </tr> <tr> <td>ANSI T1.413</td> <td>ADSL</td> <td>at1</td> </tr> </tbody> </table> | Web      | Description | UCI | Annex A+L+M (all) |                            | a      | Annex B + J (all) |                            | bj       | Annex B only |                  | b    | Annex J only |                 | j | Annex M (all) |  | m | Annex A G992.5 | ADSL 2+ | a2p | Annex A G.992.3 | ADSL 2 | a2 | Annex A G.992.1 | ADSL | admt | Annex B G.992.5 | ADSL 2+ | b2p | Annex B G.992.3 | ADSL | b2 | Annex B G.992.1 | ADSL | bdmt | Annex L G.992.3 | READSL 2 | l | Annex M G.992.5 | ADSL 2+ | m2p | Annex M G.992.3 | ADSL 2 | m2 | Annex A G.992.2 | ADSL Lite | alite | ANSI T1.413 | ADSL | at1 |
| Web   | Description   | UCI      |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Annex A+L+M (all)   |   | a        |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Annex B + J (all)   |   | bj       |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Annex B only  |   | b        |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Annex J only  |   | j        |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Annex M (all)   |   | m        |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Annex A G992.5  | ADSL 2+   | a2p      |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Annex A G.992.3   | ADSL 2  | a2       |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Annex A G.992.1   | ADSL  | admt     |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Annex B G.992.5   | ADSL 2+   | b2p      |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Annex B G.992.3   | ADSL  | b2       |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Annex B G.992.1   | ADSL  | bdmt     |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Annex L G.992.3   | READSL 2  | l        |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Annex M G.992.5   | ADSL 2+   | m2p      |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Annex M G.992.3   | ADSL 2  | m2       |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| Annex A G.992.2   | ADSL Lite   | alite    |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |
| ANSI T1.413   | ADSL  | at1      |             |     |                   |                            |        |                   |                            |          |              |                  |      |              |                 |   |               |  |   |                |         |     |                 |        |    |                 |      |      |                 |         |     |                 |      |    |                 |      |      |                 |          |   |                 |         |     |                 |        |    |                 |           |       |             |      |     |

| <p>Web: Handshake Tone Groups<br/>UCI: network.dsl0.handshake_tone<br/>Opt: handshake_tone</p> | <p>Defines the handshake tone groups.</p> <p>The handshaking tones allow some control over the tones used during the initial establishment of a DSL connection. In some cases, restricting the tones used can provide better compatibility with other subscribers sharing the same cable bundle. In other cases, for example, group 'av', extending the tone range used can improve compatibility with fussy DSLAMs.</p> <p>Select <b>Auto</b>.</p> <table border="1" data-bbox="683 427 1390 663"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Auto</td> <td>Automatically detect</td> <td>auto</td> </tr> <tr> <td>A43C+j43+A43</td> <td></td> <td>a</td> </tr> <tr> <td>A43C+j43+A43+V43</td> <td></td> <td>av</td> </tr> <tr> <td>B43+B43C</td> <td></td> <td>b</td> </tr> <tr> <td>B43+B43C+V43</td> <td></td> <td>bv</td> </tr> </tbody> </table> | Web  | Description | UCI | Auto | Automatically detect      | auto | A43C+j43+A43 |           | a    | A43C+j43+A43+V43 |           | av   | B43+B43C |  | b | B43+B43C+V43 |  | bv |
|--|---|------|-------------|-----|------|---------------------------|------|--------------|-----------|------|------------------|-----------|------|----------|--|---|--------------|--|----|
| Web  | Description   | UCI  |             |     |      |                           |      |              |           |      |                  |           |      |          |  |   |              |  |    |
| Auto   | Automatically detect  | auto |             |     |      |                           |      |              |           |      |                  |           |      |          |  |   |              |  |    |
| A43C+j43+A43   |   | a    |             |     |      |                           |      |              |           |      |                  |           |      |          |  |   |              |  |    |
| A43C+j43+A43+V43   |   | av   |             |     |      |                           |      |              |           |      |                  |           |      |          |  |   |              |  |    |
| B43+B43C   |   | b    |             |     |      |                           |      |              |           |      |                  |           |      |          |  |   |              |  |    |
| B43+B43C+V43   |   | bv   |             |     |      |                           |      |              |           |      |                  |           |      |          |  |   |              |  |    |
| <p>Web: n/a<br/>UCI: network.dsl0.auto_default<br/>Opt: auto_default</p>                       | <p>Defines the DSL default line mode to use on first connection attempt.</p> <p><b>Note:</b> when configured as auto, the default line mode will be automatically set when a successful connection is established.</p> <table border="1" data-bbox="683 786 1390 922"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Auto</td> <td>Automatically detect mode</td> <td>auto</td> </tr> <tr> <td>VDSL</td> <td>VDSL mode</td> <td>vdsl</td> </tr> <tr> <td>ADSL</td> <td>ADSL mode</td> <td>adsl</td> </tr> </tbody> </table>   | Web  | Description | UCI | Auto | Automatically detect mode | auto | VDSL         | VDSL mode | vdsl | ADSL             | ADSL mode | adsl |          |  |   |              |  |    |
| Web  | Description   | UCI  |             |     |      |                           |      |              |           |      |                  |           |      |          |  |   |              |  |    |
| Auto   | Automatically detect mode   | auto |             |     |      |                           |      |              |           |      |                  |           |      |          |  |   |              |  |    |
| VDSL   | VDSL mode   | vdsl |             |     |      |                           |      |              |           |      |                  |           |      |          |  |   |              |  |    |
| ADSL   | ADSL mode   | adsl |             |     |      |                           |      |              |           |      |                  |           |      |          |  |   |              |  |    |

**Table 45: Information table for xDSL settings**

**Note:** in the absence of a low-level DSL device configuration (xdsl-device config section), the router will check for an adsl-device section for backward compatibility of older model ADSL configurations. If an older ADSL configuration is found, the router configures the DSL device for ADSL-only operation in ATM mode. Otherwise, the DSL sub system is disabled.

## 15.4.2 Configuring the DSL device using the command line

To configure an xDSL device use the xsdl-device configuration section in the network package /etc/config/network.

The name of the xsdl-device section determines the physical DSL port this device section refers to using the format `dslX`, where `X` is the DSL port number. The GW2300, GW6600V and GW7600V routers currently only support one DSL port so you must configure this as **dsl0**.

### 15.4.2.1 DSL device using UCI

```
root@VA_router:~# uci show network
package network
.....
network.dsl0=xsdl-device
network.dsl0.enabled=1
network.dsl0.line_mode=auto
network.dsl0.vdsl_xfer_mode=ptm
network.dsl0.vdsl_annex=auto
```



```
network.dsl0.vdsl_vectoring=normal
network.dsl0.adsl_xfer_mode=atm
network.dsl0.adsl_annex=a
network.dsl0.handshake_tone=auto
```

### 15.4.2.2 DSL device using package options

```
root@VA_router:~# uci export network
package network
.....
config xdsl-device 'dsl0'
    option vdsl_xfer_mode 'ptm'
    option line_mode 'auto'
    option vdsl_annex 'auto'
    option vdsl_vectoring 'normal'
    option adsl_xfer_mode 'atm'
    option adsl_annex 'a'
    option handshake_tone 'auto'
```

## 15.5 Configuring an upper layer for the DSL device

The upper layer configuration required depends on the service provided by your network operator. You can configure multiple distinct upper layer interfaces. If the service is unknown or expected to change from ADSL to VDSL, you must configure two upper layer interfaces.

If VDSL is negotiated by the DSL device, only the VDSL compatible upper layer interface will be activated. If ADSL is negotiated, then only the ADSL compatible upper layer interface is activated.

The router automatically identifies an upper layer VDSL interface as one which has the interface set to **ptm0**. An upper layer ADSL interface is identified as one which has either the protocol PPPoATM or the underlying interface configured as nas0.

This section describes configuration for the two main types of VDSL service on your router:

- PTM encapsulation PPPoE connection
- PTM encapsulation bridged connection

In addition it describes configuration for the three main types of ADSL service:

- ATM encapsulation PPPoA connection
- ATM encapsulation PPPoEoA connection
- ATM encapsulation bridged connection

The following steps assume the low-level xDSL device has been correctly configured.

## 15.5.1 Configuring a VDSL PTM PPPoE connection using the web interface

### 15.5.1.1 Create a new PTM PPPoE interface

To create a new PTM PPPoE interface via the web interface, in the top menu, click **Network -> Interfaces**. The Interfaces overview page appears.

There are three sections in the Interfaces page.

| Section            | Description  |
|--------------------|--|
| Interface Overview | Shows existing interfaces and their status. You can create new, and edit existing, interfaces here.  |
| Port Map           | In this section you can map device ports to Ethernet interfaces. Ports are marked with capital letters starting with 'A'. Type in space-separated port numbers in the port map fields. |
| ATM Bridges        | ATM bridges expose encapsulated Ethernet in AAL5 connections as virtual Linux network interfaces, which can be used in conjunction with DHCP or PPP to dial into the provider network. |

In the Interface Overview section, click **Add new interface**. The Create Interface page appears.

### Create Interface

Name of the new interface:  The allowed characters are: A-Z, a-z, 0-9 and \_

Protocol of the new interface:

Cover the following interface:

- Ethernet Adapter: "eth0" (lan)
- Ethernet Adapter: "eth1"
- Ethernet Adapter: "eth2"
- Ethernet Adapter: "eth3"
- Ethernet Adapter: "eth4"
- Ethernet Adapter: "gretap0"
- Ethernet Adapter: "ip6tnl0"
- Ethernet Adapter: "l2tptun"
- Ethernet Adapter: "lo" (loopback)
- Ethernet Adapter: "ptm0"
- Ethernet Adapter: "tunl0"
- Ethernet Adapter: "wwan0"
- Custom Interface:

Note: If you select an interface in this menu which is already a part of another network, it will be moved from that network to this network.

Figure 76: The create interface page

| Web Field/UCI/Package Option  | Description   |          |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
|---|---|----------|-------------|-----|--------|--|--------|-------------|---|------|-----------|-------------|------|------------------------|---------------------------|------|----------------|-------------------------------------|------|-----|--|-----|-----|-----|-----|------|-----------------------------|------|--------|----------------------------|--------|-----|-------------------------|-----|-----|------------------------------------|------|-------|-------------------|-------|---------|--------------|-------|---------------------|---|----|-----------------|---------------|----------|------|----------------|------|
| Web: Name of the new interface<br>UCI:<br>Opt:                                  | Type the name of the new interface.<br>Allowed characters are A-Z, a-z, 0-9 and _   |          |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Web: Protocol of the new interface<br>UCI: network[..x..].proto<br>Opt: proto   | Protocol type. Select <b>PPPoE</b> . <table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Static</td> <td>Static configuration with fixed address and netmask.</td> <td>static</td> </tr> <tr> <td>DHCP Client</td> <td>Address and netmask are assigned by DHCP.</td> <td>dhcp</td> </tr> <tr> <td>Unmanaged</td> <td>Unspecified</td> <td>none</td> </tr> <tr> <td>IPv6-in-IPv4 (RFC4213)</td> <td>Used with tunnel brokers.</td> <td>6in4</td> </tr> <tr> <td>IPv6-over-IPv4</td> <td>Stateless IPv6 over IPv4 transport.</td> <td>6to4</td> </tr> <tr> <td>GRE</td> <td>Generic Routing Encapsulation protocol</td> <td>gre</td> </tr> <tr> <td>IOT</td> <td>IOT</td> <td>iot</td> </tr> <tr> <td>L2TP</td> <td>Layer 2 Tunnelling Protocol</td> <td>l2tp</td> </tr> <tr> <td>L2TPv3</td> <td>L2TPv3 Tunnelling Protocol</td> <td>l2tpv3</td> </tr> <tr> <td>PPP</td> <td>Point to Point Protocol</td> <td>ppp</td> </tr> <tr> <td>PtP</td> <td>Point to Point Tunnelling Protocol</td> <td>pptp</td> </tr> <tr> <td>PPPoE</td> <td>PPP over Ethernet</td> <td>pppoe</td> </tr> <tr> <td>PPPoATM</td> <td>PPP over ATM</td> <td>pppoa</td> </tr> <tr> <td>LTE/UMTS/GPRS/EV-DO</td> <td>CDMA, UMTS or GPRS connection using an AT-style 3G modem.</td> <td>3g</td> </tr> <tr> <td>PPP(PSTN-Modem)</td> <td>PPP v90 modem</td> <td>pppmodem</td> </tr> <tr> <td>SLIP</td> <td>Serial Line IP</td> <td>slip</td> </tr> </tbody> </table> | Web      | Description | UCI | Static | Static configuration with fixed address and netmask. | static | DHCP Client | Address and netmask are assigned by DHCP. | dhcp | Unmanaged | Unspecified | none | IPv6-in-IPv4 (RFC4213) | Used with tunnel brokers. | 6in4 | IPv6-over-IPv4 | Stateless IPv6 over IPv4 transport. | 6to4 | GRE | Generic Routing Encapsulation protocol | gre | IOT | IOT | iot | L2TP | Layer 2 Tunnelling Protocol | l2tp | L2TPv3 | L2TPv3 Tunnelling Protocol | l2tpv3 | PPP | Point to Point Protocol | ppp | PtP | Point to Point Tunnelling Protocol | pptp | PPPoE | PPP over Ethernet | pppoe | PPPoATM | PPP over ATM | pppoa | LTE/UMTS/GPRS/EV-DO | CDMA, UMTS or GPRS connection using an AT-style 3G modem. | 3g | PPP(PSTN-Modem) | PPP v90 modem | pppmodem | SLIP | Serial Line IP | slip |
| Web   | Description   | UCI      |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Static  | Static configuration with fixed address and netmask.  | static   |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| DHCP Client   | Address and netmask are assigned by DHCP.   | dhcp     |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Unmanaged   | Unspecified   | none     |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| IPv6-in-IPv4 (RFC4213)  | Used with tunnel brokers.   | 6in4     |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| IPv6-over-IPv4  | Stateless IPv6 over IPv4 transport.   | 6to4     |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| GRE   | Generic Routing Encapsulation protocol  | gre      |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| IOT   | IOT   | iot      |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| L2TP  | Layer 2 Tunnelling Protocol   | l2tp     |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| L2TPv3  | L2TPv3 Tunnelling Protocol  | l2tpv3   |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPP   | Point to Point Protocol   | ppp      |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PtP   | Point to Point Tunnelling Protocol  | pptp     |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPPoE   | PPP over Ethernet   | pppoe    |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPPoATM   | PPP over ATM  | pppoa    |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| LTE/UMTS/GPRS/EV-DO   | CDMA, UMTS or GPRS connection using an AT-style 3G modem.   | 3g       |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPP(PSTN-Modem)   | PPP v90 modem   | pppmodem |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| SLIP  | Serial Line IP  | slip     |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Web: Cover the following interface<br>UCI: network[..x..].ifname<br>Opt: ifname | Select <b>Ethernet Adapter: ptm0</b> .  |          |             |     |        |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |     |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |

**Table 46: Information table for create a new interface section**

For normal operation, select **ptm0**.

If you are configuring a service on a particular VLAN associated with ptm0, you should instead select **Custom Interface** and enter the interface name as **ptm0.X**, where X is the VLAN number to be used. For example, **ptm0.100** configures the entry to use VLAN 100 on the PTM interface.

When you configure a VLAN in this way, you do not need to configure a separate entry for the underlying ptm0 interface; it will be created automatically.

You may configure multiple upper level interfaces associated with ptm0, as long as they all use distinct VLANs.


Once your device is selected, click **Submit**. The Interfaces page appears.

## Interfaces - VDSLPPPOE

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).


### Common Configuration


General Setup   **Advanced Settings**   Physical Settings   Firewall Settings

Status  `ptm0`   RX: 0.00 B (0 Pkts.)  
TX: 0.00 B (0 Pkts.)

Protocol

PAP/CHAP username

PAP/CHAP password  

Access Concentrator   *Leave empty to autodetect*


Service Name   *Leave empty to autodetect*

Figure 77: The new interface page

| Web Field/UCI/Package Option  | Description  |
|---|--|
| Web: Protocol of the new interface<br>UCI: network[..x..].proto<br>Opt: proto | Protocol type. This shows the protocol selected for this interface.<br>Leave as PPPoE. |
| Web: PAP/CHAP username<br>UCI: network[..x..].username<br>Opt: username       | Type the <b>PAP/CHAP</b> username.   |
| Web: PAP/CHAP password<br>UCI: network[..x..].password<br>Opt: password       | Type the <b>PAP/CHAP</b> password.   |
| Web: Access Concentrator<br>UCI: network[..x..].acname<br>Opt: acname         | Leave this field empty to autodetect, or type the <b>AC name</b> .                     |
| Web: Service name<br>UCI: network[..x..].service<br>Opt: service              | Leave this field empty to autodetect, or type the <b>Service name</b> .                |

Table 47: Information table for the new PPPoEoA interface

### 15.5.1.2 PPPoE advanced settings

**Common Configuration**

General Setup | **Advanced Settings** | Physical Settings | Firewall Settings

---

Bring up on boot

Monitor interface state  This interface state would be reported to VA Monitor via keep-alive

Enable IPv6 negotiation on the PPP link

Use default gateway  If unchecked, no default route is configured

Use gateway metric

IPv6 Mode

Use DNS servers advertised by peer  If unchecked, the advertised DNS server addresses are ignored

LCP echo failure threshold  Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures

LCP echo interval  Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold

Inactivity timeout  Close inactive connection after the given amount of seconds, use 0 to persist connection

Dependant interfaces  VDSLPPPOE:   loopback:

Check interfaces which should start after this interface is started and stop after this interface is stopped

SNMP Alias ifindex  Alias ifindex SNMP agent. Alias indexes are present at 1000 offset. So setting 1 here will create snmp ifTable entry 1001. Useful when interface creates new linux interface on every startup (e.g. ppp interface). With this set the interface could be monitored via constant snmp agent interface table entry

VRF  Assign interface to this VRF

Figure 78: The PPPoEoA advanced settings page

| Web Field/UCI/Package Option   | Description  |   |           |       |          |
|--|--|---|-----------|-------|----------|
| Web: Bring up on boot<br>UCI: network.[...].auto<br>Opt: auto                        | Enables the interface to connect automatically on boot up. This option is enabled by default.<br><table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0 | Disabled. | 1     | Enabled. |
| 0  | Disabled.  |   |           |       |          |
| 1  | Enabled.   |   |           |       |          |
| Web: Monitor interface state<br>UCI: network.[...].monitored.<br>Opt: monitored      | Enabled if the status of the interface is presented on the monitoring platform.<br><table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>               | 0 | Disabled. | 1     | Enabled. |
| 0  | Disabled.  |   |           |       |          |
| 1  | Enabled.   |   |           |       |          |
| Web: Enable IPv6 negotiation on the PPP link<br>UCI: network.[...].ipv6<br>Opt: ipv6 | Enables IPv6 negotiation on the PPP<br><table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0 | Disabled. | 1     | Enabled. |
| 0  | Disabled.  |   |           |       |          |
| 1  | Enabled.   |   |           |       |          |
| Web: Use default gateway<br>UCI: network.[...].defaultroute<br>Opt: defaultroute     | If unchecked, no default route is configured.<br><table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0 | Disabled. | 1     | Enabled. |
| 0  | Disabled.  |   |           |       |          |
| 1  | Enabled.   |   |           |       |          |
| Web: Use gateway metric<br>UCI: network.[...].metric<br>Opt: metric                  | Defines the route metric for this default route. Lower metrics take priority.<br><table border="1" style="width: 100%;"> <tr> <td>0</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>                              | 0 |           | Range |          |
| 0  |  |   |           |       |          |
| Range  |  |   |           |       |          |

| <p>Web: IPv6 Mode<br/>UCI: network.3G.ipv6mode<br/>Opt: ipv6mode</p>                                  | <p>Defines the IPv6 address assignment approach for this interface.</p> <table border="1" data-bbox="676 226 1396 450"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>None</td> <td>No dynamic assignment</td> <td>none</td> </tr> <tr> <td>DHCPv6</td> <td>DHCP address assignment</td> <td>dhcp</td> </tr> <tr> <td>RA</td> <td>Router Advertisement (RA) assignment</td> <td>ra</td> </tr> <tr> <td>DHCPv6 after RA</td> <td>Wait for RA, then start DHCP</td> <td>ra_then_dhcp</td> </tr> </tbody> </table>   | Web          | Description                   | UCI   | None              | No dynamic assignment | none             | DHCPv6 | DHCP address assignment | dhcp | RA            | Router Advertisement (RA) assignment | ra | DHCPv6 after RA | Wait for RA, then start DHCP | ra_then_dhcp |
|---|---|--------------|-------------------------------|-------|-------------------|-----------------------|------------------|--------|-------------------------|------|---------------|--------------------------------------|----|-----------------|------------------------------|--------------|
| Web   | Description   | UCI          |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| None  | No dynamic assignment   | none         |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| DHCPv6  | DHCP address assignment   | dhcp         |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| RA  | Router Advertisement (RA) assignment  | ra           |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| DHCPv6 after RA   | Wait for RA, then start DHCP  | ra_then_dhcp |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| <p>Web: Use DNS servers advertised by peer<br/>UCI: network[..x..].peerdns<br/>Opt: peerdns</p>       | <p>If unchecked, DNS from a peer will not be accepted.</p> <table border="1" data-bbox="676 495 1332 562"> <tbody> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </tbody> </table>   | 0            | Disabled.                     | 1     | Enabled.          |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| 0   | Disabled.   |              |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| 1   | Enabled.  |              |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| <p>Web: LCP echo failure threshold<br/>UCI: network[..x..].keepalive<br/>Opt: keepalive</p>           | <p>Presumes a peer to be dead after a given amount of LCP echo failures. Use <b>0</b> to ignore failures.</p> <table border="1" data-bbox="676 622 1332 689"> <tbody> <tr> <td>Range</td> <td></td> </tr> <tr> <td>0</td> <td></td> </tr> </tbody> </table>   | Range        |                               | 0     |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| Range   |   |              |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| 0   |   |              |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| <p>Web: LCP echo internal<br/>UCI: network[..x..].keepalive<br/>Opt: keepalive</p>                    | <p>Sends LCP echo requests at the given interval in seconds; only effective in conjunction with failure threshold.</p> <table border="1" data-bbox="676 750 1332 817"> <tbody> <tr> <td>Range</td> <td></td> </tr> <tr> <td>5</td> <td></td> </tr> </tbody> </table>  | Range        |                               | 5     |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| Range   |   |              |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| 5   |   |              |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| <p>Web: Inactivity timeout<br/>UCI: network[..x..].demand<br/>Opt: demand</p>                         | <p>Closes an inactive connection after the given amount of seconds. Use <b>0</b> to persist the connection.</p> <table border="1" data-bbox="676 891 1332 945"> <tbody> <tr> <td>Range</td> <td></td> </tr> <tr> <td>0</td> <td></td> </tr> </tbody> </table>   | Range        |                               | 0     |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| Range   |   |              |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| 0   |   |              |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| <p>Web: Dependant Interfaces<br/>UCI: network[..x..].dependants<br/>Opt: dependants</p>               | <p>Lists interfaces that are dependant on this parent interface. Dependant interfaces will go down when the parent interface is down and will start or restart when parent interface starts. Separate multiple interfaces by a space when using UCI. Example: <code>option dependants 'PPPADSL MOBILE'</code><br/>This replaces the following previous options in child interfaces.</p> <table border="1" data-bbox="676 1153 1396 1323"> <tbody> <tr> <td>gre</td> <td>option local_interface</td> </tr> <tr> <td>lt2p</td> <td>option src_ipaddr</td> </tr> <tr> <td>iot</td> <td>option wan1 wan2</td> </tr> <tr> <td>6in4</td> <td>option ipaddr</td> </tr> <tr> <td>6to4</td> <td>option ipaddr</td> </tr> </tbody> </table> | gre          | option local_interface        | lt2p  | option src_ipaddr | iot                   | option wan1 wan2 | 6in4   | option ipaddr           | 6to4 | option ipaddr |                                      |    |                 |                              |              |
| gre   | option local_interface  |              |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| lt2p  | option src_ipaddr   |              |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| iot   | option wan1 wan2  |              |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| 6in4  | option ipaddr   |              |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| 6to4  | option ipaddr   |              |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| <p>Web: SNMP Alias ifindex<br/>UCI: network[..x..].snmp_alias_ifindex<br/>Opt: snmp_alias_ifindex</p> | <p>Defines a static SNMP interface alias index for this interface, that can be polled via the SNMP interface index (<code>snmp_alias_ifindex+1000</code>). See the 'Configuring SNMP' section for more information.</p> <table border="1" data-bbox="676 1442 1332 1509"> <tbody> <tr> <td>Blank</td> <td>No SNMP interface alias index</td> </tr> <tr> <td>Range</td> <td>0 - 4294966295</td> </tr> </tbody> </table>  | Blank        | No SNMP interface alias index | Range | 0 - 4294966295    |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| Blank   | No SNMP interface alias index   |              |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| Range   | 0 - 4294966295  |              |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| <p>Web: VRF<br/>UCI: network[..x..].vrf<br/>Opt: vrf</p>  | <p>Defines the VRF for this interface.</p> <table border="1" data-bbox="676 1547 1332 1619"> <tbody> <tr> <td>Blank</td> <td>No VRF</td> </tr> <tr> <td>Range</td> <td></td> </tr> </tbody> </table>  | Blank        | No VRF                        | Range |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| Blank   | No VRF  |              |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |
| Range   |   |              |                               |       |                   |                       |                  |        |                         |      |               |                                      |    |                 |                              |              |

Table 48: Information table for PPPoA advanced settings

### 15.5.1.3 PPPoE physical settings

Figure 79: The PPPoE physical settings page

| Web Field/UCI/Package Option  | Description  |   |           |   |          |
|---|--|---|-----------|---|----------|
| Web: Interface<br>UCI: network.[..x..].ifname<br>Opt: ifname            | Select <b>Ethernet Adapter: ptm0</b> .   |   |           |   |          |
| Web: Auto Negotiation<br>UCI: network.[..x..].autoneg<br>Opt: monitored | Defines when auto negotiation is enabled on an Ethernet port. Only valid for Ethernet switch interfaces. Leave as <b>enabled</b> . <table border="1"> <tbody> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </tbody> </table> | 0 | Disabled. | 1 | Enabled. |
| 0   | Disabled.  |   |           |   |          |
| 1   | Enabled.   |   |           |   |          |

Table 49: Information table for PPPoA physical settings

### 15.5.1.4 PPPoE firewall settings

Use this section to select the firewall zone you want to assign to this interface. For VDSL connections, this will usually be WAN, though you may create a custom zone if you wish.

Select **unspecified** to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

Click **Save & Apply**.

Figure 80: The interfaces page firewall settings tab

## 15.5.2 Configuring a VDSL PTM PPPoE connection using command line

To configure the VDSL PPPoE upper interface use the interface configuration section in the network package `/etc/config/network`.

### 15.5.2.1 VDSL PTM PPPoE using UCI

```
root@VA_router:~# uci show network
package network
.....
network.VDSLPPPOE=interface
network.VDSLPPPOE.proto=pppoe
network.VDSLPPPOE.ifname=ptm0
network.VDSLPPPOE.username=va@pppoe.com
network.VDSLPPPOE.password=dsl_password
network.VDSLPPPOE.ac=test
network.VDSLPPPOE.service=test
network.VDSLPPPOE.defaultroute=1
network.VDSLPPPOE.metric=1
```

### 15.5.2.2 VDSL PTM PPPoE using package options

```
root@VA_router:~# uci show network
package network
.....
config interface 'VDSLPPPOE'
    option proto 'pppoe'
    option ifname 'ptm0'
    option username 'test5@pppoe.com'
    option password 'dsl_password'
    option ac 'test'
    option service 'test'
    option defaultroute '1'
    option metric '1'
```



## 15.5.3 Configuring a VDSL PTM bridged connection with static IP using the web interface

### 15.5.3.1 Create a new static IP interface

To create a new VDSL PTM bridged interface with static IP via the web interface, in the top menu, click **Network -> Interfaces**. The Interfaces overview page appears.

There are three sections in the Interfaces page.

| Section            | Description  |
|--------------------|--|
| Interface Overview | Shows existing interfaces and their status. You can create new, and edit existing interfaces here.   |
| Port Map           | In this section you can map device ports to Ethernet interfaces. Ports are marked with capital letters starting with 'A'. Type in space separated port numbers in the port map fields. |
| ATM Bridges        | ATM bridges expose encapsulated Ethernet in AAL5 connections as virtual Linux network interfaces, which can be used in conjunction with DHCP or PPP to dial into the provider network. |

In the Interface Overview section, click **Add new interface**. The Create Interface page appears.

### Create Interface

Name of the new interface:  The allowed characters are: a-z, A-Z, 0-9 and \_

Protocol of the new interface:

Create a bridge over multiple interfaces:

Cover the following interface:

- Ethernet Adapter: "eth0" (lan)
- Ethernet Adapter: "eth1" (lan2)
- Ethernet Adapter: "eth2"
- Ethernet Adapter: "eth3"
- Ethernet Adapter: "eth4"
- Ethernet Adapter: "gretap0"
- Ethernet Adapter: "ip6tnl0"
- Ethernet Adapter: "lo" (loopback)
- Ethernet Adapter: "ptm0"
- Ethernet Adapter: "tunl0"
- Ethernet Adapter: "wwan0"
- Custom Interface:

Note: If you select an interface in this menu which is already a part of another network, it will be moved from that network to this network.

Figure 81: The create interface page

| Web Field/UCI/Package Option   | Description   |                     |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
|--|---|---------------------|--------------------|--------|--|--|--------|-------------|---|------|-----------|-------------|------|------------------------|---------------------------|------|----------------|-------------------------------------|------|-----|--|-----|-----|-----|-----|------|-----------------------------|------|--------|----------------------------|--------|-----|-------------------------|-----|------|------------------------------------|------|-------|-------------------|-------|---------|--------------|-------|---------------------|---|----|-----------------|---------------|----------|------|----------------|------|
| Web: Name of the new interface<br>UCI: network[..x..]<br>Opt:[..x..]                   | Allowed characters are A-Z, a-z, 0-9 and _  |                     |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Web: Protocol of the new interface<br>UCI: network[..x..].proto<br>Opt: proto          | Protocol type. Select <b>Static address</b> . <table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Static address</td> <td>Static configuration with fixed address and netmask.</td> <td>static</td> </tr> <tr> <td>DHCP Client</td> <td>Address and netmask are assigned by DHCP.</td> <td>dhcp</td> </tr> <tr> <td>Unmanaged</td> <td>Unspecified</td> <td>none</td> </tr> <tr> <td>IPv6-in-IPv4 (RFC4213)</td> <td>Used with tunnel brokers.</td> <td>6in4</td> </tr> <tr> <td>IPv6-over-IPv4</td> <td>Stateless IPv6 over IPv4 transport.</td> <td>6to4</td> </tr> <tr> <td>GRE</td> <td>Generic Routing Encapsulation protocol</td> <td>gre</td> </tr> <tr> <td>IOT</td> <td>IOT</td> <td>iot</td> </tr> <tr> <td>L2TP</td> <td>Layer 2 Tunnelling Protocol</td> <td>l2tp</td> </tr> <tr> <td>L2TPv3</td> <td>L2TPv3 Tunnelling Protocol</td> <td>l2tpv3</td> </tr> <tr> <td>PPP</td> <td>Point to Point Protocol</td> <td>ppp</td> </tr> <tr> <td>PPtP</td> <td>Point to Point Tunnelling Protocol</td> <td>pptp</td> </tr> <tr> <td>PPPoE</td> <td>PPP over Ethernet</td> <td>pppoe</td> </tr> <tr> <td>PPPoATM</td> <td>PPP over ATM</td> <td>pppoa</td> </tr> <tr> <td>LTE/UMTS/GPRS/EV-DO</td> <td>CDMA, UMTS or GPRS connection using an AT-style 3G modem.</td> <td>3g</td> </tr> <tr> <td>PPP(PSTN-Modem)</td> <td>PPP v90 modem</td> <td>pppmodem</td> </tr> <tr> <td>SLIP</td> <td>Serial Line IP</td> <td>slip</td> </tr> </tbody> </table> | Web                 | Description        | UCI    | Static address                                   | Static configuration with fixed address and netmask. | static | DHCP Client | Address and netmask are assigned by DHCP. | dhcp | Unmanaged | Unspecified | none | IPv6-in-IPv4 (RFC4213) | Used with tunnel brokers. | 6in4 | IPv6-over-IPv4 | Stateless IPv6 over IPv4 transport. | 6to4 | GRE | Generic Routing Encapsulation protocol | gre | IOT | IOT | iot | L2TP | Layer 2 Tunnelling Protocol | l2tp | L2TPv3 | L2TPv3 Tunnelling Protocol | l2tpv3 | PPP | Point to Point Protocol | ppp | PPtP | Point to Point Tunnelling Protocol | pptp | PPPoE | PPP over Ethernet | pppoe | PPPoATM | PPP over ATM | pppoa | LTE/UMTS/GPRS/EV-DO | CDMA, UMTS or GPRS connection using an AT-style 3G modem. | 3g | PPP(PSTN-Modem) | PPP v90 modem | pppmodem | SLIP | Serial Line IP | slip |
| Web  | Description   | UCI                 |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Static address   | Static configuration with fixed address and netmask.  | static              |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| DHCP Client  | Address and netmask are assigned by DHCP.   | dhcp                |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Unmanaged  | Unspecified   | none                |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| IPv6-in-IPv4 (RFC4213)   | Used with tunnel brokers.   | 6in4                |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| IPv6-over-IPv4   | Stateless IPv6 over IPv4 transport.   | 6to4                |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| GRE  | Generic Routing Encapsulation protocol  | gre                 |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| IOT  | IOT   | iot                 |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| L2TP   | Layer 2 Tunnelling Protocol   | l2tp                |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| L2TPv3   | L2TPv3 Tunnelling Protocol  | l2tpv3              |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPP  | Point to Point Protocol   | ppp                 |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPtP   | Point to Point Tunnelling Protocol  | pptp                |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPPoE  | PPP over Ethernet   | pppoe               |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPPoATM  | PPP over ATM  | pppoa               |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| LTE/UMTS/GPRS/EV-DO  | CDMA, UMTS or GPRS connection using an AT-style 3G modem.   | 3g                  |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPP(PSTN-Modem)  | PPP v90 modem   | pppmodem            |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| SLIP   | Serial Line IP  | slip                |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Web: Create a bridge over multiple interfaces<br>UCI: network[..x..].type<br>Opt: type | Enables a bridge between two interfaces. Leave as <b>disabled</b> . <table border="1"> <tbody> <tr> <td>No option /disabled</td> <td>Standard interface</td> </tr> <tr> <td>bridge</td> <td>A bridge containing the given ifname is created.</td> </tr> </tbody> </table>   | No option /disabled | Standard interface | bridge | A bridge containing the given ifname is created. |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| No option /disabled  | Standard interface  |                     |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| bridge   | A bridge containing the given ifname is created.  |                     |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Web: Cover the following interface<br>UCI: network[..x..].ifname<br>Opt: ifname        | Select <b>Ethernet Adapter: ptm0</b> .  |                     |                    |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |

**Table 50: Information table for creating a static interface**

For normal operation, select **ptm0**.

If you are configuring a service on a particular VLAN associated with ptm0, you should instead select **Custom Interface** and enter the interface name as **ptm0.X**, where X is the VLAN number to be used. For example, ptm0.100 configures the entry to use VLAN 100 on the PTM interface.

When you configure a VLAN in this way, you do not need to configure a separate entry for the underlying ptm0 interface, it will be created automatically.

You may configure multiple upper level interfaces associated with ptm0, as long as they all use distinct VLANs.

Once your device is selected, click **Submit**. The Interfaces page appears.

### Common Configuration

General Setup
Advanced Settings
Physical Settings
Firewall Settings

Status

ptm0

**MAC Address:** 00:E0:C8:E5:1C:91

RX: 0.00 B (0 Pkts.)

TX: 0.00 B (0 Pkts.)

Protocol Static address ▼

IPv4 address

IPv4 netmask ▼

IPv4 gateway

IPv4 broadcast

Use custom DNS servers  +

Accept router advertisements

Send router solicitations

IPv6 address

IPv6 gateway

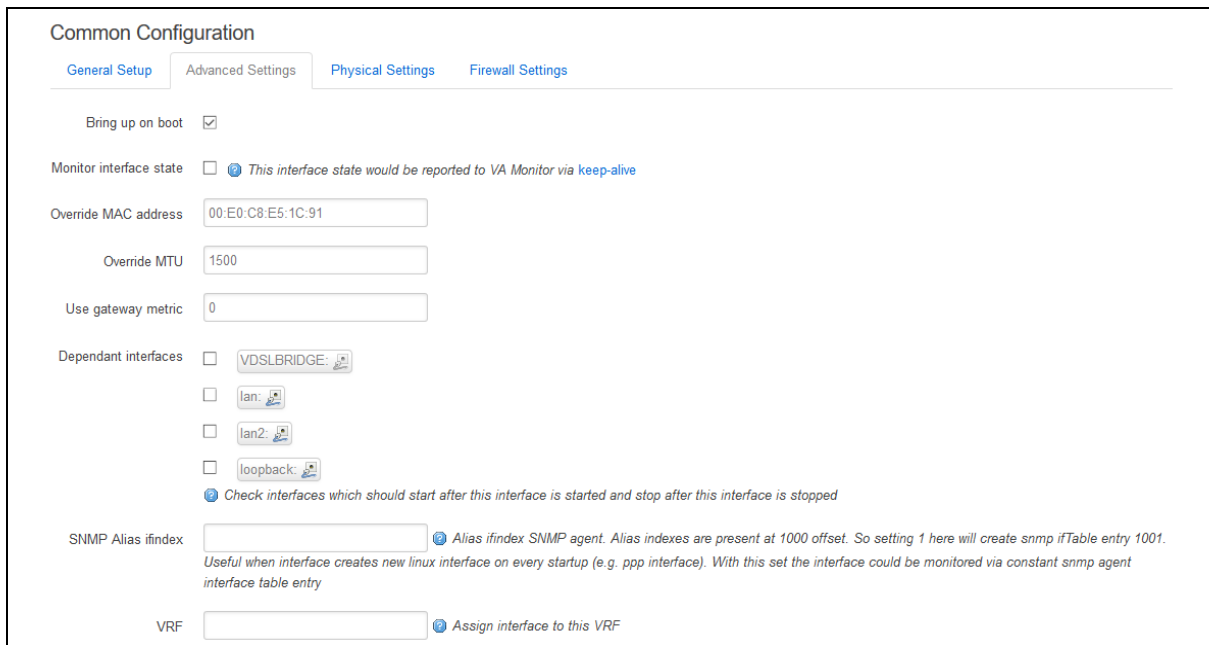
Figure 82: The new static interface page

| Web Field/UCI/Package Option   | Description   |
|--|---|
| Web: Protocol of the new interface<br>UCI: network[..x..].proto<br>Opt: proto        | Protocol type. The protocol shows the one selected for this interface.                        |
| Web: IPv4 address<br>UCI: network[..x..].ipaddrOpt:ipaddr                            | Type the <b>IP address</b> .  |
| Web: IPv4 netmask<br>UCI: network[..x..].netmask<br>Opt: netmask                     | Type or choose <b>netmask</b> .   |
| Web: IPv4 gateway<br>UCI: network[..x..].gateway<br>Opt: gateway                     | Leave this field empty or type the <b>gateway address</b> .                                   |
| Web: IPv4 broadcast<br>UCI: network[..x..].broadcast<br>Opt: broadcast               | Leave this field empty to autodetect, or type <b>broadcast IP address</b> .                   |
| Web: Use custom DNS servers<br>UCI: network[..x..].dns<br>Opt: dns                   | Leave this field empty to autodetect, or type <b>DNS IP address</b> .                         |
| Web: Accept router advertisements<br>UCI: network[..x..].accept_ra<br>Opt: accept_ra | Accept router advertisement for ipv6 addresses. Leave this field empty if ipv6 is not needed. |

|  |   |
|--|---|
| Web: IPv6 address<br>UCI: network[..x..].ip6addr<br>Opt: ip6addr | IPv6 address. Leave this field empty if ipv6 is not needed.   |
| Web: IPv6 gateway<br>UCI: network[..x..].ip6gw<br>Opt: ip6gw     | Ipv6 gateway address. Leave this field empty if ipv6 is not needed.                                     |
| Web: IP-Aliases<br>UCI: network[..x..]<br>Opt: [...]             | Provide an arbitrary name for alias interface. Leave this field blank if alias interface is not needed. |
| Web: Setup DHCP Server<br>UCI: N/A<br>Opt: N/A                   | Leave this field blank if DHCP server is not needed on this interface.                                  |

**Table 51: Information table for the new static interface**

### 15.5.3.2 Bridged connection with static IP: advanced settings



**Figure 83: The advanced settings section**

| Web Field/UCI/Package Option  | Description  |      |            |       |          |
|---|--|------|------------|-------|----------|
| Web: Bring up on boot<br>UCI: network[..x..].auto<br>Opt: auto                  | Select this option if you want the interface to start after boot up.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0    | Disabled.  | 1     | Enabled. |
| 0   | Disabled.  |      |            |       |          |
| 1   | Enabled.   |      |            |       |          |
| Web: Monitor interface state<br>UCI: network[..x..].monitored<br>Opt: monitored | This interface state will be reported to VA monitor via Keepalive.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0    | Disabled.  | 1     | Enabled. |
| 0   | Disabled.  |      |            |       |          |
| 1   | Enabled.   |      |            |       |          |
| Web: Override MAC address<br>UCI: network[..x..].macaddr<br>Opt: macaddr        | Specifies the MAC address of the interface.<br>Leave this field blank if the MAC address of the bridge interface should be copied from Ethernet interface.                           |      |            |       |          |
| Web: Override MTU<br>UCI: network[..x..].mtu<br>Opt: mtu                        | Optionally set up MTU size on the segment.<br><table border="1"> <tr> <td>1500</td> <td>1500 bytes</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>                           | 1500 | 1500 bytes | Range |          |
| 1500  | 1500 bytes   |      |            |       |          |
| Range   |  |      |            |       |          |

|  |   |       |                               |       |                   |     |                  |      |               |      |               |
|--|---|-------|-------------------------------|-------|-------------------|-----|------------------|------|---------------|------|---------------|
| <p>Web: Dependant Interfaces<br/> UCI: network[..x..].dependants<br/> Opt: dependants</p>                    | <p>Lists interfaces that are dependant on this parent interface. Dependant interfaces will go down when parent interface is down and will start or restart when parent interface starts.<br/> Separate multiple interfaces by a space when using UCI.<br/> Example: <code>option dependants 'PPPADSL MOBILE'</code><br/> This replaces the following previous options in child interfaces.</p> <table border="1" data-bbox="683 383 1390 562"> <tr> <td>gre</td> <td>option local_interface</td> </tr> <tr> <td>lt2p</td> <td>option src_ipaddr</td> </tr> <tr> <td>iot</td> <td>option wan1 wan2</td> </tr> <tr> <td>6in4</td> <td>option ipaddr</td> </tr> <tr> <td>6to4</td> <td>option ipaddr</td> </tr> </table> | gre   | option local_interface        | lt2p  | option src_ipaddr | iot | option wan1 wan2 | 6in4 | option ipaddr | 6to4 | option ipaddr |
| gre  | option local_interface  |       |                               |       |                   |     |                  |      |               |      |               |
| lt2p   | option src_ipaddr   |       |                               |       |                   |     |                  |      |               |      |               |
| iot  | option wan1 wan2  |       |                               |       |                   |     |                  |      |               |      |               |
| 6in4   | option ipaddr   |       |                               |       |                   |     |                  |      |               |      |               |
| 6to4   | option ipaddr   |       |                               |       |                   |     |                  |      |               |      |               |
| <p>Web: SNMP Alias ifindex<br/> UCI:<br/> network[..x..].snmp_alias_ifindex<br/> Opt: snmp_alias_ifindex</p> | <p>Defines a static SNMP interface alias index for this interface, that can be polled via the SNMP interface index (<code>snmp_alias_ifindex+1000</code>). For more information, read the chapter 'Configuring SNMP'.</p> <table border="1" data-bbox="683 674 1331 745"> <tr> <td>Blank</td> <td>No SNMP interface alias index</td> </tr> <tr> <td>Range</td> <td>0 - 4294966295</td> </tr> </table>   | Blank | No SNMP interface alias index | Range | 0 - 4294966295    |     |                  |      |               |      |               |
| Blank  | No SNMP interface alias index   |       |                               |       |                   |     |                  |      |               |      |               |
| Range  | 0 - 4294966295  |       |                               |       |                   |     |                  |      |               |      |               |
| <p>Web: VRF<br/> UCI: network[..x..].vrf<br/> Opt: vrf</p>   | <p>Defines the VRF for this interface.</p> <table border="1" data-bbox="683 786 1331 848"> <tr> <td>Blank</td> <td>No VRF</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | Blank | No VRF                        | Range |                   |     |                  |      |               |      |               |
| Blank  | No VRF  |       |                               |       |                   |     |                  |      |               |      |               |
| Range  |   |       |                               |       |                   |     |                  |      |               |      |               |

**Table 52: Information table for advanced settings**

### 15.5.3.3 Bridged physical settings

#### Common Configuration

General Setup
Advanced Settings
Physical Settings
Firewall Settings

Bridge interfaces  [?](#) *creates a bridge over specified interface(s)*

VLAN PCP to skb->priority mapping  [?](#) *Space separated list of <pcp>:<priority>*

skb->priority to VLAN PCP mapping  [?](#)

Interface  [?](#) Ethernet Adapter: "eth0" (lan)

[?](#) Ethernet Adapter: "eth1" (lan2)

[?](#) Ethernet Adapter: "eth2"

[?](#) Ethernet Adapter: "eth3"

[?](#) Ethernet Adapter: "eth4"

[?](#) Ethernet Adapter: "gretap0"

[?](#) Ethernet Adapter: "ip6tnl0"

[?](#) Ethernet Adapter: "lo" (loopback)

[?](#) Ethernet Adapter: "ptm0" (VDSLBRIDGE)

[?](#) Ethernet Adapter: "tunl0"

[?](#) Ethernet Adapter: "wwan0"

[?](#) Custom Interface:

Auto Negotiation

**Figure 84: The PPPoE physical settings page**

| Web Field/UCI/Package Option  | Description   |       |           |       |          |
|---|---|-------|-----------|-------|----------|
| Web: Bridge interfaces<br>UCI: network[..x..].type<br>Opt: type   | Enables a bridge between two interfaces.<br>Leave as <b>disabled</b> .<br><table border="1" style="width: 100%;"> <tr> <td style="width: 30px;">0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0     | Disabled. | 1     | Enabled. |
| 0   | Disabled.   |       |           |       |          |
| 1   | Enabled.  |       |           |       |          |
| Web: Enable STP<br>UCI: network[..x..].autoneg<br>Opt: monitored  | Enables Spanning Tree Protocol when bridging interfaces. Only displayed when bridging between two interfaces.<br><table border="1" style="width: 100%;"> <tr> <td style="width: 30px;">0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0     | Disabled. | 1     | Enabled. |
| 0   | Disabled.   |       |           |       |          |
| 1   | Enabled.  |       |           |       |          |
| Web: VLAN PCP to skb->priority mapping<br>UCI: network[..x..].vlan_qos_map_ingress<br>Opt: vlan_qos_map_ingress | Defines the VLAN QOS ingress PCP mapping as a space separated list in the format <pcp>:<priority>. Exampe: option vlan_qos_map_ingress '1:1 2:5'<br>Leave as <b>empty</b> .<br><table border="1" style="width: 100%;"> <tr> <td style="width: 30px;">Empty</td> <td>Disabled.</td> </tr> <tr> <td>Range</td> <td>Enabled.</td> </tr> </table> | Empty | Disabled. | Range | Enabled. |
| Empty   | Disabled.   |       |           |       |          |
| Range   | Enabled.  |       |           |       |          |

|  |   |       |           |       |          |
|--|---|-------|-----------|-------|----------|
| Web: Interface<br>UCI:<br>network[..x..].vlan_qos_map_egress<br>Opt: vlan_qos_map_egress | Defines the VLAN QOS egress PCP mapping as a space separated list in the format <pcp>:<priority>. Exampe:<br>option vlan_qos_map_egress '1:1 2:5'<br>Leave as <b>empty</b> . <table border="1"> <tr> <td>Empty</td> <td>Disabled.</td> </tr> <tr> <td>Range</td> <td>Enabled.</td> </tr> </table> | Empty | Disabled. | Range | Enabled. |
| Empty  | Disabled.   |       |           |       |          |
| Range  | Enabled.  |       |           |       |          |
| Web: Interface<br>UCI: network[..x..].ifname<br>Opt: ifname                              | Select <b>Ethernet Adapter: ptm0</b> .  |       |           |       |          |
| Web: Auto Negotiation<br>UCI: network[..x..].autoneg<br>Opt: monitored                   | Defines when auto negotiation is enabled on an Ethernet port. Only valid for Ethernet switch interfaces.<br>Leave as <b>enabled</b> . <table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0     | Disabled. | 1     | Enabled. |
| 0  | Disabled.   |       |           |       |          |
| 1  | Enabled.  |       |           |       |          |

Table 53: Information table for physical settings

#### 15.5.3.4 Bridged connection with static IP: firewall settings

Use this section to select the firewall zone you want to assign to this interface. For VDSL connections, this will usually be WAN though you may create a custom zone if you wish.

Select **unspecified** to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

Click **Save & Apply**.



Figure 85: The interfaces page firewall settings tab

#### 15.5.4 Configuring a VDSL PTM bridge connection with static IP using command line

A VDSL bridge upper interface is configured using the **interface** configuration section in the network package **/etc/config/network**.

##### 15.5.4.1 VDSL PTM bridge connection using UCI

```
root@VA_router:~# uci show network
network.VDSLBRIDGE=interface
network.VDSLBRIDGE.proto=static
network.VDSLBRIDGE.ifname=ptm0
network.VDSLBRIDGE.monitored=0
network.VDSLBRIDGE.ipaddr= 10.33.4.7
```

```
network.VDSLBRIDGE.netmask=255.255.255.192
network.VDSLBRIDGE.metric=2
```

### 15.5.4.2 VDSL PTM bridge connection using package options

```
root@VA_router:~# uci show network
package network
.....
config interface 'VDSLBRIDGE'
    option proto 'static'
    option ifname 'ptm0'
    option monitored '0'
    option ipaddr '10.33.4.7'
    option netmask '255.255.255.192'
    option metric '1'
```

## 15.5.5 Configuring an ADSL PPPoA connection using the web interface

### 15.5.5.1 Create a new PPPoA interface

To create a new PPPoA interface via the web interface, in the top menu, click **Network -> Interfaces**. The Interfaces overview page appears.

There are three sections in the Interfaces page.

| Section            | Description  |
|--------------------|--|
| Interface Overview | Shows existing interfaces and their status. You can create new, and edit existing, interfaces here.  |
| Port Map           | In this section you can map device ports to Ethernet interfaces. Ports are marked with capital letters starting with 'A'. Type in space separated port numbers in the port map fields. |
| ATM Bridges        | ATM bridges expose encapsulated Ethernet in AAL5 connections as virtual Linux network interfaces, which can be used in conjunction with DHCP or PPP to dial into the provider network. |

In the Interface Overview section, click **Add new interface**. The Create Interface page appears.

Figure 86: The create new interface page



| Web Field/UCI/Package Option  | Description  |          |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
|---|--|----------|-------------|-----|----------------|--|--------|-------------|---|------|-----------|-------------|------|------------------------|---------------------------|------|----------------|-------------------------------------|------|-----|--|-----|-----|-----|-----|------|-----------------------------|------|--------|----------------------------|--------|-----|-------------------------|-----|------|------------------------------------|------|-------|-------------------|-------|---------|--------------|-------|---------------------|---|----|-----------------|---------------|----------|------|----------------|------|
| Web: Name of the new interface<br>UCI: network[..x..]<br>Opt: [..x..]         | Allowed characters are A-Z, a-z, 0-9 and _   |          |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Web: Protocol of the new interface<br>UCI: network[..x..].proto<br>Opt: proto | Protocol type. Select <b>PPPoATM</b> . <table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Static address</td> <td>Static configuration with fixed address and netmask.</td> <td>static</td> </tr> <tr> <td>DHCP Client</td> <td>Address and netmask are assigned by DHCP.</td> <td>dhcp</td> </tr> <tr> <td>Unmanaged</td> <td>Unspecified</td> <td>none</td> </tr> <tr> <td>IPv6-in-IPv4 (RFC4213)</td> <td>Used with tunnel brokers.</td> <td>6in4</td> </tr> <tr> <td>IPv6-over-IPv4</td> <td>Stateless IPv6 over IPv4 transport.</td> <td>6to4</td> </tr> <tr> <td>GRE</td> <td>Generic Routing Encapsulation protocol</td> <td>gre</td> </tr> <tr> <td>IOT</td> <td>IOT</td> <td>iot</td> </tr> <tr> <td>L2TP</td> <td>Layer 2 Tunnelling Protocol</td> <td>l2tp</td> </tr> <tr> <td>L2TPv3</td> <td>L2TPv3 Tunnelling Protocol</td> <td>l2tpv3</td> </tr> <tr> <td>PPP</td> <td>Point to Point Protocol</td> <td>ppp</td> </tr> <tr> <td>PPtP</td> <td>Point to Point Tunnelling Protocol</td> <td>pptp</td> </tr> <tr> <td>PPPoE</td> <td>PPP over Ethernet</td> <td>pppoe</td> </tr> <tr> <td>PPPoATM</td> <td>PPP over ATM</td> <td>pppoa</td> </tr> <tr> <td>LTE/UMTS/GPRS/EV-DO</td> <td>CDMA, UMTS or GPRS connection using an AT-style 3G modem.</td> <td>3g</td> </tr> <tr> <td>PPP(PSTN-Modem)</td> <td>PPP v90 modem</td> <td>pppmodem</td> </tr> <tr> <td>SLIP</td> <td>Serial Line IP</td> <td>slip</td> </tr> </tbody> </table> | Web      | Description | UCI | Static address | Static configuration with fixed address and netmask. | static | DHCP Client | Address and netmask are assigned by DHCP. | dhcp | Unmanaged | Unspecified | none | IPv6-in-IPv4 (RFC4213) | Used with tunnel brokers. | 6in4 | IPv6-over-IPv4 | Stateless IPv6 over IPv4 transport. | 6to4 | GRE | Generic Routing Encapsulation protocol | gre | IOT | IOT | iot | L2TP | Layer 2 Tunnelling Protocol | l2tp | L2TPv3 | L2TPv3 Tunnelling Protocol | l2tpv3 | PPP | Point to Point Protocol | ppp | PPtP | Point to Point Tunnelling Protocol | pptp | PPPoE | PPP over Ethernet | pppoe | PPPoATM | PPP over ATM | pppoa | LTE/UMTS/GPRS/EV-DO | CDMA, UMTS or GPRS connection using an AT-style 3G modem. | 3g | PPP(PSTN-Modem) | PPP v90 modem | pppmodem | SLIP | Serial Line IP | slip |
| Web   | Description  | UCI      |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Static address  | Static configuration with fixed address and netmask.   | static   |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| DHCP Client   | Address and netmask are assigned by DHCP.  | dhcp     |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Unmanaged   | Unspecified  | none     |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| IPv6-in-IPv4 (RFC4213)  | Used with tunnel brokers.  | 6in4     |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| IPv6-over-IPv4  | Stateless IPv6 over IPv4 transport.  | 6to4     |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| GRE   | Generic Routing Encapsulation protocol   | gre      |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| IOT   | IOT  | iot      |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| L2TP  | Layer 2 Tunnelling Protocol  | l2tp     |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| L2TPv3  | L2TPv3 Tunnelling Protocol   | l2tpv3   |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPP   | Point to Point Protocol  | ppp      |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPtP  | Point to Point Tunnelling Protocol   | pptp     |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPPoE   | PPP over Ethernet  | pppoe    |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPPoATM   | PPP over ATM   | pppoa    |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| LTE/UMTS/GPRS/EV-DO   | CDMA, UMTS or GPRS connection using an AT-style 3G modem.  | 3g       |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPP(PSTN-Modem)   | PPP v90 modem  | pppmodem |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| SLIP  | Serial Line IP   | slip     |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |

**Table 54: Information table for the create new interface page**

Click **Submit**. The Common Configuration page appears. There are three sections in the Common Configurations page.

| Section           | Description   |
|-------------------|---|
| General Setup     | Configure the basic interface settings such as protocol, service type, APN information, user name and password. |
| Advanced Settings | Set forwarding mode for the connection.   |
| Firewall settings | Assign a firewall zone to the connection.   |

### 15.5.5.2 PPPoA: general setup

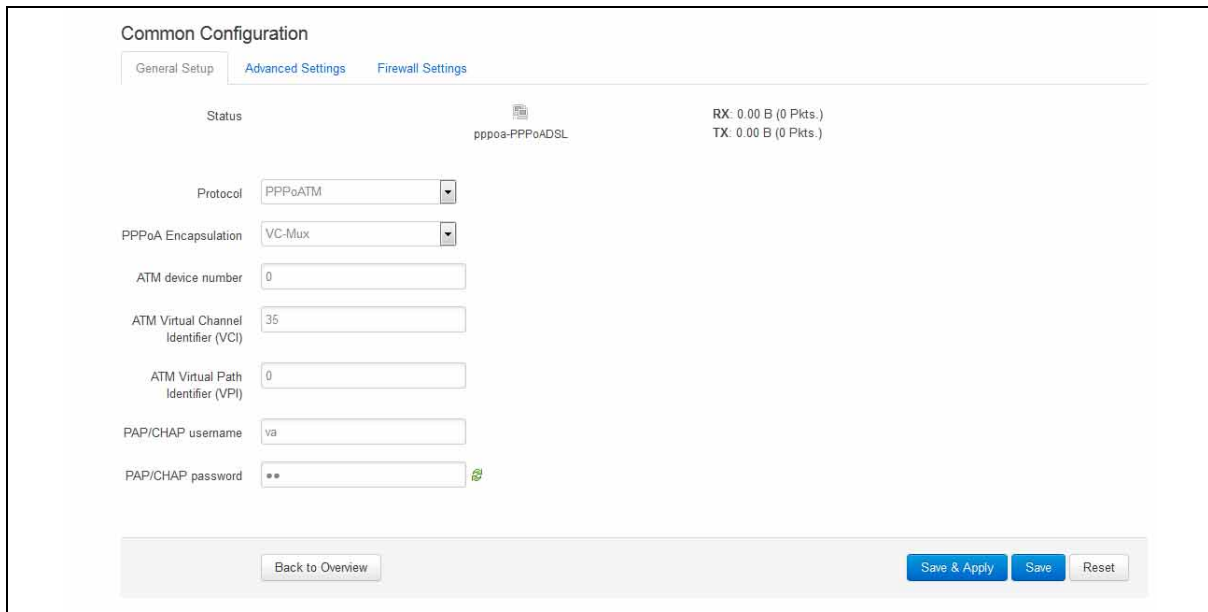


Figure 87: The PPPoA common configuration page

| Web Field/UCI/Package Option  | Description  |       |             |     |     |                      |     |        |                               |    |
|---|--|-------|-------------|-----|-----|----------------------|-----|--------|-------------------------------|----|
| Web: Status<br>UCI: N/A ifconfig<br>Opt: N/A                                    | Shows the current status of the interface.<br><b>Note:</b> run ifconfig command on SSH to check interface status.  |       |             |     |     |                      |     |        |                               |    |
| Web: Protocol<br>UCI: network.[...].proto<br>Opt: proto                         | Protocol type. The PPPoA interface protocol is showing as the selected interface.  |       |             |     |     |                      |     |        |                               |    |
| Web: PPPoA Encapsulation<br>UCI: network.[...].encaps<br>Opt: encaps            | Defines the ATM encapsulation mode. This determines the way packets are turned into frames for transmission over ATM. This is determined by the service provided by the network operator.<br>Select <b>VC-Mux</b> . <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>LLC</td> <td>Logical Link Control</td> <td>llc</td> </tr> <tr> <td>VC-Mux</td> <td>Virtual circuit multiplexing.</td> <td>vc</td> </tr> </tbody> </table> | Web   | Description | UCI | LLC | Logical Link Control | llc | VC-Mux | Virtual circuit multiplexing. | vc |
| Web   | Description  | UCI   |             |     |     |                      |     |        |                               |    |
| LLC   | Logical Link Control   | llc   |             |     |     |                      |     |        |                               |    |
| VC-Mux  | Virtual circuit multiplexing.  | vc    |             |     |     |                      |     |        |                               |    |
| Web: ATM Device Number<br>UCI: network.[...]. atmdev<br>Opt: atmdev             | Sets the ATM device number. Set to <b>0</b> . <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td style="width: 50px;">0</td> <td style="width: 50px;"></td> </tr> <tr> <td>1</td> <td></td> </tr> </tbody> </table>   | 0     |             | 1   |     |                      |     |        |                               |    |
| 0   |  |       |             |     |     |                      |     |        |                               |    |
| 1   |  |       |             |     |     |                      |     |        |                               |    |
| Web: ATM Virtual Channel Identifier (VCI)<br>UCI: network.[...].vci<br>Opt: vci | Defines the VPI. <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td style="width: 50px;">Range</td> <td style="width: 50px;"></td> </tr> <tr> <td>35</td> <td></td> </tr> </tbody> </table>   | Range |             | 35  |     |                      |     |        |                               |    |
| Range   |  |       |             |     |     |                      |     |        |                               |    |
| 35  |  |       |             |     |     |                      |     |        |                               |    |
| Web: ATM Virtual Path Identifier (VPI)<br>UCI: network.[...].vpi<br>Opt: vpi    | Defines the VCI. <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td style="width: 50px;">Range</td> <td style="width: 50px;"></td> </tr> <tr> <td>8</td> <td></td> </tr> </tbody> </table>  | Range |             | 8   |     |                      |     |        |                               |    |
| Range   |  |       |             |     |     |                      |     |        |                               |    |
| 8   |  |       |             |     |     |                      |     |        |                               |    |
| Web: PAP/CHAP username<br>UCI: network.[...].username<br>Opt: username          | User name used to authenticate PPP connection.   |       |             |     |     |                      |     |        |                               |    |
| Web: PAP/CHAP password<br>UCI: network. [...].password<br>Opt: password         | Password used to connect to authenticate PPP connection.   |       |             |     |     |                      |     |        |                               |    |

Table 55: Information table for PPPoA general set up

### 15.5.5.3 PPPoA: advanced settings

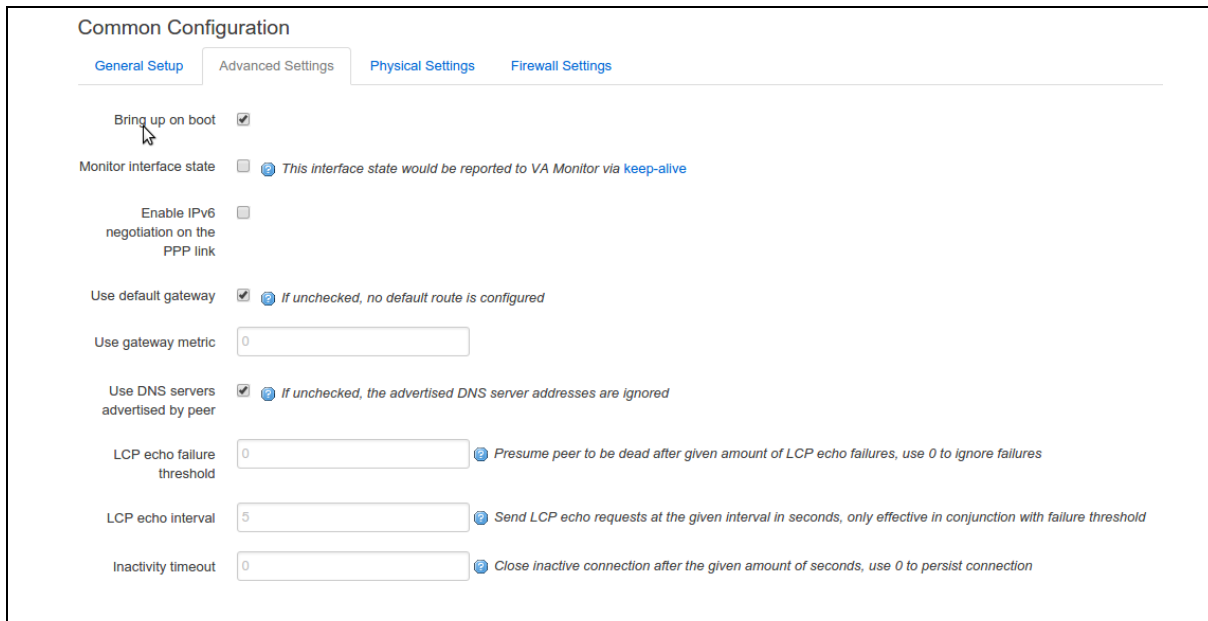


Figure 88: The PPPoA advanced settings page

| Web Field/UCI/Package Option   | Description   |   |           |       |          |
|--|---|---|-----------|-------|----------|
| Web: Bring up on boot<br>UCI: network[...].auto<br>Opt: auto                         | Enables the interface to connect automatically on boot up. This option is enabled by default.<br><table border="1"> <tr><td>0</td><td>Disabled.</td></tr> <tr><td>1</td><td>Enabled.</td></tr> </table>   | 0 | Disabled. | 1     | Enabled. |
| 0  | Disabled.   |   |           |       |          |
| 1  | Enabled.  |   |           |       |          |
| Web: Monitor interface state<br>UCI: network[...].monitored.<br>Opt: monitored       | Enabled if status of interface is presented on the monitoring platform.<br><table border="1"> <tr><td>0</td><td>Disabled.</td></tr> <tr><td>1</td><td>Enabled.</td></tr> </table>   | 0 | Disabled. | 1     | Enabled. |
| 0  | Disabled.   |   |           |       |          |
| 1  | Enabled.  |   |           |       |          |
| Web: Enable IPv6 negotiation on the PPP link<br>UCI: network[...].ipv6<br>Opt: ipv6  | Enable IPv6 negotiation on the PPP.<br><table border="1"> <tr><td>0</td><td>Disabled.</td></tr> <tr><td>1</td><td>Enabled.</td></tr> </table>   | 0 | Disabled. | 1     | Enabled. |
| 0  | Disabled.   |   |           |       |          |
| 1  | Enabled.  |   |           |       |          |
| Web: Use default gateway<br>UCI: network[...].defaultroute<br>Opt: defaultroute      | If disabled, no default route is configured.<br><table border="1"> <tr><td>0</td><td>Disabled.</td></tr> <tr><td>1</td><td>Enabled.</td></tr> </table>  | 0 | Disabled. | 1     | Enabled. |
| 0  | Disabled.   |   |           |       |          |
| 1  | Enabled.  |   |           |       |          |
| Web: Use gateway metric<br>UCI: network[...].metric<br>Opt: metric                   | Defines the route metric for this default route. Lower metrics take priority. This option is only shown when 'Use default gateway' is enabled.<br><table border="1"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>   | 0 |           | Range |          |
| 0  |   |   |           |       |          |
| Range  |   |   |           |       |          |
| Web: Use DNS servers advertised by peer<br>UCI: network[...].peerdns<br>Opt: peerdns | If disabled, DNS from peer will not be accepted.<br><table border="1"> <tr><td>0</td><td>Disabled.</td></tr> <tr><td>1</td><td>Enabled.</td></tr> </table>  | 0 | Disabled. | 1     | Enabled. |
| 0  | Disabled.   |   |           |       |          |
| 1  | Enabled.  |   |           |       |          |
| Web: LCP echo failure threshold<br>UCI: network[...].keepalive<br>Opt: keepalive     | Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures.<br>LCP echo failure threshold and LCP echo interval use the same option using a space separator between the values:<br>option keepalive 'threshold interval'<br>Example:<br>option keepalive '5 1' |   |           |       |          |

|   |  |       |                               |       |                   |     |                  |      |               |      |               |
|---|--|-------|-------------------------------|-------|-------------------|-----|------------------|------|---------------|------|---------------|
| <p>Web: LCP echo interval<br/>UCI: network[..x..].keepalive<br/>Opt: keepalive</p>                    | <p>Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold.</p> <p>LCP echo failure threshold and LCP echo interval use the same option using a space separator between the values:</p> <pre>option keepalive 'threshold interval'</pre> <p>Example:</p> <pre>option keepalive '5 1'</pre>   |       |                               |       |                   |     |                  |      |               |      |               |
| <p>Web: Inactivity timeout<br/>UCI: network[..x..].demand<br/>Opt: demand</p>                         | <p>Closes an inactive connection after the given amount of seconds, use <b>0</b> to persist connection.</p>  |       |                               |       |                   |     |                  |      |               |      |               |
| <p>Web: Dependant Interfaces<br/>UCI: network[..x..].dependants<br/>Opt: dependants</p>               | <p>Lists interfaces that are dependant on this parent interface. Dependant interfaces will go down when parent interface is down and will start or restart when parent interface starts.</p> <p>Separate multiple interfaces by a space when using UCI.</p> <p>Example: <code>option dependants 'PPPADSL MOBILE'</code></p> <p>This replaces the following previous options in child interfaces.</p> <table border="1"> <tr> <td>gre</td> <td>option local_interface</td> </tr> <tr> <td>lt2p</td> <td>option src_ipaddr</td> </tr> <tr> <td>iot</td> <td>option wan1 wan2</td> </tr> <tr> <td>6in4</td> <td>option ipaddr</td> </tr> <tr> <td>6to4</td> <td>option ipaddr</td> </tr> </table> | gre   | option local_interface        | lt2p  | option src_ipaddr | iot | option wan1 wan2 | 6in4 | option ipaddr | 6to4 | option ipaddr |
| gre   | option local_interface   |       |                               |       |                   |     |                  |      |               |      |               |
| lt2p  | option src_ipaddr  |       |                               |       |                   |     |                  |      |               |      |               |
| iot   | option wan1 wan2   |       |                               |       |                   |     |                  |      |               |      |               |
| 6in4  | option ipaddr  |       |                               |       |                   |     |                  |      |               |      |               |
| 6to4  | option ipaddr  |       |                               |       |                   |     |                  |      |               |      |               |
| <p>Web: SNMP Alias ifindex<br/>UCI: network[..x..].snmp_alias_ifindex<br/>Opt: snmp_alias_ifindex</p> | <p>Defines a static SNMP interface alias index for this interface, that can be polled via the SNMP interface index (<code>snmp_alias_ifindex+1000</code>). For more information, read the chapter 'Configuring SNMP'.</p> <table border="1"> <tr> <td>Blank</td> <td>No SNMP interface alias index</td> </tr> <tr> <td>Range</td> <td>0 - 4294966295</td> </tr> </table>   | Blank | No SNMP interface alias index | Range | 0 - 4294966295    |     |                  |      |               |      |               |
| Blank   | No SNMP interface alias index  |       |                               |       |                   |     |                  |      |               |      |               |
| Range   | 0 - 4294966295   |       |                               |       |                   |     |                  |      |               |      |               |
| <p>Web: VRF<br/>UCI: network[..x..].vrf<br/>Opt: vrf</p>  | <p>Defines the VRF for this interface</p> <table border="1"> <tr> <td>Blank</td> <td>No VRF</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | Blank | No VRF                        | Range |                   |     |                  |      |               |      |               |
| Blank   | No VRF   |       |                               |       |                   |     |                  |      |               |      |               |
| Range   |  |       |                               |       |                   |     |                  |      |               |      |               |

Table 56: Information table for PPPoA advanced settings

#### 15.5.5.4 PPPoA: firewall settings

Use this section to select the firewall zone you want to assign to this interface. For ADSL connections, this will usually be WAN, though you may create a custom zone if you wish.

Select **unspecified** to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

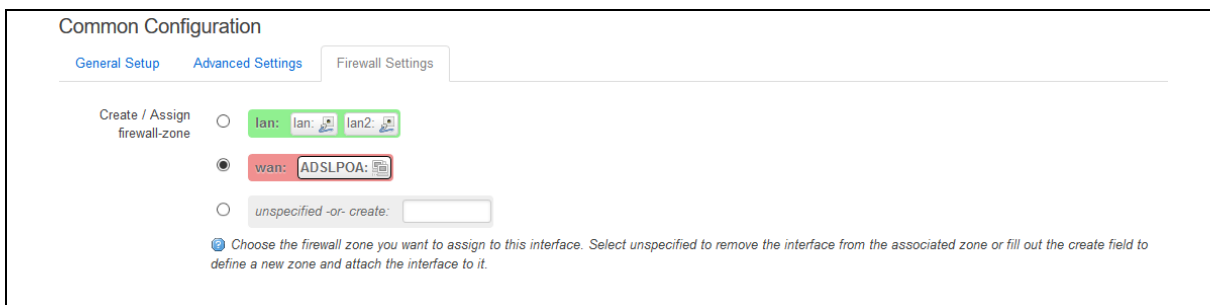


Figure 89: The PPPoA firewall settings page

| Web Field/UCI/Package Option  | Description  |
|---|--|
| <p>Web: Create/Assign firewall zone<br/>UCI: firewall.@zone[2].name<br/>Opt: name</p> | <p>Select existing firewall zone or select unspecified -or-create to create new firewall zone.</p> |

Table 57: Information table for PPPoADSL interface

## 15.5.6 Configuring an ADSL PPPoA connection using command line

An ADSL PPPoA upper layer interface is configured using the interface configuration section in the network package `/etc/config/network`.

### 15.5.6.1 ADSL PPPoA using UCI

```
root@VA_router:~# uci show network
network.ADSLPOA=interface
network.ADSLPOA.proto=pppoe
network.ADSLPOA.encaps=vc
network.ADSLPOA.atmdev=0
network.ADSLPOA.vci=35
network.ADSLPOA.vpi=0
network.ADSLPOA.username=test5@pppoe.com
network.ADSLPOA.password=test5
network.ADSL.metric=1
```

### 15.5.6.2 ADSL PPPoA using package options

```
root@VA_router:~# uci export network
package network
.....
config interface 'ADSLPOA'
    option proto 'pppoe'
    option encaps 'vc'
    option atmdev '0'
    option vci '35'
    option vpi '0'
    option username 'test5@pppoe.com'
    option password 'test5'
    option metric '1'
```

## 15.5.7 Configuring an ADSL PPPoEoA connection using the web interface

An ADSL PPPoEoA connection comprises of two steps:

- Create an ATM bridge
- Create a PPPOE interface

### 15.5.7.1 Create a new ATM bridge

From the top menu select **Network -> Interfaces**. The Interfaces Overview page appears. Scroll down to the bottom of the page until you see the ATM Bridges section. Click **Add**.

### 15.5.7.2 ATM bridges: general setup

Figure 90: The ATM bridges general setup page

| Web Field/UCI/Package Option   | Description  |       |             |     |     |                      |     |        |                               |    |
|--|--|-------|-------------|-----|-----|----------------------|-----|--------|-------------------------------|----|
| Web: ATM Virtual Channel Identifier (VCI)<br>UCI: network.@atm-bridge[x].vci<br>Opt: vci | Type the <b>VCI</b> number.<br><table border="1"> <tr><td>Range</td><td></td></tr> <tr><td>35</td><td></td></tr> </table>  | Range |             | 35  |     |                      |     |        |                               |    |
| Range  |  |       |             |     |     |                      |     |        |                               |    |
| 35   |  |       |             |     |     |                      |     |        |                               |    |
| Web: ATM Virtual Path Identifier (VPI)<br>UCI: network.@atm-bridge[x].vpi<br>Opt: vpi    | Type the <b>VPI</b> number.<br><table border="1"> <tr><td>Range</td><td></td></tr> <tr><td>8</td><td></td></tr> </table>   | Range |             | 8   |     |                      |     |        |                               |    |
| Range  |  |       |             |     |     |                      |     |        |                               |    |
| 8  |  |       |             |     |     |                      |     |        |                               |    |
| Web: Encapsulation mode<br>UCI: network.@atm-bridge[x].encaps<br>Opt: encaps             | Defines the ATM encapsulation mode. This determines the way packets are turned into frames for transmission over ATM. This is determined by the service provided by the network operator.<br>Select <b>LLC</b><br><table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>LLC</td> <td>Logical Link Control</td> <td>llc</td> </tr> <tr> <td>VC-Mux</td> <td>Virtual circuit multiplexing.</td> <td>vc</td> </tr> </tbody> </table> | Web   | Description | UCI | LLC | Logical Link Control | llc | VC-Mux | Virtual circuit multiplexing. | vc |
| Web  | Description  | UCI   |             |     |     |                      |     |        |                               |    |
| LLC  | Logical Link Control   | llc   |             |     |     |                      |     |        |                               |    |
| VC-Mux   | Virtual circuit multiplexing.  | vc    |             |     |     |                      |     |        |                               |    |

Table 58: Information table for ATM bridges

### 15.5.7.3 ATM bridges: advanced settings

Figure 91: The ATM bridges advanced settings page

| Web Field/UCI/Package Option  | Description   |         |             |     |         |  |         |        |  |        |
|---|---|---------|-------------|-----|---------|--|---------|--------|--|--------|
| Web: ATM device number<br>UCI: network.@atm-bridge[x].atmdev<br>Opt: atmdev | Defines the ATM device. Set to <b>0</b> .<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> <tr> <td>0</td> <td></td> </tr> </table>  | Range   |             | 0   |         |  |         |        |  |        |
| Range   |   |         |             |     |         |  |         |        |  |        |
| 0   |   |         |             |     |         |  |         |        |  |        |
| Web: Bridge unit number<br>UCI: network.@atm-bridge[x].unit<br>Opt: unit    | Leave the Bridge unit number. Set to <b>0</b> .<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> <tr> <td>0</td> <td></td> </tr> </table>  | Range   |             | 0   |         |  |         |        |  |        |
| Range   |   |         |             |     |         |  |         |        |  |        |
| 0   |   |         |             |     |         |  |         |        |  |        |
| Web: Forwarding mode<br>UCI: network.@atm-bridge[0].payload<br>Opt: payload | Defines the forwarding mode. Select <b>Bridged</b> .<br><table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Bridged</td> <td>The payload will be a full Ethernet packet with MAC address. Select <b>Bridged</b> for PPPOE and Ethernet bridge configurations.</td> <td>bridged</td> </tr> <tr> <td>Routed</td> <td>Select <b>Routed</b> to route based on IP address.</td> <td>routed</td> </tr> </tbody> </table> | Web     | Description | UCI | Bridged | The payload will be a full Ethernet packet with MAC address. Select <b>Bridged</b> for PPPOE and Ethernet bridge configurations. | bridged | Routed | Select <b>Routed</b> to route based on IP address. | routed |
| Web   | Description   | UCI     |             |     |         |  |         |        |  |        |
| Bridged   | The payload will be a full Ethernet packet with MAC address. Select <b>Bridged</b> for PPPOE and Ethernet bridge configurations.  | bridged |             |     |         |  |         |        |  |        |
| Routed  | Select <b>Routed</b> to route based on IP address.  | routed  |             |     |         |  |         |        |  |        |

**Table 59: Information table for the ATM bridges advanced settings page**

Click **Save**.

#### 15.5.7.4 Create a new PPPoEoA interface

Scroll to the top of the page and click **Add new interface....**the Create Interface page appears.

### Create Interface

Name of the new interface:  ⓘ The allowed characters are: A-Z, a-z, 0-9 and \_

Protocol of the new interface:

Cover the following interface:

- Ethernet Adapter: "eth0" (lan)
- Ethernet Adapter: "eth1" (lan2)
- Ethernet Adapter: "eth2"
- Ethernet Adapter: "eth3"
- Ethernet Adapter: "eth4"
- Ethernet Adapter: "gretap0"
- Ethernet Adapter: "ip6tnl0"
- Ethernet Adapter: "lo" (loopback)
- Ethernet Adapter: "ptm0"
- Ethernet Adapter: "tunl0"
- Ethernet Adapter: "wwan0"
- Custom Interface:

ⓘ Note: If you select an interface in this menu which is already a part of another network, it will be moved from that network to this network.

**Figure 92: The create interface page**

| Web Field/UCI/Package Option  | Description  |          |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
|---|--|----------|-------------|-----|----------------|--|--------|-------------|---|------|-----------|-------------|------|------------------------|---------------------------|------|----------------|-------------------------------------|------|-----|--|-----|-----|-----|-----|------|-----------------------------|------|--------|----------------------------|--------|-----|-------------------------|-----|------|------------------------------------|------|-------|-------------------|-------|---------|--------------|-------|---------------------|---|----|-----------------|---------------|----------|------|----------------|------|
| Web: Name of the new interface<br>UCI:<br>Opt:                                  | Type the name of the new interface.<br>Allowed characters are A-Z, a-z, 0-9 and _  |          |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Web: Protocol of the new interface<br>UCI: network[..x..].proto<br>Opt: proto   | <p>Protocol type. Select <b>PPPoE</b>.</p> <table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Static address</td> <td>Static configuration with fixed address and netmask.</td> <td>static</td> </tr> <tr> <td>DHCP Client</td> <td>Address and netmask are assigned by DHCP.</td> <td>dhcp</td> </tr> <tr> <td>Unmanaged</td> <td>Unspecified</td> <td>none</td> </tr> <tr> <td>IPv6-in-IPv4 (RFC4213)</td> <td>Used with tunnel brokers.</td> <td>6in4</td> </tr> <tr> <td>IPv6-over-IPv4</td> <td>Stateless IPv6 over IPv4 transport.</td> <td>6to4</td> </tr> <tr> <td>GRE</td> <td>Generic Routing Encapsulation protocol</td> <td>gre</td> </tr> <tr> <td>IOT</td> <td>IOT</td> <td>iot</td> </tr> <tr> <td>L2TP</td> <td>Layer 2 Tunnelling Protocol</td> <td>l2tp</td> </tr> <tr> <td>L2TPv3</td> <td>L2TPv3 Tunnelling Protocol</td> <td>l2tpv3</td> </tr> <tr> <td>PPP</td> <td>Point to Point Protocol</td> <td>ppp</td> </tr> <tr> <td>PPtP</td> <td>Point to Point Tunnelling Protocol</td> <td>pptp</td> </tr> <tr> <td>PPPoE</td> <td>PPP over Ethernet</td> <td>pppoe</td> </tr> <tr> <td>PPPoATM</td> <td>PPP over ATM</td> <td>pppoa</td> </tr> <tr> <td>LTE/UMTS/GPRS/EV-DO</td> <td>CDMA, UMTS or GPRS connection using an AT-style 3G modem.</td> <td>3g</td> </tr> <tr> <td>PPP(PSTN-Modem)</td> <td>PPP v90 modem</td> <td>pppmodem</td> </tr> <tr> <td>SLIP</td> <td>Serial Line IP</td> <td>slip</td> </tr> </tbody> </table> | Web      | Description | UCI | Static address | Static configuration with fixed address and netmask. | static | DHCP Client | Address and netmask are assigned by DHCP. | dhcp | Unmanaged | Unspecified | none | IPv6-in-IPv4 (RFC4213) | Used with tunnel brokers. | 6in4 | IPv6-over-IPv4 | Stateless IPv6 over IPv4 transport. | 6to4 | GRE | Generic Routing Encapsulation protocol | gre | IOT | IOT | iot | L2TP | Layer 2 Tunnelling Protocol | l2tp | L2TPv3 | L2TPv3 Tunnelling Protocol | l2tpv3 | PPP | Point to Point Protocol | ppp | PPtP | Point to Point Tunnelling Protocol | pptp | PPPoE | PPP over Ethernet | pppoe | PPPoATM | PPP over ATM | pppoa | LTE/UMTS/GPRS/EV-DO | CDMA, UMTS or GPRS connection using an AT-style 3G modem. | 3g | PPP(PSTN-Modem) | PPP v90 modem | pppmodem | SLIP | Serial Line IP | slip |
| Web   | Description  | UCI      |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Static address  | Static configuration with fixed address and netmask.   | static   |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| DHCP Client   | Address and netmask are assigned by DHCP.  | dhcp     |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Unmanaged   | Unspecified  | none     |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| IPv6-in-IPv4 (RFC4213)  | Used with tunnel brokers.  | 6in4     |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| IPv6-over-IPv4  | Stateless IPv6 over IPv4 transport.  | 6to4     |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| GRE   | Generic Routing Encapsulation protocol   | gre      |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| IOT   | IOT  | iot      |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| L2TP  | Layer 2 Tunnelling Protocol  | l2tp     |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| L2TPv3  | L2TPv3 Tunnelling Protocol   | l2tpv3   |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPP   | Point to Point Protocol  | ppp      |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPtP  | Point to Point Tunnelling Protocol   | pptp     |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPPoE   | PPP over Ethernet  | pppoe    |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPPoATM   | PPP over ATM   | pppoa    |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| LTE/UMTS/GPRS/EV-DO   | CDMA, UMTS or GPRS connection using an AT-style 3G modem.  | 3g       |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPP(PSTN-Modem)   | PPP v90 modem  | pppmodem |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| SLIP  | Serial Line IP   | slip     |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Web: Cover the following interface<br>UCI: network[..x..].ifname<br>Opt: ifname | Select <b>Custom Interface</b> , and then type <b>nas0</b> .   |          |             |     |                |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |

**Table 60: Information table for create a new interface section**

As described previously, select **ptm0** for a standard VDSL interface, or enter a custom interface **ptm0.X**, for example, **ptm0.100** to route traffic via VLAN X over PTM.

Click **Submit**. The Interfaces page appears.

**Figure 93: The new interface page**



| Web Field/UCI/Package Option   | Description   |
|--|---|
| Web: Protocol of the new interface<br>UCI: network.[..x..].proto<br>Opt: proto | Protocol type. The protocol shows the one selected for this interface.  |
| Web: PAP/CHAP username<br>UCI: network.[..x..].username<br>Opt: username       | Type the <b>PAP/CHAP username</b> .                                     |
| Web: PAP/CHAP password<br>UCI: network.[..x..].password<br>Opt: password       | Type the <b>password</b> .  |
| Web: Access Concentrator<br>UCI: network.[..x..].acname<br>Opt: acname         | Leave this field empty to autodetect, or type the <b>AC name</b> .      |
| Web: Service name<br>UCI: network.[..x..].service<br>Opt: service              | Leave this field empty to autodetect, or type the <b>Service name</b> . |

Table 61: Information table for the new PPPoEoA interface

### 15.5.7.5 PPPoEoA advanced settings

Figure 94: The PPPoEoA advanced settings page

| Web Field/UCI/Package Option   | Description   |   |           |   |          |
|--|---|---|-----------|---|----------|
| Web: Bring up on boot<br>UCI: network.[..x..].auto<br>Opt: auto                        | Enables the interface to connect automatically on boot up. This option is enabled by default.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0 | Disabled. | 1 | Enabled. |
| 0  | Disabled.   |   |           |   |          |
| 1  | Enabled.  |   |           |   |          |
| Web: Monitor interface state<br>UCI: network.[..x..].monitored.<br>Opt: monitored      | Enabled if the status of the interface is presented on the monitoring platform.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>               | 0 | Disabled. | 1 | Enabled. |
| 0  | Disabled.   |   |           |   |          |
| 1  | Enabled.  |   |           |   |          |
| Web: Enable IPv6 negotiation on the PPP link<br>UCI: network.[..x..].ipv6<br>Opt: ipv6 | Enables IPv6 negotiation on the PPP<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0 | Disabled. | 1 | Enabled. |
| 0  | Disabled.   |   |           |   |          |
| 1  | Enabled.  |   |           |   |          |

|  |   |       |                                |       |                   |     |                  |      |               |      |               |
|--|---|-------|--------------------------------|-------|-------------------|-----|------------------|------|---------------|------|---------------|
| Web: Use default gateway<br>UCI: network[..x..].defaultroute<br>Opt: defaultroute            | If unchecked, no default route is configured.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0     | Disabled.                      | 1     | Enabled.          |     |                  |      |               |      |               |
| 0  | Disabled.   |       |                                |       |                   |     |                  |      |               |      |               |
| 1  | Enabled.  |       |                                |       |                   |     |                  |      |               |      |               |
| Web: Use gateway metric<br>UCI: network[..x..].metric<br>Opt: metric                         | Defines the route metric for this default route. Lower metrics take priority.<br><table border="1"> <tr> <td>0</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 0     |                                | Range |                   |     |                  |      |               |      |               |
| 0  |   |       |                                |       |                   |     |                  |      |               |      |               |
| Range  |   |       |                                |       |                   |     |                  |      |               |      |               |
| Web: Use DNS servers advertised by peer<br>UCI: network[..x..].peerdns<br>Opt: peerdns       | If unchecked, DNS from peer will not be accepted.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0     | Disabled.                      | 1     | Enabled.          |     |                  |      |               |      |               |
| 0  | Disabled.   |       |                                |       |                   |     |                  |      |               |      |               |
| 1  | Enabled.  |       |                                |       |                   |     |                  |      |               |      |               |
| Web: LCP echo failure threshold<br>UCI: network[..x..].keepalive<br>Opt: keepalive           | Presumes peer to be dead after given amount of LCP echo failures. Use <b>0</b> to ignore failures.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> <tr> <td>0</td> <td></td> </tr> </table>   | Range |                                | 0     |                   |     |                  |      |               |      |               |
| Range  |   |       |                                |       |                   |     |                  |      |               |      |               |
| 0  |   |       |                                |       |                   |     |                  |      |               |      |               |
| Web: LCP echo interval<br>UCI: network[..x..].keepalive<br>Opt: keepalive                    | Sends LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> <tr> <td>5</td> <td></td> </tr> </table>  | Range |                                | 5     |                   |     |                  |      |               |      |               |
| Range  |   |       |                                |       |                   |     |                  |      |               |      |               |
| 5  |   |       |                                |       |                   |     |                  |      |               |      |               |
| Web: Inactivity timeout<br>UCI: network[..x..].demand<br>Opt: demand                         | Closes inactive connection after the given amount of seconds. Use <b>0</b> to persist connection.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> <tr> <td>0</td> <td></td> </tr> </table>  | Range |                                | 0     |                   |     |                  |      |               |      |               |
| Range  |   |       |                                |       |                   |     |                  |      |               |      |               |
| 0  |   |       |                                |       |                   |     |                  |      |               |      |               |
| Web: Dependant Interfaces<br>UCI: network[..x..].dependants<br>Opt: dependants               | Lists interfaces that are dependant on this parent interface. Dependant interfaces will go down when parent interface is down and will start or restart when parent interface starts.<br>Separate multiple interfaces by a space when using UCI.<br>Example: option dependants 'PPPADSL MOBILE'<br>This replaces the following previous options in child interfaces.<br><table border="1"> <tr> <td>gre</td> <td>option local_interface</td> </tr> <tr> <td>lt2p</td> <td>option src_ipaddr</td> </tr> <tr> <td>iot</td> <td>option wan1 wan2</td> </tr> <tr> <td>6in4</td> <td>option ipaddr</td> </tr> <tr> <td>6to4</td> <td>option ipaddr</td> </tr> </table> | gre   | option local_interface         | lt2p  | option src_ipaddr | iot | option wan1 wan2 | 6in4 | option ipaddr | 6to4 | option ipaddr |
| gre  | option local_interface  |       |                                |       |                   |     |                  |      |               |      |               |
| lt2p   | option src_ipaddr   |       |                                |       |                   |     |                  |      |               |      |               |
| iot  | option wan1 wan2  |       |                                |       |                   |     |                  |      |               |      |               |
| 6in4   | option ipaddr   |       |                                |       |                   |     |                  |      |               |      |               |
| 6to4   | option ipaddr   |       |                                |       |                   |     |                  |      |               |      |               |
| Web: SNMP Alias ifindex<br>UCI: network[..x..].snmp_alias_ifindex<br>Opt: snmp_alias_ifindex | Defines a static SNMP interface alias index for this interface, that can be polled via the SNMP interface index (snmp_alias_ifindex+1000). For more information, read the chapter 'Configuring SNMP'.<br><table border="1"> <tr> <td>Blank</td> <td>No SNMP interface alias index.</td> </tr> <tr> <td>Range</td> <td>0 - 4294966295</td> </tr> </table>  | Blank | No SNMP interface alias index. | Range | 0 - 4294966295    |     |                  |      |               |      |               |
| Blank  | No SNMP interface alias index.  |       |                                |       |                   |     |                  |      |               |      |               |
| Range  | 0 - 4294966295  |       |                                |       |                   |     |                  |      |               |      |               |
| Web: VRF<br>UCI: network[..x..].vrf<br>Opt: vrf  | Defines the VRF for this interface.<br><table border="1"> <tr> <td>Blank</td> <td>No VRF</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | Blank | No VRF                         | Range |                   |     |                  |      |               |      |               |
| Blank  | No VRF  |       |                                |       |                   |     |                  |      |               |      |               |
| Range  |   |       |                                |       |                   |     |                  |      |               |      |               |

Table 62: Information table for PPPoEoA advanced settings

### 15.5.7.6 PPPoEoA physical settings

Figure 95: The PPPoE physical settings page

| Web Field/UCI/Package Option  | Description   |   |           |   |          |
|---|---|---|-----------|---|----------|
| Web: Interface<br>UCI: network.[...].ifname<br>Opt: ifname            | Select <b>Ethernet Adapter: nas0</b> .  |   |           |   |          |
| Web: Auto Negotiation<br>UCI: network.[...].autoneg<br>Opt: monitored | Defines when auto negotiation is enabled on an Ethernet port. Only valid for Ethernet switch interfaces. Leave as <b>enabled</b> . <table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0 | Disabled. | 1 | Enabled. |
| 0   | Disabled.   |   |           |   |          |
| 1   | Enabled.  |   |           |   |          |

Table 63: Information table for PPPoA physical settings

### 15.5.7.7 PPPoEoA: firewall settings

Use this section to select the firewall zone you want to assign to this interface. For ADSL connections, this will usually be WAN though you may create a custom zone if you wish.

Select **unspecified** to remove the interface from the associated zone or fill out the **create** field to define a new zone and attach the interface to it.

Click **Save & Apply**.



Figure 96: The interfaces page firewall settings tab

## 15.5.8 Configuring an ADSL PPPoEoA connection using command line

Configure an ADSL PPPoEoA upper layer interface using the interface and atm-bridge configuration sections in the network package /etc/config/network.

### 15.5.8.1 ADSL PPPoEoA using UCI

```
root@VA_router:~# uci show network
network.ADSLPOEOA=interface
network.ADSLPOEOA.proto=pppoe
network.ADSLPOEOA.ifname=nas0
network.ADSLPOEOA.username=test5@pppoe.com
network.ADSLPOEOA.password=test5
network.ADSLPOEOA.ac=test
network.ADSLPOEOA.service=test
network.ADSLPOEOA.defaultroute=1
network.ADSLPOEOA.metric=1
network.@atm-bridge[0]=atm-bridge
network.@atm-bridge[0].unit=0
network.@atm-bridge[0].atmdev=0
network.@atm-bridge[0].encaps=llc
network.@atm-bridge[0].payload=bridged
network.@atm-bridge[0].vci=35
network.@atm-bridge[0].vpi=0
```

### 15.5.8.2 ADSL PPPoEoA using package options

```
root@VA_router:~# uci export network
package network
.....
config interface 'ADSLPOEOA'
    option proto 'pppoe'
    option ifname 'nas0'
```

```

option username 'test5@pppoe.com'
option password 'test5'
option ac 'test'
option service 'test'
option defaultroute '1'
option metric '1'

config atm-bridge
option unit '0'
option atmdev '0'
option encaps 'llc'
option payload 'bridged'
option vci '35'
option vpi '0'

```

### 15.5.9 Configuring an ADSL bridged connection with static IP using the web interface

An ADSL bridged connection comprises of two steps:

- Create an ATM bridge
- Create a bridge interface with static IP

#### 15.5.9.1 Create a new ATM bridge

From the top menu select **Network -> Interfaces**. The Interfaces Overview page appears. Scroll down to the bottom of the page until you see the ATM Bridges section. Click **Add**.

#### 15.5.9.2 ATM bridges: general setup

**ATM Bridges**

ATM bridges expose encapsulated ethernet in AAL5 connections as virtual Linux network interfaces which can be used in conjunction with DHCP or PPP to dial into the provider network.

Delete

General Setup [Advanced Settings](#)

ATM Virtual Channel Identifier (VCI)

ATM Virtual Path Identifier (VPI)

Encapsulation mode

Add

Figure 97: The ATM bridges general setup page

| Web Field/UCI/Package Option   | Description  |       |             |     |     |                      |     |        |                               |    |
|--|--|-------|-------------|-----|-----|----------------------|-----|--------|-------------------------------|----|
| Web: ATM Virtual Channel Identifier (VCI)<br>UCI: network.@atm-bridge[x].vci<br>Opt: vci | Type the <b>VCI</b> number.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> <tr> <td>35</td> <td></td> </tr> </table>  | Range |             | 35  |     |                      |     |        |                               |    |
| Range  |  |       |             |     |     |                      |     |        |                               |    |
| 35   |  |       |             |     |     |                      |     |        |                               |    |
| Web: ATM Virtual Path Identifier (VPI)<br>UCI: network.@atm-bridge[x].vpi<br>Opt: vpi    | Type the <b>VPI</b> number.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> <tr> <td>8</td> <td></td> </tr> </table>   | Range |             | 8   |     |                      |     |        |                               |    |
| Range  |  |       |             |     |     |                      |     |        |                               |    |
| 8  |  |       |             |     |     |                      |     |        |                               |    |
| Web: Encapsulation mode<br>UCI: network.@atm-bridge[x].encaps<br>Opt: encaps             | Defines the ATM encapsulation mode. This determines the way packets are turned into frames for transmission over ATM. This is determined by the service provided by the network operator.<br>Select <b>LLC</b> .<br><table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>LLC</td> <td>Logical Link Control</td> <td>llc</td> </tr> <tr> <td>VC-Mux</td> <td>Virtual circuit multiplexing.</td> <td>vc</td> </tr> </tbody> </table> | Web   | Description | UCI | LLC | Logical Link Control | llc | VC-Mux | Virtual circuit multiplexing. | vc |
| Web  | Description  | UCI   |             |     |     |                      |     |        |                               |    |
| LLC  | Logical Link Control   | llc   |             |     |     |                      |     |        |                               |    |
| VC-Mux   | Virtual circuit multiplexing.  | vc    |             |     |     |                      |     |        |                               |    |

Table 64: Information table for ATM bridges

### 15.5.9.3 ATM bridges: advanced settings

**ATM Bridges**

ATM bridges expose encapsulated ethernet in AAL5 connections as virtual Linux network interfaces which can be used in conjunction with DHCP or PPP to dial into the provider network.

[Delete](#)

[General Setup](#) [Advanced Settings](#)

---

ATM device number

Bridge unit number

Forwarding mode

[Add](#)

[Save & Apply](#) [Save](#) [Reset](#)

Figure 98: The ATM bridges advanced settings page

| Web Field/UCI/Package Option  | Description  |         |             |     |         |  |         |        |   |        |
|---|--|---------|-------------|-----|---------|--|---------|--------|---|--------|
| Web: ATM device number<br>UCI: network.@atm-bridge[x].atmdev<br>Opt: atmdev | Defines the ATM device. Set to <b>0</b> .<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> <tr> <td>0</td> <td></td> </tr> </table>   | Range   |             | 0   |         |  |         |        |   |        |
| Range   |  |         |             |     |         |  |         |        |   |        |
| 0   |  |         |             |     |         |  |         |        |   |        |
| Web: Bridge unit number<br>UCI: network.@atm-bridge[x].unit<br>Opt: unit    | Leaves the bridge unit number. Set to <b>0</b> .<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> <tr> <td>0</td> <td></td> </tr> </table>  | Range   |             | 0   |         |  |         |        |   |        |
| Range   |  |         |             |     |         |  |         |        |   |        |
| 0   |  |         |             |     |         |  |         |        |   |        |
| Web: Forwarding mode<br>UCI: network.@atm-bridge[0].payload<br>Opt: payload | Defines the forwarding mode. Select <b>Bridged</b> .<br><table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Bridged</td> <td>The payload will be a complete Ethernet packet with a MAC address. Select <b>bridged</b> for PPPOE and Ethernet bridge configurations.</td> <td>bridged</td> </tr> <tr> <td>Routed</td> <td>Select <b>Routed</b> to a route based on an IP address.</td> <td>routed</td> </tr> </tbody> </table> | Web     | Description | UCI | Bridged | The payload will be a complete Ethernet packet with a MAC address. Select <b>bridged</b> for PPPOE and Ethernet bridge configurations. | bridged | Routed | Select <b>Routed</b> to a route based on an IP address. | routed |
| Web   | Description  | UCI     |             |     |         |  |         |        |   |        |
| Bridged   | The payload will be a complete Ethernet packet with a MAC address. Select <b>bridged</b> for PPPOE and Ethernet bridge configurations.   | bridged |             |     |         |  |         |        |   |        |
| Routed  | Select <b>Routed</b> to a route based on an IP address.  | routed  |             |     |         |  |         |        |   |        |

Table 65: Information table for the ATM bridges advanced settings page

Click **Save**.

### 15.5.9.4 Create a new Static IP interface

To create a new VDSL PTM bridged interface with static IP via the web interface, in the top menu, click **Network -> Interfaces**. The Interfaces overview page appears.

There are three sections in the Interfaces page.

| Section            | Description  |
|--------------------|--|
| Interface Overview | Shows existing interfaces and their status. You can create new, and edit existing interfaces here.   |
| Port Map           | In this section you can map device ports to Ethernet interfaces. Ports are marked with capital letters starting with 'A'. Type in space separated port numbers in the port map fields. |
| ATM Bridges        | ATM bridges expose encapsulated Ethernet in AAL5 connections as virtual Linux network interfaces, which can be used in conjunction with DHCP or PPP to dial into the provider network. |

In the Interface Overview section, click **Add new interface**. The Create Interface page appears.

### Create Interface

Name of the new interface:  The allowed characters are: A-Z, a-z, 0-9 and \_

Protocol of the new interface:

Create a bridge over multiple interfaces:

Cover the following interface:

- Ethernet Adapter: "eth0" (lan)
- Ethernet Adapter: "eth1" (lan2)
- Ethernet Adapter: "eth2"
- Ethernet Adapter: "eth3"
- Ethernet Adapter: "eth4"
- Ethernet Adapter: "gretap0"
- Ethernet Adapter: "ip6tnl0"
- Ethernet Adapter: "lo" (loopback)
- Ethernet Adapter: "ptm0"
- Ethernet Adapter: "tunl0"
- Ethernet Adapter: "wwan0"
- Custom Interface:

Note: If you select an interface in this menu which is already a part of another network, it will be moved from that network to this network.

**Figure 99: The create interface page**

| Web Field/UCI/Package Option   | Description  |                     |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
|--|--|---------------------|---------------------|--------|--|--|--------|-------------|---|------|-----------|-------------|------|------------------------|---------------------------|------|----------------|-------------------------------------|------|-----|---|-----|-----|-----|-----|------|-----------------------------|------|--------|----------------------------|--------|-----|-------------------------|-----|------|------------------------------------|------|-------|-------------------|-------|---------|--------------|-------|---------------------|---|----|-----------------|---------------|----------|------|----------------|------|
| Web: Name of the new interface<br>UCI: network[..x..]<br>Opt:[..x..]                   | Allowed characters are A-Z, a-z, 0-9 and _   |                     |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Web: Protocol of the new interface<br>UCI: network[..x..].proto<br>Opt: proto          | Protocol type. Select <b>Static address</b> . <table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Static address</td> <td>Static configuration with fixed address and netmask.</td> <td>static</td> </tr> <tr> <td>DHCP Client</td> <td>Address and netmask are assigned by DHCP.</td> <td>dhcp</td> </tr> <tr> <td>Unmanaged</td> <td>Unspecified</td> <td>none</td> </tr> <tr> <td>IPv6-in-IPv4 (RFC4213)</td> <td>Used with tunnel brokers.</td> <td>6in4</td> </tr> <tr> <td>IPv6-over-IPv4</td> <td>Stateless IPv6 over IPv4 transport.</td> <td>6to4</td> </tr> <tr> <td>GRE</td> <td>Generic Routing Encapsulation protocol.</td> <td>gre</td> </tr> <tr> <td>IOT</td> <td>IOT</td> <td>iot</td> </tr> <tr> <td>L2TP</td> <td>Layer 2 Tunnelling Protocol</td> <td>l2tp</td> </tr> <tr> <td>L2TPv3</td> <td>L2TPv3 Tunnelling Protocol</td> <td>l2tpv3</td> </tr> <tr> <td>PPP</td> <td>Point to Point Protocol</td> <td>ppp</td> </tr> <tr> <td>PPtP</td> <td>Point to Point Tunnelling Protocol</td> <td>pptp</td> </tr> <tr> <td>PPPoE</td> <td>PPP over Ethernet</td> <td>pppoe</td> </tr> <tr> <td>PPPoATM</td> <td>PPP over ATM</td> <td>pppoa</td> </tr> <tr> <td>LTE/UMTS/GPRS/EV-DO</td> <td>CDMA, UMTS or GPRS connection using an AT-style 3G modem.</td> <td>3g</td> </tr> <tr> <td>PPP(PSTN-Modem)</td> <td>PPP v90 modem</td> <td>pppmodem</td> </tr> <tr> <td>SLIP</td> <td>Serial Line IP</td> <td>slip</td> </tr> </tbody> </table> | Web                 | Description         | UCI    | Static address                                   | Static configuration with fixed address and netmask. | static | DHCP Client | Address and netmask are assigned by DHCP. | dhcp | Unmanaged | Unspecified | none | IPv6-in-IPv4 (RFC4213) | Used with tunnel brokers. | 6in4 | IPv6-over-IPv4 | Stateless IPv6 over IPv4 transport. | 6to4 | GRE | Generic Routing Encapsulation protocol. | gre | IOT | IOT | iot | L2TP | Layer 2 Tunnelling Protocol | l2tp | L2TPv3 | L2TPv3 Tunnelling Protocol | l2tpv3 | PPP | Point to Point Protocol | ppp | PPtP | Point to Point Tunnelling Protocol | pptp | PPPoE | PPP over Ethernet | pppoe | PPPoATM | PPP over ATM | pppoa | LTE/UMTS/GPRS/EV-DO | CDMA, UMTS or GPRS connection using an AT-style 3G modem. | 3g | PPP(PSTN-Modem) | PPP v90 modem | pppmodem | SLIP | Serial Line IP | slip |
| Web  | Description  | UCI                 |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Static address   | Static configuration with fixed address and netmask.   | static              |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| DHCP Client  | Address and netmask are assigned by DHCP.  | dhcp                |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Unmanaged  | Unspecified  | none                |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| IPv6-in-IPv4 (RFC4213)   | Used with tunnel brokers.  | 6in4                |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| IPv6-over-IPv4   | Stateless IPv6 over IPv4 transport.  | 6to4                |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| GRE  | Generic Routing Encapsulation protocol.  | gre                 |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| IOT  | IOT  | iot                 |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| L2TP   | Layer 2 Tunnelling Protocol  | l2tp                |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| L2TPv3   | L2TPv3 Tunnelling Protocol   | l2tpv3              |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPP  | Point to Point Protocol  | ppp                 |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPtP   | Point to Point Tunnelling Protocol   | pptp                |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPPoE  | PPP over Ethernet  | pppoe               |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPPoATM  | PPP over ATM   | pppoa               |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| LTE/UMTS/GPRS/EV-DO  | CDMA, UMTS or GPRS connection using an AT-style 3G modem.  | 3g                  |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| PPP(PSTN-Modem)  | PPP v90 modem  | pppmodem            |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| SLIP   | Serial Line IP   | slip                |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Web: Create a bridge over multiple interfaces<br>UCI: network[..x..].type<br>Opt: type | Enables a bridge between two interfaces. Leave as <b>disabled</b> . <table border="1"> <tbody> <tr> <td>No option /disabled</td> <td>Standard interface.</td> </tr> <tr> <td>bridge</td> <td>A bridge containing the given ifname is created.</td> </tr> </tbody> </table>   | No option /disabled | Standard interface. | bridge | A bridge containing the given ifname is created. |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| No option /disabled  | Standard interface.  |                     |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| bridge   | A bridge containing the given ifname is created.   |                     |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |
| Web: Cover the following interface<br>UCI: network[..x..].ifname<br>Opt: ifname        | Select <b>Custom Interface</b> , and then type <b>nas0</b> .   |                     |                     |        |  |  |        |             |   |      |           |             |      |                        |                           |      |                |                                     |      |     |   |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |      |                |      |

**Table 66: Information table for creating a static interface**

Click **Submit**. The Interfaces page appears.




### 15.5.9.5 ADSL bridge: general setup

**Common Configuration**

General Setup | 
 Advanced Settings | 
 Physical Settings | 
 Firewall Settings

---

Status 

**MAC Address:** 00:E0:C8:E5:1C:91  
 RX: 0.00 B (0 Pkts.)  
 TX: 0.00 B (0 Pkts.)

Protocol Static address

IPv4 address

IPv4 netmask

IPv4 gateway

IPv4 broadcast

Use custom DNS servers

Accept router advertisements

Send router solicitations

IPv6 address

IPv6 gateway

**Figure 100: The new static interface page**

| Web Field/UCI/Package Option  | Description   |
|---|---|
| Web: Protocol of the new interface<br>UCI: network[..x..].proto<br>Opt: proto         | Protocol type. The protocol shows the one selected for this interface.                        |
| Web: IPv4 address<br>UCI: network[..x..].ipaddrOpt:ipaddr                             | Type the <b>IP address</b> .  |
| Web: IPv4 netmask<br>UCI: network[..x..].netmask<br>Opt: netmask                      | Type or choose <b>netmask</b> .   |
| Web: IPv4 gateway<br>UCI: network[..x..].gateway<br>Opt: gateway                      | Leave this field empty or type the <b>gateway address</b> .                                   |
| Web: IPv4 broadcast<br>UCI: network[..x..].broadcast<br>Opt: broadcast                | Leave this field empty to autodetect, or type <b>broadcast IP address</b> .                   |
| Web: Use custom DNS servers<br>UCI: network[..x..].dns<br>Opt: dns                    | Leave this field empty to autodetect, or type <b>DNS IP address</b> .                         |
| Web: Accept router advertisements<br>UCI: network[..x..]. accept_ra<br>Opt: accept_ra | Accept router advertisement for ipv6 addresses. Leave this field empty if ipv6 is not needed. |
| Web: IPv6 address<br>UCI: network[..x..].ip6addr<br>Opt: ip6addr                      | IPv6 address. Leave this field empty if ipv6 is not needed.                                   |

|   |   |
|---|---|
| Web: IPv6 gateway<br>UCI: network[..x..].ipv6gw<br>Opt: ip6gw | Ipv6 gateway address. Leave this field empty if ipv6 is not needed.                                     |
| Web: IP-Aliases<br>UCI: network[..x..]<br>Opt: [...]          | Provide an arbitrary name for alias interface. Leave this field blank if alias interface is not needed. |
| Web: Setup DHCP Server<br>UCI: N/A<br>Opt: N/A                | Leave this field blank if DHCP server is not needed on this interface.                                  |

**Table 67: Information table for the new static interface**

### 15.5.9.6 ADSL bridge: advanced settings

The screenshot shows the 'Advanced Settings' tab for a network interface configuration. It includes the following fields and options:

- Bring up on boot:** A checked checkbox.
- Monitor interface state:** A checkbox with a tooltip: "This interface state would be reported to VA Monitor via keep-alive".
- Override MAC address:** A text input field containing "00:E0:C8:E5:1C:91".
- Override MTU:** A text input field containing "1500".
- Use gateway metric:** A text input field containing "0".
- Dependant interfaces:** A list of checkboxes for "VDSLBRIDGE:", "lan:", "lan2:", and "loopback:". A tooltip indicates: "Check interfaces which should start after this interface is started and stop after this interface is stopped".
- SNMP Alias ifindex:** A text input field with a tooltip: "Alias ifindex SNMP agent. Alias indexes are present at 1000 offset. So setting 1 here will create snmp ifTable entry 1001. Useful when interface creates new linux interface on every startup (e.g. ppp interface). With this set the interface could be monitored via constant snmp agent interface table entry".
- VRF:** A text input field with a tooltip: "Assign interface to this VRF".

**Figure 101: The advanced settings section**

| Web Field/UCI/Package Option  | Description  |      |            |       |          |
|---|--|------|------------|-------|----------|
| Web: Bring up on boot<br>UCI: network[..x..].auto<br>Opt: auto                  | Select this option if you want the interface to start after boot up. <table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0    | Disabled.  | 1     | Enabled. |
| 0   | Disabled.  |      |            |       |          |
| 1   | Enabled.   |      |            |       |          |
| Web: Monitor interface state<br>UCI: network[..x..].monitored<br>Opt: monitored | This interface state will be reported to VA Monitor via Keepalive. <table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0    | Disabled.  | 1     | Enabled. |
| 0   | Disabled.  |      |            |       |          |
| 1   | Enabled.   |      |            |       |          |
| Web: Override MAC address<br>UCI: network[..x..].macaddr<br>Opt: macaddr        | Specifies the mac address of the interface.<br>Leave this field blank if the MAC address of the bridge interface should be copied from Ethernet interface.   |      |            |       |          |
| Web: Override MTU<br>UCI: network[..x..].mtu<br>Opt: mtu                        | Optionally set up MTU size on the segment. <table border="1" style="width: 100%;"> <tr> <td>1500</td> <td>1500 bytes</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>                           | 1500 | 1500 bytes | Range |          |
| 1500  | 1500 bytes   |      |            |       |          |
| Range   |  |      |            |       |          |

|   |  |       |                                |       |                   |     |                  |      |               |      |               |
|---|--|-------|--------------------------------|-------|-------------------|-----|------------------|------|---------------|------|---------------|
| <p>Web: Dependant Interfaces<br/>UCI: network[..x..].dependants<br/>Opt: dependants</p>               | <p>Lists interfaces that are dependant on this parent interface. Dependant interfaces will go down when parent interface is down and will start or restart when the parent interface starts. Separate multiple interfaces by a space when using UCI.<br/>Example: <code>option dependants 'PPPADSL MOBILE'</code><br/>This replaces the following previous options in child interfaces.</p> <table border="1" data-bbox="683 383 1390 562"> <tr> <td>gre</td> <td>option local_interface</td> </tr> <tr> <td>lt2p</td> <td>option src_ipaddr</td> </tr> <tr> <td>iot</td> <td>option wan1 wan2</td> </tr> <tr> <td>6in4</td> <td>option ipaddr</td> </tr> <tr> <td>6to4</td> <td>option ipaddr</td> </tr> </table> | gre   | option local_interface         | lt2p  | option src_ipaddr | iot | option wan1 wan2 | 6in4 | option ipaddr | 6to4 | option ipaddr |
| gre   | option local_interface   |       |                                |       |                   |     |                  |      |               |      |               |
| lt2p  | option src_ipaddr  |       |                                |       |                   |     |                  |      |               |      |               |
| iot   | option wan1 wan2   |       |                                |       |                   |     |                  |      |               |      |               |
| 6in4  | option ipaddr  |       |                                |       |                   |     |                  |      |               |      |               |
| 6to4  | option ipaddr  |       |                                |       |                   |     |                  |      |               |      |               |
| <p>Web: SNMP Alias ifindex<br/>UCI: network[..x..].snmp_alias_ifindex<br/>Opt: snmp_alias_ifindex</p> | <p>Defines a static SNMP interface alias index for this interface, that can be polled via the SNMP interface index (<code>snmp_alias_ifindex+1000</code>). For more information, read the chapter 'Configuring SNMP'.</p> <table border="1" data-bbox="683 674 1331 745"> <tr> <td>Blank</td> <td>No SNMP interface alias index.</td> </tr> <tr> <td>Range</td> <td>0 - 4294966295</td> </tr> </table>   | Blank | No SNMP interface alias index. | Range | 0 - 4294966295    |     |                  |      |               |      |               |
| Blank   | No SNMP interface alias index.   |       |                                |       |                   |     |                  |      |               |      |               |
| Range   | 0 - 4294966295   |       |                                |       |                   |     |                  |      |               |      |               |
| <p>Web: VRF<br/>UCI: network[..x..].vrf<br/>Opt: vrf</p>  | <p>Defines the VRF for this interface.</p> <table border="1" data-bbox="683 781 1331 848"> <tr> <td>Blank</td> <td>No VRF</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | Blank | No VRF                         | Range |                   |     |                  |      |               |      |               |
| Blank   | No VRF   |       |                                |       |                   |     |                  |      |               |      |               |
| Range   |  |       |                                |       |                   |     |                  |      |               |      |               |

**Table 68: Information table for advanced settings**

### 15.5.9.7 ADSL bridge physical settings

#### Common Configuration

General Setup
Advanced Settings
Physical Settings
Firewall Settings

Bridge interfaces  *creates a bridge over specified interface(s)*

VLAN PCP to skb->priority mapping    
*Space separated list of <pcp>:<priority>*

skb->priority to VLAN PCP mapping

Interface

- Ethernet Adapter: "eth0" (lan)
- Ethernet Adapter: "eth1" (lan2)
- Ethernet Adapter: "eth2"
- Ethernet Adapter: "eth3"
- Ethernet Adapter: "eth4"
- Ethernet Adapter: "gretap0"
- Ethernet Adapter: "ip6tnl0"
- Ethernet Adapter: "lo" (loopback)
- Ethernet Adapter: "nas0" (ADSLBRIDGE)
- Ethernet Adapter: "ptm0"
- Ethernet Adapter: "tunl0"
- Ethernet Adapter: "wwan0"
- Custom Interface:

Auto Negotiation

Figure 102: The PPPoE physical settings page

| Web Field/UCI/Package Option  | Description  |       |           |       |          |
|---|--|-------|-----------|-------|----------|
| Web: Bridge interfaces<br>UCI: network.[...].type<br>Opt: type  | Enables a bridge between two interfaces.<br>Leave as <b>disabled</b> .<br><table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0     | Disabled. | 1     | Enabled. |
| 0   | Disabled.  |       |           |       |          |
| 1   | Enabled.   |       |           |       |          |
| Web: Enable STP<br>UCI: network.[...].autoneg<br>Opt: monitored   | Enables Spanning Tree Protocol (STP) when bridging interfaces.<br>Only displayed when bridging between two interfaces.<br><table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0     | Disabled. | 1     | Enabled. |
| 0   | Disabled.  |       |           |       |          |
| 1   | Enabled.   |       |           |       |          |
| Web: VLAN PCP to skb->priority mapping<br>UCI:<br>network.[...].vlan_qos_map_ingress<br>Opt: vlan_qos_map_ingress | Defines the VLAN QOS ingress PCP mapping as a space separated list in the format <pcp>:<priority>. Example:<br>option vlan_qos_map_ingress '1:1 2:5'<br>Leave as <b>empty</b> .<br><table border="1" style="width: 100%;"> <tr> <td>Empty</td> <td>Disabled.</td> </tr> <tr> <td>Range</td> <td>Enabled.</td> </tr> </table> | Empty | Disabled. | Range | Enabled. |
| Empty   | Disabled.  |       |           |       |          |
| Range   | Enabled.   |       |           |       |          |

|  |  |       |           |       |          |
|--|--|-------|-----------|-------|----------|
| Web: Interface<br>UCI:<br>network[..x..].vlan_qos_map_egress<br>Opt: vlan_qos_map_egress | Defines the VLAN QOS egress PCP mapping as a space separated list in the format <pcp>:<priority>. Example:<br>option vlan_qos_map_egress '1:1 2:5'<br>Leave as <b>empty</b> . <table border="1"> <tr> <td>Empty</td> <td>Disabled.</td> </tr> <tr> <td>Range</td> <td>Enabled.</td> </tr> </table> | Empty | Disabled. | Range | Enabled. |
| Empty  | Disabled.  |       |           |       |          |
| Range  | Enabled.   |       |           |       |          |
| Web: Interface<br>UCI: network[..x..].ifname<br>Opt: ifname                              | Select <b>Ethernet Adapter: nas0</b> .   |       |           |       |          |
| Web: Auto Negotiation<br>UCI: network[..x..].autoneg<br>Opt: monitored                   | Defines when auto negotiation is enabled on an Ethernet port. Only valid for Ethernet switch interfaces.<br>Leave as <b>enabled</b> . <table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0     | Disabled. | 1     | Enabled. |
| 0  | Disabled.  |       |           |       |          |
| 1  | Enabled.   |       |           |       |          |

Table 69: Information table for physical settings

### 15.5.9.8 ADSL bridge firewall settings

Use this section to select the firewall zone you want to assign to this interface.

Select **unspecified** to remove the interface from the associated zone or fill out the **create** field to define a new zone and attach the interface to it.

Click **Save & Apply**.

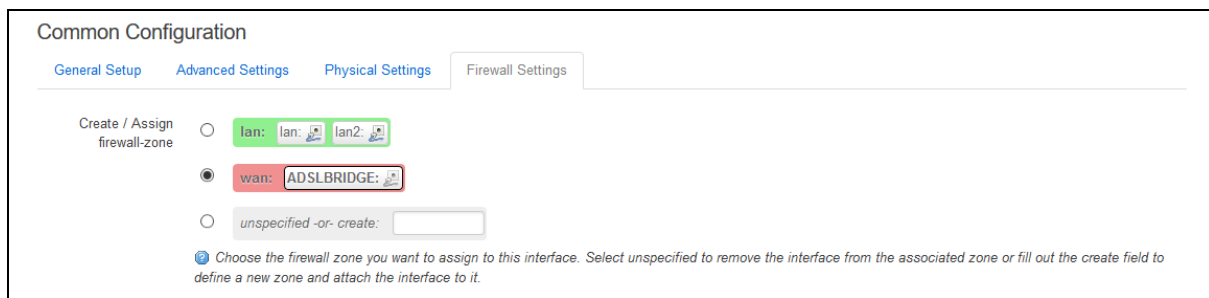


Figure 103: The interfaces page firewall settings tab

### 15.5.10 Configuring an ADSL ATM bridge connection with static IP using command line

Configure an ADSL ATM bridge upper interface using the interface and atm-bridge configuration section in the network package /etc/config/network.

#### 15.5.10.1 ADSL ATM bridge connection using UCI

```
root@VA_router:~# uci show network
network.@atm-bridge[0]=atm-bridge
network.@atm-bridge[0].unit=0
network.@atm-bridge[0].atmdev=0
network.@atm-bridge[0].payload=bridged
network.@atm-bridge[0].vpi=8
network.@atm-bridge[0].vci=39
```

```

network.@atm-bridge[0].encaps=llc
network.ADSLBRIDGE=interface
network.ADSLBRIDGE.proto=static
network.ADSLBRIDGE.ifname=nas0
network.ADSLBRIDGE.monitored=0
network.ADSLBRIDGE.ipaddr= 10.33.4.7
network.ADSLBRIDGE.netmask=255.255.255.192
network.ADSLBRIDGE.metric=2

```

### 15.5.10.2 ADSL ATM bridge connection using package options

```

root@VA_router:~# uci export network
package network
.....
config atm-bridge
    option unit '0'
    option atmdev '0'
    option payload 'bridged'
    option vpi '8'
    option vci '39'
    option encaps 'llc'

config interface 'ADSLBRIDGE'
    option proto 'static'
    option ifname 'nas0'
    option monitored '0'
    option ipaddr '10.33.4.7'
    option netmask '255.255.255.192'
    option metric '2'

```

### 15.5.11 Example VDSL and ADSL interface configuration using command line

The example below shows a configuration that runs PPPoEoA for ADSL connections and on PTM PPPoE for VDSL connections.

```

root@VA_router:~# uci export network
package network
.....
config atm-bridge
    option unit '0'
    option atmdev '0'

```

```
option encaps 'llc'
option payload 'bridged'
option vci '35'
option vpi '8'

config xdsl-device 'dsl0'
option enabled '1'
option vdsl_xfer_mode 'ptm'
option line_mode 'auto'
option vdsl_annex 'auto'
option vdsl_vectoring 'normal'
option adsl_xfer_mode 'atm'
option handshake_tone 'auto'
option adsl_annex 'a'

config interface 'ADSLPOE'
option proto 'pppoe'
option ifname 'nas0'
option dsltype 'adsl'
option username 'vodafone@vodafone.ie'
option password 'broadband'
option monitored '0'
option keepalive '6 5'
option ipv6_disable_ipv6 '1'
option defaultroute '1'

config interface 'VDSLPPPOE'
option proto 'pppoe'
option ifname 'ptm0'
option dsltype 'vdsl'
option username 'bthomehub@btbroadband.com'
option password 'any'
option defaultroute '1'
option metric '1'
option monitored '0'
```

## 15.6 xDSL diagnostics

### 15.6.1 xDSL line status

To check the status of an xDSL line, in the top menu, select **Network -> xDSL**. The xDSL page appears.

| xDSL                   |                      |  |
|------------------------|----------------------|--|
| Configuration of xDSL. |                      |  |
| Status                 | Chipset              | Lantiq-VRX300 v7.8.0.9.0.1 (ADSL mode)               |
|                        | Front End            | Hybrid Type A: Worldwide (POTS)                      |
|                        | State                | UP (0x801, showtime TC sync)                         |
|                        | Mode                 | ADSL G.992.5 Annex A                                 |
|                        | VDSL Profile         | -  |
|                        | DSLAM Vector Support | -  |
|                        | Vectoring Active     | -  |
|                        | ATU-C Info           | Broadcom   |
|                        | ATU-R Info           | Virtual Access (Infineon) v7.8.1.5.0.7, 00E0C812D123 |
|                        | Data Rate            | 16.107 Mb/s / 765 Kb/s                               |
|                        | Max Rate             | 16.068 Mb/s / 1.065 Mb/s                             |
|                        | Line Attenuation     | 22.3 dB / 9.4 dB                                     |
|                        | Signal Attenuation   | 22.3 dB / 9.4 dB                                     |
|                        | Noise Margin         | 6 dB / 15 dB   |
|                        | Transmit Power       | 17.3 dB / 12 dB                                      |
|                        | Interleave Depth     | 160 / 8  |
|                        | Last Error           | Comms problem (protocol): timeout, fwcode=65         |
|                        | Previous Error       | Configuration error: timeout, fwcode=553             |
|                        | Uptime               | 90036 seconds  |

Figure 104: The ADSL status page

To show the xDSL status using the command line, enter:

```
root@VA_router:~# /etc/init.d/dsl_control status
Chipset:                Lantiq-VRX300 v7.8.0.9.0.1 (ADSL mode)
Front End:              Hybrid Type A: Worldwide (POTS)
Line State:             UP [0x801: showtime TC sync]
Line Mode:              ADSL G.992.5 Annex A
...
```

### 15.6.2 xDSL line stats

To check statistics for an xDSL line, in the top menu, select **Status -> xDSL Stats**.



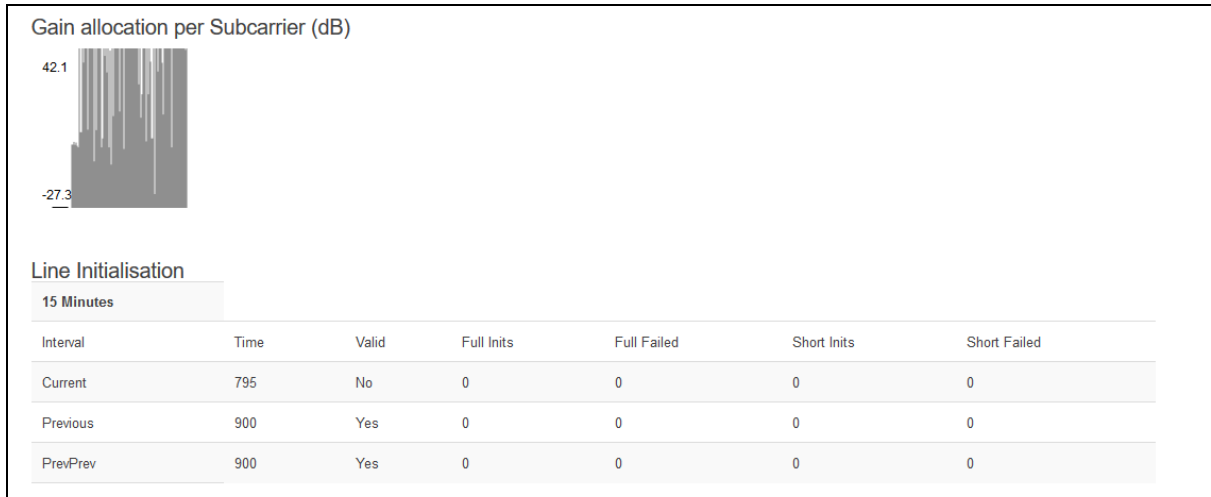


Figure 105: The ADSL status page

To show the xDSL statistics using the command line, enter:

```
root@VA_router:~# dsl_stats
.....
==== Line Initialisation ====
---- 15Min ----
Interval          Time      Valid    Full Inits      Full Failed      Short Inits
Short Failed
Current 842       No        0         0         0         0
Previous          900      Yes        0         0         0         0
PrevPrev          900      Yes        0         0         0         0
.....
```

### 15.6.3 xDSL interface status

To check an IP address, transmit and received counter on an ADSL interface, in the top menu, select **Network -> Interfaces**. The Interface Overview page appears.

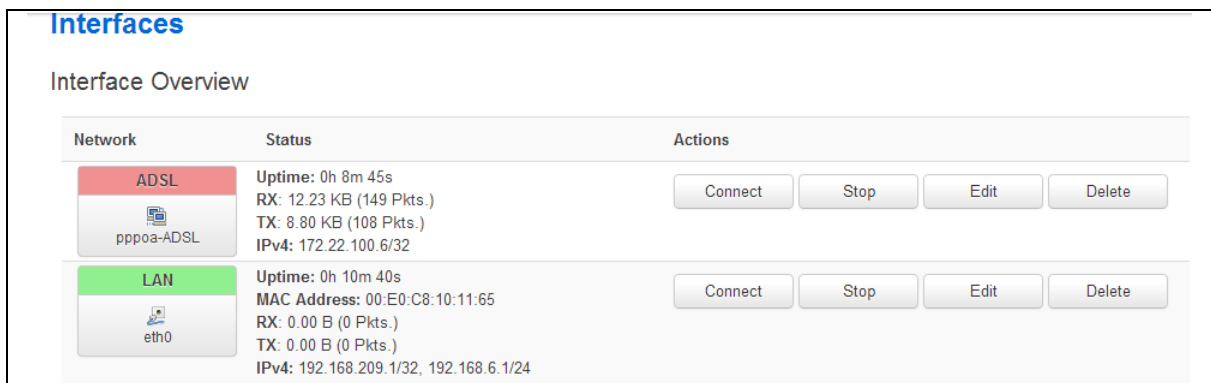


Figure 106: The interfaces overview page

To show the interface statistics using the command line, enter:

```
root@VA_router:~# ifconfig
.....
pppoe-POEADSL Link encap:Point-to-Point Protocol
    inet addr:109.79.70.147  P-t-P:89.19.65.140  Mask:255.255.255.255
    UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1492  Metric:1
    RX packets:5815387 errors:0 dropped:0 overruns:0 frame:0
    TX packets:2873416 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:3
    RX bytes:7379087712 (6.8 GiB)  TX bytes:277101958 (264.2 MiB)
```

### 15.6.4 DSL process using UCI

The DSL process has its own subset of commands.

```
root@VA_router:~# /etc/init.d/dsl_control
Syntax: /etc/init.d/dsl_control [command]
```

Available commands:

```
start    Start the service
stop     Stop the service
restart  Restart the service
reload   Reload configuration files (or restart if that fails)
enable   Enable service autostart
disable  Disable service autostart
status   Get DSL status information
lucistat Get status information in lua friendly format
```

To restart the xDSL interface, enter:

```
root@VA_router:~# /etc/init.d/dsl_control restart
```

## 16 Configuring a mobile connection

### 16.1 Configuration package used

| Package | Sections  |
|---------|-----------|
| network | interface |

### 16.2 Configuring a mobile connection using the web interface

**Note:** if you are creating multiple mobile interfaces, simply repeat the steps in this chapter for each interface. Multiple interfaces are required for dual SIM or multiple radio module scenarios. Configuring static routes and/or Multi-WAN can be used to manage these interfaces.

In the top menu, select **Network -> Interfaces**. The Interfaces Overview page appears.

#### 16.2.1 Create a new mobile interface

To create a new mobile interface, in the Interface Overview section, click **Add new interface**. The Create Interface page appears. In the examples below, 3G has been used for the interface name.

Figure 107: The create interface page

| Web Field/UCI/Package Option   | Description   |        |             |        |  |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |
|--|---|--------|-------------|--------|--|-------------|---|-----------|-------------|--------------|--|----------------|--|-----|--|-----|--|------|------------------------------|-----|--|-------|--|---------|--|---------------------|---|
| Web: Name of the new interface<br>UCI: network.3G=interface<br>Opt: interface      | Allowed characters are A-Z, a-z, 0-9 and _  |        |             |        |  |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |
| Web: Protocol of the new interface<br>UCI: network.3G.proto<br>Opt: proto          | Protocol type. Select <b>LTE/UMTS/GPRS/EV-DO</b> . <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Static</td> <td>Static configuration with fixed address and netmask.</td> </tr> <tr> <td>DHCP Client</td> <td>Address and netmask are assigned by DHCP.</td> </tr> <tr> <td>Unmanaged</td> <td>Unspecified</td> </tr> <tr> <td>IPv6-in-IPv4</td> <td></td> </tr> <tr> <td>IPv6-over-IPv4</td> <td></td> </tr> <tr> <td>GRE</td> <td></td> </tr> <tr> <td>IOT</td> <td></td> </tr> <tr> <td>L2TP</td> <td>Layer 2 Tunnelling Protocol.</td> </tr> <tr> <td>PPP</td> <td></td> </tr> <tr> <td>PPPoE</td> <td></td> </tr> <tr> <td>PPPoATM</td> <td></td> </tr> <tr> <td>LTE/UMTS/GPRS/EV-DO</td> <td>CDMA, UMTS or GPRS connection using an AT-style 3G modem.</td> </tr> </tbody> </table> | Option | Description | Static | Static configuration with fixed address and netmask. | DHCP Client | Address and netmask are assigned by DHCP. | Unmanaged | Unspecified | IPv6-in-IPv4 |  | IPv6-over-IPv4 |  | GRE |  | IOT |  | L2TP | Layer 2 Tunnelling Protocol. | PPP |  | PPPoE |  | PPPoATM |  | LTE/UMTS/GPRS/EV-DO | CDMA, UMTS or GPRS connection using an AT-style 3G modem. |
| Option   | Description   |        |             |        |  |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |
| Static   | Static configuration with fixed address and netmask.  |        |             |        |  |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |
| DHCP Client  | Address and netmask are assigned by DHCP.   |        |             |        |  |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |
| Unmanaged  | Unspecified   |        |             |        |  |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |
| IPv6-in-IPv4   |   |        |             |        |  |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |
| IPv6-over-IPv4   |   |        |             |        |  |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |
| GRE  |   |        |             |        |  |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |
| IOT  |   |        |             |        |  |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |
| L2TP   | Layer 2 Tunnelling Protocol.  |        |             |        |  |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |
| PPP  |   |        |             |        |  |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |
| PPPoE  |   |        |             |        |  |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |
| PPPoATM  |   |        |             |        |  |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |
| LTE/UMTS/GPRS/EV-DO  | CDMA, UMTS or GPRS connection using an AT-style 3G modem.   |        |             |        |  |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |
| Web: Create a bridge over multiple interfaces<br>UCI: network.3G.type<br>Opt: type | Enables bridge between two interfaces.<br>Not relevant when configuring a mobile interface. <table border="1"> <tbody> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </tbody> </table>   | 0      | Disabled.   | 1      | Enabled.   |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |
| 0  | Disabled.   |        |             |        |  |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |
| 1  | Enabled.  |        |             |        |  |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |
| Web: Cover the following interface<br>UCI: network.3G.ifname<br>Opt: ifname        | Select interfaces for bridge connection.<br>Not relevant when configuring a mobile interface.   |        |             |        |  |             |   |           |             |              |  |                |  |     |  |     |  |      |                              |     |  |       |  |         |  |                     |   |

**Table 70: Information table for the create interface page**

Click **Submit**. The Common Configuration page appears. There are three sections in the mobile interface common configurations.

| Section           | Description  |
|-------------------|--|
| General Setup     | Configure the basic interface settings such as protocol, service type, APN information, user name and password.    |
| Advanced Settings | Set up more in-depth features such as initialisation timeout, LCP echo failure thresholds and inactivity timeouts. |
| Firewall settings | Assign a firewall zone to the connection.  |

### 16.2.1.1 Mobile interface: general setup

Figure 108: The common configuration page

| Web Field/UCI/Package Option                         | Description   |          |             |     |        |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
|--|---|----------|-------------|-----|--------|--|--------|-------------|---|------|-----------|-------------|------|------------------------|---------------------------|--|----------------|-------------------------------------|--|-----|--|-----|-----|-----|-----|------|-----------------------------|------|--------|----------------------------|--------|-----|-------------------------|-----|------|------------------------------------|------|-------|-------------------|-------|---------|--------------|-------|---------------------|---|----|-----------------|---------------|----------|
| Web: Status<br>UCI: n/a<br>Opt: n/a                  | Shows the current status of the interface.  |          |             |     |        |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Web: Protocol<br>UCI: network.3G.proto<br>Opt: proto | <p>Protocol type. Select <b>LTE/UMTS/GPRS/EV-DO</b>.</p> <table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Static</td> <td>Static configuration with fixed address and netmask.</td> <td>static</td> </tr> <tr> <td>DHCP Client</td> <td>Address and netmask are assigned by DHCP.</td> <td>dhcp</td> </tr> <tr> <td>Unmanaged</td> <td>Unspecified</td> <td>none</td> </tr> <tr> <td>IPv6-in-IPv4 (RFC4213)</td> <td>Used with tunnel brokers.</td> <td></td> </tr> <tr> <td>IPv6-over-IPv4</td> <td>Stateless IPv6 over IPv4 transport.</td> <td></td> </tr> <tr> <td>GRE</td> <td>Generic Routing Encapsulation protocol</td> <td>gre</td> </tr> <tr> <td>IOT</td> <td>IOT</td> <td>iot</td> </tr> <tr> <td>L2TP</td> <td>Layer 2 Tunnelling Protocol</td> <td>l2tp</td> </tr> <tr> <td>L2TPv3</td> <td>L2TPv3 Tunnelling Protocol</td> <td>l2tpv3</td> </tr> <tr> <td>PPP</td> <td>Point to Point Protocol</td> <td>ppp</td> </tr> <tr> <td>PptP</td> <td>Point to Point Tunnelling Protocol</td> <td>pptp</td> </tr> <tr> <td>PPPoE</td> <td>PPP over Ethernet</td> <td>pppoe</td> </tr> <tr> <td>PPPoATM</td> <td>PPP over ATM</td> <td>pppoa</td> </tr> <tr> <td>LTE/UMTS/GPRS/EV-DO</td> <td>CDMA, UMTS or GPRS connection using an AT-style 3G modem.</td> <td>3g</td> </tr> <tr> <td>PPP(PSTN-Modem)</td> <td>PPP v90 modem</td> <td>pppmodem</td> </tr> </tbody> </table> | Web      | Description | UCI | Static | Static configuration with fixed address and netmask. | static | DHCP Client | Address and netmask are assigned by DHCP. | dhcp | Unmanaged | Unspecified | none | IPv6-in-IPv4 (RFC4213) | Used with tunnel brokers. |  | IPv6-over-IPv4 | Stateless IPv6 over IPv4 transport. |  | GRE | Generic Routing Encapsulation protocol | gre | IOT | IOT | iot | L2TP | Layer 2 Tunnelling Protocol | l2tp | L2TPv3 | L2TPv3 Tunnelling Protocol | l2tpv3 | PPP | Point to Point Protocol | ppp | PptP | Point to Point Tunnelling Protocol | pptp | PPPoE | PPP over Ethernet | pppoe | PPPoATM | PPP over ATM | pppoa | LTE/UMTS/GPRS/EV-DO | CDMA, UMTS or GPRS connection using an AT-style 3G modem. | 3g | PPP(PSTN-Modem) | PPP v90 modem | pppmodem |
| Web  | Description   | UCI      |             |     |        |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Static   | Static configuration with fixed address and netmask.  | static   |             |     |        |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| DHCP Client  | Address and netmask are assigned by DHCP.   | dhcp     |             |     |        |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| Unmanaged  | Unspecified   | none     |             |     |        |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| IPv6-in-IPv4 (RFC4213)                               | Used with tunnel brokers.   |          |             |     |        |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| IPv6-over-IPv4                                       | Stateless IPv6 over IPv4 transport.   |          |             |     |        |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| GRE  | Generic Routing Encapsulation protocol  | gre      |             |     |        |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| IOT  | IOT   | iot      |             |     |        |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| L2TP   | Layer 2 Tunnelling Protocol   | l2tp     |             |     |        |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| L2TPv3   | L2TPv3 Tunnelling Protocol  | l2tpv3   |             |     |        |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| PPP  | Point to Point Protocol   | ppp      |             |     |        |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| PptP   | Point to Point Tunnelling Protocol  | pptp     |             |     |        |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| PPPoE  | PPP over Ethernet   | pppoe    |             |     |        |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| PPPoATM  | PPP over ATM  | pppoa    |             |     |        |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| LTE/UMTS/GPRS/EV-DO                                  | CDMA, UMTS or GPRS connection using an AT-style 3G modem.   | 3g       |             |     |        |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |
| PPP(PSTN-Modem)                                      | PPP v90 modem   | pppmodem |             |     |        |  |        |             |   |      |           |             |      |                        |                           |  |                |                                     |  |     |  |     |     |     |     |      |                             |      |        |                            |        |     |                         |     |      |                                    |      |       |                   |       |         |              |       |                     |   |    |                 |               |          |

| <p>Web: service Preference<br/>UCI: network.3G.service_order<br/>Opt: service_order</p> | <p>Defines a space separated list of services, in preferred order. Valid options are <code>gprs</code>, <code>umts</code>, <code>lte</code>, <code>auto</code>.</p> <p>If no valid <code>service_order</code> is defined, then the configured Service Type is used. Example:<br/><code>network.3G.service_order="gprs umts lte auto"</code></p> <table border="1" data-bbox="683 347 1390 421"> <tr> <td>Blank</td> <td>Use configured service type.</td> </tr> <tr> <td>Range</td> <td><code>gprs umts lte auto</code></td> </tr> </table>  | Blank | Use configured service type.       | Range      | <code>gprs umts lte auto</code>                    |                      |   |   |       |   |   |       |   |
|---|--|-------|------------------------------------|------------|--|----------------------|---|---|-------|---|---|-------|---|
| Blank   | Use configured service type.   |       |                                    |            |  |                      |   |   |       |   |   |       |   |
| Range   | <code>gprs umts lte auto</code>  |       |                                    |            |  |                      |   |   |       |   |   |       |   |
| <p>Web: Operator PLMN code<br/>UCI: network.3G.operator<br/>Opt: operator</p>           | <p>Specifies an operator PLMN code to force the connection to a particular carrier. The PLMN code is identified as a combination of the MCC and the MNC.</p> <p><b>Note:</b> the operator option is used in conjunction with the operator format option <code>option opformat</code> which is used to define how the operator string is parsed. If configuring via the web GUI, the <code>opformat</code> is automatically set to <code>'2'</code> to indicate it is a PLMN code.</p> <p>See below for alternative options for the operator format option.</p>                       |       |                                    |            |  |                      |   |   |       |   |   |       |   |
| <p>Web: n/a<br/>UCI: network.3G.opformat<br/>Opt: opformat</p>                          | <p>Defines the operator format. We recommended you use a PLMN code.</p> <p>The operator is case sensitive so if using long or short character format it must match the operator exactly.</p> <p>To see the current operator using SSH enter the command: <code>cat /var/state/mobile</code> or using the web mobile stats page at <b>Status -&gt; Mobile Stats</b>.</p> <table border="1" data-bbox="683 891 1390 994"> <tr> <td>0</td> <td>Long character format</td> </tr> <tr> <td>1</td> <td>Short character format</td> </tr> <tr> <td>2</td> <td>PLMN code</td> </tr> </table> | 0     | Long character format              | 1          | Short character format                             | 2                    | PLMN code   |   |       |   |   |       |   |
| 0   | Long character format  |       |                                    |            |  |                      |   |   |       |   |   |       |   |
| 1   | Short character format   |       |                                    |            |  |                      |   |   |       |   |   |       |   |
| 2   | PLMN code  |       |                                    |            |  |                      |   |   |       |   |   |       |   |
| <p>Web: SIM<br/>UCI: network.3G.sim<br/>Opt: sim</p>                                    | <p>Defines which SIM is used on this interface.</p> <table border="1" data-bbox="683 1032 1390 1173"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Auto</td> <td>automatically detect</td> <td>any</td> </tr> <tr> <td>1</td> <td>SIM 1</td> <td>1</td> </tr> <tr> <td>2</td> <td>SIM 2</td> <td>2</td> </tr> </tbody> </table>   | Web   | Description                        | UCI        | Auto   | automatically detect | any   | 1 | SIM 1 | 1 | 2 | SIM 2 | 2 |
| Web   | Description  | UCI   |                                    |            |  |                      |   |   |       |   |   |       |   |
| Auto  | automatically detect   | any   |                                    |            |  |                      |   |   |       |   |   |       |   |
| 1   | SIM 1  | 1     |                                    |            |  |                      |   |   |       |   |   |       |   |
| 2   | SIM 2  | 2     |                                    |            |  |                      |   |   |       |   |   |       |   |
| <p>Web: APN<br/>UCI: network.3G.apn<br/>Opt: apn</p>                                    | <p>APN name of Mobile Network Operator.</p>  |       |                                    |            |  |                      |   |   |       |   |   |       |   |
| <p>Web: APN username<br/>UCI: network.3G.username<br/>Opt: username</p>                 | <p>Username used to connect to APN.</p>  |       |                                    |            |  |                      |   |   |       |   |   |       |   |
| <p>Web: APN password<br/>UCI: network.3G.password<br/>Opt: password</p>                 | <p>Password used to connect to APN.</p>  |       |                                    |            |  |                      |   |   |       |   |   |       |   |
| <p>Web: n/a<br/>UCI: network.3G.retry_interval_sec<br/>Opt: retry_interval_sec</p>      | <p>Specifies the interval in seconds between connection attempts.</p> <table border="1" data-bbox="683 1520 1390 1778"> <tr> <td>60</td> <td>Retry connection after 60 seconds.</td> </tr> <tr> <td>1-infinite</td> <td>Attempt to connect again after specified interval.</td> </tr> <tr> <td>Range</td> <td>Attempt to connect within specified range. The exact interval is calculated randomly from specified range.<br/>Example:<br/><code>uci set network.3G.retry_interval_sec='60 180'</code></td> </tr> </table>  | 60    | Retry connection after 60 seconds. | 1-infinite | Attempt to connect again after specified interval. | Range                | Attempt to connect within specified range. The exact interval is calculated randomly from specified range.<br>Example:<br><code>uci set network.3G.retry_interval_sec='60 180'</code> |   |       |   |   |       |   |
| 60  | Retry connection after 60 seconds.   |       |                                    |            |  |                      |   |   |       |   |   |       |   |
| 1-infinite  | Attempt to connect again after specified interval.   |       |                                    |            |  |                      |   |   |       |   |   |       |   |
| Range   | Attempt to connect within specified range. The exact interval is calculated randomly from specified range.<br>Example:<br><code>uci set network.3G.retry_interval_sec='60 180'</code>  |       |                                    |            |  |                      |   |   |       |   |   |       |   |

**Table 71: Information table for common configuration settings**

The Modem Configuration link at the bottom of the page is used for SIM pin code and SMS configuration. For more information, read the chapter 'Configuring mobile manager'.

### 16.2.1.2 Mobile interface: advanced settings

**Common Configuration**

General Setup   **Advanced Settings**   Firewall Settings

---

Bring up on boot

Monitor interface state  ⓘ This interface state would be reported to VA Monitor via keep-alive

Authentication type: CHAP ⓘ Selects APN authentication type

Enable IPv6 negotiation on the PPP link

Modem init timeout: 20 ⓘ Maximum amount of seconds to wait for the modem to become ready

Use default gateway  ⓘ If unchecked, no default route is configured

Use gateway metric: 0

IPv4 Mode: DHCP

IPv6 Mode: None


Use DNS servers advertised by peer  ⓘ If unchecked, the advertised DNS server addresses are ignored

LCP echo failure threshold: 0 ⓘ Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures

LCP echo interval: 5 ⓘ Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold

Inactivity timeout: 0 ⓘ Close inactive connection after the given amount of seconds, use 0 to persist connection

Select Operator on Every Start  ⓘ When operator is not enforced use this to make modem select operator every time interface starts

Dependant interfaces  lan: 

**Figure 109: The advanced settings tab**

| Web Field/UCI/Package Option  | Description   |     |                             |       |                    |                     |   |     |                    |   |
|---|---|-----|-----------------------------|-------|--------------------|---------------------|---|-----|--------------------|---|
| Web: Bring up on boot<br>UCI: network.3G.auto<br>Opt: auto                        | Enables the interface to connect automatically on boot up or reconnect automatically when disconnected.   |     |                             |       |                    |                     |   |     |                    |   |
| Web: Monitor interface state<br>UCI: network.3G.monitored<br>Opt: monitored       | Enabled if status of interface is presented on monitoring platform.<br><table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Does not monitor interface.</td> </tr> <tr> <td>1</td> <td>Monitor interface.</td> </tr> </table>  | 0   | Does not monitor interface. | 1     | Monitor interface. |                     |   |     |                    |   |
| 0   | Does not monitor interface.   |     |                             |       |                    |                     |   |     |                    |   |
| 1   | Monitor interface.  |     |                             |       |                    |                     |   |     |                    |   |
| Web: Authentication Type<br>UCI: network.3G.auth<br>Opt: auth                     | Enabled if the status of the interface is presented on the monitoring platform.<br><table border="1" style="width: 100%;"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>CHAP</td> <td>CHAP authentication</td> <td>2</td> </tr> <tr> <td>PAP</td> <td>PAP authentication</td> <td>1</td> </tr> </tbody> </table> | Web | Description                 | UCI   | CHAP               | CHAP authentication | 2 | PAP | PAP authentication | 1 |
| Web   | Description   | UCI |                             |       |                    |                     |   |     |                    |   |
| CHAP  | CHAP authentication   | 2   |                             |       |                    |                     |   |     |                    |   |
| PAP   | PAP authentication  | 1   |                             |       |                    |                     |   |     |                    |   |
| Web: Enable IPv6 negotiation on the PPP link<br>UCI: network.3G.ipv6<br>Opt: ipv6 | Enables IPv6 routing on the interface.<br><table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Does not enable IPv6.</td> </tr> <tr> <td>1</td> <td>Enable IPv6.</td> </tr> </table>   | 0   | Does not enable IPv6.       | 1     | Enable IPv6.       |                     |   |     |                    |   |
| 0   | Does not enable IPv6.   |     |                             |       |                    |                     |   |     |                    |   |
| 1   | Enable IPv6.  |     |                             |       |                    |                     |   |     |                    |   |
| Web: Modem int timeout<br>UCI: network.3G.maxwait<br>Opt: maxwait                 | Maximum amount of seconds to wait for the modem to become ready.<br><table border="1" style="width: 100%;"> <tr> <td>20</td> <td>Seconds</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 20  | Seconds                     | Range |                    |                     |   |     |                    |   |
| 20  | Seconds   |     |                             |       |                    |                     |   |     |                    |   |
| Range   |   |     |                             |       |                    |                     |   |     |                    |   |

| <p>Web: Use default gateway<br/>UCI: network.3G.defaultroute<br/>Opt: defaultroute</p>      | <p>Enables this interface as a default route.</p> <table border="1" data-bbox="679 226 1393 300"> <tr> <td>0</td> <td>Do not use as a default route.</td> </tr> <tr> <td>1</td> <td>Use as a default route.</td> </tr> </table>   | 0            | Do not use as a default route.   | 1     | Use as a default route. |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
|---|---|--------------|----------------------------------|-------|-------------------------|------------------------|------|--------|--------------------------|------|----|---------------------------------------|----|-----------------|------------------------------|--------------|
| 0   | Do not use as a default route.  |              |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| 1   | Use as a default route.   |              |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| <p>Web: Use gateway metric<br/>UCI: network.3G.metric<br/>Opt: metric</p>                   | <p>Defines the metric for the default route. Lower number metrics are used first when the route is up.</p> <table border="1" data-bbox="679 360 1393 427"> <tr> <td>0</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 0            |                                  | Range |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| 0   |   |              |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| Range   |   |              |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| <p>Web: IPv4 Mode<br/>UCI: network.3G.ipv4mode<br/>Opt: ipv4mode</p>                        | <p>Defines the IPv4 address assignment approach for mobile interfaces in Ethernet Mode.<br/><b>Note:</b> by default, mobile interfaces are in Ethernet mode.</p> <table border="1" data-bbox="679 528 1393 633"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>None</td> <td>No dynamic assignment.</td> <td>none</td> </tr> <tr> <td>DHCP</td> <td>DHCP address assignment.</td> <td>dhcp</td> </tr> </tbody> </table>   | Web          | Description                      | UCI   | None                    | No dynamic assignment. | none | DHCP   | DHCP address assignment. | dhcp |    |                                       |    |                 |                              |              |
| Web   | Description   | UCI          |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| None  | No dynamic assignment.  | none         |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| DHCP  | DHCP address assignment.  | dhcp         |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| <p>Web: IPv6 Mode<br/>UCI: network.3G.ipv6mode<br/>Opt: ipv6mode</p>                        | <p>Defines the IPv6 address assignment approach for mobile interfaces in Ethernet Mode.<br/><b>Note:</b> by default, mobile interfaces are in Ethernet mode.</p> <table border="1" data-bbox="679 730 1393 958"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>None</td> <td>No dynamic assignment.</td> <td>none</td> </tr> <tr> <td>DHCPv6</td> <td>DHCP address assignment.</td> <td>dhcp</td> </tr> <tr> <td>RA</td> <td>Router Advertisement (RA) assignment.</td> <td>ra</td> </tr> <tr> <td>DHCPv6 after RA</td> <td>Wait for RA then start DHCP.</td> <td>ra_then_dhcp</td> </tr> </tbody> </table> | Web          | Description                      | UCI   | None                    | No dynamic assignment. | none | DHCPv6 | DHCP address assignment. | dhcp | RA | Router Advertisement (RA) assignment. | ra | DHCPv6 after RA | Wait for RA then start DHCP. | ra_then_dhcp |
| Web   | Description   | UCI          |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| None  | No dynamic assignment.  | none         |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| DHCPv6  | DHCP address assignment.  | dhcp         |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| RA  | Router Advertisement (RA) assignment.   | ra           |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| DHCPv6 after RA   | Wait for RA then start DHCP.  | ra_then_dhcp |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| <p>Web: Use DNS servers advertised by peer<br/>UCI: network.3G.peerdns<br/>Opt: peerdns</p> | <p>If unchecked, the advertised DNS server addresses are ignored.</p> <table border="1" data-bbox="679 994 1393 1064"> <tr> <td>0</td> <td>Use static DNS.</td> </tr> <tr> <td>1</td> <td>Use advertised DNS.</td> </tr> </table>   | 0            | Use static DNS.                  | 1     | Use advertised DNS.     |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| 0   | Use static DNS.   |              |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| 1   | Use advertised DNS.   |              |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| <p>Web: Use custom DNS servers<br/>UCI: network.3G.dns<br/>Opt: dns</p>                     | <p>Specifies DNS server. Only available if <b>Use DNS servers advertised by peer</b> is unselected. When multiple DNS servers are required separate using space for UCI or option value.<br/>Example:<br/><code>uci set network.3G.dns='1.1.1.1 2.2.2.2'</code></p>   |              |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| <p>Web: LCP echo failure threshold<br/>UCI: network.3G.keepalive<br/>Opt: keepalive</p>     | <p>Presumes peer to be dead after a given amount of LCP echo failures, use <b>0</b> to ignore failures.<br/>This command is used in conjunction with the LCP echo interval. The syntax is as follows:<br/><code>uci network.3G.keepalive=&lt;echo failure threshold&gt; &lt;echo interval&gt;</code><br/>Example:<br/><code>uci set network.3G.keepalive='15 10'</code></p> <table border="1" data-bbox="679 1442 1393 1514"> <tr> <td>5</td> <td>PPP peer dead after 5 failures</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 5            | PPP peer dead after 5 failures   | Range |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| 5   | PPP peer dead after 5 failures  |              |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| Range   |   |              |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| <p>Web: LCP echo interval<br/>UCI: network.3G.keepalive<br/>Opt: keepalive</p>              | <p>Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure<br/>This command is used in conjunction with the LCP echo failure threshold. The syntax is as follows:<br/><code>uci network.3G.keepalive=&lt;echo failure threshold&gt; &lt;echo interval&gt;</code><br/>Example:<br/><code>uci set network.3G.keepalive='15 10'</code></p> <table border="1" data-bbox="679 1733 1393 1805"> <tr> <td>1</td> <td>LCP echo request every 1 second</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 1            | LCP echo request every 1 second  | Range |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| 1   | LCP echo request every 1 second   |              |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| Range   |   |              |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| <p>Web: Inactivity timeout<br/>UCI: network.3G.demand<br/>Opt: demand</p>                   | <p>Closes an inactive connection after the given amount of seconds. Use <b>0</b> to persist connection.</p> <table border="1" data-bbox="679 1865 1393 1930"> <tr> <td>0</td> <td>Do not disconnect on inactivity.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 0            | Do not disconnect on inactivity. | Range |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| 0   | Do not disconnect on inactivity.  |              |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |
| Range   |   |              |                                  |       |                         |                        |      |        |                          |      |    |                                       |    |                 |                              |              |



|   |  |       |  |       |   |     |                  |      |               |      |               |
|---|--|-------|--|-------|---|-----|------------------|------|---------------|------|---------------|
| <p>Web: Select Operator on Every Start<br/>UCI: network.3G.operator_reselect<br/>Opt: operator_reselect</p> | <p>Defines whether to force the modem to run operator selection (with AT+COPS=0 command) on every interface restart.</p> <table border="1" data-bbox="683 253 1390 376"> <tr> <td>0</td> <td>Operator selection will not happen on interface restart.</td> </tr> <tr> <td>1</td> <td>Force modem to run operator selection on every interface restart.</td> </tr> </table>   | 0     | Operator selection will not happen on interface restart. | 1     | Force modem to run operator selection on every interface restart. |     |                  |      |               |      |               |
| 0   | Operator selection will not happen on interface restart.   |       |  |       |   |     |                  |      |               |      |               |
| 1   | Force modem to run operator selection on every interface restart.  |       |  |       |   |     |                  |      |               |      |               |
| <p>Web: Dependant Interfaces<br/>UCI: network.3G.dependants<br/>Opt: dependants</p>                         | <p>Lists interfaces that are dependent on this parent interface. Dependant interfaces will go down when the parent interface is down and will start or restart when the parent interface starts. Separate multiple interfaces by a space when using UCI. Example: <code>option dependants 'PPPADSL MOBILE'</code><br/>This replaces the following previous options in child interfaces.</p> <table border="1" data-bbox="683 562 1390 734"> <tr> <td>gre</td> <td>option local_interface</td> </tr> <tr> <td>lt2p</td> <td>option src_ipaddr</td> </tr> <tr> <td>iot</td> <td>option wan1 wan2</td> </tr> <tr> <td>6in4</td> <td>option ipaddr</td> </tr> <tr> <td>6to4</td> <td>option ipaddr</td> </tr> </table> | gre   | option local_interface                                   | lt2p  | option src_ipaddr   | iot | option wan1 wan2 | 6in4 | option ipaddr | 6to4 | option ipaddr |
| gre   | option local_interface   |       |  |       |   |     |                  |      |               |      |               |
| lt2p  | option src_ipaddr  |       |  |       |   |     |                  |      |               |      |               |
| iot   | option wan1 wan2   |       |  |       |   |     |                  |      |               |      |               |
| 6in4  | option ipaddr  |       |  |       |   |     |                  |      |               |      |               |
| 6to4  | option ipaddr  |       |  |       |   |     |                  |      |               |      |               |
| <p>Web: SNMP Alias ifindex<br/>UCI: network.[..x..].snmp_alias_ifindex<br/>Opt: snmp_alias_ifindex</p>      | <p>Defines a static SNMP interface alias index for this interface that can be polled via the SNMP interface index. (<code>snmp_alias_ifindex+1000</code>). For more information, read the chapter 'Configuring SNMP'.</p> <table border="1" data-bbox="683 853 1331 922"> <tr> <td>Blank</td> <td>No SNMP interface alias index.</td> </tr> <tr> <td>Range</td> <td>0 - 4294966295</td> </tr> </table>   | Blank | No SNMP interface alias index.                           | Range | 0 - 4294966295  |     |                  |      |               |      |               |
| Blank   | No SNMP interface alias index.   |       |  |       |   |     |                  |      |               |      |               |
| Range   | 0 - 4294966295   |       |  |       |   |     |                  |      |               |      |               |
| <p>Web: VRF<br/>UCI: network.3G.vrf<br/>Opt: vrf</p>  | <p>Defines VRF for this interface.</p> <table border="1" data-bbox="683 958 1390 1025"> <tr> <td>blank</td> <td>No VFR.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | blank | No VFR.  | Range |   |     |                  |      |               |      |               |
| blank   | No VFR.  |       |  |       |   |     |                  |      |               |      |               |
| Range   |  |       |  |       |   |     |                  |      |               |      |               |

Table 72: Information table for general set up page

### 16.2.1.3 Mobile interface: firewall settings

Use this section to select the firewall zone you want to assign to the interface.

Select **unspecified** to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.



Common Configuration

General Setup   Advanced Settings   **Firewall Settings**

Create / Assign firewall-zone  unspecified -or- create:

 Choose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

Figure 110: Firewall settings page

## 16.3 Configuring a mobile connection using CLI

### 16.3.1 UCI

To establish a basic mobile connection, enter:

```
root@VA_router:~# uci show network
network.3G=interface
network.3G.proto=3g
network.3G.monitored=0
network.3G.sim=any
network.3G.auto=1
network.3G.defaultroute=1
network.3G.metric=1
network.3G.service_order=auto lte umts gprs
network.3G.apn=test.apn
network.3G.username=username
network.3G.password=password
network.3G.ipv4mode=dhcp
network.3G.ipv6mode=none
network.3G.keepalive='5 1'
network.3G.operator_reselect=0
network.3G.auth=2
```

### 16.3.2 Package options

```
root@VA_router:~#
package network

config interface '3G'
    option proto '3g'
    option monitored '0'
    option auto '1'
    option sim 'any'
    option defaultroute '1'
    option metric '1'
    option service_order 'auto lte umts gprs'
    option apn 'test.apn'
    option username 'username'
```

```

option password 'password'
option ipv4mode 'dhcp'
option ipv6mode 'none'
option keepalive '15 10'
option operator_reselect '0'
option auth '2'

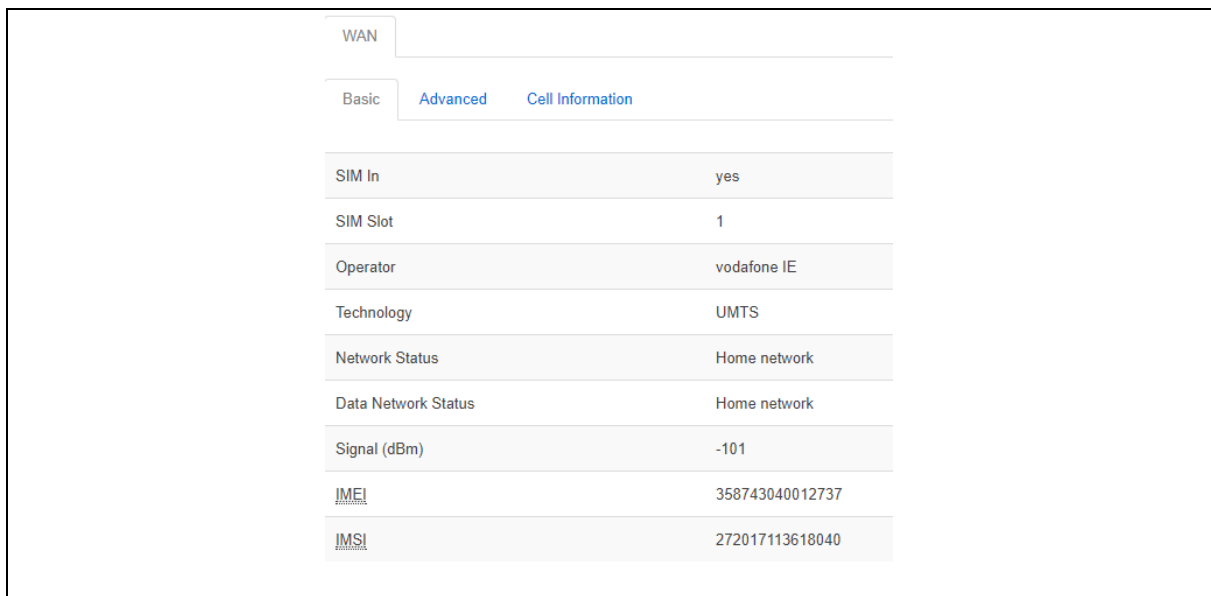
```

## 16.4 Diagnostcs

**Note:** the information presented on screen and data output using UCI depends on the actual mobile hardware being used. Therefore, the interfaces or output you see may differ from the samples shown here.

### 16.4.1 Mobile status via the web

To view mobile connectivity information, in the top menu, select **Status -> Mobile Information**. The Mobile Information page appears. The information presented depends on the actual mobile hardware used; therefore, it might differ from the samples shown here.



The screenshot shows a web interface for mobile information. At the top, there are tabs for 'WAN', 'Basic', 'Advanced', and 'Cell Information'. Below the tabs is a table with the following data:

|                     |                 |
|---------------------|-----------------|
| SIM In              | yes             |
| SIM Slot            | 1               |
| Operator            | vodafone IE     |
| Technology          | UMTS            |
| Network Status      | Home network    |
| Data Network Status | Home network    |
| Signal (dBm)        | -101            |
| <u>IMEI</u>         | 358743040012737 |
| <u>IMSI</u>         | 272017113618040 |

**Figure 111: The mobile information page**

| WAN                                       |                     |
|---|---------------------|
| Basic    Advanced <b>Cell Information</b> |                     |
| Network Status                            | Home network        |
| Data Network Status                       | Home network        |
| <u>IMEI</u>                               | 358743040012737     |
| <u>IMSI</u>                               | 272017113618040     |
| Operator                                  | vodafone IE         |
| Phone Number                              | +353874512040       |
| SIM In                                    | yes                 |
| SIM Slot                                  | 1                   |
| <u>SIM1 ICCID</u>                         | 8935301140701270414 |
| Signal (dBm)                              | -101                |
| Technology                                | UMTS                |
| Temperature (C)                           | 28                  |
| Hardware Revision                         | R1C08               |

**Figure 112: The advanced information page**

| WAN                                       |         |
|---|---------|
| <b>Basic</b> Advanced    Cell Information |         |
| Cell ID                                   | 2007516 |
| Location Area Code                        | 3023    |
| Mobile Country Code                       | 272     |
| Mobile Network Code                       | 01      |

**Figure 113: The cell information page**

## 16.4.2 Mobile status using UCI

To display information and status of mobile interfaces such as 3G, 4G or CDMA, enter:

```
root@VA_router:~# mobile_status

Mobile Interface      : WAN
Status                : idle
SIM In                : yes
SIM Slot              : 1
Operator              : vodafone IE
Technology             : UMTS
CS Network Status    : Home network
PS Network Status    : Home network
Signal (dBm)         : -107
IMEI                  : 358743040012737
IMSI                  : 272017113618040
```

For more advanced information, enter:

```
root@ VA_router:~# mobile_status -a

Mobile Interface      : WAN
Status                : idle
CS Network Status    : Home network
PS Network Status    : Home network
IMEI                  : 358743040012737
IMSI                  : 272017113618040
Operator              : vodafone IE
Phone Number          : +353874512040
SIM In                : yes
SIM Slot              : 1
SIM1 ICCID            : 8935301140701270414
Signal (dBm)         : -107
Technology             : UMTS
Temperature (C)       : 28
Hardware Revision     : R1C0
```

### 16.4.3 Mobile operator scan

To perform and display results of an operator scan, enter:

```
root@VA_router:~# mobile_operators -s
Starting operator search on phy 3-1.1 (may take some time)
Operator search finished
```

| ICCID               | Status    | MCC/MNC | Name         | Service      |
|---------------------|-----------|---------|--------------|--------------|
| 8945020184544181234 | Current   | 27201   | SimService   | LTE UMTS     |
| 8945020184544181234 | Available | 27203   | IRL - METEOR | GSM UMTS LTE |
| 8945020184544181234 | Available | 27202   | 3            | UMTS         |
| 8945020184544181234 | Available | 27205   | 3            | LTE          |

### 16.4.4 Restarting mobile

To restart all instances of vmobile on the system, enter:

```
root@ VA_router:~# /etc/init.d/usb_start_up restartmobile
usb startup: Restarting va-mobile on PHY 1-1
```

## 17 Configuring mobile manager

The Mobile Manager feature allows you to configure SIM settings.

### 17.1 Configuration package used

| Package | Sections         |
|---------|------------------|
| mobile  | main             |
|         | callers          |
|         | roaming_template |

### 17.2 Configuring mobile manager using the web interface

Select **Services -> Mobile Manager**. The Mobile Manager page appears.

There are four sections in the mobile manager page:

| Section                    | Description   |
|----------------------------|---|
| Basic                      | Enable SMS, configure SIM pin code and select roaming SIM.                          |
| Advanced                   | Configure advanced options such as collect ICCIDs and temperature polling interval. |
| CDMA*                      | CDMA configuration.   |
| Callers                    | Configure callers that can use SMS.   |
| Roaming Interface Template | Configure Preferred Roaming List options.   |

\*Option available only for CDMA modules.

#### 17.2.1 Mobile manager: basic settings

The screenshot shows the 'MAIN' configuration page for the mobile manager. It features three tabs: 'Basic', 'Advanced', and 'CDMA'. The 'Basic' tab is selected. The settings include:

- SMS Enable:** A checkbox that is checked.
- PIN-code for SIM1:** An empty text input field.
- PIN-code for SIM2:** An empty text input field.
- LTE Bands for SIM1:** An empty text input field.
- LTE Bands for SIM2:** An empty text input field.

Figure 114: The mobile manager basic page

| Web Field/UCI/Package Option  | Description   |       |           |       |                               |
|---|---|-------|-----------|-------|-------------------------------|
| Web: SMS Enable<br>UCI: mobile.main.sms<br>Opt: sms                               | Enables or disables SMS functionality.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0     | Disabled. | 1     | Enabled.                      |
| 0   | Disabled.   |       |           |       |                               |
| 1   | Enabled.  |       |           |       |                               |
| Web: PIN code for SIM1<br>UCI: mobile.main.sim1pin<br>Opt: sim1pin                | Depending on the SIM card specify the pin code for SIM 1.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>Depends on the SIM provider.</td> </tr> </table>  | Blank |           | Range | Depends on the SIM provider.  |
| Blank   |   |       |           |       |                               |
| Range   | Depends on the SIM provider.  |       |           |       |                               |
| Web: PIN code for SIM2<br>UCI: mobile.main.sim2pin<br>Opt: sim2pin                | Depending on the SIM card specify the pin code for SIM 2.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>Depends on the SIM provider.</td> </tr> </table>  | Blank |           | Range | Depends on the SIM provider.  |
| Blank   |   |       |           |       |                               |
| Range   | Depends on the SIM provider.  |       |           |       |                               |
| Web: LTE bands for SIM1<br>UCI: mobile.main.sim1_lte_bands<br>Opt: sim1_lte_bands | Depending on the SIM card, specify the LTE bands for SIM 1. Comma delimiter. Example:<br><pre>option sim1_lte_bands '3,20'</pre> Limits LTE bands to 3 and 20.<br><b>Note:</b> currently only supported by Hucom/Wetelcom, SIMCom7100, Cellient MPL200 and Asiatel.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>LTE bands range from 1 to 70.</td> </tr> </table> | Blank |           | Range | LTE bands range from 1 to 70. |
| Blank   |   |       |           |       |                               |
| Range   | LTE bands range from 1 to 70.   |       |           |       |                               |
| Web: LTE bands for SIM2<br>UCI: mobile.main.sim2_lte_bands<br>Opt:sim2_lte_bands  | Depending on the SIM card, specify the LTE bands for SIM 2. Comma delimiter. Example:<br><pre>option sim1_lte_bands '3,20'</pre> Limits LTE bands to 3 and 20.<br><b>Note:</b> currently only supported by Hucom/Wetelcom, SIMCom7100, Cellient MPL200 and Asiatel.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>LTE bands range from 1 to 70.</td> </tr> </table> | Blank |           | Range | LTE bands range from 1 to 70. |
| Blank   |   |       |           |       |                               |
| Range   | LTE bands range from 1 to 70.   |       |           |       |                               |

Table 73: Information table for mobile manager basic settings

## 17.2.2 Mobile manager: advanced settings

**MAIN**

Basic   **Advanced**   CDMA

---

Collect ICCIDs  [? Collect ICCIDs on startup](#)

Force Mode  [? Select network interface mode](#)

Temperature Polling Interval (Seconds)

Automatic Firmware Selection  [? Select firmware based on network operator - only supported on some radio modules](#)

Allow USB Power Cycle  [? Power cycle usb bus if modem disappeared from the USB bus for more then 40 seconds](#)

Figure 115: The mobile manager advanced page



| Web Field/UCI/Package Option   | Description   |           |                                     |       |                  |
|--|---|-----------|-------------------------------------|-------|------------------|
| Web: Collect ICCIDs<br>UCI: mobile.main.init_get_iccids<br>Opt: init_get_iccids  | Enables or disables integrated circuit card identifier ICCIDs collection functionality. If enabled then both SIM 1 and SIM 2 ICCIDs will be collected; otherwise it will default to SIM 1. This will be displayed under mobile stats. <table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0         | Disabled.                           | 1     | Enabled.         |
| 0  | Disabled.   |           |                                     |       |                  |
| 1  | Enabled.  |           |                                     |       |                  |
| Web: Force Mode<br>UCI: mobile.main.force_mode<br>Opt: force_mode  | Defines whether to operate mobile modem in PPP or Ethernet mode. The mode will be dependent on the service provided by the mobile provider. In general, this is Ethernet mode (default). <table border="1"> <tr> <td>Automatic</td> <td>Ethernet mode (option not present).</td> </tr> <tr> <td>PPP</td> <td>Enable PPP mode.</td> </tr> </table>   | Automatic | Ethernet mode (option not present). | PPP   | Enable PPP mode. |
| Automatic  | Ethernet mode (option not present).   |           |                                     |       |                  |
| PPP  | Enable PPP mode.  |           |                                     |       |                  |
| Web: Temperature Polling Interval<br>UCI: mobile.main.temp_poll_interval_sec<br>Opt: temp_poll_interval_sec            | Defines the time in seconds to poll the mobile module for temperature. Set to <b>0</b> to disable. <table border="1"> <tr> <td>61</td> <td>61 seconds.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 61        | 61 seconds.                         | Range |                  |
| 61   | 61 seconds.   |           |                                     |       |                  |
| Range  |   |           |                                     |       |                  |
| Web: Automatic Firmware Selection<br>UCI:<br>mobile.main.enable_firmware_autoselect<br>Opt: enable_firmware_autoselect | Enables the selection of an operator-specific firmware in the radio module. The selection is based on the ICCID of the used SIM. At module initialisation the IMSI is checked and if necessary the correct firmware image in the module will be activated. <p><b>Note:</b> activation of the firmware will lead to a delayed startup of the network interface associated with the radio module.</p> <p><b>Note:</b> this feature is currently only supported for the Telit LE910NA V2 module. Here Verizon-specific firmware will be selected if the ICCID starts with "891480".</p> <table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0         | Disabled.                           | 1     | Enabled.         |
| 0  | Disabled.   |           |                                     |       |                  |
| 1  | Enabled.  |           |                                     |       |                  |
| Web: Allow USB Power Cycle<br>UCI: mobile.main.allow_usb_powercycle<br>Opt: allow_usb_powercycle                       | Defines whether to automatically power cycle the USB modem if a mobile module is not detected for 40 seconds. <table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0         | Disabled.                           | 1     | Enabled.         |
| 0  | Disabled.   |           |                                     |       |                  |
| 1  | Enabled.  |           |                                     |       |                  |

**Table 74: Information table for mobile manager advanced settings**

### 17.2.3 Mobile manager: CDMA settings

This configuration page is only supported for CDMA modules.

**MAIN**

Basic   **Advanced**   CDMA

---

IMSI   ⓘ If specified over-writes IMSI stored in radio module

HDR Auth User ID   ⓘ AN-PPP user id. Supported on Cellient module only

HDR Auth Password   ⓘ AN-PPP password. Supported on Cellient module only

Ordered Registration triggers module reboot

Station Class Mark

Slot Cycle Index

Slot Mode

Mobile Directory Number

MOB\_TERM\_HOME registration flag

MOB\_TERM\_FOR\_SID registration flag

MOB\_TERM\_FOR\_NID

**Figure 116: The mobile manager CDMA page**

| Web Field/UCI/Package Option   | Description   |         |                       |        |                               |
|--|---|---------|-----------------------|--------|-------------------------------|
| Web: IMSI<br>UCI: mobile.main.imsi<br>Opt: imsi  | Allows the IMSI (International Mobile Subscriber Identity) to be changed.<br><table border="1"> <tr> <td>Default</td> <td>Programmed in module.</td> </tr> <tr> <td>Digits</td> <td>Up to 15 digits.</td> </tr> </table>  | Default | Programmed in module. | Digits | Up to 15 digits.              |
| Default  | Programmed in module.   |         |                       |        |                               |
| Digits   | Up to 15 digits.  |         |                       |        |                               |
| Web: HDR Auth User ID<br>UCI: mobile.main.hdr_userid<br>Opt: hdr_userid  | AN-PPP user ID. Supported on Cellient CDMA modem only.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>Depends on the CDMA provider.</td> </tr> </table>                                | Blank   |                       | Range  | Depends on the CDMA provider. |
| Blank  |   |         |                       |        |                               |
| Range  | Depends on the CDMA provider.   |         |                       |        |                               |
| Web: HDR Auth User Password<br>UCI: mobile.main.hdr_password<br>Opt: hdr_password  | AN-PPP password. Supported on Cellient CDMA modem only.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>Depends on the CDMA provider.</td> </tr> </table>                               | Blank   |                       | Range  | Depends on the CDMA provider. |
| Blank  |   |         |                       |        |                               |
| Range  | Depends on the CDMA provider.   |         |                       |        |                               |
| Web: Ordered Registration triggers module reboot<br>UCI: mobile.main.mobile.main.cdma_ordered_registration_reboot_enabled<br>Opt: cdma_ordered_registration_reboot_enabled | Enables or disables rebooting the module after the order registration command is received from a network.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0       | Disabled.             | 1      | Enabled.                      |
| 0  | Disabled.   |         |                       |        |                               |
| 1  | Enabled.  |         |                       |        |                               |
| Web: Station Class Mark<br>UCI: mobile.main.cdma_station_class_mark<br>Opt: cdma_station_class_mark  | Allows the station class mark for the MS to be changed.<br><table border="1"> <tr> <td>58</td> <td></td> </tr> <tr> <td>0-255</td> <td></td> </tr> </table>   | 58      |                       | 0-255  |                               |
| 58   |   |         |                       |        |                               |
| 0-255  |   |         |                       |        |                               |
| Web: Slot Cycle Index<br>UCI: mobile.main.cdma_slot_cycle_index<br>Opt: cdma_slot_cycle_index  | Defines the desired slot cycle index if different from the default.<br><table border="1"> <tr> <td>2</td> <td></td> </tr> <tr> <td>0-7</td> <td></td> </tr> </table>  | 2       |                       | 0-7    |                               |
| 2  |   |         |                       |        |                               |
| 0-7  |   |         |                       |        |                               |

|   |   |
|---|---|
| Web: Slot Mode<br>UCI: mobile.main.cdma_slot_mode<br>Opt: cdma_slot_mode  | Specifies the slot mode.<br>0   |
| Web: Mobile Directory Number<br>UCI: mobile.main.cdma_mobile_directory_number<br>Opt: cdma_mobile_directory_number                                  | Allows the mobile directory number (MDN) to be changed.<br>Default Programmed in module.<br>Digits Up to 15 digits.                                 |
| Web: MOB_TERM_HOME registration flag<br>UCI: mobile.main.cdma_mob_term_home_registration_flag<br>Opt: cdma_mob_term_home_registration_flag          | The MOB_TERM_HOME registration flag.<br>0 Disabled.<br>1 Enabled.   |
| Web: MOB_TERM_FOR_SID registration flag<br>UCI: mobile.main.cdma_mob_term_for_sid_registration_flag<br>Opt: cdma_mob_term_for_sid_registration_flag | The MOB_TERM_FOR_SID registration flag.<br>0 Disabled.<br>1 Enabled.  |
| Web: MOB_TERM_FOR_NID registration flag<br>UCI: mobile.main.cdma_mob_term_for_nid_registration_flag<br>Opt: cdma_mob_term_for_nid_registration_flag | The MOB_TERM_FOR_NID registration flag.<br>0 Disabled.<br>1 Enabled.  |
| Web: Access Overload Control<br>UCI: mobile.main.cdma_access_overload_control<br>Opt: cdma_access_overload_control                                  | Allows the access overload class to be changed.<br>Default Programmed into module as part of IMSI.<br>Range 0-7                                     |
| Web: Preferred Serving System<br>UCI: mobile.main.cdma_preferred_serving_system<br>Opt: cdma_preferred_serving_system                               | The CDMA Preferred Serving System(A/B).<br>5  |
| Web: Digital Analog Mode Preference<br>UCI: cdma_digital_analog_mode_preference<br>Opt: cdma_digital_analog_mode_preference                         | Digital/analog mode preference.<br>4  |
| Web: Primary Channel A<br>UCI: mobile.main.cdma_primary_channel_a<br>Opt: cdma_primary_channel_a.   | Allows the primary channel (A) to be changed.<br>283<br>1-2016 Any band class 5 channel number.   |
| Web: Primary Channel B<br>UCI: mobile.main.cdma_primary_channel_b<br>Opt: cdma_primary_channel_b  | Allows the primary channel (B) to be changed.<br>384<br>1-2016 Any band class 5 channel number.   |
| Web: Secondary Channel A<br>UCI: mobile.main.cdma_secondary_channel_a<br>Opt: cdma_secondary_channel_a  | Allows the secondary channel (A) to be changed.<br>691<br>1-2016 Any band class 5 channel number.   |
| Web: Secondary Channel B<br>UCI: mobile.main.cdma_secondary_channel_b<br>Opt: cdma_secondary_channel_b  | Allows the secondary channel (B) to be changed.<br>777<br>1-2016 Any band class 5 channel number.   |
| Web: Preferred Forward & Reverse RC<br>UCI: mobile.main.cdma_preferred_forward_and_reverse_rc<br>Opt:cdma_preferred_forward_and_reverse_rc          | The preferred forward & reverse RC value, this takes the form "forward_rc,reverse_rc"<br>0,0<br>Format forward radio channel, reverse radio channel |
| Web: SID-NID pairs<br>UCI: mobile.main.cdma_sid_nid_pairs<br>Opt:cdma_sid_nid_pairs   | Allows specification of SID:NID pairs, this takes the form "SID1,NID1,SID2,NID2,"<br>0,0<br>Format SID1 (0-65535),NID (0-65535)                     |

Table 75: Information table for mobile manager CDMA settings

## 17.2.4 Mobile manager: callers

**Callers**  
Configure caller numbers that may use the SMS service.

Name  Name of the caller.

Number  Number of the caller. Use \* for wildcard matching.

Enable

Respond

Figure 117: The mobile manager CDMA page

| Web Field/UCI/Package Option                                   | Description  |       |           |       |           |            |   |
|--|--|-------|-----------|-------|-----------|------------|---|
| Web: Name<br>UCI: mobile.@caller[0].name<br>Opt:name           | Name assigned to the caller.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>No limit.</td> </tr> </table>   | Blank |           | Range | No limit. |            |   |
| Blank  |  |       |           |       |           |            |   |
| Range  | No limit.  |       |           |       |           |            |   |
| Web: Number<br>UCI: mobile.@caller[0].number<br>Opt:number     | Number of the caller allowed to SMS the router. Add in specific caller numbers, or use the * wildcard symbol.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>No limit.</td> </tr> <tr> <td>Characters</td> <td>Global value (*) is accepted.<br/>International value (+) is accepted.</td> </tr> </table> | Blank |           | Range | No limit. | Characters | Global value (*) is accepted.<br>International value (+) is accepted. |
| Blank  |  |       |           |       |           |            |   |
| Range  | No limit.  |       |           |       |           |            |   |
| Characters   | Global value (*) is accepted.<br>International value (+) is accepted.  |       |           |       |           |            |   |
| Web: Enable<br>UCI: mobile.@caller[0].enabled<br>Opt:enabled   | Enables or disables incoming caller ID.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0     | Disabled. | 1     | Enabled.  |            |   |
| 0  | Disabled.  |       |           |       |           |            |   |
| 1  | Enabled.   |       |           |       |           |            |   |
| Web: Respond<br>UCI: mobile.@caller[0].respond<br>Opt: respond | If checked, the router will return an SMS. Select <b>Respond</b> if you want the router to reply.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0     | Disabled. | 1     | Enabled.  |            |   |
| 0  | Disabled.  |       |           |       |           |            |   |
| 1  | Enabled.   |       |           |       |           |            |   |

Table 76: Information table for mobile manager callers settings

## 17.2.5 Mobile manager: roaming interface template

For more information on Roaming Interface Template configuration, read the chapter, 'Automatic Operator Selection'.

## 17.3 Configuring mobile manager using command line

### 17.3.1 Mobile manager using UCI

The configuration files for mobile manager are stored on **/etc/config/mobile**

The following example shows how to enable the SMS functionality to receive and respond from certain caller ID numbers.

```
root@VA_router:~# uci show mobile
uci set mobile.main=mobile
```

```
uci set mobile.main.sim1pin=0000
uci set mobile.main.sim2pin=0000
uci set mobile.main.sim1_lte_bands='3,20'
uci set mobile.main.sim2_lte_bands='4,5'
uci set mobile.main.temp_poll_interval_sec=61
uci set mobile.main.enable_firmware_autoselect=0
uci set mobile.main.allow_usb_powercycle=1
uci set mobile.main.roaming_sim=none
uci set mobile.main.sms=1
uci set mobile.main.hdr_password=5678
uci set mobile.main.hdr_userid=1234
uci set mobile.main.init_get_iccids=1
uci set mobile.@caller[0]=caller
uci set mobile.@caller[0].name=user1
uci set mobile.@caller[0].number=3538712345678
uci set mobile.@caller[0].enabled=1
uci set mobile.@caller[0].respond=1
uci set mobile.@caller[1]=caller
uci set mobile.@caller[1].name=user2
uci set mobile.@caller[1].number=3538723456789
uci set mobile.@caller[1].enabled=1
uci set mobile.@caller[1].respond=1
```

### 17.3.2 Mobile manager using package options

```
root@VA_router:~# uci export mobile
package mobile
config mobile 'main'
    option sim1pin '0000'
    option sim2pin '0000'
    option roaming_sim 'none'
    option sms '1'
    option hdr_password '5678'
    option hdr_userid '1234'
    option init_get_iccids '1'
    option sim1_lte_bands '3,20'
    option sim2_lte_bands '4,5'
```

```

option temp_poll_interval_sec '61'
option enable_firmware_autoselect '0'
option allow_usb_powercycle '1'

config caller
option name 'vasupport'
option number '353871234567'
option enabled '1'
option respond '1'

config caller
option name 'vasupport1'
option number '353872345678'
option enabled '1'
option respond '1'

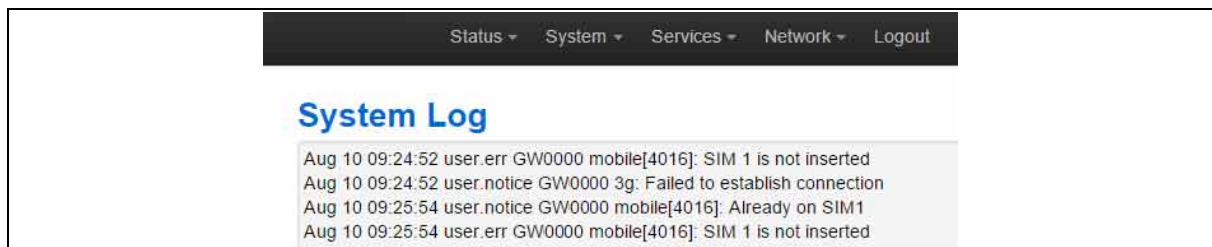
```

## 17.4 Monitoring SMS

You can monitor inbound SMS messages using the router's web browser or via an SSH session.

To monitor SMS using the web browser, login and select **Status > system log**.

Scroll to the bottom of the log to view the SMS message.



**Figure 118: Example of output from system log**

To monitor using SSH, login and enter:

```
logread -f &
```

Or, when logging system messages to a flash file at `/root/syslog.messages`

```
tail -f /root/syslog.messages &
```

## 17.5 Sending SMS from the router

You can send an outgoing message via the command line using the following syntax:

```
sendsms 353879876543 'hello'  
root@VirtualAccess:~# Aug 10 16:29:1 user.notice VirtualAccess  
mobile[1737]: Queue sms to 353879876543 "hello"
```

## 17.6 Sending SMS to the router

The router can accept UCI show and set commands via SMS if the caller is enabled.

**Note:** commands are case sensitive.

An example would be to SMS the SIM card number by typing the following command on the phone and checking the SMS received from the router.

```
uci show mobile.@caller[0].number
```

Multiple commands can be sent in a single SMS using a semicolon (;) separator; for example, to set the router to factory config and then reboot.

```
vacmd set next config factconf;reboot
```

## 18 Configuring multi-APNs for mobile interfaces

The GW1000M, GW1150 and GW2300 Series routers support simultaneous multiple APN connections to be connected using a single SIM card. Up to two APNs per SIM are currently supported.

Support for this feature is limited to specific mobile modules.

### 18.1 Supported mobile modules

| Vendor  | Module        |
|---------|---------------|
| Quectel | Quectel EC25  |
| SIMCOM  | SIMCOM7600E-H |

### 18.2 Multi-APN overview

A PDP (Packet Data Protocol) context is a data structure that exists within the mobile service provider's network that contains a subscriber's session information when the subscriber has an active session. The PDP context data structure contains:

- the subscriber's IP address,
- IMSI (International Mobile Subscriber Identity), and
- APN (Access Point Name).

It is sometimes required to connect to two different APNs at the same time. This can be achieved with a single SIM card using separate PDP contexts.

**Note:** the SIM card must allow connection to each of the APNs. Also, two PDP contexts from the same SIM card cannot use the same APN.

You can use routing and VRF support for each PDP context by referring to the unique interface name that the APN is configured under. Routing and VRF support can be utilised for each PDP context. For more information on these features, read chapters 'Configuring Static Routes' and 'VRF: Virtual Router Forwarding'.

Multi-WAN can control routing to each PDP context in the same way it can control routing to other interfaces. However, in package multiwan `option manage_state`, set to **no** for both multiwan interface configurations. Multiwan will then control routing through each PDP context by altering the interface metric to '-1' when it determines the interface has failed its health check.

### 18.3 Configuration package used

| Package | Sections  |
|---------|-----------|
| network | interface |



## 18.4 Configuring multi-APN

### 18.4.1 Configuring multi-APN using the web UI

To configure Multi-APN, select **Network -> Interface**. A unique PDP context needs to be configured on each mobile interface. For more information on how to configure a mobile interface, read the chapter 'Configuring a mobile connection'.

**Note:** on each mobile interface set **option sim** to the same number and not to **any**.

| Network                 | Status   | Actions                  |
|-------------------------|--|--------------------------|
| MOBILE1<br>qmimux0      | Uptime: 0h 10m 23s<br>RX: 616.00 B (2 Pkts.)<br>TX: 1.23 KB (8 Pkts.)<br>IPv4: 10.208.85.53/30   | Connect Stop Edit Delete |
| MOBILE2<br>qmimux1      | Uptime: 0h 10m 21s<br>RX: 4.51 KB (47 Pkts.)<br>TX: 7.19 KB (101 Pkts.)<br>IPv4: 10.209.38.182/30  | Connect Stop Edit Delete |
| LAN<br>Master "OpenWrt" | MAC Address: 00:AA:BB:CC:DD:13<br>RX: 0.00 B (0 Pkts.)<br>TX: 1.13 KB (10 Pkts.)<br>IPv4: 192.168.100.1/24   | Connect Stop Edit Delete |
| LOOPBACK<br>lo          | Uptime: 0h 10m 49s<br>MAC Address: 00:00:00:00:00:00<br>RX: 46.83 KB (374 Pkts.)<br>TX: 46.83 KB (374 Pkts.)<br>IPv4: 127.0.0.1/8<br>IPv6: ::1/128 | Connect Stop Edit Delete |
| WLAN<br>wlan            | Unsupported protocol type.<br><a href="#">Install protocol extensions...</a>   | Connect Stop Edit Delete |

Add new interface...

Figure 119: The network interface page

On the the desired mobile interface, select **Edit** and then select **Advanced Settings**.

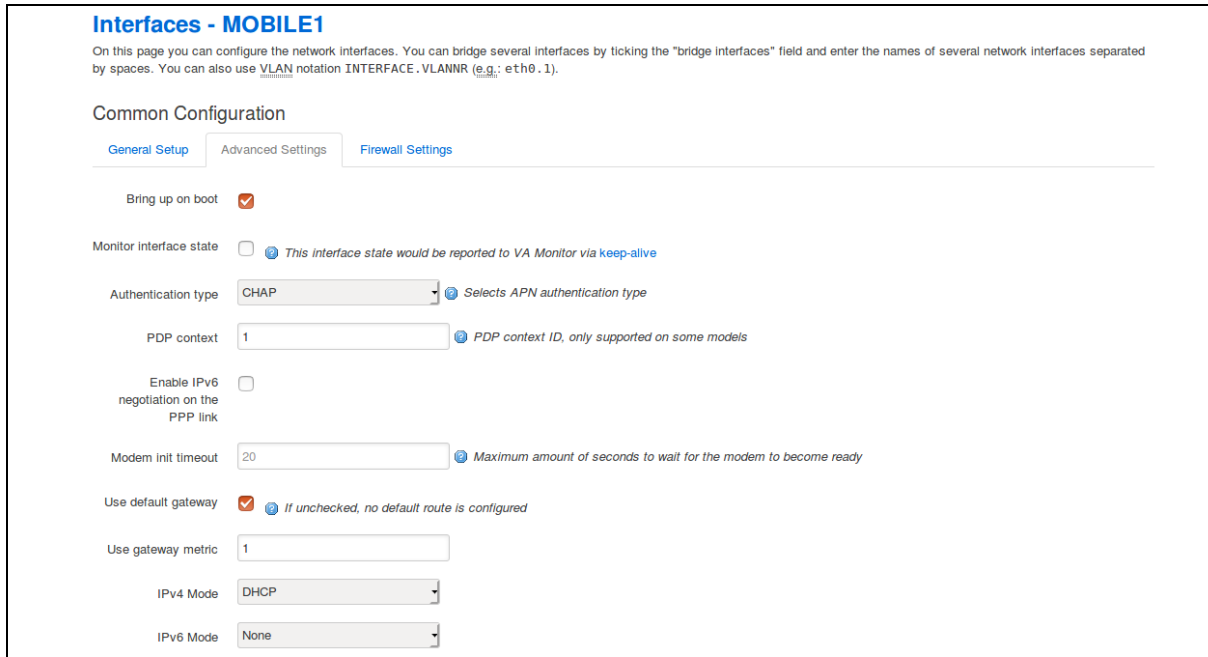


Figure 120: Mobile interface advanced settings page

| Web Field/UCI/Package Option  | Description   |   |  |       |       |
|---|---|---|--|-------|-------|
| Web: PDP context<br>UCI: network.[interface].pdp_context<br>Opt:pdp_context | Defines the PDP context ID. Should multiple active PDP contexts be supported, you must configure interfaces with different PDP context IDs. |   |  |       |       |
|   | <table border="1"> <tr> <td>1</td> <td></td> </tr> <tr> <td>Range</td> <td>1 - 4</td> </tr> </table>  | 1 |  | Range | 1 - 4 |
| 1   |   |   |  |       |       |
| Range   | 1 - 4   |   |  |       |       |

Table 77: Information table for Multi-APN

## 18.4.2 Configuring multi-APN using the command line

You can configure multi-APN using the interface configuration section in the network package /etc/config/network using the option `pdp_context`. The option value should be an integer that is unique to each APN configuration.

### 18.4.2.1 Multi-APN using UCI

```

root@VA_router:~# uci show network
package network
.....
network.Mobile1=interface
network.Mobile1.proto=3g
network.Mobile1.apn=open.internet
network.Mobile1.username=gprs
network.Mobile1.password=gprs
network.Mobile1.sim=1
network.Mobile1.service=auto
network.Mobile1.metric=1
    
```

```

network.Mobile1.pdp_context=1
network.Mobile2=interface
network.Mobile2.proto=3g
network.Mobile2.apn=3ireland.ie
network.Mobile2.sim=1
network.Mobile2.service=auto
network.Mobile2.metric=1
network.Mobile2.pdp_context=2

```

### 18.4.2.2 Configuring multi-APN using package options

```

root@VA_router:~# uci export network
package network
.....
config interface 'Mobile1'
    option proto '3g'
    option apn 'open.internet'
    option username 'gprs'
    option password 'gprs'
    option sim '1'
    option service 'auto'
    option metric '1'
    option pdp_context '1'

config interface 'Mobile2'
    option proto '3g'
    option apn '3ireland.ie'
    option sim '1'
    option service 'auto'
    option metric '1'
    option pdp_context '2'

```

### 18.4.2.3 Example of simple routing over multi-APN using UCI

```

root@VA_router:~# uci show network
package network
.....
network.Mobile1=interface

```

```

network.Mobile1.proto=3g
network.Mobile1.apn=open.internet
network.Mobile1.username=gprs
network.Mobile1.password=gprs
network.Mobile1.sim=1
network.Mobile1.service=auto
network.Mobile1.metric=1
network.Mobile1.pdp_context=1
network.Mobile1.defaultroute=0
network.Mobile2=interface
network.Mobile2.proto=3g
network.Mobile2.apn=3ireland.ie
network.Mobile2.sim=1
network.Mobile2.service=auto
network.Mobile2.metric=1
network.Mobile2.pdp_context=2
network.Mobile1.defaultroute=0
.....
network.8888=route
network.8888.interface=Mobile1
network.8888.target=8.8.8.8
network.8888.netmask=255.255.255.255
network.8844=route
network.8844.interface=Mobile1
network.8844.target=8.8.4.4
network.8844.netmask=255.255.255.255

```

## 18.5 Multi-APN diagnostics

### 18.5.1 Interface status

When active, to see the status of interfaces with multiple APNs, enter:

```

root@VA_router:~# ifconfig
.....

qmimux0  Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.205.77.223  P-t-P:10.205.77.223  Mask:255.255.255.192
          inet6 addr: fe80::9bb3:25f7:278c:a8f1/64  Scope:Link

```

```

UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
RX packets:5 errors:0 dropped:0 overruns:0 frame:0
TX packets:23 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:1540 (1.5 KiB)  TX bytes:3976 (3.8 KiB)

qmimux1  Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00
inet addr:10.209.38.182  P-t-P:10.209.38.182  Mask:255.255.255.252
inet6 addr: fe80::89f2:b5d5:f017:ae91/64  Scope:Link
UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
RX packets:94 errors:0 dropped:0 overruns:0 frame:0
TX packets:293 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:9032 (8.8 KiB)  TX bytes:20860 (20.3 KiB)

```

To check which mobile interface corresponds to the output from the `ifconfig` command shown above, enter:

```

root@VA_router:~# network_status -a

Interface:      Mobile1
Status:         Up
Uptime:         00h 05m 30s
IPv4 addresses: 10.202.187.228/29
MAC address:    00:00:00:00:00:00
Device name:    "qmimux0"

Interface:      Mobile2
Status:         Up
Uptime:         00h 05m 27s
IPv4 addresses: 10.201.206.252/29
MAC address:    00:00:00:00:00:00
Device name:    "qmimux1"

```

## 18.5.2 Routing table

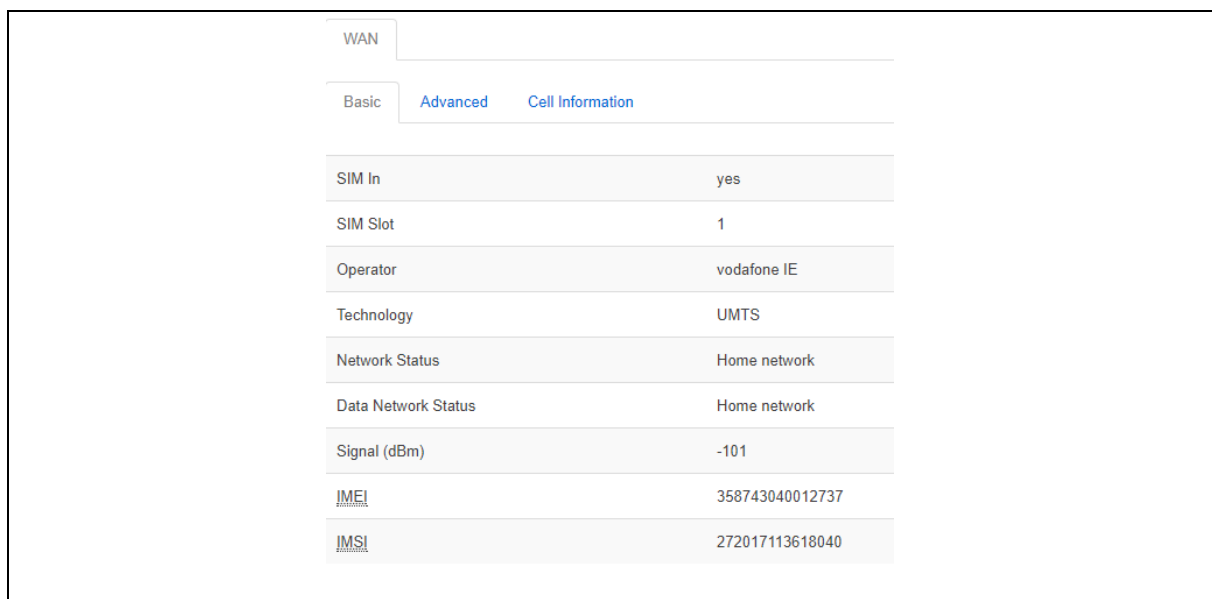
To check the routing table, enter:

```
root@VA_router:~# ip route
8.8.4.4 via 10.204.5.101 dev qmimux0
8.8.8.8 via 10.204.5.101 dev qmimux0
10.204.5.100/30 dev qmimux0 proto kernel scope link src 10.204.5.102
10.209.38.180/30 dev qmimux1 proto kernel scope link src 10.209.38.182
192.168.100.0/24 dev eth0 proto kernel scope link src 192.168.100.1
192.168.101.0/24 dev wlan0 proto kernel scope link src 192.168.101.1
192.168.101.0/24 dev wlan1 proto kernel scope link src 192.168.101.1
```

## 18.5.3 Mobile status

### 18.5.3.1 Mobile status via the web

To view mobile connectivity information, in the top menu, select **Status -> Mobile Information**. The Mobile Information page appears. The information presented depends on the actual mobile hardware used; it might therefore differ from the samples shown in this document.



| WAN                                    |                 |
|--|-----------------|
| Basic <b>Advanced</b> Cell Information |                 |
| SIM In                                 | yes             |
| SIM Slot                               | 1               |
| Operator                               | vodafone IE     |
| Technology                             | UMTS            |
| Network Status                         | Home network    |
| Data Network Status                    | Home network    |
| Signal (dBm)                           | -101            |
| <u>IMEI</u>                            | 358743040012737 |
| <u>IMSI</u>                            | 272017113618040 |

Figure 121: The mobile information page

| WAN                                   |                     |
|---------------------------------------|---------------------|
| Basic    Advanced    Cell Information |                     |
| Network Status                        | Home network        |
| Data Network Status                   | Home network        |
| <u>IMEI</u>                           | 358743040012737     |
| <u>IMSI</u>                           | 272017113618040     |
| Operator                              | vodafone IE         |
| Phone Number                          | +353874512040       |
| SIM In                                | yes                 |
| SIM Slot                              | 1                   |
| <u>SIM1 ICCID</u>                     | 8935301140701270414 |
| Signal (dBm)                          | -101                |
| Technology                            | UMTS                |
| Temperature (C)                       | 28                  |
| Hardware Revision                     | R1C08               |

**Figure 122: The advanced information page**

| WAN                                   |         |
|---------------------------------------|---------|
| Basic    Advanced    Cell Information |         |
| Cell ID                               | 2007516 |
| Location Area Code                    | 3023    |
| Mobile Country Code                   | 272     |
| Mobile Network Code                   | 01      |

**Figure 123: The cell information page**

### 18.5.3.2 Mobile status using UCI

To display information and status of mobile interfaces such as 3G, 4G or CDMA, enter:

```
root@VA_router:~# mobile_status

Mobile Interface      : WAN
Status               : idle
SIM In               : yes
SIM Slot             : 1
Operator             : vodafone IE
Technology           : UMTS
CS Network Status    : Home network
PS Network Status    : Home network
Signal (dBm)        : -107
IMEI                 : 358743040012737
IMSI                 : 272017113618040
```

For more advanced information, enter `mobile_status -a`:

```
root@ VA_router:~# mobile_status -a

Mobile Interface      : WAN
Status               : idle
CS Network Status    : Home network
PS Network Status    : Home network
IMEI                 : 358743040012737
IMSI                 : 272017113618040
Operator             : vodafone IE
Phone Number         : +353874512040
SIM In               : yes
SIM Slot             : 1
SIM1 ICCID           : 8935301140701270414
Signal (dBm)        : -107
Technology           : UMTS
Temperature (C)      : 28
Hardware Revision    : R1C0
```



## 19 Configuring a GRE interface

General Routing Encapsulation (GRE) is a tunnelling protocol used for encapsulation of other communication protocols inside point to point links over IP.

### 19.1 Configuration packages used

| Package | Sections  |
|---------|-----------|
| network | interface |

### 19.2 Creating a GRE connection using the web interface

To create GRE interfaces through the web interface, in the top menu, select **Network - > Interfaces**.

There are three sections in the Interfaces page.

| Section            | Description  |
|--------------------|--|
| Interface Overview | Shows existing interfaces and their status. You can create new, and edit existing interfaces here.   |
| Port Map           | In this section you can map device ports to Ethernet interfaces. Ports are marked with capital letters starting with 'A'. Type in space separated port numbers in the port map fields. |
| ATM Bridges        | ATM bridges expose encapsulated Ethernet in AAL5 connections as virtual Linux network interfaces, which can be used in conjunction with DHCP or PPP to dial into the provider network. |

In the Interface Overview section, click **Add new interface**. The Create Interface page appears.

Figure 124: The create interface page

| Web Field/UCI/Package Option  | Description   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |            |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
|---|---|--------|-------------|--------|--|-------------|---|-----------|-------------|------------------------|---------------------------|----------------|-------------------------------------|------------|--|-----|--|------|-----------------------------|-----|-------------------------|-------|-------------------|---------|--------------|---------------------|---|
| Web: Name of the new interface<br>UCI: network. <if name><br>Opt: config interface  | Assigns a logical name to the GRE tunnel. The network interface section will be assigned this name <if name>.<br>Type the name of the new interface.<br>Allowed characters are A-Z, a-z, 0-9 and _.<br>Must be less than 11 characters.   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |            |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| Web: Protocol of the new interface<br>UCI: network.<if name>.proto<br>Opt: proto    | Specifies what protocol the interface will operate on. Select <b>GRE</b> . <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Static</td> <td>Static configuration with fixed address and netmask.</td> </tr> <tr> <td>DHCP Client</td> <td>Address and netmask are assigned by DHCP.</td> </tr> <tr> <td>Unmanaged</td> <td>Unspecified</td> </tr> <tr> <td>IPv6-in-IPv4 (RFC4213)</td> <td>Used with tunnel brokers.</td> </tr> <tr> <td>IPv6-over-IPv4</td> <td>Stateless IPv6 over IPv4 transport.</td> </tr> <tr> <td><b>GRE</b></td> <td>Generic Routing Encapsulation protocol</td> </tr> <tr> <td>IOT</td> <td></td> </tr> <tr> <td>L2TP</td> <td>Layer 2 Tunnelling Protocol</td> </tr> <tr> <td>PPP</td> <td>Point-to-Point protocol</td> </tr> <tr> <td>PPPoE</td> <td>PPP over Ethernet</td> </tr> <tr> <td>PPPoATM</td> <td>PPP over ATM</td> </tr> <tr> <td>LTE/UMTS/GPRS/EV-DO</td> <td>CDMA, UMTS or GPRS connection using an AT-style 3G modem.</td> </tr> </tbody> </table> | Option | Description | Static | Static configuration with fixed address and netmask. | DHCP Client | Address and netmask are assigned by DHCP. | Unmanaged | Unspecified | IPv6-in-IPv4 (RFC4213) | Used with tunnel brokers. | IPv6-over-IPv4 | Stateless IPv6 over IPv4 transport. | <b>GRE</b> | Generic Routing Encapsulation protocol | IOT |  | L2TP | Layer 2 Tunnelling Protocol | PPP | Point-to-Point protocol | PPPoE | PPP over Ethernet | PPPoATM | PPP over ATM | LTE/UMTS/GPRS/EV-DO | CDMA, UMTS or GPRS connection using an AT-style 3G modem. |
| Option  | Description   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |            |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| Static  | Static configuration with fixed address and netmask.  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |            |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| DHCP Client   | Address and netmask are assigned by DHCP.   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |            |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| Unmanaged   | Unspecified   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |            |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| IPv6-in-IPv4 (RFC4213)  | Used with tunnel brokers.   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |            |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| IPv6-over-IPv4  | Stateless IPv6 over IPv4 transport.   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |            |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| <b>GRE</b>  | Generic Routing Encapsulation protocol  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |            |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| IOT   |   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |            |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| L2TP  | Layer 2 Tunnelling Protocol   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |            |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| PPP   | Point-to-Point protocol   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |            |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| PPPoE   | PPP over Ethernet   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |            |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| PPPoATM   | PPP over ATM  |        |             |        |  |             |   |           |             |                        |                           |                |                                     |            |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| LTE/UMTS/GPRS/EV-DO   | CDMA, UMTS or GPRS connection using an AT-style 3G modem.   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |            |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| Web: Create a bridge over multiple interfaces<br>UCI: network.<if name><br>Opt: n/a | Not applicable for GRE.   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |            |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |
| Web: Cover the following interface<br>UCI: network.<if name><br>Opt:n/a             | Not applicable for GRE.   |        |             |        |  |             |   |           |             |                        |                           |                |                                     |            |  |     |  |      |                             |     |                         |       |                   |         |              |                     |   |

**Table 78: Information table for the create new interface page**

Click **Submit**. The Common Configuration page appears. There are three sections in the Common Configurations page.

| Section           | Description  |
|-------------------|--|
| General Setup     | Configure the basic interface settings such as protocol, IP address, mask length, local interface, remote IP address, TTL, tunnel key and MTU. |
| Advanced Settings | 'Bring up on boot' and 'monitor interface state' settings.   |
| Firewall settings | Assign a firewall zone to the connection.  |

### 19.2.1 GRE connection: common configuration: general setup

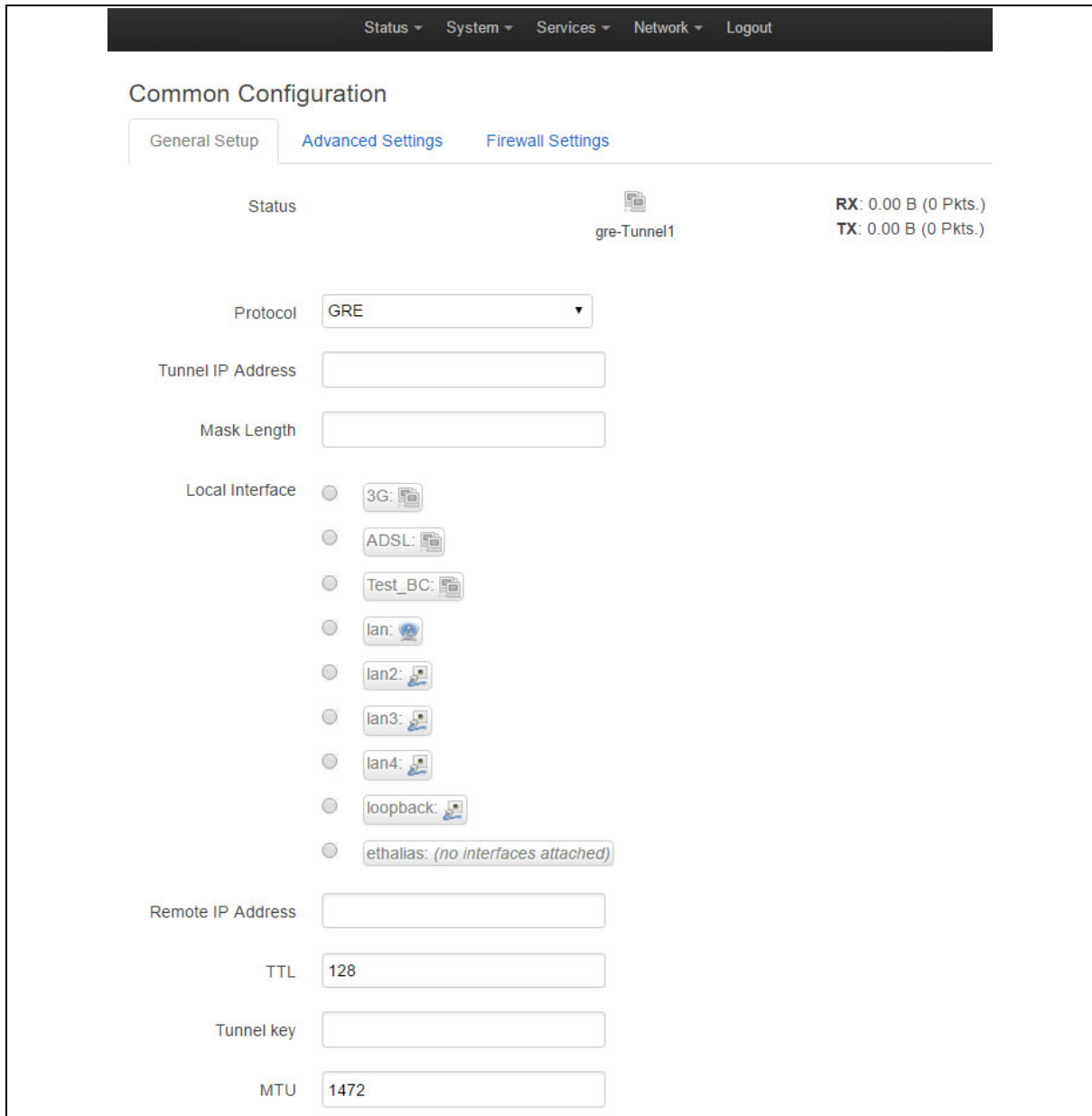


Figure 125: The GRE common configuration page

| Web Field/UCI/Package Option   | Description  |    |  |       |        |
|--|--|----|--|-------|--------|
| Web: Protocol of the new interface<br>UCI: network.<if name>.proto<br>Opt: proto | Shows the protocol the interface will operate on. GRE should be currently selected.                    |    |  |       |        |
| Web: Tunnel IP Address<br>UCI: network.<if name>.ipaddr<br>Opt: ipaddr           | Configures local IP address of the GRE interface.  |    |  |       |        |
| Web: Mask Length<br>UCI: network.<if name>.mask_length<br>Opt: mask_length       | Subnet mask, in CIDR notation, to be applied to the tunnel. Typically '30' for point-to-point tunnels. |    |  |       |        |
|  | <table border="1"> <tr> <td>24</td> <td></td> </tr> <tr> <td>Range</td> <td>0 - 30</td> </tr> </table> | 24 |  | Range | 0 - 30 |
| 24   |  |    |  |       |        |
| Range  | 0 - 30   |    |  |       |        |

|  |  |      |  |       |  |
|--|--|------|--|-------|--|
| Web: Local Interface<br>UCI: network.<if name>.local_interface<br>Opt: local_interface | Specifies which interface is going to be linked with the GRE tunnel interface (optional).  |      |  |       |  |
| Web: Remote IP address<br>UCI: network.<if name>.remote_ip<br>Opt: remote_ip           | For point to point tunnels; specifies remote IP address.   |      |  |       |  |
| Web: TTL<br>UCI: network.<if name>.ttl<br>Opt: ttl                                     | Sets Time-To-Live value on the interface.<br><table border="1" style="width: 100%;"> <tr><td style="text-align: center;">128</td><td></td></tr> <tr><td style="text-align: center;">Range</td><td></td></tr> </table>                                      | 128  |  | Range |  |
| 128  |  |      |  |       |  |
| Range  |  |      |  |       |  |
| Web: Tunnel key<br>UCI: network.<if name>.key<br>Opt: key                              | Sets GRE tunnel ID key (optional).<br>Usually an integer.  |      |  |       |  |
| Web: MTU<br>UCI: network.<if name>.mtu<br>Opt: mtu                                     | Configures MTU (maximum transmission unit) size of PDUs using this interface.<br><table border="1" style="width: 100%;"> <tr><td style="text-align: center;">1472</td><td></td></tr> <tr><td style="text-align: center;">Range</td><td></td></tr> </table> | 1472 |  | Range |  |
| 1472   |  |      |  |       |  |
| Range  |  |      |  |       |  |

Table 79: Information table for GRE

## 19.2.2 GRE connection: common configuration-advanced settings

Common Configuration

General Setup   **Advanced Settings**   Firewall Settings

---

Bring up on boot

Monitor interface state  This interface state would be reported to VA Monitor via [keep-alive](#)

Dependant interfaces

- GRETUNNEL1:
- MOBILE\_amlan:
- MOBILE\_voda:
- PoAADSL:
- SUBNET1: (no interfaces attached)
- SUBNET2:
- SUBNET3:
- SUBNET4:
- loopback:

Check interfaces which should start after this interface is started and stop after this interface is stopped

SNMP Alias ifindex  Alias ifindex SNMP agent. Alias indexes are present at 1000 offset. So setting 1 here will create snmp ifTable entry 1001.  
Useful when interface creates new linux interface on every startup (e.g. ppp interface). With this set the interface could be monitored via constant snmp agent interface table entry

Figure 126: GRE advanced settings page

| Web Field/UCI/Package Option   | Description   |       |                                |       |                   |     |                  |      |               |      |               |
|--|---|-------|--------------------------------|-------|-------------------|-----|------------------|------|---------------|------|---------------|
| Web: Bring up on boot<br>UCI: network.<if name>.auto<br>Opt: auto                            | Enables the interface to connect automatically on boot up.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0     | Disabled.                      | 1     | Enabled.          |     |                  |      |               |      |               |
| 0  | Disabled.   |       |                                |       |                   |     |                  |      |               |      |               |
| 1  | Enabled.  |       |                                |       |                   |     |                  |      |               |      |               |
| Web: Monitor interface state<br>UCI: network.<if name>.monitored<br>Opt: monitored           | Enabled if status of interface is presented on Monitoring platform.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0     | Disabled.                      | 1     | Enabled.          |     |                  |      |               |      |               |
| 0  | Disabled.   |       |                                |       |                   |     |                  |      |               |      |               |
| 1  | Enabled.  |       |                                |       |                   |     |                  |      |               |      |               |
| Web: Dependant Interfaces<br>UCI: network[..x..].dependants<br>Opt: dependants               | Lists interfaces that are dependant on this parent interface. Dependant interfaces will go down when parent interface is down and will start or restart when parent interface starts. Separate multiple interfaces by a space when using UCI. Example: option dependants 'PPPADSL MOBILE'<br>This replaces the following previous options in child interfaces.<br><table border="1"> <tr> <td>gre</td> <td>option local_interface</td> </tr> <tr> <td>lt2p</td> <td>option src_ipaddr</td> </tr> <tr> <td>iot</td> <td>option wan1 wan2</td> </tr> <tr> <td>6in4</td> <td>option ipaddr</td> </tr> <tr> <td>6to4</td> <td>option ipaddr</td> </tr> </table> | gre   | option local_interface         | lt2p  | option src_ipaddr | iot | option wan1 wan2 | 6in4 | option ipaddr | 6to4 | option ipaddr |
| gre  | option local_interface  |       |                                |       |                   |     |                  |      |               |      |               |
| lt2p   | option src_ipaddr   |       |                                |       |                   |     |                  |      |               |      |               |
| iot  | option wan1 wan2  |       |                                |       |                   |     |                  |      |               |      |               |
| 6in4   | option ipaddr   |       |                                |       |                   |     |                  |      |               |      |               |
| 6to4   | option ipaddr   |       |                                |       |                   |     |                  |      |               |      |               |
| Web: SNMP Alias ifindex<br>UCI: network[..x..].snmp_alias_ifindex<br>Opt: snmp_alias_ifindex | Defines a static SNMP interface alias index for this interface, that can be polled via the SNMP interface index (snmp_alias_ifindex+1000). For more information, read the chapter 'Configuring SNMP'.<br><table border="1"> <tr> <td>Blank</td> <td>No SNMP interface alias index.</td> </tr> <tr> <td>Range</td> <td>0 - 4294966295</td> </tr> </table>  | Blank | No SNMP interface alias index. | Range | 0 - 4294966295    |     |                  |      |               |      |               |
| Blank  | No SNMP interface alias index.  |       |                                |       |                   |     |                  |      |               |      |               |
| Range  | 0 - 4294966295  |       |                                |       |                   |     |                  |      |               |      |               |

Table 80: Information table for GRE advanced settings

### 19.2.3 GRE connection: firewall settings

Use this section to select the firewall zone you want to assign to this interface.

Select **unspecified** to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

Figure 127: GRE firewall settings

Click **Save and Apply**. This will save the current settings and return you to the Interface Overview page. To configure further settings on the GRE interface select **EDIT** for the relevant GRE interface.

#### 19.2.4 GRE connection: adding a static route

After you have configured the GRE interface, you must configure a static route, to route the desired traffic over the GRE tunnel. To do this, browse to **Network -> Static Routes**. For more information, read the chapter 'Configuring Static Routes'.

### 19.3 GRE configuration using command line

The configuration file is stored on `/etc/config/network`

For the examples below, tunnel1 is used as the interface logical name.

#### 19.4 GRE configuration using UCI

```
root@VA_router:~# uci show network
network.tunnel1=interface
network.tunnel1.proto=gre
network.tunnel1.monitored=0
network.tunnel1.ipaddr=172.255.255.2
network.tunnel1.mask_length=24
network.tunnel1.local_interface=wan
network.tunnel1.remote_ip=172.255.255.100
network.tunnel1.ttl=128
network.tunnel1.key=1234
network.tunnel1.mtu=1472
network.tunnel1.auto=1
```

#### 19.5 GRE configuration using package options

```
root@VA_router:~# uci export network
config interface 'tunnel1'
    option proto 'gre'
    option monitored '0'
    option ipaddr '172.255.255.2'
    option mask_length '24'
    option local_interface 'wan'
    option remote_ip '172.255.255.100'
    option ttl '128'
```

```
option key '1234'
option mtu '1472'
option auto '1'
```

To change any of the above values use `uci set` command.

## 19.6 GRE diagnostics

### 19.6.1 GRE interface status

To show the current running interfaces, enter:

```
root@VA_router:~# ifconfig
base0      Link encap:Ethernet  HWaddr 00:00:00:00:01:01
            inet6 addr: fe80::200:ff:fe00:101/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1504  Metric:1
            RX packets:39810 errors:0 dropped:0 overruns:0 frame:0
            TX packets:365 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:10889090 (10.3 MiB)  TX bytes:68820 (67.2 KiB)
eth4       Link encap:Ethernet  HWaddr 00:1E:10:1F:00:00
            inet addr:10.68.66.54  Bcast:10.68.66.55  Mask:255.255.255.252
            inet6 addr: fe80::21e:10ff:felf:0/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:81 errors:0 dropped:0 overruns:0 frame:0
            TX packets:127 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:8308 (8.1 KiB)  TX bytes:12693 (12.3 KiB)
gre-Tunnell1 Link encap:UNSPEC  HWaddr 0A-44-42-36-DB-B0-00-48-00-00-00-00-00-00-00-00
            inet addr:13.13.13.2  Mask:255.255.255.248
            inet6 addr: fe80::5efe:a44:4236/64 Scope:Link
            UP RUNNING MULTICAST  MTU:1472  Metric:1
            RX packets:7 errors:0 dropped:0 overruns:0 frame:0
            TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:912 (912.0 B)  TX bytes:884 (884.0 B)
lo         Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
```

```

UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:1465 errors:0 dropped:0 overruns:0 frame:0
TX packets:1465 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:166202 (162.3 KiB) TX bytes:166202 (162.3 KiB)

```

To display a specific GRE interface, enter `ifconfig gre-<if name>`:

```

root@VA_router:~# ifconfig gre-Tunnell
gre-Tunnell  Link encap:UNSPEC HWaddr 0A-44-42-36-00-00-7F-E2-00-00-00-00-00-00-00-00
              inet addr:13.13.13.2  Mask:255.255.255.248
              inet6 addr: fe80::5efe:a44:4236/64 Scope:Link
              UP RUNNING MULTICAST MTU:1472 Metric:1
              RX packets:7 errors:0 dropped:0 overruns:0 frame:0
              TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:0
              RX bytes:912 (912.0 B) TX bytes:8GRE route status

```

To show the current GRE route status, enter:

```

root@VA_router:~# route -n
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use
Iface
0.0.0.0          10.68.66.53     0.0.0.0         UG    0      0      0 eth4
0.0.0.0          13.13.13.1      0.0.0.0         UG    1      0      0 gre-
Tunnell
10.68.66.52     0.0.0.0         255.255.255.252 U    0      0      0 eth4
13.13.13.0      0.0.0.0         255.255.255.248 U    0      0      0 gre-
Tunnell
172.19.101.3    13.13.13.1      255.255.255.255 UGH   0      0      0 gre-
Tunnell

```

**Note:** a GRE route will only be displayed in the routing table when the interface is up.



## 20 Configuring VRF (Virtual Router Forwarding)

Virtual Routing and Forwarding (VRF) is a technology that allows multiple instances of a routing table to exist in a router and work simultaneously. Traffic between routing tables is segregated and so increases security.

### 20.1 VRF overview

An interface is configured to belong to a VRF. Interfaces included in the VRF form an independent routing domain, so routing of incoming and outgoing packets only happens within a VRF. It is also possible to add individual routes to a VRF using static routes.

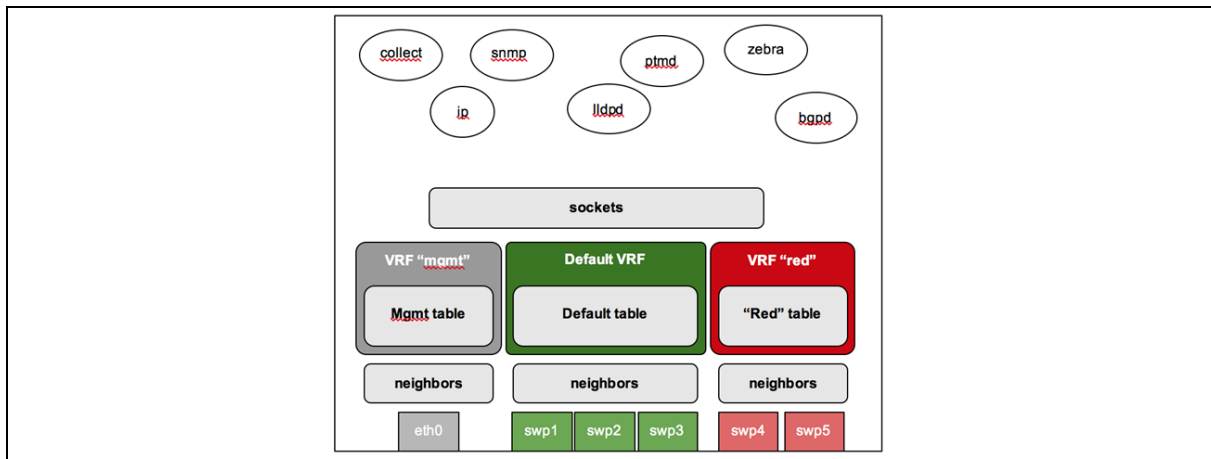


Figure 128: VRF architecture

### 20.2 Configuration package used

| Package | Sections           |
|---------|--------------------|
| network | interface<br>route |

### 20.3 Configuring VRF

#### 20.3.1 Configuring VRF using the web UI

##### 20.3.1.1 Setting the VRF for an interface

To create VRFs, you must add interfaces. To add an interface to a VRF instance, select **Network - > Interfaces**, select the desired interface to edit then select **Common Configuration - > Advanced Settings**.

Enter in the relevant VRF name in the VRF field.

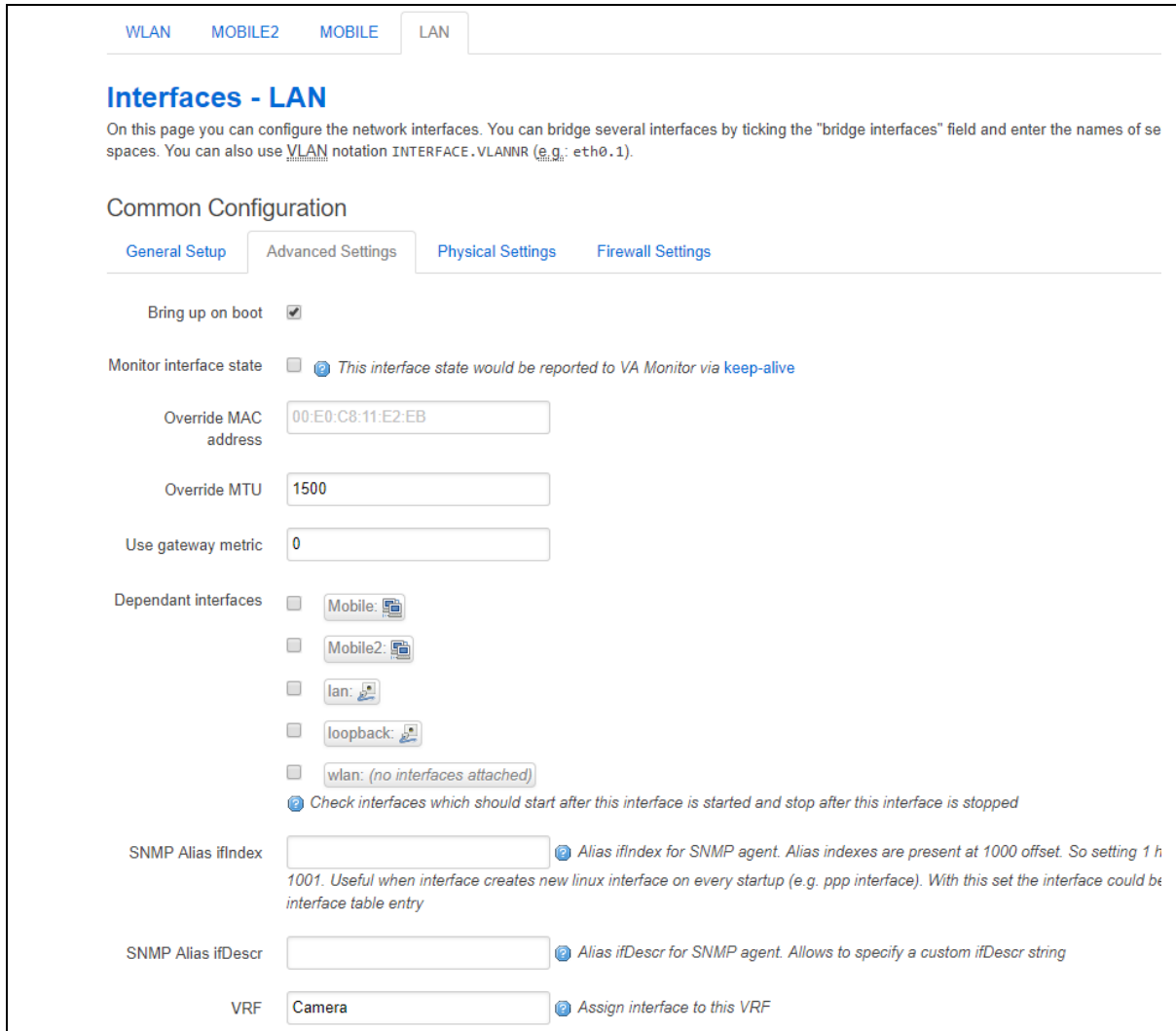


Figure 129: The interfaces configuration page

| Web Field/UCI/Package Option                       | Description  |
|--|--|
| Web: VRF<br>UCI: network.<if name>.vrf<br>Opt: vrf | Defines the VRF name to which this interface belongs.<br><b>Note:</b> the name must be consistent across all interfaces that want to reside on that VRF. |
|  | (Empty) Interface is not attached to a VRF.  |
|  | Range 0 – 15 characters  |

Table 81: Information table for VRF interface configuration

To add additional interfaces to a VRF, repeat the above for the relevant interface(s).

For example, the above configuration creates a VRF on a LAN interface. To configure this VRF to be used by traffic from a camera on a LAN interface to a VRF on a mobile interface, repeat the above instructions for a mobile interface so the camera VRF will now contain a local network and mobile interface to route traffic.

**Note:** the default VRF is created automatically and is not assigned any VRF name. It is recommended to use this default VRF to access router services and applications; for example, HTTP, SSH, SNMP etc.

### 20.3.1.2 Configuring a VRF on a static route

Each VRF has its own routing table and static routes can be added to a VRF routing table. To define a static route on a VRF, select **Network - >Static Routes**.

Figure 130: The static routes configuration page

| Web Field/UCI/Package Option | Description   |
|------------------------------|---|
| Web: VRF                     | Defines the VRF name.   |
| UCI: network.route.vrf       | <b>Note:</b> 'none' is a special name to move a route out of a VRF. |
| Opt: vrf                     | Example: network.route.vrf=none                                     |
|                              | (Empty) Interface is not attached to a VRF                          |
|                              | Range 0 - 15 characters   |

Table 82: Information table for VRF static route configuration

## 20.3.2 Configuring the VRFs using the command line

You configure a VRF using the interface configuration section in the network etc/config/network.

The VRF name must be consistent across all interfaces that want to reside on that VRF.

For the command line examples below, two VRFs called Camera and Management are configured.

### 20.3.2.1 VRF using UCI

```
root@VA_router:~# uci show network | grep vrf
network.lan.vrf=Camera
network.Mobile1.vrf=Camera
network.Mobile2.vrf=Management
```

### 20.3.2.2 VRF using package options

```
root@VA_router:~# uci export network
package network

config interface lan
    option vrf 'Camera'

config interface Mobile1
```

```
option vrf 'Camera'  
  
config interface Mobile2  
option vrf 'Management'
```

## 20.4 VRF diagnostics

### 20.4.1 VRF table

To display a list of running VRFs, enter:

```
root@VA_router:~# ip vrf  
Name           Table  
-----  
Management     10  
Camera         10
```

### 20.4.2 VRF routes

To display the routing table for a VRF, enter the command  
`ip route list vrf <vrf name>`.

```
root@VA_router:~# ip route list vrf Camera  
default via 10.92.163.130 dev qmimux0  
10.92.163.128/30 dev qmimux0 proto kernel scope link src 10.92.163.129  
172.16.100.0/24 dev eth1 proto kernel scope link src 172.16.100.1  
  
root@VA_router:~# ip route list vrf Management  
default via 10.176.120.94 dev qmimux1  
10.176.120.92/30 dev qmimux1 proto kernel scope link src 10.176.120.93
```

## 21 Configuring static routes

It is possible to define arbitrary IPv4 routes on specific interfaces using route sections. As for aliases, multiple sections can be attached to an interface. These types of routes are most commonly known as static routes.

You can add static routes to the routing table to forward traffic to specific subnets when dynamic routing protocols are not used or they are not configured for such subnets. They can be created based on an outgoing interface or next hop IP address.

### 21.1 Configuration package used

| Package | Sections |
|---------|----------|
| network | route    |

### 21.2 Configuring static routes using the web interface

In the top menu, select **Network -> Static Routes**. The Routes page appears.

Figure 131: The routes page

In the IPv4 Routes section, click **Add**.

| Web Field/UCI/Package Option   | Description   |
|--|---|
| Web: Interface<br>UCI: network.@route[0].interface<br>Opt: Interface | Specifies the logical interface name of the parent or master interface this route belongs to. It must refer to one of the defined interface sections. |
| Web: target<br>UCI: network.@route[0].target<br>Opt: target          | Specifies the route network IP address.   |
| Web: netmask<br>UCI: network.@route[0].netmask<br>Opt: netmask       | Defines the route netmask. If omitted, 255.255.255.255 is assumed, which makes the target a host address.   |

|  |  |       |  |       |  |
|--|--|-------|--|-------|--|
| Web: Gateway<br>UCI: network.@route[0].gateway<br>Opt: Gateway | Network gateway. If omitted, the gateway from the parent interface is taken. If set to 0.0.0.0 no gateway will be specified for the route.   |       |  |       |  |
| Web: Metric<br>UCI: network.@route[0].metric<br>Opt: metric    | Specifies the route metric to use.<br><table border="1"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>  | 0     |  | Range |  |
| 0  |  |       |  |       |  |
| Range  |  |       |  |       |  |
| Web: MTU<br>UCI: network.@route[0].mtu<br>Opt:mtu              | Defines a specific MTU for this route. If omitted, the MTU from the parent interface will be taken.<br><table border="1"> <tr><td>Blank</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table> | Blank |  | Range |  |
| Blank  |  |       |  |       |  |
| Range  |  |       |  |       |  |

Table 83: Information table for IPv4 static routes section

## 21.3 Configuring IPv6 routes using the web interface

You can also specify IPv6 routes by defining one or more IPv6 routes. In the IPv6 routes section, click **Add**.

| Web Field/UCI/Package Option   | Description   |       |  |       |  |
|--|---|-------|--|-------|--|
| Web: Interface<br>UCI: network.@route[1].interface<br>Opt: interface | Specifies the logical interface name of the parent or master interface this route belongs to. It must refer to one of the defined interface sections.   |       |  |       |  |
| Web: target<br>UCI: network.@route[1].target<br>Opt: target          | Specifies the route network IP address, or subnet in CIDR notation:<br>Example: 2001:0DB8:100:F00:BA3::1/64   |       |  |       |  |
| Web: Gateway<br>UCI: network.@route[1].gateway<br>Opt: Gateway       | Network gateway. If omitted, the gateway from the parent interface is taken. If set to 0.0.0.0 no gateway will be specified for the route.  |       |  |       |  |
| Web: Metric<br>UCI: network.@route[1].metric<br>Opt: metric          | Specifies the route metric to use.<br><table border="1"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>   | 0     |  | Range |  |
| 0  |   |       |  |       |  |
| Range  |   |       |  |       |  |
| Web: MTU<br>UCI: network.@route[1].mtu<br>Opt:mtu                    | Defines a specific MTU for this route. If omitted the MTU from the parent interface will be taken.<br><table border="1"> <tr><td>Empty</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table> | Empty |  | Range |  |
| Empty  |   |       |  |       |  |
| Range  |   |       |  |       |  |

Table 84: Information table for IPv6 routes

When you have made your changes, click **Save & Apply**.

## 21.4 Configuring routes using command line

By default all routes are named 'route', it is identified by @route then the route's position in the package as a number. For example, for the first route in the package using UCI:

```
network.@route[0]=route
network.@route[0].interface=lan
```

Or using package options:

```
config route
    option 'interface' 'lan'
```

However, you can give a route a name if desired. For example, a route named 'myroute' will be `network.myroute`.

To define a named route using UCI, enter:

```
network.name_your_route=route
network.name_your_route.interface=lan
```

To define a named route using package options, enter:

```
config route 'name_your_route'
    option 'interface' 'lan'
```

## 21.5 IPv4 routes using UCI

The command line example routes in the subsections below do not have a configured name.

```
root@VA_router:~# uci show network
network.@route[0]=route
network.@route[0].interface=lan
network.@route[0].target=3.3.3.10
network.@route[0].netmask=255.255.255.255
network.@route[0].gateway=10.1.1.2
network.@route[0].metric=3
network.@route[0].mtu=1400
```

## 21.6 IPv4 routes using package options

```
root@VA_router:~# uci export network
package network
...
config route
    option interface 'lan'
    option target '2.2.2.2'
    option netmask '255.255.255.255'
    option gateway '192.168.100.1'
    option metric '1'
    option mtu '1500'
```

## 21.7 IPv6 routes using UCI

```
root@VA_router:~# uci show network
network.@route[1]=route
network.@route[1].interface=lan
network.@route[1].target=2001:0DB8:100:F00:BA3::1/64
network.@route[1].gateway=2001:0DB8:99::1
network.@route[1].metric=1
network.@route[1].mtu=1500
```

## 21.8 IPv6 routes using package options

```
root@VA_router:~# uci export network
package network
...
config route
    option interface 'lan'
    option target '2001:0DB8:100:F00:BA3::1/64'
    option gateway '2001:0DB8:99::1'
    option metric '1'
    option mtu '1500'
```



## 21.9 Static routes diagnostics

### 21.9.1 Route status

To show the current routing status, enter:

```
root@VA_router:~# route -n
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
192.168.100.0    *                255.255.255.0  U        0      0      0 eth0
```

**Note:** a route will only be displayed in the routing table when the interface is up.

## 22 Configuring BGP (Border Gateway Protocol)

BGP is a protocol for exchanging routing information between gateway hosts, each with its own router, in a network of autonomous systems. BGP is often the protocol used between gateway hosts on the internet. The routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen.

### 22.1 Configuration package used

| Package | Sections |
|---------|----------|
| bgpd    | routing  |
|         | peer     |
|         | routemap |

### 22.2 Configuring BGP using the web interface

In the top menu, select **Network -> BGP**. The BGP configuration page appears. The page has three sections: Global Settings, BGP Neighbours and BGP Route Map.

The screenshot shows the BGP configuration page in a web interface. At the top, there is a navigation menu with 'Status', 'System', 'Services', 'Network', and 'Logout'. The main heading is 'BGP'. Below it, there are three sections: 'Global Settings' with an 'Add' button; 'BGP Route Map' with a text input field and an 'Add' button; and 'BGP Neighbours' with a table header containing 'IP Address', 'Autonomous System Number', 'Route Map', and 'Route Map Direction'. Below the table is a text input field and an 'Add' button. At the bottom right, there are three buttons: 'Save & Apply', 'Save', and 'Reset'.

Figure 132: The BGP page

## 22.2.1 BGP global settings

To configure global BGP settings, click **Add**. The Global Settings page appears.

### BGP

#### Global Settings

BGP Enabled

Router ID

Scan Time  [?](#) The interval in seconds between RIB scans

Autonomous System Number

Log keepalives

Log events

Log filters

Log fsm

Log updates

Network  [?](#) These networks will be announced to neighbours

**Figure 133: The BGP global settings page**

| Web Field/UCI/Package Option   | Description  |              |
|--|--|--------------|
| Web: BGP Enabled<br>UCI: bgpd.bgpd.enabled<br>Opt: enabled                     | Enables or disables BGP protocol.                              |              |
|  | 1  | Enabled.     |
|  | 0  | Disabled.    |
| Web: Router ID<br>UCI: bgpd.bgpd.router_id<br>Opt: router_id                   | Sets a unique router ID in 4 byte format 0.0.0.0.              |              |
| Web: Scan Time<br>UCI: bgpd.bgpd.scan_time<br>Opt: scan_time                   | Defines the interval in seconds between RIB scans.             |              |
|  | 60   | 60 seconds   |
|  | Range  |              |
| Web: Autonomous System Number<br>UCI: bgpd.bgpd.asn<br>Opt: asn                | Defines the ASN for the local router. Type in the ASN.         |              |
|  | Blank  |              |
|  | Range  | 1-4294967295 |
| Web: Log keepalives<br>UCI: bgpd.bgpd.debug_keepalive<br>Opt: debug_keepalives | Defines whether to enable BGP keepalives to the system log.    |              |
|  | 1  | Enabled.     |
|  | 0  | Disabled.    |
| Web: Log events<br>UCI: bgpd.bgpd.debug_events<br>Opt: debug_events            | Defines whether to enable BGP event to the system log.         |              |
|  | 1  | Enabled.     |
|  | 0  | Disabled.    |
| Web: Log filters<br>UCI: bgpd.bgpd.debug_filters<br>Opt: debug_filters         | Defines whether to enable BGP filter events to the system log. |              |
|  | 1  | Enabled.     |
|  | 0  | Disabled.    |

|  |   |       |          |   |           |
|--|---|-------|----------|---|-----------|
| Web: Log fsm<br>UCI: bgpd.bgpd.debug_fsm<br>Opt: debug_fsm             | Defines whether to enable BGP state changes to the system log.<br><table border="1"> <tr><td>1</td><td>Enabled.</td></tr> <tr><td>0</td><td>Disabled.</td></tr> </table>  | 1     | Enabled. | 0 | Disabled. |
| 1  | Enabled.  |       |          |   |           |
| 0  | Disabled.   |       |          |   |           |
| Web: Log Updates<br>UCI: bgpd.bgpd.debug_updates<br>Opt: debug_updates | Defines whether to enable BGP updates to the system log.<br><table border="1"> <tr><td>1</td><td>Enabled.</td></tr> <tr><td>0</td><td>Disabled.</td></tr> </table>  | 1     | Enabled. | 0 | Disabled. |
| 1  | Enabled.  |       |          |   |           |
| 0  | Disabled.   |       |          |   |           |
| Web: Network<br>UCI: bgpd.bgpd.network<br>Opt: list network            | Sets the list of networks that will be advertised to neighbours in prefix format 0.0.0.0/0. Separate multiple networks by a space using UCI. Ensure the network prefix matches the one shown in the routing table. For more information, read the 'Routes' section below. |       |          |   |           |
| Web: n/a<br>UCI: bgpd.bgpd.vrf<br>Opt: vrf                             | Defines the VRF with which to associate this BGP routing instance<br><table border="1"> <tr><td>Range</td><td></td></tr> <tr><td></td><td>No VRF</td></tr> </table>   | Range |          |   | No VRF    |
| Range  |   |       |          |   |           |
|  | No VRF  |       |          |   |           |

Table 85: Information table for BGP global settings

### 22.2.2 Optionally configure a BGP route map

Route maps provide a means to both filter and/or apply actions to a route. This allows a policy to be applied to routes. Route maps are an ordered list of route map entries each with a set of criteria that must be matched before specific attributes of the route are modified.

Scroll down to the BGP Route Map section.

Type in a name for the BGP route map name and then click **Add**. The BGP Route Map configuration section appears. You can configure multiple route maps. The examples below are for a route map named ROUTEMAP.

**ROUTEMAP**

Order

Policy Type

Match Type

Match Value  Format depends on Match Type. In case of IP Address and BGP Community value is parsed as list of items to match. Use ':' prefix to deny match

Set Option

Set Value

Figure 134: The routemap section

| Web Field/UCI/Package Option                                 | Description  |       |                   |        |  |
|--|--|-------|-------------------|--------|--|
| Web: Order<br>UCI: bgpd.ROUTEMAP.order<br>Opt: order         | Defines the route map order number.<br><table border="1"> <tr><td>Blank</td><td></td></tr> <tr><td>Range</td><td>1-65535</td></tr> </table>  | Blank |                   | Range  | 1-65535  |
| Blank  |  |       |                   |        |  |
| Range  | 1-65535  |       |                   |        |  |
| Web: Policy Type<br>UCI: bgpd.ROUTEMAP.permit<br>Opt: permit | Defines the actions taken if the entry is matched.<br><table border="1"> <tr><td>Deny</td><td>Denies the route.</td></tr> <tr><td>Permit</td><td>Permits the route to process the set actions for this entry.</td></tr> </table> | Deny  | Denies the route. | Permit | Permits the route to process the set actions for this entry. |
| Deny   | Denies the route.  |       |                   |        |  |
| Permit   | Permits the route to process the set actions for this entry.   |       |                   |        |  |

|  |   |            |                     |             |                                 |                  |                                      |              |                                  |               |   |                    |  |               |                                   |                      |  |                     |   |
|--|---|------------|---------------------|-------------|---------------------------------|------------------|--------------------------------------|--------------|----------------------------------|---------------|---|--------------------|--|---------------|-----------------------------------|----------------------|--|---------------------|---|
| <p>Web: Match Type<br/>UCI: bgpd.ROUTEMAP.match_type<br/>Opt: match_type</p> | <p>Defines match type. Available options are as follows:</p> <table border="1"> <tr> <td>IP address</td> <td>Matches IP address.</td> </tr> <tr> <td>IP Next Hop</td> <td>Matches next hop IP address.</td> </tr> <tr> <td>AS-Path</td> <td>Matches AS-path.</td> </tr> <tr> <td>Route Metric</td> <td>Matches route metric.</td> </tr> <tr> <td>BGP Community</td> <td>Matches BGP community.</td> </tr> </table>  | IP address | Matches IP address. | IP Next Hop | Matches next hop IP address.    | AS-Path          | Matches AS-path.                     | Route Metric | Matches route metric.            | BGP Community | Matches BGP community.  |                    |  |               |                                   |                      |  |                     |   |
| IP address   | Matches IP address.   |            |                     |             |                                 |                  |                                      |              |                                  |               |   |                    |  |               |                                   |                      |  |                     |   |
| IP Next Hop  | Matches next hop IP address.  |            |                     |             |                                 |                  |                                      |              |                                  |               |   |                    |  |               |                                   |                      |  |                     |   |
| AS-Path  | Matches AS-path.  |            |                     |             |                                 |                  |                                      |              |                                  |               |   |                    |  |               |                                   |                      |  |                     |   |
| Route Metric   | Matches route metric.   |            |                     |             |                                 |                  |                                      |              |                                  |               |   |                    |  |               |                                   |                      |  |                     |   |
| BGP Community  | Matches BGP community.  |            |                     |             |                                 |                  |                                      |              |                                  |               |   |                    |  |               |                                   |                      |  |                     |   |
| <p>Web: Match value<br/>UCI: bgpd.ROUTEMAP.match<br/>Opt: match</p>          | <p>Defines the value of the match type. Format depends on the match type selected. In the case of IP address and BGP Community values, the match value is parsed as a list of items to match.<br/>Enter ` ` prefix to deny match.</p>   |            |                     |             |                                 |                  |                                      |              |                                  |               |   |                    |  |               |                                   |                      |  |                     |   |
| <p>Web: Set Option<br/>UCI: bgpd.ROUTEMAP.set_type<br/>Opt: set_type</p>     | <p>Defines the set option to be processed on a match. Available options are shown below.</p> <table border="1"> <tr> <td>None</td> <td></td> </tr> <tr> <td>IP Next Hop</td> <td>Setting option for IP next hop.</td> </tr> <tr> <td>Local Preference</td> <td>Setting option for Local Preference.</td> </tr> <tr> <td>Route Weight</td> <td>Setting option for Route Weight.</td> </tr> <tr> <td>BGP MED</td> <td>Setting option for BGP multi-exit discriminator (BGP metric).</td> </tr> <tr> <td>AS Path to Prepend</td> <td>Setting option to prepend AS to AS path.</td> </tr> <tr> <td>BGP Community</td> <td>Setting option for BGP community.</td> </tr> <tr> <td>IPv6 Next Hop Global</td> <td>Setting option for IPv6 Next Hop Global.</td> </tr> <tr> <td>IPv6 Next Hop Local</td> <td>Setting option for IPv6 Next Hop Local.</td> </tr> </table> | None       |                     | IP Next Hop | Setting option for IP next hop. | Local Preference | Setting option for Local Preference. | Route Weight | Setting option for Route Weight. | BGP MED       | Setting option for BGP multi-exit discriminator (BGP metric). | AS Path to Prepend | Setting option to prepend AS to AS path. | BGP Community | Setting option for BGP community. | IPv6 Next Hop Global | Setting option for IPv6 Next Hop Global. | IPv6 Next Hop Local | Setting option for IPv6 Next Hop Local. |
| None   |   |            |                     |             |                                 |                  |                                      |              |                                  |               |   |                    |  |               |                                   |                      |  |                     |   |
| IP Next Hop  | Setting option for IP next hop.   |            |                     |             |                                 |                  |                                      |              |                                  |               |   |                    |  |               |                                   |                      |  |                     |   |
| Local Preference   | Setting option for Local Preference.  |            |                     |             |                                 |                  |                                      |              |                                  |               |   |                    |  |               |                                   |                      |  |                     |   |
| Route Weight   | Setting option for Route Weight.  |            |                     |             |                                 |                  |                                      |              |                                  |               |   |                    |  |               |                                   |                      |  |                     |   |
| BGP MED  | Setting option for BGP multi-exit discriminator (BGP metric).   |            |                     |             |                                 |                  |                                      |              |                                  |               |   |                    |  |               |                                   |                      |  |                     |   |
| AS Path to Prepend   | Setting option to prepend AS to AS path.  |            |                     |             |                                 |                  |                                      |              |                                  |               |   |                    |  |               |                                   |                      |  |                     |   |
| BGP Community  | Setting option for BGP community.   |            |                     |             |                                 |                  |                                      |              |                                  |               |   |                    |  |               |                                   |                      |  |                     |   |
| IPv6 Next Hop Global   | Setting option for IPv6 Next Hop Global.  |            |                     |             |                                 |                  |                                      |              |                                  |               |   |                    |  |               |                                   |                      |  |                     |   |
| IPv6 Next Hop Local  | Setting option for IPv6 Next Hop Local.   |            |                     |             |                                 |                  |                                      |              |                                  |               |   |                    |  |               |                                   |                      |  |                     |   |
| <p>Web: Value<br/>UCI: bgpd.ROUTEMAP.set<br/>Opt: set</p>                    | <p>Defines the set value when a match occurs. Value format depends on the set option you have selected.</p>   |            |                     |             |                                 |                  |                                      |              |                                  |               |   |                    |  |               |                                   |                      |  |                     |   |
| <p>Web: n/a<br/>UCI: bgpd.ROUTEMAP.routing<br/>Opt: set</p>                  | <p>Defines the routing section this BGP route map is related to.</p>  |            |                     |             |                                 |                  |                                      |              |                                  |               |   |                    |  |               |                                   |                      |  |                     |   |

**Table 86: Information table for routemap**

### 22.2.3 Configure BGP neighbours

To configure BGP neighbours, in the BGP neighbours section, click **Add**. The BGP Neighbours page appears. You can configure multiple BGP neighbours.

**Figure 135: The BGP neighbours section**

| Web Field/UCI/Package Option  | Description   |       |    |       |              |
|---|---|-------|----|-------|--------------|
| Web: IP Address<br>UCI: bgpd.@peer[0].ipaddr<br>Opt: ipaddr                       | Sets the IP address of the neighbour.   |       |    |       |              |
| Web: Autonomous System Number<br>UCI: bgpd.@peer[0].asn<br>Opt: asn               | Sets the ASN of the remote peer.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>1-4294967295</td> </tr> </table>   | Blank |    | Range | 1-4294967295 |
| Blank   |   |       |    |       |              |
| Range   | 1-4294967295  |       |    |       |              |
| Web: Route Map<br>UCI: bgpd.@peer[0].route_map<br>Opt: route_map                  | Sets route map name to use with this neighbour.   |       |    |       |              |
| Web: Route Map Direction<br>UCI: bgpd.@peer[0].route_map_in<br>Opt: route_map_in  | Defines what direction to apply to the route map.<br><table border="1"> <tr> <td>1</td> <td>In</td> </tr> <tr> <td>0</td> <td>Out</td> </tr> </table>   | 1     | In | 0     | Out          |
| 1   | In  |       |    |       |              |
| 0   | Out   |       |    |       |              |
| Web: IPv6<br>UCI: bgpd.@peer[0].ipv6<br>Opt: ipv6                                 | Defines whether the peer is connected over IPv6.<br><table border="1"> <tr> <td>1</td> <td></td> </tr> <tr> <td>0</td> <td></td> </tr> </table>   | 1     |    | 0     |              |
| 1   |   |       |    |       |              |
| 0   |   |       |    |       |              |
| Web: Local Peer<br>UCI: bgpd.@peer[0].next_hop_self<br>Opt: next_hop_self         | Defines an announced route's next hop as being equivalent to the address of the router if it is learned via eBGP.<br><table border="1"> <tr> <td>1</td> <td></td> </tr> <tr> <td>0</td> <td></td> </tr> </table>                                | 1     |    | 0     |              |
| 1   |   |       |    |       |              |
| 0   |   |       |    |       |              |
| Web: Holdtime<br>UCI: bgpd.@peer[0].holdtime_sec<br>Opt: holdtime_sec             | Defines how long to wait for incoming BGP messages before assuming peer is dead.<br>The timer is reset every time a BGP message is received.<br><table border="1"> <tr> <td>0</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table> | 0     |    | Range |              |
| 0   |   |       |    |       |              |
| Range   |   |       |    |       |              |
| Web: Keepalive Interval<br>UCI: bgpd.@peer[0].keepalive_sec<br>Opt: keepalive_sec | Defines the interval in seconds for between two successive BGP keep alive messages.<br><table border="1"> <tr> <td>0</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 0     |    | Range |              |
| 0   |   |       |    |       |              |
| Range   |   |       |    |       |              |
| Web: Connect Timer<br>UCI: bgpd.@peer[0].connect_sec<br>Opt: connect_sec          | Defines how long to wait after interface is up before retrying the connection on it.<br><table border="1"> <tr> <td>0</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 0     |    | Range |              |
| 0   |   |       |    |       |              |
| Range   |   |       |    |       |              |
| Web: n/a<br>UCI: bgpd.@peer[0].routing<br>Opt: routing                            | Defines the routing section this BGP peer is related to.  |       |    |       |              |

Table 87: Information table for BGP neighbours

## 22.3 Configuring BGP using command line

### 22.3.1 Configuring BGP using UCI

You can also configure BGP using UCI. The configuration file is stored on /etc/config/bgpd

```
root@VA_router:~# uci show bgpd
bgpd.bgpd=routing
bgpd.bgpd.enabled=yes
bgpd.bgpd.router_id=3.3.3.3
bgpd.bgpd.asn=1
```

```

bgpd.bgpd.network=11.11.11.0/29 192.168.103.1/32
bgpd.bgpd.vrf=datavrf
bgpd.@peer[0]=peer
bgpd.@peer[0].route_map_in=yes
bgpd.@peer[0].ipaddr=11.11.11.1
bgpd.@peer[0].asn=1
bgpd.@peer[0].route_map=ROUITEMAP
bgpd.@peer[0].ipv6=0
bgpd.@peer[0].next_hop_self=0
bgpd.@peer[0].holdtime_sec=0
bgpd.@peer[0].keepalive_sec=0
bgpd.@peer[0].connect_sec=0
bgpd.@peer[0].routing='bgpd'
bgpd.ROUITEMAP=routemap
bgpd.ROUITEMAP.order=10
bgpd.ROUITEMAP.permit=yes
bgpd.ROUITEMAP.match_type=ip address
bgpd.ROUITEMAP.match=192.168.101.1/32
bgpd.ROUITEMAP.set_type=ip next-hop
bgpd.ROUITEMAP.set='192.168.101.2/32'
bgpd.ROUITEMAP.vrf='bgpd'

```

To change any of the above values use UCI `set` command.

### 22.3.2 Configuring BGP using packages options

```

root@VA_router:~# uci export bgpd
package bgpd
config routing 'bgpd'
    option enabled 'yes'
    option router_id '3.3.3.3'
    option asn '1'
    list network '11.11.11.0/29'
    list network '192.168.103.1/32'

config peer

```

```
option route_map_in 'yes'  
option ipaddr '11.11.11.1'  
option asn '1'  
option route_map 'ROUТЕMAP'  
option ipv6 '0'  
option next_hop_self '0'  
option holdtime_sec '0'  
option keepalive_sec '0'  
option connect_sec '0'  
option routing 'bgpd'  
  
config routemap 'ROUТЕMAP'  
option order '10'  
option permit 'yes'  
option match_type 'ip address'  
option match '192.168.101.1/32'  
option set_type 'ip next-hop'  
option set '192.168.101.2/32'  
option routing 'bgpd'
```



## 22.4 View routes statistics

To view routes statistics, in the top menu click **Status -> Routes**. The routing table appears.

**Routes**  
The following rules are currently active on this system.

**ARP**

| IPv4-Address    | MAC-Address       | Interface |
|-----------------|-------------------|-----------|
| 192.168.210.100 | 50:b7:c3:0c:1e:4b | br-lan    |
| 10.1.1.124      | d4:ae:52:cd:61:21 | eth1      |
| 10.1.10.83      | 00:13:60:51:39:56 | eth1      |

**Active IPv4-Routes**

| Network | Target           | IPv4-Gateway | Metric |
|---------|------------------|--------------|--------|
| wan     | 0.0.0.0/0        | 10.64.64.64  | 0      |
| wan     | 0.0.0.0/0        | 10.64.64.64  | 1      |
| LAN2    | 10.1.0.0/16      | 0.0.0.0      | 0      |
| wan     | 10.64.64.64      | 0.0.0.0      | 0      |
| LAN2    | 192.168.101.1    | 10.1.10.83   | 0      |
| lan     | 192.168.210.0/24 | 0.0.0.0      | 0      |
| wan     | 217.67.129.143   | 10.64.64.64  | 0      |

**Active IPv6-Routes**

| Network  | Target               | IPv6-Gateway    | Metric   |
|----------|----------------------|-----------------|----------|
| loopback | 0:0:0:0:0:0:0:0      | 0:0:0:0:0:0:0:0 | FFFFFFFF |
| loopback | 0:0:0:0:0:0:0:0      | 0:0:0:0:0:0:0:0 | FFFFFFFF |
| loopback | 0:0:0:0:0:0:0:1      | 0:0:0:0:0:0:0:0 | 00000000 |
| LAN2     | FF02:0:0:0:0:0:0:FB  | 0:0:0:0:0:0:0:0 | 00000000 |
| (base0)  | FF00:0:0:0:0:0:0:0/8 | 0:0:0:0:0:0:0:0 | 00000100 |
| lan      | FF00:0:0:0:0:0:0:0/8 | 0:0:0:0:0:0:0:0 | 00000100 |
| LAN2     | FF00:0:0:0:0:0:0:0/8 | 0:0:0:0:0:0:0:0 | 00000100 |
| loopback | 0:0:0:0:0:0:0:0      | 0:0:0:0:0:0:0:0 | FFFFFFFF |

**Figure 136: The routing table**

To view routes via the command line, enter:

```
root@support:~# route -n
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
10.1.0.0         0.0.0.0         255.255.0.0    U        0      0      0 br-lan2
```

## 23 Configuring OSPF (Open Shortest Path First)

### 23.1 Introduction

OSPF is a standardised link state routing protocol, designed to scale efficiently to support larger networks. Link state protocols track the status and connection type of each link and produce a calculated metric based on these and other factors, including some set by the network administrator. Link state protocols will take a path which has more hops, but that uses a faster medium over a path using a slower medium with fewer hops.

OSPF adheres to the following link state characteristics:

- OSPF employs a hierarchical network design using areas.
- OSPF will form neighbour relationships with adjacent routers in the same area.
- Instead of advertising the distance to connected networks, OSPF advertises the status of directly connected links using Link-State Advertisements (LSAs).
- OSPF sends updates (LSAs) when there is a change to one of its links, and will only send the change in the update. LSAs are additionally refreshed every 30 minutes.
- OSPF traffic is multicast either to address 224.0.0.5 for all OSPF routers or 224.0.0.6 for all designated routers.
- OSPF uses the Dijkstra shortest path first algorithm to determine the shortest path.
- OSPF is a classless protocol, and therefore supports Variable Length Subnet Masks (VLSMs).

Other characteristics of OSPF include:

- OSPF supports only IP routing.
- OSPF routes have an administrative distance is 110.
- OSPF uses cost as its metric, which is computed based on the bandwidth of the link. OSPF has no hop-count limit.

The OSPF process builds and maintains three separate tables:

- **A neighbour table** containing a list of all neighbouring routers
- **A topology table** containing a list of all possible routes to all known networks within an area
- **A routing table** containing the best route for each known network

### 23.1.1 OSPF areas

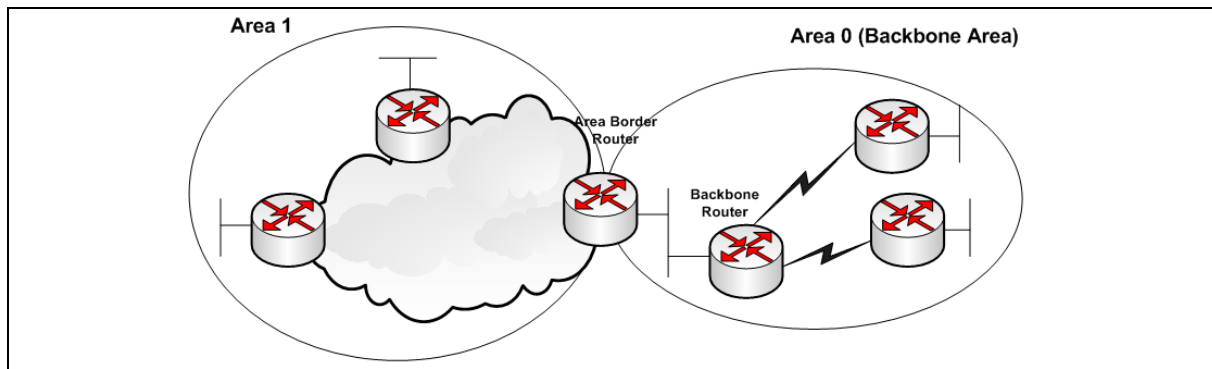


Figure 137: OSPF areas

OSPF has a number of features that allow it to scale well for larger networks. One of these features is OSPF areas. OSPF areas break up the topology so that routers in one area know less topology information about the subnets in the other area, and they do not know anything about the routers in the other area at all. With smaller topology databases, routers consume less memory and take less processing time to run SPF.

The Area Border Router (ABR) is the border between two areas. The ABR does not advertise full topology information about the part of the network in area 0 to routers in area 1. Instead the ABR advertises summary information about the subnets in area 0. Area 1 will just see a number of subnets reachable via area 0.

### 23.1.2 OSPF neighbours

OSPF forms neighbour relationships, called adjacencies, with other routers in the same area by exchanging 'hello' packets to multicast address 224.0.0.5. Only after an adjacency is formed can routers share routing information.

Each OSPF router is identified by a unique router ID. The router ID can be determined in one of three ways:

- The router ID can be manually specified.
- If not manually specified, the highest IP address configured on any loopback interface on the router will become the router ID.
- If no loopback interface exists, the highest IP address configured on any physical interface will become the router ID.

By default, hello packets are sent out of OSPF-enabled interfaces every 10 seconds for broadcast and point-to-point interfaces, and 30 seconds for non-broadcast and point-to-multipoint interfaces.

OSPF also has a 'dead interval', which indicates how long a router will wait without hearing any hellos before announcing a neighbour as 'down'. The default setting for the dead interval is 40 seconds for broadcast and point-to-point interfaces; and 120 seconds for non-broadcast and point-to-multipoint interfaces. By default, the dead interval timer is four times the hello interval.

OSPF routers will only become neighbours if the following parameters within a hello packet are identical on each router:

- Area ID
- Area type (stub, NSSA, etc.)
- Prefix
- Subnet mask
- Hello interval
- Dead interval
- Network type (broadcast, point-to-point, etc.)
- Authentication

The hello packets also serve as keepalives to allow routers to quickly discover if a neighbour is down. Hello packets also contain a neighbour field that lists the router IDs of all neighbours the router is connected to. A neighbour table is constructed from the OSPF hello packets, which includes the following information:

- The router ID of each neighbouring router
- The current 'state' of each neighbouring router
- The interface directly connecting to each neighbour
- The IP address of the remote interface of each neighbour

### 23.1.3 OSPF designated routers

In multi-access networks such as Ethernet, there is the possibility of many neighbour relationships on the same physical segment. This leads to a considerable amount of unnecessary Link State Advertisement (LSA) traffic. If a link of a router were to fail, it would flood this information to all neighbours. Each neighbour, in turn, would then flood that same information to all other neighbours. This is a waste of bandwidth and processor load.

To prevent this, OSPF will elect a Designated Router (DR) for each multi-access network, accessed via multicast address 224.0.0.6. For redundancy purposes, a Backup Designated Router (BDR) is also elected.

OSPF routers will form adjacencies with the DR and BDR. If a change occurs to a link, the update is forwarded only to the DR, which then forwards it to all other routers. This greatly reduces the flooding of LSAs. DR and BDR elections are determined by a router's OSPF priority, which is configured on a per-interface basis as a router can have interfaces in multiple multi-access networks. The router with the highest priority becomes the DR; second highest becomes the BDR. If there is a tie in priority, whichever router has the highest router ID will become the DR.

## 23.1.4 OSPF neighbour states

Neighbour adjacencies will progress through several states, described in the table below.

| State    | Description  |  |
|----------|--|--|
| Down     | Indicates that no hellos have been heard from the neighbouring router.   |  |
| Init     | Indicates a hello packet has been heard from the neighbour, but a two-way communication has not yet been initialised.  |  |
| 2-Way    | Indicates that bidirectional communication has been established. Recalls that hello packets contain a neighbour field; thus, communication is considered 2-way when a router sees its own router ID in its neighbour's hello packet. Designated and backup designated routers are elected at this stage. |  |
| ExStart  | Indicates that the routers are preparing to share link state information. Master/slave relationships are formed between routers to determine who will begin the exchange.  |  |
| Exchange | Indicates that the routers are exchanging Database Descriptors (DBDs). DBDs contain a description of the router's topology database. A router will examine a neighbour's DBD to determine if it has information to share.  |  |
| Loading  | Indicates the routers are finally exchanging link state advertisements, containing information about all links connected to each router. Essentially, routers are sharing their topology tables with each other.   |  |
| Full     | Indicates that the routers are fully synchronised. The topology table of all routers in the area should now be identical. Depending on the role of the neighbour, the state may appear as:   |  |
|          | Full/DR  | Indicating that the neighbour is a Designated Router (DR).   |
|          | Full/BDR   | Indicating that the neighbour is a Backup Designated Router (BDR).   |
|          | Full/DROther   | Indicating that the neighbour is neither the DR nor BDR. On a multi-access network, OSPF routers will only form full adjacencies with DRs and BDRs. Non-DRs and non-BDRs will still form adjacencies, but will remain in a 2-way state. This is normal OSPF behaviour. |

**Table 88: Neighbour adjacency states**

## 23.1.5 OSPF network types

OSPF's functionality is different across several different network topology types.

| State                  | Description   |
|------------------------|---|
| Broadcast Multi-Access | Indicates a topology where broadcast occurs. Examples include Ethernet, Token Ring and ATM. OSPF characteristics are:<br>OSPF will elect DRs and BDRs<br>Traffic to DRs and BDRs is multicast to 224.0.0.6.<br>Traffic from DRs and BDRs to other routers is multicast to 224.0.0.5<br>Neighbours do not need to be manually specified.   |
| Point-to-Point         | Indicates a topology where two routers are directly connected. An example would be a point-to-point T1. OSPF characteristics are:<br>OSPF will not elect DRs and BDRs<br>All OSPF traffic is multicast to 224.0.0.5<br>Neighbours do not need to be manually specified  |
| Point-to-Multipoint    | Indicates a topology where one interface can connect to multiple destinations. Each connection between a source and destination is treated as a point-to-point link. For example, point to point-to-multipoint frame relay. OSPF characteristics are:<br>OSPF will not elect DRs and BDRs.<br>All OSPF traffic is multicast to 224.0.0.5.<br>Neighbours do not need to be manually specified. |

|   |   |
|---|---|
| Non-broadcast Multi-access Network (NBMA) | <p>Indicates a topology where one interface can connect to multiple destinations; however, broadcasts cannot be sent across a NBMA network. For example, Frame Relay. OSPF characteristics are:</p> <p>OSPF will elect DRs and BDRs.</p> <p>OSPF neighbours must be manually defined, so all OSPF traffic is unicast instead of multicast.</p> <p><b>Note:</b> on non-broadcast networks, neighbours must be manually specified, as multicast hellos are not allowed.</p> |
|---|---|

**Table 89: OSPF functionality over different topology types**

### 23.1.6 The OSPF hierarchy

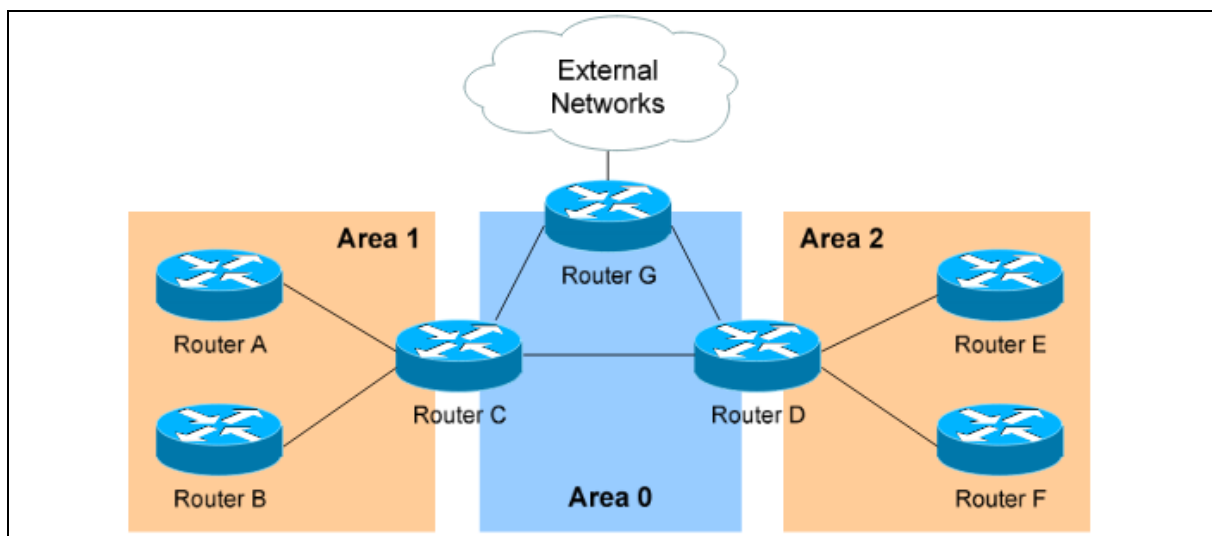
OSPF is a hierarchical system that separates an autonomous system into individual areas. OSPF traffic can either be:

- intra-area (within one area),
- inter-area (between separate areas), or
- external (from another AS).

OSPF routers build a topology database of all links within their area, and all routers within an area will have an identical topology database. Routing updates between these routers will only contain information about links local to their area. Limiting the topology database to include only the local area conserves bandwidth and reduces CPU loads.

Area 0 is required for OSPF to function, and is considered the backbone area. As a rule, all other areas must have a connection into Area 0, though this rule can be bypassed using virtual links. Area 0 is often referred to as the transit area to connect all other areas.

OSPF routers can belong to multiple areas, and therefore contain separate topology databases for each area. These routers are known as Area Border Routers (ABRs).



**Figure 138: OSPF hierarchy**

In the above example three areas exist: Area 0, Area 1, and Area 2.

Area 0 is the backbone area for this autonomous system.

Both Area 1 and Area 2 must directly connect to Area 0. Routers A and B belong fully to Area 1, while routers E and F belong fully to Area 2. These are known as internal routers.

Router C belongs to both Area 0 and Area 1; so it is an ABR. Because it has an interface in Area 0, it can also be considered a Backbone Router (BR). The same can be said for Router D, as it belongs to both Area 0 and Area 2.

Router G also belongs to Area 0 however it also has a connection to the internet, which is outside this autonomous system. This makes Router G an Autonomous System Border Router (ASBR).

A router can become an ASBR in one of two ways:

- By connecting to a separate Autonomous System, such as the internet
- By redistributing another routing protocol into the OSPF process.

ASBRs provide access to external networks. OSPF defines two types of external routes, as shown in the table below.

|                    |  |
|--------------------|--|
| <b>Type 2 (E2)</b> | Includes only the external cost to the destination network. External cost is the metric being advertised from outside the OSPF domain. This is the default type assigned to external routes.                             |
| <b>Type 1 (E1)</b> | Includes both the external cost, and the internal cost to reach the ASBR, to determine the total metric to reach the destination network. Type 1 routes are always preferred over Type 2 routes to the same destination. |

**Table 90: Types of external routes**

### 23.1.7 OSPF router types

The four separate OSPF router types are shown in the table below.

| <b>Route Type</b>                      | <b>Description</b>                                 |
|--|--|
| Internal Router                        | All router interfaces belong to only one area.     |
| Area Border Router (ABR)               | Have interfaces in at least two separate areas.    |
| Backbone Router                        | Have at least one interface in area 0.             |
| Autonomous System Border Router (ASBR) | Have a connection to a separate autonomous system. |

## 23.2 Configuration package used

| <b>Package</b> | <b>Sections</b>                 |
|----------------|---------------------------------|
| ospfd          | routing<br>network<br>interface |

## 23.3 Configuring OSPF using the web interface

Select **Network -> OSPF**. The OSPF page appears.

There are three sections in the OSPF page:

| Section                  | Description  |
|--------------------------|--|
| Global Settings          | Enables OSPF and configures the OSPF routing section containing global configuration parameters. The web automatically names the routing section ospfd |
| Topology Configuration   | Configures the network sections.   |
| Interfaces Configuration | Configures the interface sections. Defines interface configuration for OSPF and interface specific parameters  |

### 23.3.1 Global settings

The Global Settings section configures the ospfd routing section. The web automatically names the routing section 'ospfd'.

Figure 139: The OSPF global settings configuration page

| Web Field/UCI/Package Option   | Description   |       |           |       |          |
|--|---|-------|-----------|-------|----------|
| Web: OSPF Enabled<br>UCI: ospfd.ospfd.enabled<br>Opt: enabled                                      | Enables OSPF advertisements on router.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0     | Disabled. | 1     | Enabled. |
| 0  | Disabled.   |       |           |       |          |
| 1  | Enabled.  |       |           |       |          |
| Web: Router ID<br>UCI: ospfd.ospfd.router_id<br>Opt: router_id                                     | This sets the router ID of the OSPF process. The router ID may be an IP address of the router, but need not be - it can be any arbitrary 32bit number. However it MUST be unique within the entire OSPF domain to the OSPF speaker. If one is not specified, then ospfd will obtain a router-ID automatically from the zebra daemon.<br><table border="1"> <tr> <td>Empty</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table> | Empty |           | Range |          |
| Empty  |   |       |           |       |          |
| Range  |   |       |           |       |          |
| Web: Make Default Router<br>UCI: ospfd.ospfd.default_info_originate<br>Opt: default_info_originate | Defines whether to originate an AS-External (type-5) LSA describing a default route into all external-routing capable areas, of the specified metric and metric type.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0     | Disabled. | 1     | Enabled. |
| 0  | Disabled.   |       |           |       |          |
| 1  | Enabled.  |       |           |       |          |
| Web: n/a<br>UCI: ospfd.ospfd.vty_enabled<br>Opt: vty_enabled                                       | Enable vty for OSPFd (telnet to localhost:2604)   |       |           |       |          |
| Web: n/a<br>UCI: ospfd.ospfd.vrf<br>Opt: vrf   | Defines the VRF for OSPF<br><table border="1"> <tr> <td></td> <td>No VRF</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  |       | No VRF    | Range |          |
|  | No VRF  |       |           |       |          |
| Range  |   |       |           |       |          |

Table 91: Information table for OSPF global settings



### 23.3.2 Topology configuration

The Topology Configuration section configures the ospfd network section. This section specifies the OSPF enabled interface(s). The router can provide network information to the other OSPF routers via this interface.

**Note:** to advertise OSPF on an interface, the network mask prefix length for the topology configuration statement for the desired interface advertisement must be equal or smaller, that is, a larger network, than the network mask prefix length for the interface.

For example, the topology configuration statement in the screenshot below does not enable OSPF on an interface with address 12.1.1.1/23, but it would enable OSPF on an interface with address 12.1.1.129/25.

| Network  | Mask Length | Area | Stub Area                           |
|----------|-------------|------|-------------------------------------|
| 12.1.1.1 | 24          | 0    | <input checked="" type="checkbox"/> |

Only for non-backbone areas

Add

Figure 140: The OSPF topology configuration page

| Web Field/UCI/Package Option   | Description  |   |           |   |          |
|--|--|---|-----------|---|----------|
| Web: Network<br>UCI: ospfd.@network[0].ip_addr<br>Opt: ip_addr             | Specifies the IP address for OSPF enabled interface.<br>Format: A.B.C.D  |   |           |   |          |
| Web: Mask Length<br>UCI: ospfd.@network[0].mask_length<br>Opt: mask_length | Specifies the mask length for OSPF enabled interface. The mask length should be entered in CIDR notation.  |   |           |   |          |
| Web: Area<br>UCI: ospfd.@network[0].area<br>Opt: area                      | Specifies the area number for OSPF enabled interface.  |   |           |   |          |
| Web: Stub Area<br>UCI: ospfd.@network[0].stub_area<br>Opt: stub_area       | Only for non-backbone areas.<br>Configures the area to be a stub area. That is, an area where no router originates routes external to OSPF and hence an area where all external routes are via the ABR(s).<br>ABRs for such an area do not need to pass AS-External LSAs (type-5s) or ASBR-Summary LSAs (type-4) into the area. They need only pass network-summary (type-3) LSAs into such an area, along with a default-route summary. |   |           |   |          |
|  | <table border="1"> <tbody> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </tbody> </table>  | 0 | Disabled. | 1 | Enabled. |
| 0  | Disabled.  |   |           |   |          |
| 1  | Enabled.   |   |           |   |          |

Table 92: Information table for OSPF topology configuration

### 23.3.3 Interfaces configuration

The Interfaces Configuration section contains settings to configure the OSPF interface. It defines interface configurations for OSPF and interface specific parameters.

OSPFv2 allows packets to be authenticated using either an insecure plain text password, included with the packet, or by a more secure MD5 based HMAC (keyed-Hashing for

Message Authentication). Enabling authentication prevents routes being updated by unauthenticated remote routers, but still can allow routes, that is, the entire OSPF routing table, to be queried remotely, potentially by anyone on the internet, via OSPFv1. This section defines key\_chains to be used for MD5 authentication.

The screenshot shows the 'Interfaces Configuration' section. It includes a radio button selection for the interface (LAN1 is selected), a dropdown for Network Type (set to --default--), a checked checkbox for Passive, input fields for Hello Interval (10) and Dead Interval (40), a dropdown for Authentication (text), and an input field for Text Auth. Key (secret). Each input field has a help icon and a tooltip with default values.

**Figure 141: The OSPF interfaces configuration section**

| Web Field/UCI/Package Option   | Description  |         |  |           |          |               |  |                |  |                     |  |
|--|--|---------|--|-----------|----------|---------------|--|----------------|--|---------------------|--|
| Web: Interface<br>UCI: ospfd.@interface[0].ospf_interface<br>Opt: ospf_interface | Defines the interface name.  |         |  |           |          |               |  |                |  |                     |  |
| Web: Network Type<br>UCI: ospfd.@interface[0].network_type<br>Opt: network_type  | Defines the network type for specified interface. <table border="1"> <tr> <td>Default</td> <td>Autodetect: it will be broadcast. If broadcast is not supported on that interface then use point-to-point.</td> </tr> <tr> <td>broadcast</td> <td></td> </tr> <tr> <td>non-broadcast</td> <td></td> </tr> <tr> <td>point-to-point</td> <td></td> </tr> <tr> <td>point-to-multipoint</td> <td></td> </tr> </table>   | Default | Autodetect: it will be broadcast. If broadcast is not supported on that interface then use point-to-point. | broadcast |          | non-broadcast |  | point-to-point |  | point-to-multipoint |  |
| Default  | Autodetect: it will be broadcast. If broadcast is not supported on that interface then use point-to-point.   |         |  |           |          |               |  |                |  |                     |  |
| broadcast  |  |         |  |           |          |               |  |                |  |                     |  |
| non-broadcast  |  |         |  |           |          |               |  |                |  |                     |  |
| point-to-point   |  |         |  |           |          |               |  |                |  |                     |  |
| point-to-multipoint  |  |         |  |           |          |               |  |                |  |                     |  |
| Web: Passive<br>UCI: ospfd.@interface[0].passive<br>Opt: passive                 | Does not send hello packets on the given interface, but does advertise the interface as a stub link in the router-LSA (Link State Advertisement) for this router.<br><br>This allows you to advertise addresses on such connected interfaces without having to originate AS-External/Type-5 LSAs, which have global flooding scope, as would occur if connected addresses were redistributed into OSPF. This is the only way to advertise non-OSPF links into stub areas. <table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0       | Disabled.  | 1         | Enabled. |               |  |                |  |                     |  |
| 0  | Disabled.  |         |  |           |          |               |  |                |  |                     |  |
| 1  | Enabled.   |         |  |           |          |               |  |                |  |                     |  |

|  |  |    |                                   |       |   |      |   |
|--|--|----|-----------------------------------|-------|---|------|---|
| <p>Web: Hello Interval<br/>UCI: ospfd.@interface[0].hello_interval<br/>Opt: hello_interval</p> | <p>Defines the number of seconds for the Hello Interval timer value. A hello packet will be sent every x seconds, where x is the configured hello interval value on the specified interface. This value must be the same for all routers attached to a common network.</p> <p>The default is every 10 seconds for broadcast and point-to-point interfaces, and 30 seconds for non-broadcast and point-to-multipoint interfaces.</p> <table border="1" data-bbox="683 427 1390 495"> <tr> <td>10</td> <td>10 seconds</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 10 | 10 seconds                        | Range |   |      |   |
| 10   | 10 seconds   |    |                                   |       |   |      |   |
| Range  |  |    |                                   |       |   |      |   |
| <p>Web: Dead Interval<br/>UCI: ospfd.@interface[0].dead_interval<br/>Opt: dead_interval</p>    | <p>Defines the number of seconds for the dead interval timer value used for wait timer and inactivity timer. This value must be the same for all routers attached to a common network.</p> <p>The default is 40 seconds for broadcast and point-to-point interfaces, and 120 seconds for non-broadcast and point-to-multipoint interfaces. By default, the dead interval timer is four times the hello interval.</p> <table border="1" data-bbox="683 696 1390 763"> <tr> <td>40</td> <td>40 seconds</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 40 | 40 seconds                        | Range |   |      |   |
| 40   | 40 seconds   |    |                                   |       |   |      |   |
| Range  |  |    |                                   |       |   |      |   |
| <p>Web: Routing priority<br/>UCI: ospfd.@interface[0].priority<br/>Opt: priority</p>           | <p>Defines priority to become the designated router. A value of 0 means never become a designated router; other values in the range 1-255 are allowed, with 255 being most likely to be a designated router, and 1 being least likely.</p> <table border="1" data-bbox="683 887 1390 958"> <tr> <td>1</td> <td></td> </tr> <tr> <td>Range</td> <td>0 - 255</td> </tr> </table>   | 1  |                                   | Range | 0 - 255   |      |   |
| 1  |  |    |                                   |       |   |      |   |
| Range  | 0 - 255  |    |                                   |       |   |      |   |
| <p>Web: Authentication<br/>UCI: ospfd.@interface[0].auth_mode<br/>Opt: auth_mode</p>           | <p>OSPFv2 (only) allows packets to be authenticated via either an insecure plain text password, included with the packet, or via a more secure MD5 based HMAC (keyed-Hashing for Message Authentication). Enabling authentication prevents routes being updated by unauthenticated remote routers, but still can allow routes, that is, the entire OSPF routing table to be queried remotely, potentially by anyone on the internet, via OSPFv1.</p> <table border="1" data-bbox="683 1149 1390 1279"> <tr> <td>no</td> <td>Default value. No authentication.</td> </tr> <tr> <td>md5</td> <td>Set the interface with OSPF MD5 authentication.</td> </tr> <tr> <td>text</td> <td>Set the interface with OSPF simple password authentication.</td> </tr> </table> | no | Default value. No authentication. | md5   | Set the interface with OSPF MD5 authentication. | text | Set the interface with OSPF simple password authentication. |
| no   | Default value. No authentication.  |    |                                   |       |   |      |   |
| md5  | Set the interface with OSPF MD5 authentication.  |    |                                   |       |   |      |   |
| text   | Set the interface with OSPF simple password authentication.  |    |                                   |       |   |      |   |
| <p>Web: Text Auth. Key<br/>UCI: ospfd.@interface[0].text_auth_key<br/>Opt: text_auth_key</p>   | <p>This command sets authentication string for text authentication. text_auth_key option can have length up to 8 characters. Displayed only when authentication is set to <b>text</b>.</p>   |    |                                   |       |   |      |   |
| <p>Web: Key ID<br/>UCI: ospfd.@interface[0].key_id<br/>Opt: key_id</p>                         | <p>Specifies key ID. Must be unique and match at both ends. Displayed only when authentication is set to <b>MD5</b>.</p>   |    |                                   |       |   |      |   |
| <p>Web: MD5 Auth. Key<br/>UCI: ospfd.@interface[0].md5_auth_key<br/>Opt: md5_auth_key</p>      | <p>Specifies keyed MD5 chain. Displayed only when authentication is set to <b>MD5</b>.</p>   |    |                                   |       |   |      |   |

Table 93: Information table for OSPF interface commands

## 23.4 Configuring OSPF using the command line

OSPF is configured under the ospfd package /etc/config/ospfd.

There are three config sections: ospfd, interface and network.

You can configure multiple interface and network sections.

By default, all OSPF interface instances are named `interface`, instances are identified by `@interface` then the interface position in the package as a number. For example, for the first interface in the package using UCI:

```
ospfd.@interface[0]=interface
ospfd.@interface[0].ospf_interface=lan
```

Or using package options:

```
config interface
    option ospf_interface 'lan'
```

By default, all OSPF network instances are named `network`, it is identified by `@network` then the interface position in the package as a number. For example, for the first network in the package using UCI:

```
ospfd.@network[0]=network
ospfd.@network[0].ip_addr=12.1.1.1
```

Or using package options:

```
config network
    option ip_addr '12.1.1.1'
```

## 23.5 OSPF using UCI

```
root@VA_router:~# uci show ospfd
ospfd.ospfd=routing
ospfd.ospfd.enabled=yes
ospfd.ospfd.default_info_originate=yes
ospfd.ospfd.router_id=1.2.3.4
ospfd.ospfd.vrf=datavrf
ospfd.@network[0]=network
ospfd.@network[0].ip_addr=12.1.1.1
ospfd.@network[0].mask_length=24
ospfd.@network[0].area=0
ospfd.@network[0].stub_area=yes
ospfd.@interface[0]=interface
ospfd.@interface[0].ospf_interface=lan8
ospfd.@interface[0].hello_interval=10
ospfd.@interface[0].dead_interval=40
ospfd.@interface[0].priority=1ospfd.@interface[0].network_type=broadcast
ospfd.@interface[0].passive=yes
```

```
ospfd.@interface[0].auth_mode=text
ospfd.@interface[0].text_auth_key=secret
ospfd.@interface[1]=interface
ospfd.@interface[1].ospf_interface=lan7
ospfd.@interface[1].network_type=point-to-point
ospfd.@interface[1].passive=no
ospfd.@interface[1].hello_interval=30
ospfd.@interface[1].dead_interval=120
ospfd.@interface[0].priority=2
ospfd.@interface[1].auth_mode=md5
ospfd.@interface[1].key_id=1
ospfd.@interface[1].md5_auth_key=test
```

## 23.6 OSPF using package options

```
root@VA_router:~# uci export ospfd
package ospfd

config routing 'ospfd'
    option enabled 'yes'
    option default_info_originate 'yes'
    option router_id '1.2.3.4'
    option vrf 'datavrf'

config network
    option ip_addr '12.1.1.1'
    option mask_length '24'
    option area '0'
    option stub_area 'yes'

config interface
    option ospf_interface 'lan8'
    option hello_interval '10'
    option dead_interval '40'
    option priority '1'
    option network_type 'broadcast'
    option passive 'yes'
```

```

option auth_mode 'text'
option text_auth_key 'secret'

config interface
option ospf_interface 'lan7'
option network_type 'point-to-point'
option passive 'no'
option hello_interval '30'
option dead_interval '120'
option priority '2'          option auth_mode 'md5'
option key_id '1'
option md5_auth_key 'test'

```

## 23.7 OSPF diagnostics

### 23.7.1 Route status

To show the current routing status, enter:

```

root@VA_router:~# route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          10.206.4.65    0.0.0.0         UG    1     0      0 usb0
10.1.0.0          0.0.0.0        255.255.0.0     U     0     0      0 eth1
10.206.4.64      0.0.0.0        255.255.255.252 U     0     0      0 usb0
11.11.11.0       0.0.0.0        255.255.255.248 U     0     0      0 gre-
GRE
89.101.154.151   10.206.4.65    255.255.255.255 UGH   0     0      0 usb0
192.168.100.0    0.0.0.0        255.255.255.0   U     0     0      0 eth0
192.168.101.1    11.11.11.1     255.255.255.255 UGH   11    0      0 gre-
GRE
192.168.104.1    11.11.11.4     255.255.255.255 UGH   20    0      0 gre-
GRE

```

**Note:** a route will only be displayed in the routing table when the interface is up.

### 23.7.2 Tracing OSPF packets

Typically, OSPF uses IP as its transport protocol. The well-known IP protocol type for OSPF traffic is 0x59. To trace OSPF packets on any interface on the router, enter:

```
tcpdump -i any -n proto ospf &
```

```
root@VA_router:~# tcpdump -i any -n proto ospf &
root@VA_router:~# tcpdump: verbose output suppressed, use -v or -vv for
full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535
bytes
```

To stop tracing enter `fg` to bring tracing task to foreground, and then **<CTRL-C>** to stop the trace.

```
root@VA_router:~# fg
tcpdump -i any -n proto ospf
^C
33 packets captured
33 packets received by filter
0 packets dropped by kernel
```

## 23.8 Quagga/Zebra console

Quagga is the routing protocol suite embedded in the router firmware. Quagga is split into different daemons for implementation of each routing protocol. Zebra is a core daemon for Quagga, providing the communication layer to the underlying Linux kernel, and routing updates to the client daemons.

Quagga has a console interface to Zebra for advanced debugging of the routing protocols.

To access, enter:

```
root@VA_router:~# telnet localhost zebra

Entering character mode
Escape character is '^]'.

Hello, this is Quagga (version 0.99.21).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
```

To see OSPF routing from Zebra console, enter:

```

root@VA_router:~# sh ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, H - HSLs, o - OLSR,
       b - BATMAN, A - Babel,
       > - selected route, * - FIB route

K>* 0.0.0.0/0 via 10.206.4.65, usb0
O   10.1.0.0/16 [110/11] via 11.11.11.1, gre-GRE, 02:35:28
C>* 10.1.0.0/16 is directly connected, eth1
C>* 10.206.4.64/30 is directly connected, usb0
O   11.11.11.0/29 [110/10] is directly connected, gre-GRE, 02:35:29
C>* 11.11.11.0/29 is directly connected, gre-GRE
K>* 89.101.154.151/32 via 10.206.4.65, usb0
C>* 127.0.0.0/8 is directly connected, lo
C>* 192.168.100.0/24 is directly connected, eth0
O>* 192.168.101.1/32 [110/11] via 11.11.11.1, gre-GRE, 02:35:28
O>* 192.168.104.1/32 [110/20] via 11.11.11.4, gre-GRE, 02:30:45
O   192.168.105.1/32 [110/10] is directly connected, lo, 02:47:52
C>* 192.168.105.1/32 is directly connected, lo

```

### 23.8.1 OSPF debug console

When option `vty_enabled` is enabled in the OSPF configuration, the OSPF debug console can be accessed for advanced OSPF debugging. For more information, read the Global Settings section above.

To access OSPF debug console enter: `telnet localhost ospfd (password zebra)`

```

root@VA_router:~# telnet localhost ospfd

Entering character mode
Escape character is '^]'.

Hello, this is Quagga (version 0.99.21).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:

```



To see OSPF routing from OSPF debug console, enter:

```

UUT> sh ip ospf route
===== OSPF network routing table =====
N    10.1.0.0/16          [11] area: 0.0.0.0
                                via 11.11.11.1, gre-GRE
N    11.11.11.0/29       [10] area: 0.0.0.0
                                directly attached to gre-GRE
N    192.168.101.1/32    [11] area: 0.0.0.0
                                via 11.11.11.1, gre-GRE
N    192.168.104.1/32    [20] area: 0.0.0.0
                                via 11.11.11.4, gre-GRE
N    192.168.105.1/32    [10] area: 0.0.0.0
                                directly attached to lo

===== OSPF router routing table =====

===== OSPF external routing table =====

```

To see OSPF neighbours from OSPF debug console, enter:

```

root@VA_router:~# sh ip ospf neighbor

Neighbor ID Pri State      Dead Time Address      Interface      RXmtL RqstL
DBsmL
1.1.1.1      255 Full/DR   33.961s 11.11.11.1   gre-GRE:11.11.11.5
0           0           0

```

To see OSPF interface details from OSPF debug console, enter:

```

root@VA_router:~# sh ip ospf interface
base0 is up
  ifindex 8, MTU 1518 bytes, BW 0 Kbit <UP,BROADCAST,RUNNING,MULTICAST>
  OSPF not enabled on this interface
eth0 is up
  ifindex 9, MTU 1500 bytes, BW 0 Kbit <UP,BROADCAST,RUNNING,MULTICAST>
  OSPF not enabled on this interface
eth1 is up

```

```
  ifindex 10, MTU 1500 bytes, BW 0 Kbit
<UP,BROADCAST,RUNNING,PROMISC,MULTICAST>
  OSPF not enabled on this interface
eth2 is down
  ifindex 11, MTU 1500 bytes, BW 0 Kbit <BROADCAST,MULTICAST>
  OSPF not enabled on this interface
eth3 is down
  ifindex 12, MTU 1500 bytes, BW 0 Kbit <BROADCAST,MULTICAST>
  OSPF not enabled on this interface
eth4 is down
  ifindex 13, MTU 1500 bytes, BW 0 Kbit <BROADCAST,MULTICAST>
  OSPF not enabled on this interface
eth5 is down
  ifindex 14, MTU 1500 bytes, BW 0 Kbit <BROADCAST,MULTICAST>
  OSPF not enabled on this interface
eth6 is down
  ifindex 15, MTU 1500 bytes, BW 0 Kbit <BROADCAST,MULTICAST>
  OSPF not enabled on this interface
eth7 is down
  ifindex 16, MTU 1500 bytes, BW 0 Kbit <BROADCAST,MULTICAST>
  OSPF not enabled on this interface
gre-GRE is up
  ifindex 19, MTU 1472 bytes, BW 0 Kbit <UP,RUNNING,MULTICAST>
  Internet Address 11.11.11.5/29, Area 0.0.0.0
  MTU mismatch detection:enabled
  Router ID 192.168.105.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State Backup, Priority 1
  Designated Router (ID) 1.1.1.1, Interface Address 11.11.11.1
  Backup Designated Router (ID) 192.168.105.1, Interface Address 11.11.11.5
  Multicast group memberships: OSPFAllRouters OSPFDesignatedRouters
  Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5
    Hello due in 3.334s
  Neighbor Count is 1, Adjacent neighbor count is 1
gre0 is down
  ifindex 6, MTU 1476 bytes, BW 0 Kbit <NOARP>
  OSPF not enabled on this interface
ifb0 is down
```

```

ifindex 2, MTU 1500 bytes, BW 0 Kbit <BROADCAST,NOARP>
OSPF not enabled on this interface
ifb1 is down
ifindex 3, MTU 1500 bytes, BW 0 Kbit <BROADCAST,NOARP>
OSPF not enabled on this interface
lo is up
ifindex 1, MTU 16436 bytes, BW 0 Kbit <UP,LOOPBACK,RUNNING>
Internet Address 192.168.105.1/32, Broadcast 192.168.105.1, Area 0.0.0.0
MTU mismatch detection:enabled
Router ID 192.168.105.1, Network Type LOOPBACK, Cost: 10
Transmit Delay is 1 sec, State Loopback, Priority 1
No designated router on this network
No backup designated router on this network
Multicast group memberships: <None>
Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5
  Hello due in inactive
Neighbor Count is 0, Adjacent neighbor count is 0
sit0 is down
ifindex 7, MTU 1480 bytes, BW 0 Kbit <NOARP>
OSPF not enabled on this interface
teql0 is down
ifindex 4, MTU 1500 bytes, BW 0 Kbit <NOARP>
OSPF not enabled on this interface
tunl0 is down
ifindex 5, MTU 1480 bytes, BW 0 Kbit <NOARP>
OSPF not enabled on this interface
usb0 is up
ifindex 17, MTU 1500 bytes, BW 0 Kbit <UP,BROADCAST,RUNNING,MULTICAST>
OSPF not enabled on this interface

```

To see OSPF database details from OSPF debug console, enter:

```

root@VA_router:~# sh ip ospf database

OSPF Router with ID (192.168.105.1)

Router Link States (Area 0.0.0.0)

```

---

| Link ID       | ADV Router    | Age | Seq#       | CkSum  | Link count |
|---------------|---------------|-----|------------|--------|------------|
| 1.1.1.1       | 1.1.1.1       | 873 | 0x80006236 | 0xd591 | 3          |
| 192.168.104.1 | 192.168.104.1 | 596 | 0x8000000a | 0x3a2d | 2          |
| 192.168.105.1 | 192.168.105.1 | 879 | 0x8000000b | 0x4919 | 2          |

Net Link States (Area 0.0.0.0)

| Link ID    | ADV Router | Age | Seq#       | CkSum  |
|------------|------------|-----|------------|--------|
| 11.11.11.1 | 1.1.1.1    | 595 | 0x80000004 | 0x5712 |

## 24 Configuring VRRP

### 24.1 Overview

Virtual Router Redundancy Protocol (VRRP) is a networking protocol designed to eliminate the single point of failure inherent in the static default routed environment.

VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process provides dynamic failover in the forwarding responsibility from the Master to a backup router should the Master become unavailable. This process allows the virtual router IP address(es) on the LAN to be used as the default first hop router by end hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end host.

Two or more routers forming the redundancy cluster are configured with the same router ID and virtual IP address. A VRRP router group operates within the scope of the single LAN. Additionally, the VRRP routers are configured with its initial role (Master or Backup) and the router priority, which is a factor in the master router election process. You can also configure a password authentication to protect VRRP protocol messages against spoofing.

The VRRP protocol is implemented according to internet standard RFC2338.

### 24.2 Configuration package used

| Package | Sections           |
|---------|--------------------|
| vrrp    | main<br>vrrp_group |

### 24.3 Configuring VRRP using the web interface

To configure VRRP through the web interface, in the top menu, select **Network -> VRRP**. The VRRP page appears.

There are two sections in the VRRP page:

| Section                  | Description                         |
|--------------------------|-------------------------------------|
| Global Settings          | Enables VRRP                        |
| VRRP Group Configuration | Configures the VRRP group settings. |

### 24.3.1 Global settings

The Global Settings section configures the vrrp package main section.

To access configuration settings, click **ADD**.



Figure 142: The VRRP global settings configuration page

| Web Field/UCI/Package Option | Description                          |
|------------------------------|--------------------------------------|
| Web: VRRP Enabled            | Globally enables VRRP on the router. |
| UCI: vrrp.main.enabled       | 0 Disabled.                          |
| Opt: Enabled                 | 1 Enabled.                           |

### 24.3.2 VRRP group configuration settings

The VRRP Group Configuration section configures vrrp package vrrp\_group section.

To access configuration settings, enter a VRRP group name and click **ADD**.

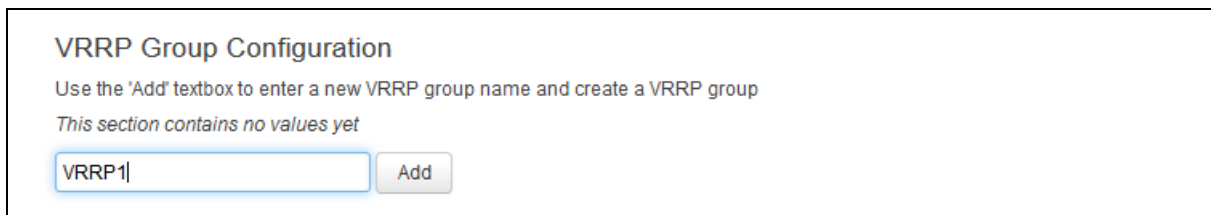


Figure 143: The VRRP group name configuration page

### VRRP Group Configuration

Group enabled

Interface  LAN1: (no interfaces attached)

LAN2:

LAN3:

MOBILE1:

PoAADSL:

loopback:

Interface to serve

Current State

Track interfaces  LAN1: (no interfaces attached)

LAN2:

LAN3:

MOBILE1:

PoAADSL:

loopback:

Interfaces to monitor

Track IPsec Tunnel  IPsecTunnel1

IPsecTunnel2

IPsec connection(s) to monitor

Track IPsec Fail Time   Consider IPsec tunnel failed if tunnel is down for that many seconds

IPsec Connection   IPsec connection to bring down/up when VRRP enters BACKUP/MASTER state

Start role

Router ID

Priority

**Figure 144: The VRRP group configuration page**

| Web Field/UCI/Package Option   | Description   |     |           |       |          |
|--|---|-----|-----------|-------|----------|
| Web: Group Enabled<br>UCI: vrrp.@vrrp_group[X].enabled<br>Opt: Enabled | Enables a VRRP group on the router.<br><table border="1" style="width: 100%;"> <tr> <td style="width: 50px; text-align: center;">0</td> <td>Disabled.</td> </tr> <tr> <td style="text-align: center;">1</td> <td>Enabled.</td> </tr> </table>   | 0   | Disabled. | 1     | Enabled. |
| 0  | Disabled.   |     |           |       |          |
| 1  | Enabled.  |     |           |       |          |
| Web: Interface<br>UCI: vrrp.@vrrp_group[X].interface<br>Opt: interface | Sets the local LAN interface name in which the VRRP cluster is to operate. For example, 'lan'. The interface name is taken from the network package and all configured interfaces will be displayed.<br><table border="1" style="width: 100%;"> <tr> <td style="width: 50px; text-align: center;">lan</td> <td></td> </tr> <tr> <td style="text-align: center;">Range</td> <td></td> </tr> </table> | lan |           | Range |          |
| lan  |   |     |           |       |          |
| Range  |   |     |           |       |          |

|   |  |        |                                |        |       |
|---|--|--------|--------------------------------|--------|-------|
| <p>Web: Track Interfaces<br/>UCI: vrrp.@vrrp_group[X].track_iface<br/>Opt: list track_iface</p>                   | <p>Defines one or more WAN interfaces that VRRP should monitor. If a monitored interface goes down on the master VRRP router, it goes into 'Fault' state and the backup VRRP router becomes the master.</p> <p>Multiple interfaces are entered using <code>uci set</code> and <code>uci add_list</code> commands. Example:<br/> <pre>uci set vrrp.@vrrp_group[0].track_iface=wan1 uci add_list vrrp.@vrrp_group[0].track_iface=wan2</pre> or using a list of options via package options<br/> <pre>list track_iface 'wan1' list track_iface 'wan2'</pre> </p> <table border="1" data-bbox="683 528 1390 600"> <tr><td>wan</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>   | wan    |                                | Range  |       |
| wan   |  |        |                                |        |       |
| Range   |  |        |                                |        |       |
| <p>Web: Track IPsec Tunnel<br/>UCI: vrrp.@vrrp_group[X].track_ipsec<br/>Opt: list track_ipsec</p>                 | <p>Defines one or more IPsec tunnels that VRRP should monitor. If a monitored tunnel goes down on the master VRRP router for the configured Track IPsec Fail Time, it goes into 'Fault' state and the backup VRRP router becomes the master.</p> <p>Multiple IPsec connections are entered using <code>uci set</code> and <code>uci add_list</code> commands. Example:<br/> <pre>uci set vrrp.@vrrp_group[0].track_ipsec=Tunnel1 uci add_list vrrp.@vrrp_group[0].track_ipsec=Tunnel2</pre> or using a list of options via package options<br/> <pre>list track_ipsec 'Tunnel1' list track_ipsec 'Tunnel2'</pre> </p> <table border="1" data-bbox="683 940 1390 1010"> <tr><td>Blank</td><td>No IPsec connection to track.</td></tr> <tr><td>Range</td><td></td></tr> </table> | Blank  | No IPsec connection to track.  | Range  |       |
| Blank   | No IPsec connection to track.  |        |                                |        |       |
| Range   |  |        |                                |        |       |
| <p>Web: Track IPsec Fail Time<br/>UCI: vrrp.@vrrp_group[X].track_ipsec_fail_sec<br/>Opt: track_ipsec_fail_sec</p> | <p>Defines duration in seconds to determine IPsec tunnel failure.</p> <table border="1" data-bbox="683 1048 1390 1120"> <tr><td>300</td><td>300 seconds</td></tr> <tr><td>Range</td><td></td></tr> </table>  | 300    | 300 seconds                    | Range  |       |
| 300   | 300 seconds  |        |                                |        |       |
| Range   |  |        |                                |        |       |
| <p>Web: IPsec connection<br/>UCI: vrrp.@vrrp_group[X].ipsec_connection<br/>Opt: ipsec_connection</p>              | <p>Sets which IPsec connection to bring up or down when VRRP enters 'backup/master' state.</p> <p>Multiple IPsec connections are entered via the package option using a space separator. Example:<br/> <pre>option ipsec_connection 'IPsecTunnel1 IPsecTunnel2'</pre> </p> <table border="1" data-bbox="683 1292 1390 1361"> <tr><td>Blank</td><td>No IPsec connection to toggle.</td></tr> <tr><td>Range</td><td></td></tr> </table>  | Blank  | No IPsec connection to toggle. | Range  |       |
| Blank   | No IPsec connection to toggle.   |        |                                |        |       |
| Range   |  |        |                                |        |       |
| <p>Web: Start role<br/>UCI: vrrp.@vrrp_group[X].init_state<br/>Opt: init_state</p>                                | <p>Sets the initial role in which a VRRP router starts up. In a cluster of VRRP routes, set one as a master and the others as backup.</p> <table border="1" data-bbox="683 1424 1390 1489"> <tr><td>BACKUP</td><td></td></tr> <tr><td>MASTER</td><td></td></tr> </table>   | BACKUP |                                | MASTER |       |
| BACKUP  |  |        |                                |        |       |
| MASTER  |  |        |                                |        |       |
| <p>Web: Router ID<br/>UCI: vrrp.@vrrp_group[X].router_id<br/>Opt: router_id</p>                                   | <p>Sets the VRRP router ID (1 to 255). All co-operating VRRP routers serving the same LAN must be configured with the same router ID.</p> <table border="1" data-bbox="683 1583 1390 1653"> <tr><td>1</td><td></td></tr> <tr><td>Range</td><td>1-255</td></tr> </table>  | 1      |                                | Range  | 1-255 |
| 1   |  |        |                                |        |       |
| Range   | 1-255  |        |                                |        |       |
| <p>Web: Priority<br/>UCI: vrrp.@vrrp_group[X].priority<br/>Opt: priority</p>                                      | <p>Sets the VRRP router's priority. Higher values equal higher priority. The VRRP routers must use priority values between 1-254. The master router uses a higher priority.</p> <table border="1" data-bbox="683 1740 1390 1809"> <tr><td>100</td><td></td></tr> <tr><td>Range</td><td>0-255</td></tr> </table>  | 100    |                                | Range  | 0-255 |
| 100   |  |        |                                |        |       |
| Range   | 0-255  |        |                                |        |       |
| <p>Web: Advert intvl<br/>UCI: vrrp.@vrrp_group[X].advert_int_sec<br/>Opt: advert_int_sec</p>                      | <p>Sets the VRRP hello value in seconds. This value must match the value set on a peer.</p> <table border="1" data-bbox="683 1872 1390 1939"> <tr><td>120</td><td>120 seconds</td></tr> <tr><td>Range</td><td></td></tr> </table>  | 120    | 120 seconds                    | Range  |       |
| 120   | 120 seconds  |        |                                |        |       |
| Range   |  |        |                                |        |       |



|  |  |   |           |       |  |
|--|--|---|-----------|-------|--|
| Web: Password<br>UCI: vrrp.@vrrp_group[X].password<br>Opt: password                  | Sets the password to use in the VRRP authentication (simple password authentication method). This field may be left blank if no authentication is required.  |   |           |       |  |
| Web: Virtual IP<br>UCI: vrrp.@vrrp_group[X].virtual_ipaddr<br>Opt: virtual_ipaddr    | Sets the virtual IP address and mask in prefix format. For example, '11.1.1.99/24'. All co-operating VRRP routers serving the same LAN must be configured with the same virtual IP address.        |   |           |       |  |
| Web: GARP delay<br>UCI:<br>vrrp.@vrrp_group[X].garp_delay_sec<br>Opt: garp_delay_sec | Sets the gratuitous ARP message sending delay in seconds.<br><table border="1" data-bbox="683 443 1393 517"> <tr> <td>5</td> <td>5 seconds</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table> | 5 | 5 seconds | Range |  |
| 5  | 5 seconds  |   |           |       |  |
| Range  |  |   |           |       |  |

Table 94: Information table for VRRP group settings

## 24.4 Configuring VRRP using command line

The configuration file is stored on /etc/config/vrrp.

There are two config sections: main and vrrp\_group.

You can configure multiple VRRP groups. By default, all VRRP group instances are named 'vrrp\_group'. Instances are identified by @vrrp\_group then the vrrp\_group position in the package as a number. For example, for the first vrrp\_group in the package using UCI:

```
vrrp.@vrrp_group[0]=vrrp_group
vrrp.@vrrp_group[0].enabled=1
```

Or using package options:

```
config vrrp_group
    option enabled '1'
```

However, to better identify, it is recommended to give the vrrp\_group instance a name. For example, to define a vrrp\_group instance named 'g1' using UCI, enter:

```
vrrp.g1.vrrp_group
vrrp.g1.enabled=1
```

To define a named keepalive instance using package options, enter:

```
config vrrp_group 'g1'
    option enabled '1'
```

### 24.4.1 VRRP using UCI

To view the configuration in UCI format, enter:

```
root@VA_router:~# uci show vrrp
vrrp.main=vrrp
```

```

vrrp.main.enabled=yes
vrrp.g1=vrrp_group
vrrp.g1.enabled=yes
vrrp.g1.interface=lan
vrrp.g1.track_iface=WAN MOBILE
vrrp.g1.init_state=BACKUP
vrrp.g1.router_id=1
vrrp.g1.priority=100
vrrp.g1.advert_int_sec=120
vrrp.g1.password=secret
vrrp.g1.virtual_ipaddr=10.1.10.150/16
vrrp.g1.garp_delay_sec=5
vrrp.g1.ipsec_connection=Test
vrrp.g1.track_ipsec=conn1 conn2

```

## 24.4.2 VRRP using package options

To view the configuration in package option format, enter:

```

root@VA_router:~# uci export vrrp
package vrrp

config vrrp 'main'
    option enabled 'yes'

config vrrp_group 'g1'
    option enabled 'yes'
    option interface 'lan'
    list track_iface 'WAN'
    list track_iface 'MOBILE'
    option init_state 'BACKUP'
    option router_id '1'
    option priority '100'
    option advert_int_sec '120'
    option password 'secret'
    option virtual_ipaddr '10.1.10.150/16'
    option garp_delay_sec '5'
    option ipsec_connection 'Test'

```

```
list track_ipsec 'conn1'  
list track_ipsec 'conn2'
```

## 24.5 VRRP diagnostics

### 24.5.1 VRRP process using UCI

The VRRP process has its own subset of commands.

```
root@VA_router:~# /etc/init.d/vrrp  
Syntax: /etc/init.d/vrrp [command]
```

Available commands:

```
start    Start the service  
stop     Stop the service  
restart  Restart the service  
reload   Reload configuration files (or restart if that fails)  
enable   Enable service autostart  
disable  Disable service autostart
```

To restart VRRP, enter:

```
root@VA_router:~# /etc/init.d/vrrp restart
```

## 25 Configuring Routing Information Protocol (RIP)

### 25.1 Introduction

RIP is a dynamic routing algorithm used on IP-based internet networks.

A distance vector routing algorithm is used by RIP to assist in maintaining network convergence. It uses a metric or 'hop' count as the only routing criteria. Each route is advertised with the number of hops a datagram would take to reach the destination network. The maximum metric for RIP is 15. This limits the size of the network that RIP can support. Smaller metrics are more efficient-based on the cost associated with each metric.

RIP protocol is most useful as an Interior Gateway Protocol (IGP). An IGP refers to the routing protocol used within a single autonomous system. There may be a number of autonomous systems, using different routing protocols, combined together to form a large network.

In most networking environments, RIP is not the preferred choice for routing as its time to converge and scalability are poor compared to EIGRP or OSPF.

#### 25.1.1 RIP characteristics

RIP is a standardised distance vector protocol, designed for use on smaller networks. RIP was one of the first true distance vector routing protocols, and is supported on a wide variety of systems.

RIP adheres to the following distance vector characteristics:

- RIP sends out periodic routing updates, every 30 seconds
- RIP sends out the full routing table every periodic update
- RIP uses a form of distance as its metric, in this case, hopcount
- RIP uses the Bellman-Ford distance vector algorithm to determine the best path to a particular destination

Other characteristics of RIP include:

- RIP supports IP and IPX routing
- RIP utilises UDP port 520
- RIP routes have an administrative distance of 120
- RIP has a maximum hopcount of 15 hops. Any network that is 16 hops away or more is considered unreachable to RIP, thus the maximum diameter of the network is 15 hops. A metric of 16 hops in RIP is considered a poison route or infinity metric.

If multiple paths exist to a particular destination, RIP will load balance between those paths, by default, up to 4, only if the metric (hopcount) is equal. RIP uses a round-robin system of load balancing between equal metric routes, which can lead to pinhole congestion.

For example, two paths might exist to a particular destination, one going through a 9600 baud link, the other via a T1. If the metric (hopcount) is equal, RIP will load balance, sending an equal amount of traffic down the 9600 baud link and the T1. This will cause the slower link to become congested.

## 25.1.2 RIP versions

RIP has two versions, Version 1 (RIPv1) and Version2 (RIPv2).

RIPv1 (RFC 1058) is classful, and therefore does not include the subnet mask with its routing table updates. Because of this, RIPv1 does not support Variable Length Subnet Masks (VLSMs). When using RIPv1, networks must be contiguous, and subnets of a major network must be configured with identical subnet masks. Otherwise, route table inconsistencies or worse will occur.

RIPv1 sends updates as broadcasts to address 255.255.255.255.

RIPv2 (RFC 2453) is classless, and therefore does include the subnet mask with its routing table updates. RIPv2 fully supports VLSMs, allowing discontinuous networks and varying subnet masks to exist.

Other enhancements offered by RIPv2 include:

- Routing updates are sent via multicast, using address 224.0.0.9
- Encrypted authentication can be configured between RIPv2 routers
- Route tagging is supported

RIPv2 can interoperate with RIPv1. By default:

- RIPv1 routers will sent only Version 1 packets
- RIPv1 routers will receive both Version 1 and 2 updates
- RIPv2 routers will both send and receive only Version 2 updates

Virtual Access **ripd** package supports RIP version 2 as described in RFC2453 and RIP version 1 as described in RFC1058. It is part of Quagga suite of applications for routing.

## 25.2 Configuration package used

| Package | Sections                                    |
|---------|---|
| ripd    | routing<br>interface<br>key_chain<br>offset |

## 25.3 Configuring RIP using the web interface

To configure RIP using the web interface, select **Network -> RIP**. The RIP page appears.

There are four sections in the RIP page.

| Section                       | Description  |
|-------------------------------|--|
| Global Settings               | Enables RIP and configures the RIP routing section containing global configuration parameters. The web automatically names the routing section <code>ripd</code> |
| Interfaces Configuration      | Configures the <code>interface</code> sections. Defines interface configuration for RIP and interface specific parameters.                                       |
| Offset Configuration          | Configures the <code>offset</code> sections for metric manipulation.   |
| MD5 Authentication Key Chains | Configures the <code>key_chain</code> sections. Defines MD5 authentication settings.   |

### 25.3.1 Global settings

The web browser automatically names the routing section 'ripd'.

**RIP**

Global Settings Delete

RIP Enabled

RIP Version

Network/Interface   
  
A.B.C.D/mask or interface name, e.g. 192.168.100.100/24 or gre1

RIP Neighbor Address   
  
A.B.C.D, e.g. 192.168.100.100

Update Timer  Every update timer seconds, the RIP process is awakened to send an unsolicited Response message containing the complete routing table to all neighboring RIP routers

Timeout Timer  Upon expiration of the timeout, the route is no longer valid; however, it is retained in the routing table for a short time so that neighbors can be notified that the route has been dropped

Garbage Collect Timer  Upon expiration, the route is finally removed from the routing table.

Make Default Router

Redistribute Kernel Routes

Figure 145: The RIP global settings configuration page

| Web Field/UCI/Package Option   | Description   |     |               |       |               |
|--|---|-----|---------------|-------|---------------|
| Web: RIP Enabled<br>UCI: ripd.ripd.enabled<br>Opt: enabled                         | Enables RIP advertisements on router. <table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0   | Disabled.     | 1     | Enabled.      |
| 0  | Disabled.   |     |               |       |               |
| 1  | Enabled.  |     |               |       |               |
| Web: RIP Version<br>UCI: ripd.ripd.version<br>Opt: version                         | Specifies the RIP version that will be used. Version 2 is recommended. <table border="1"> <tr> <td>1</td> <td>RIP version 1</td> </tr> <tr> <td>2</td> <td>RIP version 2</td> </tr> </table>  | 1   | RIP version 1 | 2     | RIP version 2 |
| 1  | RIP version 1   |     |               |       |               |
| 2  | RIP version 2   |     |               |       |               |
| Web: Network/Interface<br>UCI: ripd.ripd.network<br>Opt: list network              | Defines the list of the interfaces that will be used to advertise RIP packets.<br>Format: A.B.C.D/mask or interface name<br>Multiple RIP interfaces are entered using <code>uci set</code> and <code>uci add_list</code> commands. Example:<br><pre>uci set ripd.ripd.network=lan1 uci add_list ripd.ripd.network=lan2</pre> or using a list of options via package options<br><pre>list network 'lan1' list network 'lan2'</pre>   |     |               |       |               |
| Web: RIP Neighbor Address<br>UCI: ripd.ripd.neighbor<br>Opt: list neighbor         | Specifies the list of RIP neighbours. When a neighbour does not understand multicast, this command is used to specify neighbours. In some cases, not all routers will be able to understand multicasting, where packets are sent to a network or a group of addresses. In a situation where a neighbour cannot process multicast packets, it is necessary to establish a direct link between routers. The neighbour command allows the network administrator to specify a router as a RIP neighbour.<br>Multiple RIP neighbours are entered using <code>uci set</code> and <code>uci add_list</code> commands. Example:<br><pre>uci set ripd.ripd.neighbor=1.1.1.1 uci add_list ripd.ripd.neighbor=2.2.2.2</pre> or using a list of options via package options<br><pre>list neighbor '1.1.1.1' list neighbor '2.2.2.2'</pre> |     |               |       |               |
| Web: Update Timer<br>UCI: ripd.ripd.tb_update_sec<br>Opt: tb_update_sec            | Every update timer seconds, the RIP process is awakened to send an unsolicited response message containing the complete routing table to all neighbouring RIP routers. <table border="1"> <tr> <td>30</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 30  |               | Range |               |
| 30   |   |     |               |       |               |
| Range  |   |     |               |       |               |
| Web: Timeout Timer<br>UCI: ripd.ripd.tb_timeout_sec<br>Opt:tb_timeout_sec          | Defines timeout in seconds. Upon expiration of the timeout, the route is no longer valid; however, it is retained in the routing table for a short time so that neighbours can be notified that the route has been dropped. <table border="1"> <tr> <td>180</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 180 |               | Range |               |
| 180  |   |     |               |       |               |
| Range  |   |     |               |       |               |
| Web: Garbage Collect Timer<br>UCI: ripd.ripd.tb_garbage_sec<br>Opt: tb_garbage_sec | Upon expiration of the garbage-collection timer, the route is finally removed from the routing table. This timer starts when Timeout timer expires or when route is advertised as "unreachable".<br>The reason for using this two-stage marking and deleting removal method is to give the router that declared the route no longer reachable a chance to propagate this information to other routers. When the timer expires the route is deleted. If during the garbage collection period a new RIP response for the route is received, then the deletion process is aborted: the garbage-collection timer is cleared, the route is marked as valid again, and a new Timeout timer starts. <table border="1"> <tr> <td>120</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>                                | 120 |               | Range |               |
| 120  |   |     |               |       |               |
| Range  |   |     |               |       |               |

|   |   |
|---|---|
| Web: Make Default Router<br>UCI: ripd.ripd.default_info_originate<br>Opt: default_info_originate                | Advertising a default route via RIP.<br>0 Disable.<br>1 Enable.   |
| Web: Redistribute Kernel Routes<br>UCI: ripd.ripd.redistribute_kernel_routes<br>Opt: redistribute_kernel_routes | Redistributes routing information from kernel route entries into the RIP tables.<br>0 Disable.<br>1 Enable. |
| Web: n/a<br>UCI: ripd.ripd.vty_enabled<br>Opt: vty_enabled  | Enable vty for RIPd (telnet to localhost:2602).   |

Table 95: Information table for RIP global settings

### 25.3.2 Offset configuration

This section is used for RIP metric manipulation. RIP metric is a value for distance in the network. Usually, ripd package increments the metric when the network information is received. Redistributed routes' metric is set to 1.

Figure 146: The RIP global settings configuration page

| Web Field/UCI/Package Option   | Description   |
|--|---|
| Web: Metric<br>UCI: ripd.@offset[0].metric<br>Opt: metric              | Defines the metric offset value. This modifies the default metric value for redistributed and connected routes.<br>1<br>Range |
| Web: Match<br>UCI: ripd.@offset[0].match_network<br>Opt: match_network | Defines the prefixes to match.<br>Format: A.B.C.D/mask  |

Table 96: Information table for RIP offset commands

### 25.3.3 Interfaces configuration

Figure 147: The RIP interfaces configuration page



| Web Field/UCI/Package Option   | Description   |    |                                   |     |   |      |   |
|--|---|----|-----------------------------------|-----|---|------|---|
| Web: Interface<br>UCI: ripd.@interface[0].rip_interface<br>Opt: rip_interface        | Specifies the interface name.   |    |                                   |     |   |      |   |
| Web: Split Horizon<br>UCI: ripd.@interface[0].split_horizon<br>Opt: split_horizon    | Prohibits the router from advertising a route back onto the interface from which it was learned.<br><table border="1"> <tr> <td>0</td> <td>Disable.</td> </tr> <tr> <td>1</td> <td>Enable.</td> </tr> </table>  | 0  | Disable.                          | 1   | Enable.   |      |   |
| 0  | Disable.  |    |                                   |     |   |      |   |
| 1  | Enable.   |    |                                   |     |   |      |   |
| Web: Poison Reverse<br>UCI: ripd.@interface[0].poison_reverse<br>Opt: poison_reverse | Router tells its neighbour gateways that one of the gateways is no longer connected. Notifies the gateway, setting the hop count to the unconnected gateway to 16 which would mean "infinite".<br><table border="1"> <tr> <td>0</td> <td>Disable.</td> </tr> <tr> <td>1</td> <td>Enable.</td> </tr> </table>  | 0  | Disable.                          | 1   | Enable.   |      |   |
| 0  | Disable.  |    |                                   |     |   |      |   |
| 1  | Enable.   |    |                                   |     |   |      |   |
| Web: Passive<br>UCI: ripd.@interface[0].passive<br>Opt: passive                      | Sets the specified interface to passive mode. On passive mode interface, all receiving packets are processed as normal and ripd does not send either multicast or unicast RIP packets except to RIP neighbour specified with a neighbour command.<br><table border="1"> <tr> <td>0</td> <td>Disable</td> </tr> <tr> <td>1</td> <td>Enable</td> </tr> </table>   | 0  | Disable                           | 1   | Enable  |      |   |
| 0  | Disable   |    |                                   |     |   |      |   |
| 1  | Enable  |    |                                   |     |   |      |   |
| Web: Authentication<br>UCI: ripd.@interface[0].auth_mode<br>Opt: auth_mode           | RIPv2 (only) allows packets to be authenticated via either an insecure plain text password, included with the packet, or via a more secure MD5 based HMAC (keyed-Hashing for Message Authentication). Enabling authentication prevents routes being updated by unauthenticated remote routers, but still can allow routes, that is, the entire RIP routing table, to be queried remotely, potentially by anyone on the internet, via RIPv1.<br><table border="1"> <tr> <td>no</td> <td>Default value. No authentication.</td> </tr> <tr> <td>md5</td> <td>Sets the interface with RIPv2 MD5 authentication.</td> </tr> <tr> <td>text</td> <td>Sets the interface with RIPv2 simple password authentication.</td> </tr> </table> | no | Default value. No authentication. | md5 | Sets the interface with RIPv2 MD5 authentication. | text | Sets the interface with RIPv2 simple password authentication. |
| no   | Default value. No authentication.   |    |                                   |     |   |      |   |
| md5  | Sets the interface with RIPv2 MD5 authentication.   |    |                                   |     |   |      |   |
| text   | Sets the interface with RIPv2 simple password authentication.   |    |                                   |     |   |      |   |
| Web: Text Auth. Key<br>UCI: ripd.@interface[0].auth_key<br>Opt: auth_key             | This command sets the authentication string for text authentication. The string must be shorter than 16 characters.   |    |                                   |     |   |      |   |
| Web: MD5 Key Chain Name<br>UCI: ripd.@interface[0].key_chain<br>Opt: key_chain       | Specify Keyed MD5 chain.  |    |                                   |     |   |      |   |

Table 97: Information table for RIP interface configuration

### 25.3.4 MD5 authentication key chains

RIPv2 (only) allows packets to be authenticated using either an insecure plain text password, included with the packet, or by a more secure MD5 based HMAC (keyed-Hashing for Message Authentication). Enabling authentication prevents routes being updated by unauthenticated remote routers, but still can allow routes, that is, the entire RIP routing table, to be queried remotely, potentially by anyone on the internet, using RIPv1.

This section defines key\_chains to be used for MD5 authentication.

**Figure 148: The MD5 authentication key chains configuration section**

| Web Field/UCI/Package Option   | Description  |
|--|--|
| Web: Key Chain Name<br>UCI: ripd.@key_chain[0].key_chain_name<br>Opt: key_chain_name | Specifies the chain name.                                    |
| Web: Key ID<br>UCI: ripd.@key_chain[0].key_id<br>Opt: key_id                         | Specifies the key ID. Must be unique and match at both ends. |
| Web: Authentication key<br>UCI: ripd.@key_chain[0].auth_key<br>Opt: auth_key         | Specifies the keyed MD5 chain.                               |

**Table 98: Information table for MD5 authentication key chains commands**

## 25.4 Configuring RIP using command line

RIP is configured under the ripd package **/etc/config/ripd**.

There are four config sections ripd, interface, key\_chain and offset.

You can configure multiple interface, key\_chain and offset sections.

By default, all RIP interface instances are named interface, it is identified by @interface then the interface position in the package as a number. For example, for the first interface in the package using UCI:

```
ripd.@interface[0]=interface
ripd.@interface[0].rip_interface=lan
```

Or using package options:

```
config interface
    option rip_interface 'lan'
```

By default, all RIP key\_chain instances are named key\_chain, it is identified by @key\_chain then the key\_chain position in the package as a number. For example, for the first key\_chain in the package using UCI:

```
ripd.@key_chain[0]=key_chain
ripd.@key_chain[0].key_chain_name=Keychain1
```

Or using package options:

```
config key_chain
    option key_chain_name 'Keychain1'
```

By default, all RIP offset instances are named `offset`, it is identified by `@offset` then the offset position in the package as a number. For example, for the first offset in the package using UCI:

```
ripd.@offset[0]=offset
ripd.@offset[0].metric=1
```

Or using package options:

```
config offset
    option metric '1'
```

### 25.4.1 RIP using UCI

```
root@VA_router:~# uci show ripd
ripd.ripd=routing
ripd.ripd.version=2
ripd.ripd.enabled=yes
ripd.ripd.network=lan2 gre1
ripd.ripd.neighbor=10.1.1.100 10.1.2.100
ripd.ripd.tb_update_sec=30
ripd.ripd.tb_timeout_sec=180
ripd.ripd.tb_garbage_sec=120
ripd.ripd.default_info_originate=yes
ripd.ripd.redistribute_kernel_routes=yes
ripd.@interface[0]=interface
ripd.@interface[0].rip_interface=lan
ripd.@interface[0].auth_mode=no
ripd.@interface[0].split_horizon=1
ripd.@interface[0].poison_reverse=0
ripd.@interface[0].passive=0
ripd.@interface[1]=interface
ripd.@interface[1].rip_interface=lan2
ripd.@interface[1].split_horizon=1
ripd.@interface[1].poison_reverse=0
```

```
ripd.@interface[1].passive=0
ripd.@interface[1].auth_mode=text
ripd.@interface[1].auth_key=secret
ripd.@interface[2]=interface
ripd.@interface[2].rip_interface=lan3
ripd.@interface[2].split_horizon=1
ripd.@interface[2].poison_reverse=0
ripd.@interface[2].passive=0
ripd.@interface[2].auth_mode=md5
ripd.@interface[2].key_chain=Keychain1
ripd.@key_chain[0]=key_chain
ripd.@key_chain[0].key_chain_name=Keychain1
ripd.@key_chain[0].key_id=1
ripd.@key_chain[0].auth_key=123
ripd.@offset[0]=offset
ripd.@offset[0].metric=1
ripd.@offset[0].match_network=10.1.1.1/24
```

## 25.4.2 RIP using package options

```
root@VA_router:~# uci export ripd
package ripd

config routing 'ripd'
    option version '2'
    option enabled 'yes'
    list network 'lan2'
    list network 'grel'
    list neighbor '10.1.1.100'
    list neighbor '10.1.2.100'
    option tb_update_sec '30'
    option tb_timeout_sec '180'
    option tb_garbage_sec '120'
    option default_info_originate 'yes'
    option redistribute_kernel_routes 'yes'

config interface
```

```
option rip_interface 'lan'
option auth_mode 'no'
option split_horizon '1'
option poison_reverse '0'
option passive '0'

config interface
option rip_interface 'lan2'
option split_horizon '1'
option poison_reverse '0'
option passive '0'
option auth_mode 'text'
option auth_key 'textsecret'

config interface
option rip_interface 'lan3'
option split_horizon '1'
option poison_reverse '0'
option passive '0'
option auth_mode 'md5'
option key_chain 'keychain1'

config key_chain
option key_chain_name 'Keychain1'
option key_id '1'
option auth_key '123'

config offset
option metric '1'
option match_network '10.1.1.1/24'
```

## 25.5 RIP diagnostics

### 25.5.1 Route status

To show the current routing status, enter:

```
root@VA_router:~#
route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use
Iface
0.0.0.0          10.205.154.65   0.0.0.0          UG    1     0     0 usb0
10.1.0.0         0.0.0.0         255.255.0.0      U     0     0     0 eth1
10.205.154.64   0.0.0.0         255.255.255.252 U     0     0     0 usb0
11.11.11.0      0.0.0.0         255.255.255.248 U     0     0     0 gre-
GRE
89.101.154.151 10.205.154.65   255.255.255.255 UGH   0     0     0 usb0
192.168.100.0   0.0.0.0         255.255.255.0    U     0     0     0 eth0
192.168.104.1   11.11.11.4      255.255.255.255 UGH   3     0     0 gre-
GRE
192.168.154.154 11.11.11.1      255.255.255.255 UGH   2     0     0 gre-
GRE
```

**Note:** a route will only be displayed in the routing table when the interface is up.

### 25.5.2 Tracing RIP packets

RIP uses UDP port 520. To trace RIP packets on any interface on the router, enter:

```
tcpdump -i any -n -p port 520 &
```

```
root@VA_router:~# tcpdump -i any -n -p port 520 &
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535
bytes
```

To stop tracing enter `fg` to bring tracing task to foreground, and then **<CTRL-C>** to stop the trace.

```
root@VA_router:~# fg
tcpdump -i any -n -p port 67
^C
33 packets captured
33 packets received by filter
0 packets dropped by kernel
```

### 25.5.3 Quagga/Zebra console

Quagga is the routing protocol suite embedded in the router firmware. Quagga is split into different daemons for implementation of each routing protocol. Zebra is a core daemon for Quagga, providing the communication layer to the underlying Linux kernel, and routing updates to the client daemons.

Quagga has a console interface to Zebra for advanced debugging of the routing protocols.

To access, enter: `telnet localhost zebra (password: zebra)`

```
root@VA_router:~# telnet localhost zebra

Entering character mode
Escape character is '^]'.

Hello, this is Quagga (version 0.99.21).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
```

To see RIP routing information from Zebra console, enter:

```
root@VA_router:~# sh ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, H - HSL, o - OLSR,
       b - BATMAN, A - Babel,
       > - selected route, * - FIB route

K>* 0.0.0.0/0 via 10.205.154.65, usb0
C>* 10.1.0.0/16 is directly connected, eth1
C>* 10.205.154.64/30 is directly connected, usb0
C>* 11.11.11.0/29 is directly connected, gre-GRE
K>* 89.101.154.151/32 via 10.205.154.65, usb0
C>* 127.0.0.0/8 is directly connected, lo
C>* 192.168.100.0/24 is directly connected, eth0
R>* 192.168.104.1/32 [120/3] via 11.11.11.4, gre-GRE, 15:54:47
```

```
C>* 192.168.105.1/32 is directly connected, lo
R>* 192.168.154.154/32 [120/2] via 11.11.11.1, gre-GRE, 16:09:51
```

## 25.5.4 RIP debug console

When option `vty_enabled` (see Global settings section above) is enabled in the RIP configuration, RIP debug console can be accessed for advanced RIP debugging.

To access RIP debug console enter: `telnet localhost ripd` (password zebra)

```
root@VA_router:~# telnet localhost ripd

Entering character mode
Escape character is '^]'.

Hello, this is Quagga (version 0.99.21).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
```

To see RIP status from RIP debug console, enter:

```
root@VA_router:~# show ip rip
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
      (n) - normal, (s) - static, (d) - default, (r) - redistribute,
      (i) - interface

      Network          Next Hop          Metric From          Tag Time
C(i) 11.11.11.0/29     0.0.0.0           1 self              0
R(n) 192.168.104.1/32 11.11.11.4        3 11.11.11.1        0 02:48
C(i) 192.168.105.1/32 0.0.0.0           1 self              0
R(n) 192.168.154.154/32 11.11.11.1       2 11.11.11.1        0 02:48
```



To see RIP status from RIP debug console, enter:

```
root@VA_router:~# sh ip rip status
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 17 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive version 2
    Interface      Send  Recv  Key-chain
  gre-GRE         2     2
  lo              2     2
  Routing for Networks:
    11.0.0.0/8
    192.168.105.1/32
  Routing Information Sources:
    Gateway          BadPackets  BadRoutes  Distance  Last Update
  11.11.11.1         0           0          120      00:00:20
  Distance: (default is 120)
```

## 26 Configuring Multi-WAN

Multi-WAN is used for managing WAN interfaces on the router, for example, 3G interfaces to ensure high-availability. You can customise Multi-WAN for various needs, but its main use is to ensure WAN connectivity and provide a failover system in the event of failure or poor coverage.

Multi-WAN periodically does a health check on the interface. A health check comprises of a configurable combination of the following:

- interface state
- pings to an ICMP target
- signal level checks using signal threshold, RSCP threshold and ECIO threshold option values

A fail for any of the above health checks, results in a fail. After a configurable number of health check failures, Multi-WAN will move to the next highest priority interface. Multi-WAN will optionally stop the failed interface and start the new interface, if required.

In some circumstances, particularly in mobile environments, it is desirable for a primary interface to be used whenever possible. In this instance Multi-WAN will perform a health check on the primary interface after a configurable period. If the health checks pass for the configured number of recovery health checks then the primary will be used.

### 26.1 Configuration package used

| Package  | Sections      |
|----------|---------------|
| multiwan | config<br>wan |

### 26.2 Configuring Multi-WAN using the web interface

In the top menu, select **Network -> Multi-Wan**. The Multi-WAN page appears.

**Multi-WAN**  
Multi-WAN allows for the use of multiple uplinks for load balancing and failover.

Enable

Preempt

Alternate Mode  ⓘ It will use alternate interface after reboot

**Figure 149: The multi-WAN page**

| Web Field/UCI/Package Option  | Description  |   |           |   |          |
|---|--|---|-----------|---|----------|
| Web: Enable<br>UCI: multiwan.config.enabled<br>Opt: enabled           | Enables or disables Multi-WAN.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0 | Disabled. | 1 | Enabled. |
| 0   | Disabled.  |   |           |   |          |
| 1   | Enabled.   |   |           |   |          |
| Web: Preempt<br>UCI: multiwan.config.preempt<br>Opt: preempt          | Enables or disables pre-emption for Multi-WAN. If enabled the router will keep trying to connect to a higher priority interface depending on timer set by ifup_retry_sec<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0 | Disabled. | 1 | Enabled. |
| 0   | Disabled.  |   |           |   |          |
| 1   | Enabled.   |   |           |   |          |
| Web: Alternate Mode<br>UCI: multiwan.config.alt_mode<br>Opt: alt_mode | Enables or disables alternate mode for Multi-WAN. If enabled the router will use an alternate interface after reboot.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0 | Disabled. | 1 | Enabled. |
| 0   | Disabled.  |   |           |   |          |
| 1   | Enabled.   |   |           |   |          |

**Table 99: Information table for multi-WAN page**

When you have enabled Multi-WAN, you can add the interfaces that will be managed by Multi-WAN, for example 3G interfaces.

The name used for Multi-WAN must be identical, including upper and lowercases, to the actual interface name defined in your network configuration. To check the names and settings are correct, select **Network -> Interfaces** and view the Interfaces Overview page.

In the WAN interfaces section, enter the name of the WAN interface to configure, and then click **Add**. The new section for configuring specific parameters appears.

### WAN Interfaces

Health Monitor detects and corrects network changes and failed connections.

#### WAN

|                                      |                                     |  |
|--------------------------------------|-------------------------------------|--|
| Health Monitor Interval              | 10 sec.                             |  |
| Health Monitor ICMP Host(s)          | DNS Server(s)                       |  |
| Health Monitor Contrack Test Host(s) | Default                             |  |
| Health Monitor ICMP Timeout          | 3 sec.                              |  |
| Health Monitor ICMP Interval         | 1 sec.                              |  |
| Attempts Before WAN Failover         | 3                                   |  |
| Attempts Before WAN Recovery         | 5                                   |  |
| Priority                             | 0                                   | <a href="#">?</a> Higher value is higher priority                                  |
| Exclusive Group                      | 0                                   | <a href="#">?</a> Only one interface in group could be up in the same time         |
| Manage Interface State (Up/Down)     | <input checked="" type="checkbox"/> |  |
| Minimum ifup Interval                | 300 sec.                            | <a href="#">?</a> Minimum interval between two successive interface start attempts |
| Interface Start Timeout              | 40 sec.                             | <a href="#">?</a> Time for interface to startup                                    |
| Signal Threshold (dBm)               | -115                                | <a href="#">?</a> Below is a failure   |
| RSCP Threshold for 3G (dBm)          | -115                                | <a href="#">?</a> Below is a failure   |
| ECIO Threshold for 3G (dB)           | -115                                | <a href="#">?</a> Below is a failure   |
| Signal Test                          |                                     | <a href="#">?</a> Free form expression to test signal value                        |

**Figure 150: Example interface showing failover traffic destination as the added multi-WAN interface**

| Web Field/UCI/Package Option  | Description  |         |   |             |                                |             |   |        |  |
|---|--|---------|---|-------------|--------------------------------|-------------|---|--------|--|
| Web: Health Monitor Interval<br>UCI: multiwan.wan.health_interval<br>Opt: health_interval                         | Sets the period to check the health status of the interface. The Health Monitor interval will be used for: <ul style="list-style-type: none"> <li>Interface state checks</li> <li>Ping interval</li> <li>Signal strength checks</li> </ul> The health monitor interval has a granularity of 5 seconds. Configured values will be rounded up to the next 5 second value. <table border="1"> <tr> <td>10</td> <td>Perform a health check every 10 seconds.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 10      | Perform a health check every 10 seconds.  | Range       |                                |             |   |        |  |
| 10  | Perform a health check every 10 seconds.   |         |   |             |                                |             |   |        |  |
| Range   |  |         |   |             |                                |             |   |        |  |
| Web: Health Monitor ICMP Host(s)<br>UCI: multiwan.wan.icmp_hosts<br>Opt: icmp_hosts                               | Sends health ICMPs to configured value DNS servers by default. Configure to any address. <table border="1"> <tr> <td>Disable</td> <td>Disables the option.</td> </tr> <tr> <td>DNS servers</td> <td>DNS IP addresses will be used.</td> </tr> <tr> <td>WAN Gateway</td> <td>Gateway IP address will be used.</td> </tr> <tr> <td>Custom</td> <td>Ability to provide IP address. Multiple pings targets can be entered, comma separated. Pings to both must fail for health check to fail. Example:<br/>option icmp_hosts '1.1.1.1,2.2.2.2'</td> </tr> </table>   | Disable | Disables the option.  | DNS servers | DNS IP addresses will be used. | WAN Gateway | Gateway IP address will be used.                                | Custom | Ability to provide IP address. Multiple pings targets can be entered, comma separated. Pings to both must fail for health check to fail. Example:<br>option icmp_hosts '1.1.1.1,2.2.2.2' |
| Disable   | Disables the option.   |         |   |             |                                |             |   |        |  |
| DNS servers   | DNS IP addresses will be used.   |         |   |             |                                |             |   |        |  |
| WAN Gateway   | Gateway IP address will be used.   |         |   |             |                                |             |   |        |  |
| Custom  | Ability to provide IP address. Multiple pings targets can be entered, comma separated. Pings to both must fail for health check to fail. Example:<br>option icmp_hosts '1.1.1.1,2.2.2.2'   |         |   |             |                                |             |   |        |  |
| Web: Health Monitor Contrack Test Host(s)<br>UCI: multiwan.wan.contrack_hosts<br>Opt: contrack_hosts              | Contrack is the feature used to track if there is any traffic to and from an IP destination within the health interval.<br>The Contrack_hosts option defines the IP for contrack to track, usually the icmp_host IP is used.<br>If traffic to the contrack_hosts IP is detected then multiwan does not send a ping health check to the icmp_host; otherwise a ping is sent as normal to the icmp_host.<br>By default the contrack_hosts is checked if the health interval is greater than 5 minutes. This time threshold currently cannot be manipulated.<br>Contrack is generally used to limit the traffic sent on a GSM network. <table border="1"> <tr> <td>Default</td> <td>Contrack checks for traffic from icmp_host IP when health_interval is greater than 5 minutes.</td> </tr> <tr> <td>Disable</td> <td>Contrack disabled.</td> </tr> <tr> <td>Custom</td> <td>Specifies an IP other than the icmp_host for contrack to track.</td> </tr> </table> | Default | Contrack checks for traffic from icmp_host IP when health_interval is greater than 5 minutes. | Disable     | Contrack disabled.             | Custom      | Specifies an IP other than the icmp_host for contrack to track. |        |  |
| Default   | Contrack checks for traffic from icmp_host IP when health_interval is greater than 5 minutes.  |         |   |             |                                |             |   |        |  |
| Disable   | Contrack disabled.   |         |   |             |                                |             |   |        |  |
| Custom  | Specifies an IP other than the icmp_host for contrack to track.  |         |   |             |                                |             |   |        |  |
| Web: Health Monitor ICMP Timeout<br>UCI: multiwan.wan.timeout<br>Opt: timeout                                     | Sets Ping timeout in seconds. Choose the time in seconds that the health monitor ICMP will timeout at. <table border="1"> <tr> <td>3</td> <td>Wait 3 seconds for ping reply.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 3       | Wait 3 seconds for ping reply.  | Range       |                                |             |   |        |  |
| 3   | Wait 3 seconds for ping reply.   |         |   |             |                                |             |   |        |  |
| Range   |  |         |   |             |                                |             |   |        |  |
| Web: Health Monitor ICMP Interval<br>UCI: multiwan.wan.icmp_interval<br>Opt: icmp_interval                        | Defines the interval between multiple pings sent at each health check <table border="1"> <tr> <td>1</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 1       |   | Range       |                                |             |   |        |  |
| 1   |  |         |   |             |                                |             |   |        |  |
| Range   |  |         |   |             |                                |             |   |        |  |
| Web: Health Monitor ICMP Count<br>UCI: multiwan.wan.icmp_count<br>Opt: icmp_count                                 | Defines the number of pings to send at each health check. <table border="1"> <tr> <td>1</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 1       |   | Range       |                                |             |   |        |  |
| 1   |  |         |   |             |                                |             |   |        |  |
| Range   |  |         |   |             |                                |             |   |        |  |
| Web: Attempts Before WAN Failover<br>UCI: multiwan.wan.health_fail_retries<br>Opt: health_fail_retries            | Sets the amount of health monitor retries before the interface is considered a failure. <table border="1"> <tr> <td>3</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 3       |   | Range       |                                |             |   |        |  |
| 3   |  |         |   |             |                                |             |   |        |  |
| Range   |  |         |   |             |                                |             |   |        |  |
| Web: Attempts Before WAN Recovery<br>UCI:<br>multiwan.wan.health_recovery_retries<br>Opt: health_recovery_retries | Sets the number of health monitor checks before the interface is considered healthy. Only relevant if pre-empt mode is enabled. <table border="1"> <tr> <td>5</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 5       |   | Range       |                                |             |   |        |  |
| 5   |  |         |   |             |                                |             |   |        |  |
| Range   |  |         |   |             |                                |             |   |        |  |

|  |  |
|--|--|
| Web: Priority<br>UCI: multiwan.wan.priority<br>Opt: priority                                 | Specifies the priority of the interface. The higher the value, the higher the priority.<br>0<br>Range  |
| Web: Manage Interface State (Up/Down)<br>UCI: multiwan.wan.manage_state<br>Opt: manage_state | Defines whether multi-wan will start and stop the interface.<br>1 Enabled.<br>0 Disabled.  |
| Web: Exclusive Group<br>UCI: multiwan.wan.exclusive_group<br>Opt: exclusive_group            | Defines the group to which the interface belongs; only one interface can be active.<br>0<br>Range  |
| Web: Minimum ifup Interval<br>UCI: multiwan.wan.ifup_retry_sec<br>Opt: ifup_retry_sec        | Specifies the interval in seconds before retrying the primary interface when pre-empt mode is enabled.<br>300 Retry primary interface every 300 seconds.<br>Range  |
| Web: Interface Start Timeout<br>UCI: multiwan.wan.ifup_timeout<br>Opt: ifup_timeout          | Specifies the time in seconds for interface to start up. If it is not up after this period, it will be considered a fail.<br>40 40 seconds.<br>Range   |
| Web: Signal Threshold (dBm)<br>UCI: multiwan.wan.signal_threshold<br>Opt: signal_threshold   | Specifies the minimum signal strength in dBm before considering if the interface fails signal health check. Uses the value stored for sig_dbm in mobile diagnostics.-115.<br>Disabled<br>Range -46 to -115 dBm   |
| Web: RSCP Threshold (dBm)<br>UCI: multiwan.wan.rscp_threshold<br>Opt: rscp_threshold         | Specifies the minimum RSCP signal strength in dBm before considering if the interface fails signal health check. Uses the value stored for rscp_dbm in mobile diagnostics.<br>-115 Disabled<br>Range -46 to -115 dBm   |
| Web: ECIO Threshold (dB)<br>UCI: multiwan.wan.ecio_threshold<br>Opt: ecio_threshold          | Specifies the minimum ECIO signal strength in dB before considering if the interface fails signal health check. Uses the value stored for ecio_db in mobile diagnostics.<br>-115 Disabled<br>Range -46 to -115 dB  |
| Web: Signal Test<br>UCI: multiwan.wan.signal_test<br>Opt: signal_test                        | Defines a script to test various signal characteristics in multiwan signal test. For example:<br><pre>option signal_test '(tech == 0) then (sig_dbm &gt; -70) else (rscp_dbm &gt; -105 and ecio_db &gt; -15)'</pre><br>This states that when technology is GSM, a health fail is determined when signal strength is less than -70dBm. When technology is not GSM a health fail occurs when either rscp_dbm falls below -105dBm or ecio_db falls below -15dB<br>Tech values are:<br>0 GSM<br>1 GSM Compact<br>2 UTRAN<br>3 GSM w/EGPRS<br>4 UTRAN w/HSPDA<br>5 UTRAN w/HSUPA<br>6 UTRAN w/HSUPA and HSDPA<br>7 E-UTRAN<br><b>Note:</b> a signal test can also take a UDS script name as a parameter. For example:<br><pre>option signal_test 'uds(script name)'</pre> |

Table 100: Information table for multi-WAN interface page

## 26.3 Configuring Multi-WAN using UCI

Multi-WAN UCI configuration settings are stored on `/etc/config/multiwan`.

Run `UCI export` or `show` commands to see multiwan UCI configuration settings. A sample is shown below.

```
root@VA_router:~# uci export multiwan

package multiwan

config multiwan 'config'
    option preempt 'yes'
    option alt_mode 'no'
    option enabled 'yes'
config interface 'wan'
    option disabled '0'
    option health_interval '10'          option health_fail_retries '3'
    option health_recovery_retries '5'
    option priority '2'
    option manage_state 'yes'
    option exclusive_group '0'
    option ifup_retry_sec '40'
    option icmp_hosts 'disable'
    option icmp_interval '1'
    option timeout '3'
    option icmp_count '1'
    option conntrack_hosts 'disable'    option signal_threshold '-
111'
    option rscp_threshold '-90'
    option ecio_threshold '-15'
    option ifup_timeout_sec '120'

root@VA_router:~# uci show multiwan
multiwan.config=multiwan
multiwan.config.preempt=yes
multiwan.config.alt_mode=no
multiwan.config.enabled=yes
multiwan.wan=interface
```

```
multiwan.wan.disabled=0
multiwan.wan.health_interval=10multiwan.wan.health_fail_retries=3
multiwan.wan.health_recovery_retries=5
multiwan.wan.priority=2
multiwan.wan.manage_state=yes
multiwan.wan.exclusive_group=0
multiwan.wan.ifup_retry_sec=36000
multiwan.wan.icmp_hosts=disable
multiwan.wan.timeout=3
multiwan.wan.icmp_interval '1'
multiwan.wan.timeout '3'
multiwan.wan.icmp_count '1'
multiwan.wan.conntrack_hosts 'disable'
multiwan.wan.signal_threshold=-111
multiwan.wan.rscp_threshold=-90
multiwan.wan.ecio_threshold=-15
```

## 26.4 Multi-WAN diagnostics

The multiwan package is linked to the network interfaces within `/etc/config/network`.

**Note:** Multi-WAN will not work if the WAN connections are on the same subnet and share the same default gateway.

To view the multiwan package, enter:

```
root@VA_router:~# uci export multiwan
package multiwan

config multiwan 'config'
    option enabled 'yes'
    option preempt 'yes'
    option alt_mode 'no'

config interface 'ADSL'
    option health_interval '10'
    option icmp_hosts 'dns'
    option timeout '3'
    option health_fail_retries '3'
    option health_recovery_retries '5'
```



```

option priority '1'
option manage_state 'yes'
option exclusive_group '0'
option ifup_retry_sec '300'
option ifup_timeout_sec '40'

config interface 'Ethernet'
option health_interval '10'
option icmp_hosts 'dns'
option timeout '3'
option health_fail_retries '3'
option health_recovery_retries '5'
option priority '2'
option manage_state 'yes'
option exclusive_group '0'
option ifup_retry_sec '300'
option ifup_timeout_sec '40'

```

The following output shows the multiwan standard stop/start commands for troubleshooting.

```

root@VA_router:~# /etc/init.d/multiwan
Syntax: /etc/init.d/multiwan [command]

```

#### Available commands:

```

start    Start the service
stop     Stop the service
restart  Restart the service
reload   Reload configuration files (or restart if that fails)
enable   Enable service autostart
disable  Disable service autostart

```

When troubleshooting, make sure that the routing table is correct using `route -n`.

Ensure all parameters in the multiwan package are correct. The name used for Multi-WAN interfaces must be identical, including upper and lowercases, to the interface name defined in the network configuration.

To check the names and settings are correct, browse to **Network -> interfaces** (or alternatively, run: `cat/etc/config/network` through CLI).

Enter the name of the WAN interface to configure, and then click **Add**. The new section for configuring specific parameters will appear.

## 27 Automatic operator selection

This section describes how to configure and operate the Automatic Operator Selection feature of a Virtual Access router.

When the roaming SIM is connected, the radio module has the ability to scan available networks. The router, using mobile and multiwan packages, finds available networks to create and sort interfaces according to their signal strength. These interfaces are used for failover purposes.

### 27.1 Configuration package used

| Package  | Sections                 |
|----------|--------------------------|
| Multiwan | General, interfaces      |
| Mobile   | Main, template interface |
| Network  | 2G/3G/4G interface       |

### 27.2 Configuring automatic operator selection via the web interface

While the router boots up it checks for mobile networks. Based on available networks, the router creates interfaces and the multiwan package is used to run failover between interfaces. Typically these auto-generated interfaces are sorted by signal strength.

Details for these interfaces are provided in the mobile package. When you have created the interfaces, Multi-WAN manages the operation of primary (predefined) and failover (auto created) interfaces.

Multi-WAN periodically does a health check on the active interface. A health check comprises of a configurable combination of the following:

- interface state
- pings to an ICMP target
- signal level checks using signal threshold, RSCP threshold and ECIO threshold option values

A fail for any of the above health checks results in an overall fail. After a configurable number of health check failures, multiwan will move to the next highest priority interface. Multi-WAN will optionally stop the failed interface and start the new interface, if required.

In some circumstances, particularly in mobile environments, it is desirable for a primary interface to be used whenever possible. In this instance, if the active interface is not the primary interface, multiwan will perform a health check on the primary interface after a configurable period. If the health checks pass for the configured number of recovery health checks then the primary interface will be used.

There are typically three scenarios:

- Primary Mobile Provider (PMP) + roaming: pre-empt enabled
- PMP + roaming: pre-empt disabled
- No PMP + roaming

## 27.2.1 Scenario 1: PMP + roaming: pre-empt enabled

### 27.2.1.1 Overview

In this scenario, the PMP interface is used whenever possible.

The PMP interface is attempted first. When the health checks fail on the PMP interface, and Multi-WAN moves to an autogenerated interface, a timer is started `multiwan option ifup_retry_sec`. On expiration of this timer, multiwan will disconnect the current interface and retry the PMP interface.

The PMP interface will then be used if the configurable number of health checks pass the checks.

### 27.2.1.2 Software operation

1. multiwan first attempts to bring up the PMP interface. If the PMP interface connects within the time set by multiwan option `ifup_timeout` continue to step 2. Otherwise go to step 4.
2. A health check is periodically done on the PMP interface as determined by the multiwan option `health_interval`. If the health check fails for the number of retries (multiwan option `health_fail_retries`), disconnect the PMP interface.
3. Connect the first auto-generated interface.
4. If the interface connects within the time set by multiwan option `ifup_timeout` continue to step 5, otherwise multiwan moves to the next auto-generated interface.
5. Wait until the health check fails on the auto-generated interface, or until the PMP interface is available to connect after it was disconnected in step 2. (multiwan option `ifup_retry_sec`).
6. Disconnect auto-generated interface.
7. If the interface was disconnected due to health check failure then connect the next auto-generated interface and repeat step 4. If the interface was disconnected because `ifup_retry_sec` of PMP interface timed out, then go back to step 1 and repeat the process.

The PMP predefined interface is defined in the network package. Ensure the interface name matches the interface name defined in the multiwan package.

### 27.2.1.3 Create a primary predefined interface

In the web interface top menu, go to **Network -> Interfaces**. The Interfaces page appears.

The screenshot shows the 'Interface Overview' page. It features a table with columns for 'Network', 'Status', and 'Actions'. The 'LAN' interface (eth0) is highlighted in green. Its status shows an uptime of 6h 37m 34s, MAC address 00:E0:C8:10:0E:E6, RX of 431.31 MB (4672877 Pkts.), TX of 1.68 MB (21023 Pkts.), and IPv4 address 10.1.10.93/16. The 'LOOPBACK' interface (lo) also shows an uptime of 6h 37m 38s, MAC address 00:00:00:00:00:00, RX of 9.99 MB (109997 Pkts.), TX of 9.99 MB (109997 Pkts.), IPv4 address 127.0.0.1/8, and IPv6 address 0:0:0:0:0:0:0:1/128. Below the table is an 'Add new interface...' button.

Figure 151: The interface overview page

Click **Add new interface...** The Create Interface page appears.

The 'Create Interface' page has a form with the following elements:
 

- Name of the new interface:** A text input field with a help icon and a note: 'The allowed characters are: A-Z, a-z, 0-9 and \_'.
- Protocol of the new interface:** A dropdown menu currently set to 'Static address'.
- Create a bridge over multiple interfaces:** An unchecked checkbox.
- Cover the following interface:** A section with radio buttons for:
  - Ethernet Adapter: "eth0" (lan)
  - Ethernet Adapter: "gre0"
  - Ethernet Adapter: "lo" (loopback)
  - Custom Interface: [input field]
- Note:** 'Note: If you choose an interface here which is part of another network, it will be moved into this network.'

Figure 152: The create interface page

| Web Field/UCI/Package Option   | Description   |               |                                 |             |      |         |      |        |      |
|--|---|---------------|---------------------------------|-------------|------|---------|------|--------|------|
| Web: Name of the new interface<br>UCI: network.3g_s<sim-number>_<short-operator-name>.<br>Opt: 3g_s<sim-number>_<short-operator-name>. | Type the name of the new interface.<br>Type the interface name in following format:<br>3g_s<sim-number>_<short-operator-name>. Where <sim-number> is number of roaming SIM (1 or 2) and <short-operator-name> is first four alphanumeric characters of operator name (as reported by 'AT+COPS=?' command).<br>Type the short operator name in lower case, for example: <table border="1" data-bbox="683 1787 1391 1928"> <thead> <tr> <th>Operator name</th> <th>First four alphanumeric numbers</th> </tr> </thead> <tbody> <tr> <td>Vodafone UK</td> <td>voda</td> </tr> <tr> <td>O2 - UK</td> <td>o2uk</td> </tr> <tr> <td>Orange</td> <td>oran</td> </tr> </tbody> </table> | Operator name | First four alphanumeric numbers | Vodafone UK | voda | O2 - UK | o2uk | Orange | oran |
| Operator name  | First four alphanumeric numbers   |               |                                 |             |      |         |      |        |      |
| Vodafone UK  | voda  |               |                                 |             |      |         |      |        |      |
| O2 - UK  | o2uk  |               |                                 |             |      |         |      |        |      |
| Orange   | oran  |               |                                 |             |      |         |      |        |      |

| <p>Web: Protocol of the new interface<br/>UCI: network[..x..].proto<br/>Opt: proto</p>     | <p>Protocol type. Select <b>LTE/UMTS/GPRS/EV-DO</b>.</p> <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Static</td> <td>Static configuration with fixed address and netmask.</td> </tr> <tr> <td>DHCP Client</td> <td>Address and netmask are assigned by DHCP.</td> </tr> <tr> <td>Unmanaged</td> <td>Unspecified</td> </tr> <tr> <td>IPv6-in-IPv4 (RFC4213)</td> <td>IPv4 tunnels that carry IPv6.</td> </tr> <tr> <td>IPv6 over IPv4</td> <td>IPv6 over IPv4 tunnel.</td> </tr> <tr> <td>GRE</td> <td>Generic Routing Encapsulation.</td> </tr> <tr> <td>IOT</td> <td></td> </tr> <tr> <td>L2TP</td> <td>Layer 2 Tunnelling Protocol.</td> </tr> <tr> <td>PPP</td> <td>Point to Point Protocol.</td> </tr> <tr> <td>PPPoE</td> <td>Point to Point Protocol over Ethernet.</td> </tr> <tr> <td>PPPoATM</td> <td>Point to Point Protocol over ATM.</td> </tr> <tr> <td>LTE/UMTS/GPRS/EV-DO</td> <td>CDMA, UMTS or GPRS connection using an AT-style 3G modem.</td> </tr> </tbody> </table> | Option | Description | Static | Static configuration with fixed address and netmask. | DHCP Client | Address and netmask are assigned by DHCP. | Unmanaged | Unspecified | IPv6-in-IPv4 (RFC4213) | IPv4 tunnels that carry IPv6. | IPv6 over IPv4 | IPv6 over IPv4 tunnel. | GRE | Generic Routing Encapsulation. | IOT |  | L2TP | Layer 2 Tunnelling Protocol. | PPP | Point to Point Protocol. | PPPoE | Point to Point Protocol over Ethernet. | PPPoATM | Point to Point Protocol over ATM. | LTE/UMTS/GPRS/EV-DO | CDMA, UMTS or GPRS connection using an AT-style 3G modem. |
|--|---|--------|-------------|--------|--|-------------|---|-----------|-------------|------------------------|-------------------------------|----------------|------------------------|-----|--------------------------------|-----|--|------|------------------------------|-----|--------------------------|-------|--|---------|-----------------------------------|---------------------|---|
| Option   | Description   |        |             |        |  |             |   |           |             |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| Static   | Static configuration with fixed address and netmask.  |        |             |        |  |             |   |           |             |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| DHCP Client  | Address and netmask are assigned by DHCP.   |        |             |        |  |             |   |           |             |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| Unmanaged  | Unspecified   |        |             |        |  |             |   |           |             |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| IPv6-in-IPv4 (RFC4213)   | IPv4 tunnels that carry IPv6.   |        |             |        |  |             |   |           |             |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| IPv6 over IPv4   | IPv6 over IPv4 tunnel.  |        |             |        |  |             |   |           |             |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| GRE  | Generic Routing Encapsulation.  |        |             |        |  |             |   |           |             |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| IOT  |   |        |             |        |  |             |   |           |             |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| L2TP   | Layer 2 Tunnelling Protocol.  |        |             |        |  |             |   |           |             |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| PPP  | Point to Point Protocol.  |        |             |        |  |             |   |           |             |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| PPPoE  | Point to Point Protocol over Ethernet.  |        |             |        |  |             |   |           |             |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| PPPoATM  | Point to Point Protocol over ATM.   |        |             |        |  |             |   |           |             |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| LTE/UMTS/GPRS/EV-DO  | CDMA, UMTS or GPRS connection using an AT-style 3G modem.   |        |             |        |  |             |   |           |             |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| <p>Web: Create a bridge over multiple interfaces<br/>UCI: network[..x..].typeOpt: type</p> | <p>Enables bridge between two interfaces.</p> <table border="1"> <tbody> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </tbody> </table>   | 0      | Disabled.   | 1      | Enabled.   |             |   |           |             |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| 0  | Disabled.   |        |             |        |  |             |   |           |             |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| 1  | Enabled.  |        |             |        |  |             |   |           |             |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| <p>Web: Cover the following interface<br/>UCI: network[..x..].ifname<br/>Opt: ifname</p>   | <p>Selects interfaces for bridge connection.</p>  |        |             |        |  |             |   |           |             |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |

**Table 101: Information table for the create interface page**

Click **Submit**. The Common Configuration page appears.

The screenshot shows the 'Common Configuration' page for a 3G interface. The 'Advanced Settings' tab is selected. The interface configuration includes:

- Status: 3g-3g\_s2\_voda
- RX: 0.00 B (0 Pkts.)
- TX: 0.00 B (0 Pkts.)
- Protocol: UMTS/GPRS/EV-DO
- Service Type: UMTS/GPRS
- SIM: 1
- APN: internet
- PIN: (empty)
- PAP/CHAP username: internet
- PAP/CHAP password: (masked)

At the bottom of the page, there are four buttons: 'Back to Overview', 'Save & Apply', 'Save', and 'Reset'.

**Figure 153: The common configuration page**

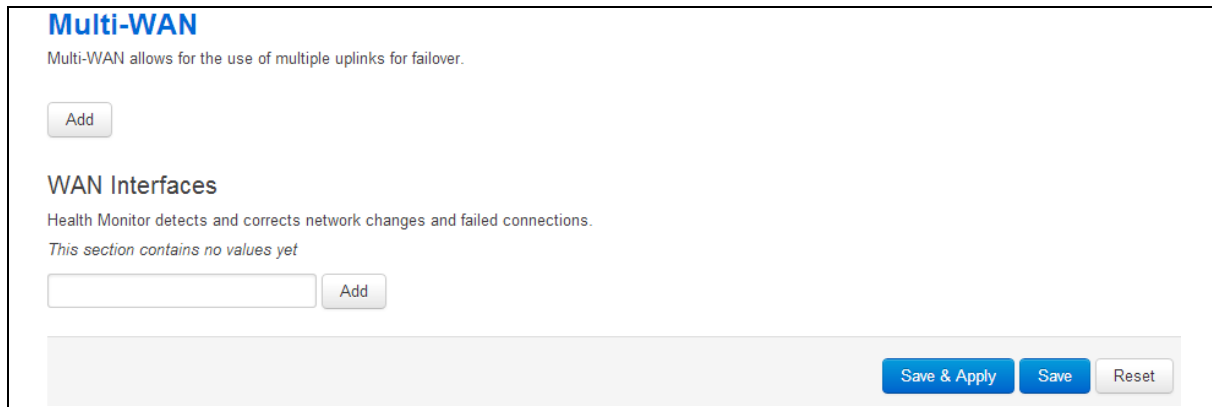
| Web Field/UCI/Package Option  | Description   |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
|---|---|-----------|--|----------|--|-------------|--|-----------|--|------------------------|-------------------------------|----------------|------------------------|-----|--------------------------------|-----|--|------|------------------------------|-----|--------------------------|-------|--|---------|-----------------------------------|---------------------|---|
| Web: Protocol<br>UCI: network.[..x..].proto<br>Opt: proto           | Protocol type. Select <b>LTE/UMTS/GPRS/EV-DO</b> . <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Static</td> <td>Static configuration with fixed address and netmask.</td> </tr> <tr> <td>DHCP Client</td> <td>Address and netmask are assigned by DHCP.</td> </tr> <tr> <td>Unmanaged</td> <td>Unspecified</td> </tr> <tr> <td>IPv6-in-IPv4 (RFC4213)</td> <td>IPv4 tunnels that carry IPv6.</td> </tr> <tr> <td>IPv6 over IPv4</td> <td>IPv6 over IPv4 tunnel.</td> </tr> <tr> <td>GRE</td> <td>Generic Routing Encapsulation.</td> </tr> <tr> <td>IOT</td> <td></td> </tr> <tr> <td>L2TP</td> <td>Layer 2 Tunnelling Protocol.</td> </tr> <tr> <td>PPP</td> <td>Point to Point Protocol.</td> </tr> <tr> <td>PPPoE</td> <td>Point to Point Protocol over Ethernet.</td> </tr> <tr> <td>PPPoATM</td> <td>Point to Point Protocol over ATM.</td> </tr> <tr> <td>LTE/UMTS/GPRS/EV-DO</td> <td>CDMA, UMTS or GPRS connection using an AT-style 3G modem.</td> </tr> </tbody> </table> | Option    | Description  | Static   | Static configuration with fixed address and netmask. | DHCP Client | Address and netmask are assigned by DHCP.          | Unmanaged | Unspecified  | IPv6-in-IPv4 (RFC4213) | IPv4 tunnels that carry IPv6. | IPv6 over IPv4 | IPv6 over IPv4 tunnel. | GRE | Generic Routing Encapsulation. | IOT |  | L2TP | Layer 2 Tunnelling Protocol. | PPP | Point to Point Protocol. | PPPoE | Point to Point Protocol over Ethernet. | PPPoATM | Point to Point Protocol over ATM. | LTE/UMTS/GPRS/EV-DO | CDMA, UMTS or GPRS connection using an AT-style 3G modem. |
| Option  | Description   |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| Static  | Static configuration with fixed address and netmask.  |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| DHCP Client   | Address and netmask are assigned by DHCP.   |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| Unmanaged   | Unspecified   |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| IPv6-in-IPv4 (RFC4213)  | IPv4 tunnels that carry IPv6.   |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| IPv6 over IPv4  | IPv6 over IPv4 tunnel.  |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| GRE   | Generic Routing Encapsulation.  |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| IOT   |   |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| L2TP  | Layer 2 Tunnelling Protocol.  |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| PPP   | Point to Point Protocol.  |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| PPPoE   | Point to Point Protocol over Ethernet.  |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| PPPoATM   | Point to Point Protocol over ATM.   |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| LTE/UMTS/GPRS/EV-DO   | CDMA, UMTS or GPRS connection using an AT-style 3G modem.   |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| Web: Service Type<br>UCI: network.[..x..].service<br>Opt: service   | Service type that will be used to connect to the network. <table border="1"> <tbody> <tr> <td>gprs_only</td> <td>Allows GSM module to only connect to GPRS network.</td> </tr> <tr> <td>lte_only</td> <td>Allows GSM module to only connect to LTE network.</td> </tr> <tr> <td>cdma</td> <td>Allows GSM module to only connect to CDMA network.</td> </tr> <tr> <td>auto</td> <td>GSM module will automatically detect the best available technology code.</td> </tr> </tbody> </table>  | gprs_only | Allows GSM module to only connect to GPRS network. | lte_only | Allows GSM module to only connect to LTE network.    | cdma        | Allows GSM module to only connect to CDMA network. | auto      | GSM module will automatically detect the best available technology code. |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| gprs_only   | Allows GSM module to only connect to GPRS network.  |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| lte_only  | Allows GSM module to only connect to LTE network.   |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| cdma  | Allows GSM module to only connect to CDMA network.  |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| auto  | GSM module will automatically detect the best available technology code.  |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| Web: SIM<br>UCI: network.[..x..].sim<br>Opt: sim                    | Select <b>SIM 1</b> or <b>SIM 2</b> . <table border="1"> <tbody> <tr> <td>auto</td> <td>Automatically detects which SIM slot is used.</td> </tr> <tr> <td>SIM 1</td> <td>Selects SIM from slot 1.</td> </tr> <tr> <td>SIM 2</td> <td>Selects SIM from slot 2.</td> </tr> </tbody> </table>  | auto      | Automatically detects which SIM slot is used.      | SIM 1    | Selects SIM from slot 1.                             | SIM 2       | Selects SIM from slot 2.                           |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| auto  | Automatically detects which SIM slot is used.   |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| SIM 1   | Selects SIM from slot 1.  |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| SIM 2   | Selects SIM from slot 2.  |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| Web: APN<br>UCI: network.[..x..].apn<br>Opt: apn                    | APN name of Mobile Network Operator.  |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| Web: APN username<br>UCI: network.[..x..].username<br>Opt: username | Username used to connect to APN.  |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| Web: APN password<br>UCI: network.[..x..].password<br>Opt: password | Password used to connect to APN.  |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |
| Web: Modem Configuration<br>UCI: N/A<br>Opt: N/A                    | Click the link if you need to configure additional options from Mobile Manager.   |           |  |          |  |             |  |           |  |                        |                               |                |                        |     |                                |     |  |      |                              |     |                          |       |  |         |                                   |                     |   |

**Table 102: Information table for the general set up section**

Click **Save & Apply**.

### 27.2.1.4 Set multi-WAN options for primary predefined interface

On the web interface go to **Network -> Multi-Wan**. The Multi-WAN page appears.



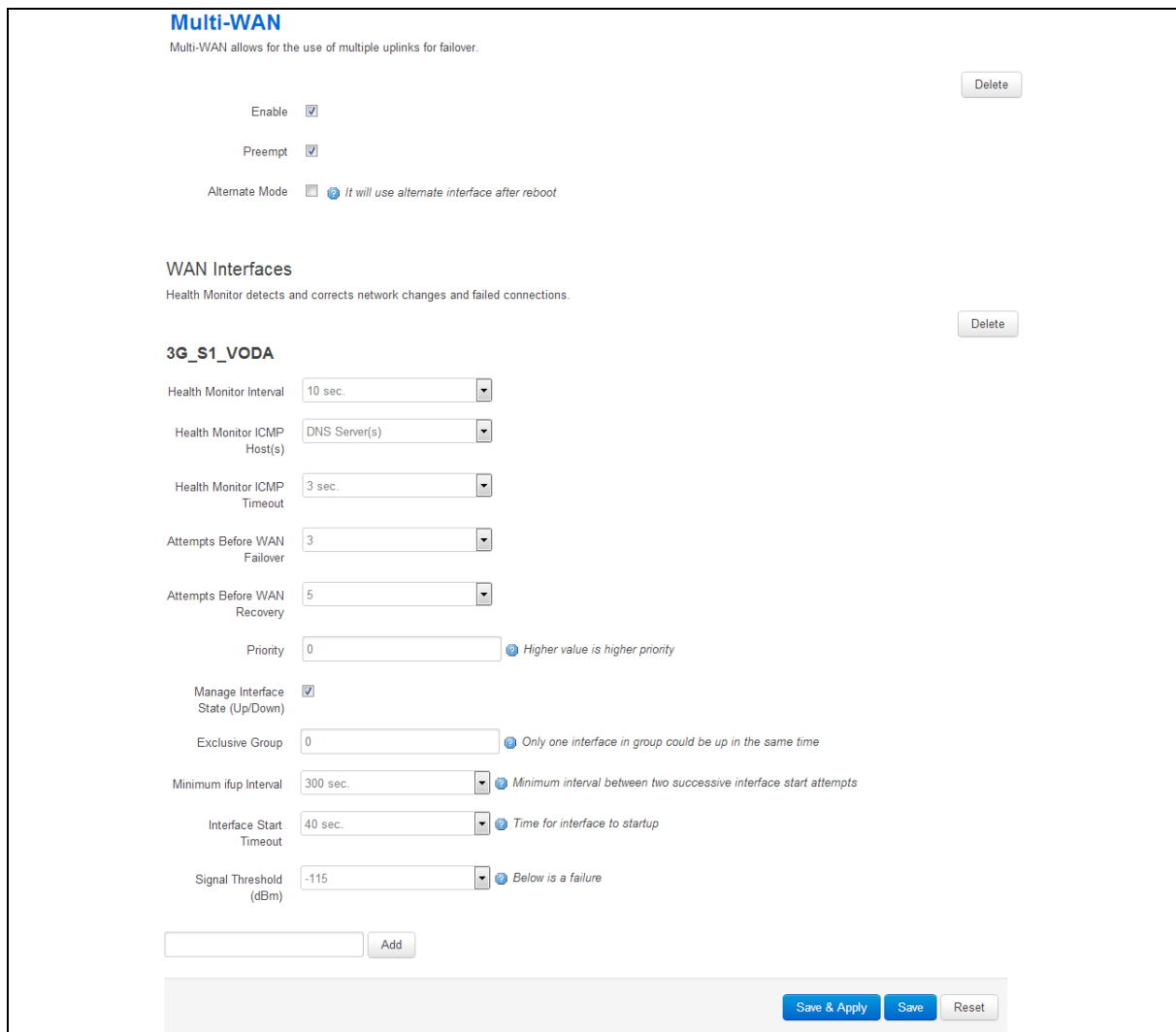
**Multi-WAN**  
Multi-WAN allows for the use of multiple uplinks for failover.

**WAN Interfaces**  
Health Monitor detects and corrects network changes and failed connections.  
*This section contains no values yet*

**Figure 154: The multi-WAN page**

In the WAN Interfaces section, type in the name of the Multi-WAN interface.

Click **Add**. The Multi-WAN page appears.



**Multi-WAN**  
Multi-WAN allows for the use of multiple uplinks for failover.

Enable

Preempt

Alternate Mode   It will use alternate interface after reboot

**WAN Interfaces**  
Health Monitor detects and corrects network changes and failed connections.

**3G\_S1\_VODA**

Health Monitor Interval

Health Monitor ICMP Host(s)

Health Monitor ICMP Timeout

Attempts Before WAN Failover

Attempts Before WAN Recovery

Priority   Higher value is higher priority

Manage Interface State (Up/Down)

Exclusive Group   Only one interface in group could be up in the same time

Minimum ifup Interval   Minimum interval between two successive interface start attempts

Interface Start Timeout   Time for interface to startup

Signal Threshold (dBm)   Below is a failure

**Figure 155: The multi-WAN page**



| Web Field/UCI/Package Option   | Description   |         |   |             |                                |             |   |        |                                |
|--|---|---------|---|-------------|--------------------------------|-------------|---|--------|--------------------------------|
| Web: Enable<br>UCI: multiwan.config.enabled<br>Opt: enabled  | Enables multiwan.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0       | Disabled.   | 1           | Enabled.                       |             |   |        |                                |
| 0  | Disabled.   |         |   |             |                                |             |   |        |                                |
| 1  | Enabled.  |         |   |             |                                |             |   |        |                                |
| Web: Preempt<br>UCI: multiwan.config.preempt<br>Opt: preempt   | Enables or disables pre-emption for multiwan. If enabled, the router will keep trying to connect to a higher priority interface depending on timer set.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0       | Disabled.   | 1           | Enabled.                       |             |   |        |                                |
| 0  | Disabled.   |         |   |             |                                |             |   |        |                                |
| 1  | Enabled.  |         |   |             |                                |             |   |        |                                |
| Web: Alternate Mode<br>UCI: multiwan.config.alt<br>Opt: alt  | Enables or disables alternate mode for multiwan. If enabled, the router will use an alternate interface after reboot.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0       | Disabled.   | 1           | Enabled.                       |             |   |        |                                |
| 0  | Disabled.   |         |   |             |                                |             |   |        |                                |
| 1  | Enabled.  |         |   |             |                                |             |   |        |                                |
| Web: WAN Interfaces<br>UCI: multiwan.3g_s<sim-number>_<short-operator-name><br>Opt: 3g_s<sim-number>_<short-operator-name> | Provide the same interface name as chosen in multiwan section below and click <b>Add</b> .  |         |   |             |                                |             |   |        |                                |
| Web: Health Monitor Interval<br>UCI: multiwan[..x..].health_interval<br>Opt: health_interval                               | Sets the period to check the health status of the interface. The Health Monitor interval will be used for: <ul style="list-style-type: none"> <li>• Interface state checks</li> <li>• Ping interval</li> <li>• Signal strength checks</li> </ul>  |         |   |             |                                |             |   |        |                                |
| Web: Health Monitor ICMP Host(s)<br>UCI: multiwan[..x..].icmp_hosts<br>Opt: icmp_hosts                                     | Specifies the target IP address for ICMP packets.<br><table border="1"> <tr> <td>Disable</td> <td>Disables the option.</td> </tr> <tr> <td>DNS servers</td> <td>DNS IP addresses will be used.</td> </tr> <tr> <td>WAN Gateway</td> <td>Gateway IP address will be used.</td> </tr> <tr> <td>custom</td> <td>Ability to provide IP address.</td> </tr> </table>   | Disable | Disables the option.  | DNS servers | DNS IP addresses will be used. | WAN Gateway | Gateway IP address will be used.                                | custom | Ability to provide IP address. |
| Disable  | Disables the option.  |         |   |             |                                |             |   |        |                                |
| DNS servers  | DNS IP addresses will be used.  |         |   |             |                                |             |   |        |                                |
| WAN Gateway  | Gateway IP address will be used.  |         |   |             |                                |             |   |        |                                |
| custom   | Ability to provide IP address.  |         |   |             |                                |             |   |        |                                |
| Web: Health Monitor Contrack Test Host(s)<br>UCI: multiwan.wan.contrack_hosts<br>Opt: contrack_hosts                       | Contrack is the feature used to track if there is any traffic to and from an IP destination within the health interval.<br>Contrack_hosts option defines the IP for contrack to track – usually the icmp_host IP is used.<br>If traffic to the contrack_hosts IP is detected then multiwan does not send a ping health check to the icmp_host otherwise a ping is sent as normal to the icmp_host.<br>By default the contrack_hosts is checked if the health interval is greater than 5 minutes. This time threshold currently cannot be manipulated.<br>Contrack is generally used to limit the traffic sent on a GSM network.<br><table border="1"> <tr> <td>Default</td> <td>Contrack checks for traffic from icmp_host IP when health_interval is greater than 5 minutes.</td> </tr> <tr> <td>Disable</td> <td>Contrack disabled.</td> </tr> <tr> <td>Custom</td> <td>Specifies an IP other than the icmp_host for contrack to track.</td> </tr> </table> | Default | Contrack checks for traffic from icmp_host IP when health_interval is greater than 5 minutes. | Disable     | Contrack disabled.             | Custom      | Specifies an IP other than the icmp_host for contrack to track. |        |                                |
| Default  | Contrack checks for traffic from icmp_host IP when health_interval is greater than 5 minutes.   |         |   |             |                                |             |   |        |                                |
| Disable  | Contrack disabled.  |         |   |             |                                |             |   |        |                                |
| Custom   | Specifies an IP other than the icmp_host for contrack to track.   |         |   |             |                                |             |   |        |                                |
| Web: Health Monitor ICMP Timeout<br>UCI: multiwan[..x..].timeout<br>Opt: timeout   | Sets ping timeout in seconds. Choose the time in seconds that the health monitor ICMP will timeout at.<br><table border="1"> <tr> <td>3</td> <td>Wait 3 seconds for ping reply.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 3       | Wait 3 seconds for ping reply.  | Range       |                                |             |   |        |                                |
| 3  | Wait 3 seconds for ping reply.  |         |   |             |                                |             |   |        |                                |
| Range  |   |         |   |             |                                |             |   |        |                                |
| Web: Health Monitor ICMP Interval<br>UCI: multiwan.wan.icmp_interval<br>Opt: icmp_interval                                 | Defines the interval between multiple pings sent at each health check.<br><table border="1"> <tr> <td>1</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 1       |   | Range       |                                |             |   |        |                                |
| 1  |   |         |   |             |                                |             |   |        |                                |
| Range  |   |         |   |             |                                |             |   |        |                                |
| Web: Health Monitor ICMP Count<br>UCI: multiwan.wan.icmp_count<br>Opt: icmp_count  | Defines the number of pings to send at each health check.<br><table border="1"> <tr> <td>1</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 1       |   | Range       |                                |             |   |        |                                |
| 1  |   |         |   |             |                                |             |   |        |                                |
| Range  |   |         |   |             |                                |             |   |        |                                |

|   |   |      |            |       |                 |
|---|---|------|------------|-------|-----------------|
| <p>Web: Attempts Before WAN Failover<br/>UCI: multiwan.[..x..].health_fail_retries<br/>Opt: health_fail_retries</p>         | <p>Sets the amount of health monitor retries before the interface is considered a failure.</p> <table border="1"> <tr> <td>3</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 3    |            | Range |                 |
| 3   |   |      |            |       |                 |
| Range   |   |      |            |       |                 |
| <p>Web: Attempts Before WAN Recovery<br/>UCI: multiwan.[..x..].health_recovery_retries<br/>Opt: health_recovery_retries</p> | <p>Sets the number of health monitor checks before the interface is considered healthy. Only relevant if pre-empt mode is enabled.</p> <table border="1"> <tr> <td>5</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 5    |            | Range |                 |
| 5   |   |      |            |       |                 |
| Range   |   |      |            |       |                 |
| <p>Web: Priority<br/>UCI: multiwan.[..x..].priority<br/>Opt: priority</p>   | <p>Specifies the priority of the interface. The higher the value, the higher the priority.</p> <p>This multiwan interface priority must be higher than the one specified in the priority field in the 'Roaming Interface Template' page described in the following section.</p> <table border="1"> <tr> <td>0</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table> | 0    |            | Range |                 |
| 0   |   |      |            |       |                 |
| Range   |   |      |            |       |                 |
| <p>Web: Exclusive Group<br/>UCI: multiwan.[..x..].exclusive_group<br/>Opt: exclusive_group</p>                              | <p>Defines the group to which the interface belongs; only one interface can be active.</p> <table border="1"> <tr> <td>0</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 0    |            | Range |                 |
| 0   |   |      |            |       |                 |
| Range   |   |      |            |       |                 |
| <p>Web: Manage Interface State (Up/Down)<br/>UCI: multiwan.[..x..].manage_state<br/>Opt: manage_state</p>                   | <p>Defines whether multiwan will start and stop the interface.</p> <p>Select <b>Enabled</b>.</p> <table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0    | Disabled.  | 1     | Enabled.        |
| 0   | Disabled.   |      |            |       |                 |
| 1   | Enabled.  |      |            |       |                 |
| <p>Web: Minimum ifup Interval<br/>UCI: multiwan.[..x..].ifup_retry_sec<br/>Opt: ifup_retry_sec</p>                          | <p>Specifies the interval in seconds before retrying the primary interface when pre-empt mode is enabled.</p>   |      |            |       |                 |
| <p>Web: Interface Start Timeout<br/>UCI: multiwan.[..x..].ifup_timeout<br/>Opt: ifup_timeout</p>                            | <p>Specifies the time in seconds for interface to start up. If it is not up after this period, it will be considered a fail.</p> <p>Choose timer greater than 120 seconds.</p> <table border="1"> <tr> <td>40</td> <td>40 seconds</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 40   | 40 seconds | Range |                 |
| 40  | 40 seconds  |      |            |       |                 |
| Range   |   |      |            |       |                 |
| <p>Web: Signal Threshold (dBm)<br/>UCI: multiwan.[..x..].signal_threshold<br/>Opt: signal_threshold</p>                     | <p>Specifies the minimum signal strength in dBm before considering if the interface fails signal health check. Uses the value stored for sig_dbm in mobile diagnostics.</p> <table border="1"> <tr> <td>-115</td> <td>Disabled.</td> </tr> <tr> <td>Range</td> <td>-46 to -115 dBm</td> </tr> </table>  | -115 | Disabled.  | Range | -46 to -115 dBm |
| -115  | Disabled.   |      |            |       |                 |
| Range   | -46 to -115 dBm   |      |            |       |                 |
| <p>Web: RSCP Threshold (dBm)<br/>UCI: multiwan.[..x..].rscp_threshold<br/>Opt: rscp_threshold</p>                           | <p>Specifies the minimum RSCP signal strength in dBm before considering if the interface fails signal health check. Uses the value stored for rscp_dbm in mobile diagnostics.</p> <table border="1"> <tr> <td>-115</td> <td>Disabled.</td> </tr> <tr> <td>Range</td> <td>-46 to -115 dBm</td> </tr> </table>  | -115 | Disabled.  | Range | -46 to -115 dBm |
| -115  | Disabled.   |      |            |       |                 |
| Range   | -46 to -115 dBm   |      |            |       |                 |
| <p>Web: ECIO Threshold (dB)<br/>UCI: multiwan.[..x..].ecio_threshold<br/>Opt: ecio_threshold</p>                            | <p>Specifies the minimum ECIO signal strength in dB before considering if the interface fails signal health check. Uses the value stored for ecio_db in mobile diagnostics.</p> <table border="1"> <tr> <td>-115</td> <td>Disabled.</td> </tr> <tr> <td>Range</td> <td>-46 to -115 dB</td> </tr> </table>   | -115 | Disabled.  | Range | -46 to -115 dB  |
| -115  | Disabled.   |      |            |       |                 |
| Range   | -46 to -115 dB  |      |            |       |                 |

|  |   |   |     |   |             |   |       |   |             |   |               |   |               |   |                         |   |         |
|--|---|---|-----|---|-------------|---|-------|---|-------------|---|---------------|---|---------------|---|-------------------------|---|---------|
| <p>Web: Signal Test<br/>         UCI: multiwan.[...].signal_test<br/>         Opt: signal_test</p> | <p>Defines script to test various signal characteristics in multiwan signal test. For example:<br/> <pre>option signal_test '(tech == 0) then (sig_dbm &gt; -70) else (rscp_dbm &gt; -105 and ecio_db &gt; -15)'</pre>         This states that when technology is GSM a health fail is determined when signal strength is less than -70dBm. When technology is not GSM a health fail occurs when either rscp_dbm falls below -105dBm or ecio_db falls below -15dB.</p> <p>Tech values are:</p> <table border="1"> <tr><td>0</td><td>GSM</td></tr> <tr><td>1</td><td>GSM Compact</td></tr> <tr><td>2</td><td>UTRAN</td></tr> <tr><td>3</td><td>GSM w/EGPRS</td></tr> <tr><td>4</td><td>UTRAN w/HSPDA</td></tr> <tr><td>5</td><td>UTRAN w/HSUPA</td></tr> <tr><td>6</td><td>UTRAN w/HSUPA and HSDPA</td></tr> <tr><td>7</td><td>E-UTRAN</td></tr> </table> | 0 | GSM | 1 | GSM Compact | 2 | UTRAN | 3 | GSM w/EGPRS | 4 | UTRAN w/HSPDA | 5 | UTRAN w/HSUPA | 6 | UTRAN w/HSUPA and HSDPA | 7 | E-UTRAN |
| 0  | GSM   |   |     |   |             |   |       |   |             |   |               |   |               |   |                         |   |         |
| 1  | GSM Compact   |   |     |   |             |   |       |   |             |   |               |   |               |   |                         |   |         |
| 2  | UTRAN   |   |     |   |             |   |       |   |             |   |               |   |               |   |                         |   |         |
| 3  | GSM w/EGPRS   |   |     |   |             |   |       |   |             |   |               |   |               |   |                         |   |         |
| 4  | UTRAN w/HSPDA   |   |     |   |             |   |       |   |             |   |               |   |               |   |                         |   |         |
| 5  | UTRAN w/HSUPA   |   |     |   |             |   |       |   |             |   |               |   |               |   |                         |   |         |
| 6  | UTRAN w/HSUPA and HSDPA   |   |     |   |             |   |       |   |             |   |               |   |               |   |                         |   |         |
| 7  | E-UTRAN   |   |     |   |             |   |       |   |             |   |               |   |               |   |                         |   |         |

**Table 103: Information table for multi-WAN page**

Click **Save**.

## 27.2.2 Set options for automatically created interfaces (failover)

From the top menu on the web interface page, select **Services -> Mobile Manager**. The Mobile Manager page appears.

There are four sections in the mobile manager page:

| Section   | Description  |
|---|--|
| Basic settings                                    | Enable SMS, configure SIM pin code, select roaming SIM, collect ICCIDs and set IMSI. |
| Advanced  | Configure advanced options such as collect ICCIDs and temperature polling interval.  |
| CDMA*   | CDMA configuration   |
| Callers   | Configure callers that can use SMS.  |
| Roaming Interface Template                        | Configure Preferred Roaming List options.  |
| *Option available only for Telit CE910-SL module. |  |

## 27.2.3 Mobile manager: basic settings

Figure 156: The mobile manager basic page

| Web Field/UCI/Package Option  | Description  |       |           |       |                               |
|---|--|-------|-----------|-------|-------------------------------|
| Web: SMS Enable<br>UCI: mobile.main.sms<br>Opt: sms                               | Enables or disables SMS functionality.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0     | Disabled. | 1     | Enabled.                      |
| 0   | Disabled.  |       |           |       |                               |
| 1   | Enabled.   |       |           |       |                               |
| Web: PIN code for SIM1<br>UCI: mobile.main.sim1pin<br>Opt: sim1pin                | Depending on the SIM card specifies the pin code for SIM 1.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>Depends on the SIM provider.</td> </tr> </table>   | Blank |           | Range | Depends on the SIM provider.  |
| Blank   |  |       |           |       |                               |
| Range   | Depends on the SIM provider.   |       |           |       |                               |
| Web: PIN code for SIM2<br>UCI: mobile.main.sim2pin<br>Opt: sim2pin                | Depending on the SIM card specify the pin code for SIM 2.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>Depends on the SIM provider.</td> </tr> </table>   | Blank |           | Range | Depends on the SIM provider.  |
| Blank   |  |       |           |       |                               |
| Range   | Depends on the SIM provider.   |       |           |       |                               |
| Web: LTE bands for SIM1<br>UCI: mobile.main.sim1_lte_bands<br>Opt: sim1_lte_bands | Depending on the SIM card specify the LTE bands for SIM 1. Comma delimiter. Example:<br><pre>option sim1_lte_bands '3,20'</pre> Limits LTE bands to 3 and 20.<br><b>Note:</b> currently only supported by Hucom/Wetelcom, SIMCom7100, Cellient MPL200 and Asiatel.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>LTE bands range from 1 to 70.</td> </tr> </table>   | Blank |           | Range | LTE bands range from 1 to 70. |
| Blank   |  |       |           |       |                               |
| Range   | LTE bands range from 1 to 70.  |       |           |       |                               |
| Web: LTE bands for SIM2<br>UCI: mobile.main.sim2_lte_bands<br>Opt:sim2_lte_bands  | Depending on the SIM card specifies the LTE bands for SIM 2. Comma delimiter. Example:<br><pre>option sim1_lte_bands '3,20'</pre> Limits LTE bands to 3 and 20.<br><b>Note:</b> currently only supported by Hucom/Wetelcom, SIMCom7100, Cellient MPL200 and Asiatel.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>LTE bands range from 1 to 70.</td> </tr> </table> | Blank |           | Range | LTE bands range from 1 to 70. |
| Blank   |  |       |           |       |                               |
| Range   | LTE bands range from 1 to 70.  |       |           |       |                               |

Table 104: Information table for mobile manager basic settings

## 27.2.4 Mobile manager: advanced settings

**MAIN**

Basic   **Advanced**   CDMA

---

Collect ICCIDs  [Collect ICCIDs on startup](#)

Force Mode  [Select network interface mode](#)

Temperature Polling Interval (Seconds)

Automatic Firmware Selection  [Select firmware based on network operator - only supported on some radio modules](#)

Allow USB Power Cycle  [Power cycle usb bus if modem disappeared from the USB bus for more then 40 seconds](#)

**Figure 157: The mobile manager advanced page**

| Web Field/UCI/Package Option   | Description  |           |                                     |       |                  |
|--|--|-----------|-------------------------------------|-------|------------------|
| Web: Collect ICCIDs<br>UCI: mobile.main.init_get_iccids<br>Opt: init_get_iccids  | Enables or disables integrated circuit card identifier ICCID's collection functionality. If enabled then both SIM 1 and SIM 2 ICCIDs will be collected otherwise it will default to SIM 1. This will be displayed under mobile stats. <table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0         | Disabled.                           | 1     | Enabled.         |
| 0  | Disabled.  |           |                                     |       |                  |
| 1  | Enabled.   |           |                                     |       |                  |
| Web: Force Mode<br>UCI: mobile.main.force_mode<br>Opt: force_mode  | Defines whether to operate mobile modem in PPP or Ethernet mode. The mode will be dependent on the service provided by the mobile provider. In general, this is Ethernet mode (default). <table border="1" style="width: 100%;"> <tr> <td>Automatic</td> <td>Ethernet mode (option not present).</td> </tr> <tr> <td>PPP</td> <td>Enable PPP mode.</td> </tr> </table>   | Automatic | Ethernet mode (option not present). | PPP   | Enable PPP mode. |
| Automatic  | Ethernet mode (option not present).  |           |                                     |       |                  |
| PPP  | Enable PPP mode.   |           |                                     |       |                  |
| Web: Temperature Polling Interval<br>UCI: mobile.main.temp_poll_interval_sec<br>Opt: temp_poll_interval_sec            | Defines the time in seconds to poll the mobile module for temperature. Set to <b>0</b> to disable. <table border="1" style="width: 100%;"> <tr> <td>61</td> <td>61 seconds.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 61        | 61 seconds.                         | Range |                  |
| 61   | 61 seconds.  |           |                                     |       |                  |
| Range  |  |           |                                     |       |                  |
| Web: Automatic Firmware Selection<br>UCI:<br>mobile.main.enable_firmware_autoselect<br>Opt: enable_firmware_autoselect | Defines whether to use time obtained from the mobile carrier to update the system clock when NTP is enabled. <table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0         | Disabled.                           | 1     | Enabled.         |
| 0  | Disabled.  |           |                                     |       |                  |
| 1  | Enabled.   |           |                                     |       |                  |
| Web: Allow USB Power Cycle<br>UCI: mobile.main.allow_usb_powercycle<br>Opt: allow_usb_powercycle                       | Enables the selection of an operator-specific firmware in the radio module. The selection is based on the ICCID of the used SIM. At module initialisation the IMSI is checked and if necessary the correct firmware image in the module will be activated. <p><b>Note:</b> activation of the firmware will lead to delayed startup of the network interface associated with the radio module.</p> <p><b>Note:</b> this feature is currently only supported for the Telit LE910NA V2 module. Here a Verizon-specific firmware will be selected if the ICCID starts with "891480".</p> <table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0         | Disabled.                           | 1     | Enabled.         |
| 0  | Disabled.  |           |                                     |       |                  |
| 1  | Enabled.   |           |                                     |       |                  |
| Web: n/a<br>UCI: mobile.main.disable_time<br>Opt: disable_time   | Defines whether to use time obtained from the mobile carrier to update the system clock when NTP is enabled. <table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0         | Disabled.                           | 1     | Enabled.         |
| 0  | Disabled.  |           |                                     |       |                  |
| 1  | Enabled.   |           |                                     |       |                  |

**Table 105: Information table for mobile manager advanced settings**

## 27.2.5 Mobile manager: CDMA settings

This configuration page is only supported for the Telit CE910-SL CDMA module.

**MAIN**

Basic    Advanced    **CDMA**

---

IMSI  ⓘ *If specified over-writes IMSI stored in radio module*

HDR Auth User ID  ⓘ *AN-PPP user id. Supported on Cellient module only*

HDR Auth Password  ⓘ *AN-PPP password. Supported on Cellient module only*

Ordered Registration triggers module reboot

Station Class Mark

Slot Cycle Index

Slot Mode

Mobile Directory Number

MOB\_TERM\_HOME registration flag

MOB\_TERM\_FOR\_SID registration flag

MOB TERM FOR NID

**Figure 158: The mobile manager CDMA page**

| Web Field/UCI/Package Option  | Description  |         |                       |        |                               |
|---|--|---------|-----------------------|--------|-------------------------------|
| Web: IMSI<br>UCI: mobile.main.imsi<br>Opt: imsi   | Allows the IMSI (International Mobile Subscriber Identity) to be changed.<br><table border="1"> <tr> <td>Default</td> <td>Programmed in module.</td> </tr> <tr> <td>Digits</td> <td>Up to 15 digits.</td> </tr> </table> | Default | Programmed in module. | Digits | Up to 15 digits.              |
| Default   | Programmed in module.  |         |                       |        |                               |
| Digits  | Up to 15 digits.   |         |                       |        |                               |
| Web: HDR Auth User ID<br>UCI: mobile.main.hdr_userid<br>Opt: hdr_userid   | AN-PPP user ID. Supported on Cellient (CDMA) modem only.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>Depends on the CDMA provider.</td> </tr> </table>                             | Blank   |                       | Range  | Depends on the CDMA provider. |
| Blank   |  |         |                       |        |                               |
| Range   | Depends on the CDMA provider.  |         |                       |        |                               |
| Web: HDR Auth User Password<br>UCI: mobile.main.hdr_password<br>Opt: hdr_password   | AN-PPP password. Supported on Cellient (CDMA) modem only.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>Depends on the CDMA provider.</td> </tr> </table>                            | Blank   |                       | Range  | Depends on the CDMA provider. |
| Blank   |  |         |                       |        |                               |
| Range   | Depends on the CDMA provider.  |         |                       |        |                               |
| Web: Ordered Registration triggers module reboot<br>UCI: mobile.main.<br>mobile.main.cdma_ordered_registration_reboot_enabled<br>Opt:<br>cdma_ordered_registration_reboot_enabled | Enables or disables rebooting the module after an Order Registration command is received from a network.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0       | Disabled.             | 1      | Enabled.                      |
| 0   | Disabled.  |         |                       |        |                               |
| 1   | Enabled.   |         |                       |        |                               |

|  |   |
|--|---|
| Web: Station Class Mark<br>UCI: mobile.main.cdma_station_class_mark<br>Opt: cdma_station_class_mark  | Allows the station class mark for the MS to be changed.<br>58<br>0-255  |
| Web: Slot Cycle Index<br>UCI: mobile.main.cdma_slot_cycle_index<br>Opt: cdma_slot_cycle_index  | The desired slot cycle index if different from the default.<br>2<br>0-7   |
| Web: Slot Mode<br>UCI: mobile.main.cdma_slot_mode<br>Opt: cdma_slot_mode   | Specifies the slot mode.<br>0   |
| Web: Mobile Directory Number<br>UCI:<br>mobile.main.cdma_mobile_directory_number<br>Opt: cdma_mobile_directory_number                                      | Allows the mobile directory number (MDN) to be changed.<br>Default Programmed in module.<br>Digits Up to 15 digits. |
| Web: MOB_TERM_HOME registration flag<br>UCI: mobile.main.<br>cdma_mob_term_home_registration_flag<br>Opt:<br>cdma_mob_term_home_registration_flag          | The MOB_TERM_HOME registration flag.<br>0 Disabled.<br>1 Enabled.   |
| Web: MOB_TERM_FOR_SID registration flag<br>UCI: mobile.main.<br>cdma_mob_term_for_sid_registration_flag<br>Opt:<br>cdma_mob_term_for_sid_registration_flag | The MOB_TERM_FOR_SID registration flag.<br>0 Disabled.<br>1 Enabled.  |
| Web: MOB_TERM_FOR_NID registration flag<br>UCI: mobile.main.<br>cdma_mob_term_for_nid_registration_flag<br>Opt:<br>cdma_mob_term_for_nid_registration_flag | The MOB_TERM_FOR_NID registration flag<br>0 Disabled.<br>1 Enabled.   |
| Web: Access Overload Control<br>UCI:<br>mobile.main.cdma_access_overload_control<br>Opt: cdma_access_overload_control                                      | Allows the access overload class to be changed.<br>Default Programmed into module as part of IMSI.<br>Range 0-7     |
| Web: Preferred Serving System<br>UCI:<br>mobile.main.cdma_preferred_serving_system<br>Opt: cdma_preferred_serving_system                                   | The CDMA Preferred Serving System(A/B).<br>5  |
| Web: Digital Analog Mode Preference<br>UCI: cdma_digital_analog_mode_preference<br>Opt: cdma_digital_analog_mode_preference                                | Digital/Analog Mode Preference.<br>4  |
| Web: Primary Channel A<br>UCI: mobile.main.cdma_primary_channel_a<br>Opt: cdma_primary_channel_a.  | Allows the primary channel (A) to be changed.<br>283<br>1-2016 Any band class 5 channel number.                     |
| Web: Primary Channel B<br>UCI: mobile.main.cdma_primary_channel_b<br>Opt: cdma_primary_channel_b   | Allows the primary channel (B) to be changed.<br>384<br>1-2016 Any band class 5 channel number                      |
| Web: Secondary Channel A<br>UCI:<br>mobile.main.cdma_secondary_channel_a<br>Opt: cdma_secondary_channel_a  | Allows the secondary channel (A) to be changed.<br>691<br>1-2016 Any band class 5 channel number.                   |
| Web: Secondary Channel B<br>UCI:<br>mobile.main.cdma_secondary_channel_b<br>Opt: cdma_secondary_channel_b  | Allows the secondary channel (B) to be changed.<br>777<br>1-2016 Any band class 5 channel number.                   |

|  |   |
|--|---|
| Web: Preferred Forward & Reverse RC<br>UCI: mobile.main.cdma_preferred_forward_and_reverse_rc<br>Opt:cdma_preferred_forward_and_reverse_rc | The Preferred Forward & Reverse RC value, this takes the form "forward_rc,reverse_rc"<br>Format: forward radio channel, reverse radio channel<br>Default: 0,0 |
| Web: SID-NID pairs<br>UCI: mobile.main.cdma_sid_nid_pairs<br>Opt:cdma_sid_nid_pairs  | Allows specification of SID:NID pairs, this takes the form "SID1,NID1,SID2,NID2, ..."<br>Format: SID1 (0-65535),NID (0-65535)<br>Default: 0,65535             |

Table 106: Information table for mobile manager CDMA settings

## 27.2.6 Mobile manager: callers

**Callers**  
Configure caller numbers that may use the SMS service.

Name  Name of the caller.

Number  Number of the caller. Use \* for wildcard matching.

Enable

Respond

Figure 159: The mobile manager CDMA page

| Web Field/UCI/Package Option                                   | Description   |       |           |       |           |            |   |
|--|---|-------|-----------|-------|-----------|------------|---|
| Web: Name<br>UCI: mobile.@caller[0].name<br>Opt:name           | Name assigned to the caller.<br><table border="1"> <tr><td>Blank</td><td></td></tr> <tr><td>Range</td><td>No limit.</td></tr> </table>  | Blank |           | Range | No limit. |            |   |
| Blank  |   |       |           |       |           |            |   |
| Range  | No limit.   |       |           |       |           |            |   |
| Web: Number<br>UCI: mobile.@caller[0].number<br>Opt:number     | Number of the caller allowed to SMS the router. Add in specific caller numbers, or use the * wildcard symbol.<br><table border="1"> <tr><td>Blank</td><td></td></tr> <tr><td>Range</td><td>No limit.</td></tr> <tr><td>Characters</td><td>Global value (*) is accepted.<br/>International value (+) is accepted.</td></tr> </table> | Blank |           | Range | No limit. | Characters | Global value (*) is accepted.<br>International value (+) is accepted. |
| Blank  |   |       |           |       |           |            |   |
| Range  | No limit.   |       |           |       |           |            |   |
| Characters   | Global value (*) is accepted.<br>International value (+) is accepted.   |       |           |       |           |            |   |
| Web: Enable<br>UCI: mobile.@caller[0].enabled<br>Opt:enabled   | Enables or disables incoming caller ID.<br><table border="1"> <tr><td>0</td><td>Disabled.</td></tr> <tr><td>1</td><td>Enabled.</td></tr> </table>   | 0     | Disabled. | 1     | Enabled.  |            |   |
| 0  | Disabled.   |       |           |       |           |            |   |
| 1  | Enabled.  |       |           |       |           |            |   |
| Web: Respond<br>UCI: mobile.@caller[0].respond<br>Opt: respond | If checked, the router will return an SMS. Select <b>Respond</b> if you want the router to reply.<br><table border="1"> <tr><td>0</td><td>Disabled.</td></tr> <tr><td>1</td><td>Enabled.</td></tr> </table>   | 0     | Disabled. | 1     | Enabled.  |            |   |
| 0  | Disabled.   |       |           |       |           |            |   |
| 1  | Enabled.  |       |           |       |           |            |   |

Table 107: Information table for mobile manager callers settings



## 27.2.7 Roaming interface template

**Roaming Interface Template**  
Common config values for interfaces created by Automatic Operator Selection Delete

Interface Signal Sort   Sort interfaces by signal strength so those having better signal strength at the startup would be tried first

Roaming SIM  In which slot roaming sim-card is inserted

Firewall Zone  lan: lan:  lan1: lan1:  wlan: wlan:  wlan1: wlan1:

wan: wan:  unspecified -or- create:

Append all the generated interfaces to this zone

APN

PIN

PAP/CHAP username

PAP/CHAP password

Service Preference   
UMTS  
GPRS  
CDMA/EV-DO  
Auto Order of service preference for the generated interfaces (Use Control button to select multiple)

Health Monitor Interval

Health Monitor ICMP Host(s)

Health Monitor Contrack Test Host(s)

Health Monitor ICMP Timeout

Health Monitor ICMP Interval

Attempts Before WAN Failover

Attempts Before WAN Recovery

**Figure 160: The roaming interface template page**

| Web Field/UCI/Package Option   | Description  |   |             |   |             |
|--|--|---|-------------|---|-------------|
| Web: Interface Signal Sort<br>UCI: mobile.@roaming_template[0].sort_sig_strength<br>Opt: sort_sig_strength | Sorts interfaces by signal strength priority, so those that have a better signal strength will be tried first.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0 | Disabled.   | 1 | Enabled.    |
| 0  | Disabled.  |   |             |   |             |
| 1  | Enabled.   |   |             |   |             |
| Web: Roaming SIM<br>UCI: mobile.main.roaming_sim<br>Opt: roaming_sim                                       | Sets in which slot to insert roaming SIM card.<br><table border="1"> <tr> <td>1</td> <td>SIM slot 1.</td> </tr> <tr> <td>2</td> <td>SIM slot 2.</td> </tr> </table>  | 1 | SIM slot 1. | 2 | SIM slot 2. |
| 1  | SIM slot 1.  |   |             |   |             |
| 2  | SIM slot 2.  |   |             |   |             |
| Web: Firewall Zone<br>UCI: mobile.@roaming_template[0].firewall_zone<br>Opt: firewall_zone                 | Adds all generated interfaces to this zone. Select existing zone or click <b>unspecified</b> or <b>create</b> to create new zone.  |   |             |   |             |
| Web: APN<br>UCI: mobile.@roaming_template[0].apn<br>Opt: apn   | APN name of Mobile Network Operator.   |   |             |   |             |

| Web: PIN<br>UCI:<br>mobile.@roaming_template[0].pincode<br>Opt: pincode                                     | SIM card's PIN number.  |         |                                    |       |                    |                      |         |             |                                |     |             |                                  |         |        |  |  |
|---|---|---------|------------------------------------|-------|--------------------|----------------------|---------|-------------|--------------------------------|-----|-------------|----------------------------------|---------|--------|--|--|
| Web: PAP/CHAP username<br>UCI:<br>mobile.@roaming_template[0].username<br>Opt: username                     | Username used to connect to APN.  |         |                                    |       |                    |                      |         |             |                                |     |             |                                  |         |        |  |  |
| Web: PAP/CHAP password<br>UCI:<br>mobile.@roaming_template[0].password<br>Opt: password                     | Password used to connect to APN.  |         |                                    |       |                    |                      |         |             |                                |     |             |                                  |         |        |  |  |
| Web: Service Order<br>UCI:<br>mobile.@roaming_template[0].service_order<br>Opt: service_order               | Defines a space separated list of services, in preferred order. Valid options are <i>gprs</i> , <i>umts</i> , <i>lte</i> , <i>auto</i> .<br>If no valid <i>service_order</i> is defined, then the configured Service Type is used. Example:<br>mobile.@roaming_template[0].service_order="gprs umts lte auto"<br><table border="1"> <tr> <td>Blank</td> <td>Automatically detect best service.</td> </tr> <tr> <td>Range</td> <td>gprs umts lte auto</td> </tr> </table>  | Blank   | Automatically detect best service. | Range | gprs umts lte auto |                      |         |             |                                |     |             |                                  |         |        |  |  |
| Blank   | Automatically detect best service.  |         |                                    |       |                    |                      |         |             |                                |     |             |                                  |         |        |  |  |
| Range   | gprs umts lte auto  |         |                                    |       |                    |                      |         |             |                                |     |             |                                  |         |        |  |  |
| Web: Health Monitor Interval<br>UCI:<br>mobile.@roaming_template[0].health_interval<br>Opt: health_interval | Sets the period, in seconds, to check the health status of the interface. The Health Monitor interval will be used for:<br>Interface state checks<br>Ping interval<br>Signal strength checks<br><table border="1"> <tr> <td>10</td> <td>Health check every 10 seconds.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 10      | Health check every 10 seconds.     | Range |                    |                      |         |             |                                |     |             |                                  |         |        |  |  |
| 10  | Health check every 10 seconds.  |         |                                    |       |                    |                      |         |             |                                |     |             |                                  |         |        |  |  |
| Range   |   |         |                                    |       |                    |                      |         |             |                                |     |             |                                  |         |        |  |  |
| Web: Health Monitor ICMP Host(s)<br>UCI:<br>mobile.@roaming_template[0].icmp_hosts<br>Opt: icmp_hosts       | Specifies target IP address for ICMP packets.<br><table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Disable</td> <td>Disables the option.</td> <td>disable</td> </tr> <tr> <td>DNS servers</td> <td>DNS IP addresses will be used.</td> <td>dns</td> </tr> <tr> <td>WAN gateway</td> <td>Gateway IP address will be used.</td> <td>gateway</td> </tr> <tr> <td>custom</td> <td>Ability to provide IP address. Multiple pings targets can be entered, comma separated. Pings to both must fail for health check to fail. Example:<br/>option icmp_hosts '1.1.1.1,2.2.2.2'</td> <td></td> </tr> </tbody> </table> | Web     | Description                        | UCI   | Disable            | Disables the option. | disable | DNS servers | DNS IP addresses will be used. | dns | WAN gateway | Gateway IP address will be used. | gateway | custom | Ability to provide IP address. Multiple pings targets can be entered, comma separated. Pings to both must fail for health check to fail. Example:<br>option icmp_hosts '1.1.1.1,2.2.2.2' |  |
| Web   | Description   | UCI     |                                    |       |                    |                      |         |             |                                |     |             |                                  |         |        |  |  |
| Disable   | Disables the option.  | disable |                                    |       |                    |                      |         |             |                                |     |             |                                  |         |        |  |  |
| DNS servers   | DNS IP addresses will be used.  | dns     |                                    |       |                    |                      |         |             |                                |     |             |                                  |         |        |  |  |
| WAN gateway   | Gateway IP address will be used.  | gateway |                                    |       |                    |                      |         |             |                                |     |             |                                  |         |        |  |  |
| custom  | Ability to provide IP address. Multiple pings targets can be entered, comma separated. Pings to both must fail for health check to fail. Example:<br>option icmp_hosts '1.1.1.1,2.2.2.2'  |         |                                    |       |                    |                      |         |             |                                |     |             |                                  |         |        |  |  |

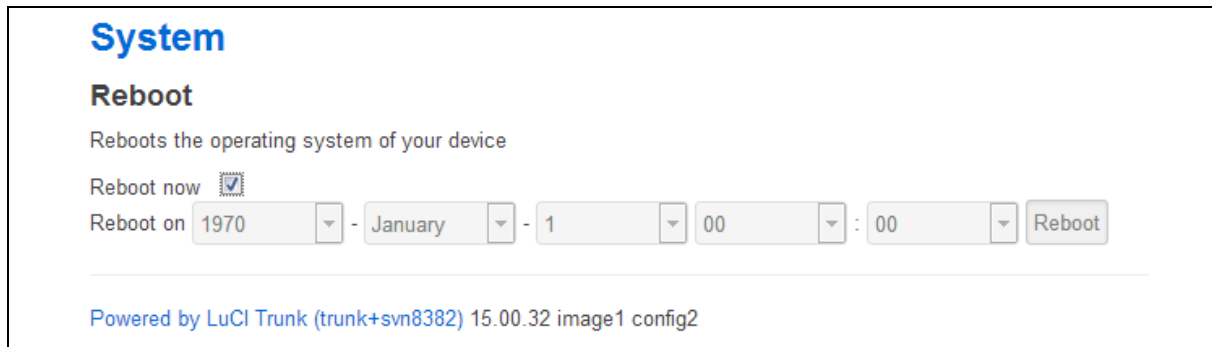
| <p>Web: Health Monitor Contrack Test Host(s)<br/>UCI: mobile.@roaming_template[0].contrack_hosts<br/>Opt: contrack_hosts</p>           | <p>Contrack is the feature used to track if there is any traffic to and from an IP destination within the health interval.<br/>The Contrack_hosts option defines the IP for contrack to track, usually the icmp_host IP is used.<br/>If traffic to the contrack_hosts IP is detected then multiwan does not send a ping health check to the icmp_host; otherwise a ping is sent as normal to the icmp_host.<br/>By default the contrack_hosts is checked if the health interval is greater than 5 minutes. This time threshold currently cannot be manipulated.<br/>Contrack is generally used to limit the traffic sent on a GSM network.</p> <table border="1" data-bbox="683 544 1393 813"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Default</td> <td>Contrack checks for traffic from icmp_host IP when health_interval is greater than 5 minutes.</td> <td></td> </tr> <tr> <td>Disable</td> <td>Contrack checks for traffic from icmp_host IP when health_interval is greater than 5 minutes.</td> <td>disable</td> </tr> <tr> <td>custom</td> <td>Specifies an IP other than the icmp_host for contrack to track.</td> <td></td> </tr> </tbody> </table> | Web     | Description                                | UCI   | Default | Contrack checks for traffic from icmp_host IP when health_interval is greater than 5 minutes. |  | Disable | Contrack checks for traffic from icmp_host IP when health_interval is greater than 5 minutes. | disable | custom | Specifies an IP other than the icmp_host for contrack to track. |  |
|--|--|---------|--|-------|---------|---|--|---------|---|---------|--------|---|--|
| Web  | Description  | UCI     |  |       |         |   |  |         |   |         |        |   |  |
| Default  | Contrack checks for traffic from icmp_host IP when health_interval is greater than 5 minutes.  |         |  |       |         |   |  |         |   |         |        |   |  |
| Disable  | Contrack checks for traffic from icmp_host IP when health_interval is greater than 5 minutes.  | disable |  |       |         |   |  |         |   |         |        |   |  |
| custom   | Specifies an IP other than the icmp_host for contrack to track.  |         |  |       |         |   |  |         |   |         |        |   |  |
| <p>Web: Health Monitor ICMP Timeout<br/>UCI: mobile.@roaming_template[0].timeout<br/>Opt: timeout</p>                                  | <p>Specifies the time in seconds that Health Monitor ICMP will timeout at.<br/>Sets ping timeout in seconds. Choose the time in seconds that the health monitor ICMP will timeout at.</p> <table border="1" data-bbox="683 936 1393 1003"> <tr> <td>3</td> <td>Wait 3 seconds for ping reply.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 3       | Wait 3 seconds for ping reply.             | Range |         |   |  |         |   |         |        |   |  |
| 3  | Wait 3 seconds for ping reply.   |         |  |       |         |   |  |         |   |         |        |   |  |
| Range  |  |         |  |       |         |   |  |         |   |         |        |   |  |
| <p>Web: Health Monitor ICMP Interval<br/>UCI: mobile.@roaming_template[0].interval<br/>Opt: icmp_interval</p>                          | <p>Defines the interval, in seconds, between multiple pings sent at each health check.</p> <table border="1" data-bbox="683 1070 1393 1137"> <tr> <td>1</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 1       |  | Range |         |   |  |         |   |         |        |   |  |
| 1  |  |         |  |       |         |   |  |         |   |         |        |   |  |
| Range  |  |         |  |       |         |   |  |         |   |         |        |   |  |
| <p>Web: Attempts Before WAN Failover<br/>UCI: mobile.@roaming_template[1].health_fail_retries<br/>Opt: health_fail_retries</p>         | <p>Defines the number of health check failures before interface is disconnected.</p> <table border="1" data-bbox="683 1205 1393 1294"> <tr> <td>3</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 3       |  | Range |         |   |  |         |   |         |        |   |  |
| 3  |  |         |  |       |         |   |  |         |   |         |        |   |  |
| Range  |  |         |  |       |         |   |  |         |   |         |        |   |  |
| <p>Web: Attempts Before WAN Recovery<br/>UCI: mobile.@roaming_template[0].health_recovery_retries<br/>Opt: health_recovery_retries</p> | <p>Sets the number of health check passes before the interface is considered healthy. This field is not used for a roaming template.</p> <table border="1" data-bbox="683 1361 1393 1451"> <tr> <td>5</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 5       |  | Range |         |   |  |         |   |         |        |   |  |
| 5  |  |         |  |       |         |   |  |         |   |         |        |   |  |
| Range  |  |         |  |       |         |   |  |         |   |         |        |   |  |
| <p>Web: Priority<br/>UCI: mobile.@roaming_template[0].priority<br/>Opt: priority</p>   | <p>Type the priority number. The higher the value, the higher the priority.<br/>This multi-WAN interface priority must be lower than the one specified in the priority field for the PMP interface.</p> <table border="1" data-bbox="683 1570 1393 1641"> <tr> <td>0</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 0       |  | Range |         |   |  |         |   |         |        |   |  |
| 0  |  |         |  |       |         |   |  |         |   |         |        |   |  |
| Range  |  |         |  |       |         |   |  |         |   |         |        |   |  |
| <p>Web: Minimum ifup interval<br/>UCI: multiwan.wan.ifup_retry_sec<br/>Opt: ifup_retry_sec</p>   | <p>Not used for a roaming interface.</p> <table border="1" data-bbox="683 1682 1393 1753"> <tr> <td>300</td> <td>Retry primary interface every 300 seconds.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 300     | Retry primary interface every 300 seconds. | Range |         |   |  |         |   |         |        |   |  |
| 300  | Retry primary interface every 300 seconds.   |         |  |       |         |   |  |         |   |         |        |   |  |
| Range  |  |         |  |       |         |   |  |         |   |         |        |   |  |
| <p>Web: Interface Start Timeout<br/>UCI: mobile.@roaming_template[0].ifup_timeout_sec<br/>Opt: ifup_timeout</p>                        | <p>Specifies the time in seconds for interface to start up. If it is not up after this period, it will be considered a fail.</p> <table border="1" data-bbox="683 1809 1393 1899"> <tr> <td>40</td> <td>40 seconds</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 40      | 40 seconds                                 | Range |         |   |  |         |   |         |        |   |  |
| 40   | 40 seconds   |         |  |       |         |   |  |         |   |         |        |   |  |
| Range  |  |         |  |       |         |   |  |         |   |         |        |   |  |

|  |  |                 |
|--|--|-----------------|
| Web: Signal Threshold (dBm)                              | Specifies the minimum RSCP signal strength in dBm before considering if the interface fails signal health check. Uses the value stored for rscp_dbm in mobile diagnostics. |                 |
| UCI:<br>mobile.@roaming_template[0].signal_thre<br>shold |  |                 |
| Opt: signal_threshold                                    |  |                 |
|  | Range  | -46 to -115 dBm |
|  |  | -115dBm         |

**Table 108: Information table for roaming interface template**

When you have configured your settings, click **Save & Apply**.

In the top menu, select **System -> Reboot**. The System page appears.



**Figure 161: The reboot page**

Check the **Reboot now** check box and then click **Reboot**.

## 27.2.8 Scenario 2: PMP + roaming: pre-empt disabled

As in the previous section, Multi-WAN connects the PMP interface and uses auto-created interfaces for failover.

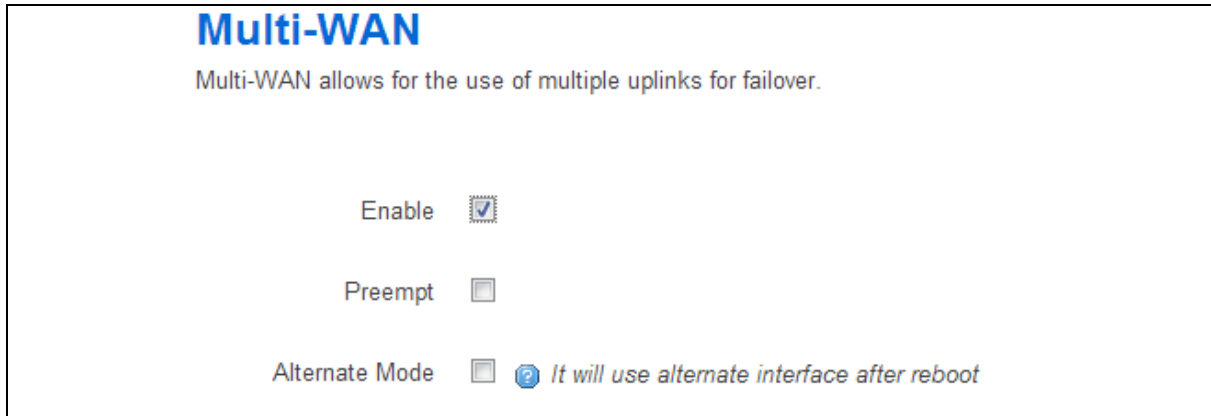
However, in this scenario, the auto-created interface will not be disconnected as soon as the `ifup_retry_sec` expires for the PMP interface. The primary interface will be reconnected when the current auto-created interface fails multiwan health checks after expiration of the `ifup_retry_sec` timer.

Follow the instructions in the section above for creation of the PMP interface, Multi-WAN and Mobile Manager roaming interfaces. The only change in configuration compared to the PMP + roaming: pre-empt enabled scenario is that you must disable the pre-empt option in the multi-WAN package.

### 27.2.8.1 Set multi-WAN options for pre-empt disabled

To disable PMP + roaming pre-empt, in the top menu, select **Network -> Multi-Wan**.

In the Multi-WAN page, ensure Preempt is not selected.



**Figure 162: The multi-wan page, pre-empt not selected**

Click **Save & Apply**.

In the top menu, select **System -> Reboot**. The System Reboot page appears.



**Figure 163: The system reboot page**

Check the **Reboot now** check box and then click **Reboot**.

### 27.2.9 Scenario 3: No PMP + roaming

In this scenario there is no PMP interface that can be used for a connection. The router scans the available mobile networks at boot and sorts the networks according to signal strength.

The network that offers the best signal strength will be the first to connect. Multi-WAN then controls the failover between the available networks.

Multi-WAN periodically does a health check on the interface. A health check comprises of a configurable combination of the following:

- Interface state
- Pings to an ICMP target
- Signal level checks using signal threshold, RSCP threshold and ECIO threshold option values

A fail for any of the above health checks results in a fail. After a configurable number of health check failures, Multi-WAN will disconnect the failed interface and attempt to connect to the next best roaming interface.

### 27.2.10 Set options for automatically created interfaces (failover)

In the top menu on the web interface page, select **Services -> Mobile Manager**. The Mobile Manager page appears.

There are three sections:

|                            |  |
|----------------------------|--|
| Basic settings             | Configure SMS, select roaming SIM and collect ICCIDs.                          |
| Callers                    | Configure callers that can use SMS.  |
| Roaming Interface Template | Configure common values for interface created by Automatic Operator Selection. |

#### 27.2.10.1 Basic settings

| Web Field/UCI/Package Option  | Description   |
|---|---|
| Web: SMS Enable<br>UCI: mobile.main.sms<br>Opt: sms                             | Enables SMS.<br>no Disabled.<br>yes Enabled.  |
| Web: Collect ICCIDs<br>UCI: mobile.main.init_get_iccids<br>Opt: init_get_iccids | Enables or disables integrated circuit card identifier ICCID's collection functionality. If enabled then both SIM 1 and SIM 2 ICCIDs will be collected otherwise it will default to SIM 1. This will be display under mobile stats.<br>no Disabled.<br>yes Enabled. |
| Web: PIN code for SIM1<br>UCI: mobile.main.sim2pin<br>Opt: sim2pin              | Depending on the SIM card specify the pin code for SIM 1.<br>Blank<br>range   |
| Web: PIN code for SIM2<br>UCI: mobile.main.sim2pin<br>Opt: sim2pin              | Depending on the SIM card specify the pin code for SIM 2.<br>Blank<br>Range   |
| Web: HDR Auto User ID<br>UCI: mobile.main.hdr_userid<br>Opt: hdr_userid         | AN-PPP user ID. Supported on Cellient (CDMA) modem only.<br>Blank<br>Range  |

**Table 109: Information table for mobile manager basic settings**

## 27.2.10.2 Caller settings

| Web Field/UCI/Package Option                                   | Description  |
|--|--|
| Web: Name<br>UCI: mobile.@caller[0].name<br>Opt: name          | Name assigned to the caller.<br>Blank<br>Range   |
| Web: Number<br>UCI: mobile.@caller[0].number<br>Opt: number    | Number of the caller allowed to SMS the router. Add in specific caller numbers, or use the wildcard symbol.<br>Blank<br>Range  |
| Web: Enable<br>UCI: mobile.@caller[0].enabled<br>Opt: enabled  | Enables or disables incoming caller ID.<br>no Disabled.<br>yes Enabled.  |
| Web: Respond<br>UCI: mobile.@caller[0].respond<br>Opt: respond | If checked, the router will return an SMS. Select <b>Respond</b> if you want the router to reply.<br>0 Disabled.<br>1 Enabled. |

Table 110: Information table for mobile manager caller settings

## 27.2.11 Roaming interface template

**Roaming Interface Template**  
Common config values for interfaces created by Automatic Operator Selection Delete

Interface Signal Sort   Sort interfaces by signal strength so those having better signal strength at the startup would be tried first

Roaming SIM   In which slot roaming sim-card is inserted

Firewall Zone  lan: lan: wlan: wlan:  wan: wan:  unspecified -or- create:

Append all the generated interfaces to this zone

APN

PIN

PAP/CHAP username

PAP/CHAP password

Service Preference   Order of service preference for the generated interfaces (Use Control button to select multiple)

Health Monitor Interval

Health Monitor ICMP Host(s)

Health Monitor Conntrack Test Host(s)

Health Monitor ICMP Timeout

Health Monitor ICMP Interval

Attempts Before WAN Failover

Attempts Before WAN Recovery

Figure 164: The roaming interface template page

| Web Field/UCI/Package Option  | Description   |         |                                   |       |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |
|---|---|---------|-----------------------------------|-------|---------------------------------|----------------------|---------|-------------|--------------------------------|-----|-------------|----------------------------------|---------|--------|---|--|
| Web: Interface Signal Sort<br>UCI:<br>mobile.@roaming_template[0].sort_sig_strength<br>Opt: sort_sig_strength | Sorts interfaces by signal strength priority so those that have a better signal strength will be tried first.   |         |                                   |       |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |
| Web: Roaming SIM<br>UCI: mobile.main.roaming_sim<br>Opt: roaming_sim  | Sets which slot to insert roaming SIM card. <table border="1"> <tr> <td>1</td> <td>SIM slot 1.</td> </tr> <tr> <td>2</td> <td>SIM slot 2.</td> </tr> </table>   | 1       | SIM slot 1.                       | 2     | SIM slot 2.                     |                      |         |             |                                |     |             |                                  |         |        |   |  |
| 1   | SIM slot 1.   |         |                                   |       |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |
| 2   | SIM slot 2.   |         |                                   |       |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |
| Web: Firewall Zone<br>UCI:<br>mobile.@roaming_template[0].firewall_zone<br>Opt: firewall_zone                 | Adds all generated interfaces to this zone.<br>Select <b>existing zone</b> or click <b>unspecified</b> or <b>create</b> to create a new zone.   |         |                                   |       |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |
| Web: APN<br>UCI: mobile.@roaming_template[0].apn<br>Opt: apn  | APN name of Mobile Network Operator.  |         |                                   |       |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |
| Web: PIN<br>UCI:<br>mobile.@roaming_template[0].pincode<br>Opt: pincode                                       | SIM card's PIN number.  |         |                                   |       |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |
| Web: PAP/CHAP username<br>UCI:<br>mobile.@roaming_template[0].username<br>Opt: username                       | Username used to connect to APN.  |         |                                   |       |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |
| Web: PAP/CHAP password<br>UCI:<br>mobile.@roaming_template[0].password<br>Opt: password                       | Password used to connect to APN.  |         |                                   |       |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |
| Web: Service Order<br>UCI:<br>mobile.@roaming_template[0].service_order<br>Opt: service_order                 | Defines a space separated list of services, in preferred order. Valid options are <code>gprs</code> , <code>umts</code> , <code>lte</code> , <code>auto</code> .<br>If no valid <code>service_order</code> is defined, then the configured Service Type is used. Example:<br><code>mobile.@roaming_template[0].service_order="gprs umts lte auto"</code> <table border="1"> <tr> <td>Blank</td> <td>Automatically detect best service</td> </tr> <tr> <td>Range</td> <td><code>gprs umts lte auto</code></td> </tr> </table>  | Blank   | Automatically detect best service | Range | <code>gprs umts lte auto</code> |                      |         |             |                                |     |             |                                  |         |        |   |  |
| Blank   | Automatically detect best service   |         |                                   |       |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |
| Range   | <code>gprs umts lte auto</code>   |         |                                   |       |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |
| Web: Health Monitor Interval<br>UCI:<br>mobile.@roaming_template[0].health_interval<br>Opt: health_interval   | Sets the period to check the health status of the interface. The Health Monitor interval will be used for: <ul style="list-style-type: none"> <li>Interface state checks</li> <li>Ping interval</li> <li>Signal strength checks</li> </ul> <table border="1"> <tr> <td>10</td> <td>health check every 10 seconds</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 10      | health check every 10 seconds     | Range |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |
| 10  | health check every 10 seconds   |         |                                   |       |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |
| Range   |   |         |                                   |       |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |
| Web: Health Monitor ICMP Host(s)<br>UCI:<br>mobile.@roaming_template[0].icmp_hosts<br>Opt: icmp_hosts         | Specifies target IP address for ICMP packets. <table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Disable</td> <td>Disables the option.</td> <td>disable</td> </tr> <tr> <td>DNS servers</td> <td>DNS IP addresses will be used.</td> <td>dns</td> </tr> <tr> <td>WAN gateway</td> <td>Gateway IP address will be used.</td> <td>gateway</td> </tr> <tr> <td>custom</td> <td>Ability to provide IP address. Multiple pings targets can be entered, comma separated. Pings to both must fail for health check to fail. Example:<br/><code>option icmp_hosts '1.1.1.1,2.2.2.2'</code></td> <td></td> </tr> </tbody> </table> | Web     | Description                       | UCI   | Disable                         | Disables the option. | disable | DNS servers | DNS IP addresses will be used. | dns | WAN gateway | Gateway IP address will be used. | gateway | custom | Ability to provide IP address. Multiple pings targets can be entered, comma separated. Pings to both must fail for health check to fail. Example:<br><code>option icmp_hosts '1.1.1.1,2.2.2.2'</code> |  |
| Web   | Description   | UCI     |                                   |       |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |
| Disable   | Disables the option.  | disable |                                   |       |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |
| DNS servers   | DNS IP addresses will be used.  | dns     |                                   |       |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |
| WAN gateway   | Gateway IP address will be used.  | gateway |                                   |       |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |
| custom  | Ability to provide IP address. Multiple pings targets can be entered, comma separated. Pings to both must fail for health check to fail. Example:<br><code>option icmp_hosts '1.1.1.1,2.2.2.2'</code>   |         |                                   |       |                                 |                      |         |             |                                |     |             |                                  |         |        |   |  |



| <p>Web: Health Monitor Contrack Test Host(s)<br/>UCI: mobile.@roaming_template[0].contrack_hosts<br/>Opt: contrack_hosts</p>           | <p>Contrack is the feature used to track if there is any traffic to and from an IP destination within the health interval.<br/>The Contrack_hosts option defines the IP for contrack to track, usually the icmp_host IP is used.<br/>If traffic to the contrack_hosts IP is detected then multiwan does not send a ping health check to the icmp_host; otherwise a ping is sent as normal to the icmp_host.<br/>By default the contrack_hosts is checked if the health interval is greater than 5 minutes. This time threshold currently cannot be manipulated.<br/>Contrack is generally used to limit the traffic sent on a GSM network.</p> <table border="1" data-bbox="683 544 1390 813"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Default</td> <td>Contrack checks for traffic from icmp_host IP when health_interval is greater than 5 minutes.</td> <td></td> </tr> <tr> <td>Disable</td> <td>Contrack checks for traffic from icmp_host IP when health_interval is greater than 5 minutes.</td> <td>disable</td> </tr> <tr> <td>custom</td> <td>Specifies an IP other than the icmp_host for contrack to track.</td> <td></td> </tr> </tbody> </table> | Web     | Description                                | UCI   | Default         | Contrack checks for traffic from icmp_host IP when health_interval is greater than 5 minutes. |  | Disable | Contrack checks for traffic from icmp_host IP when health_interval is greater than 5 minutes. | disable | custom | Specifies an IP other than the icmp_host for contrack to track. |  |
|--|--|---------|--|-------|-----------------|---|--|---------|---|---------|--------|---|--|
| Web  | Description  | UCI     |  |       |                 |   |  |         |   |         |        |   |  |
| Default  | Contrack checks for traffic from icmp_host IP when health_interval is greater than 5 minutes.  |         |  |       |                 |   |  |         |   |         |        |   |  |
| Disable  | Contrack checks for traffic from icmp_host IP when health_interval is greater than 5 minutes.  | disable |  |       |                 |   |  |         |   |         |        |   |  |
| custom   | Specifies an IP other than the icmp_host for contrack to track.  |         |  |       |                 |   |  |         |   |         |        |   |  |
| <p>Web: Health Monitor ICMP Timeout<br/>UCI: mobile.@roaming_template[0].timeout<br/>Opt: timeout</p>                                  | <p>Sets ping timeout in seconds. Choose the time in seconds that the health monitor ICMP will timeout at.</p> <table border="1" data-bbox="683 880 1390 947"> <tr> <td>3</td> <td>Wait 3 seconds for ping reply.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 3       | Wait 3 seconds for ping reply.             | Range |                 |   |  |         |   |         |        |   |  |
| 3  | Wait 3 seconds for ping reply.   |         |  |       |                 |   |  |         |   |         |        |   |  |
| Range  |  |         |  |       |                 |   |  |         |   |         |        |   |  |
| <p>Web: Health Monitor ICMP Interval<br/>UCI: mobile.@roaming_template[0].interval<br/>Opt: icmp_interval</p>                          | <p>Defines the interval, in seconds, between multiple pings sent at each health check</p> <table border="1" data-bbox="683 1014 1390 1081"> <tr> <td>1</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 1       |  | Range |                 |   |  |         |   |         |        |   |  |
| 1  |  |         |  |       |                 |   |  |         |   |         |        |   |  |
| Range  |  |         |  |       |                 |   |  |         |   |         |        |   |  |
| <p>Web: Attempts Before WAN Failover<br/>UCI: mobile.@roaming_template[1].health_fail_retries<br/>Opt: health_fail_retries</p>         | <p>Defines the number of health check failures before interface is disconnected.</p> <table border="1" data-bbox="683 1149 1390 1216"> <tr> <td>3</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 3       |  | Range |                 |   |  |         |   |         |        |   |  |
| 3  |  |         |  |       |                 |   |  |         |   |         |        |   |  |
| Range  |  |         |  |       |                 |   |  |         |   |         |        |   |  |
| <p>Web: Attempts Before WAN Recovery<br/>UCI: mobile.@roaming_template[0].health_recovery_retries<br/>Opt: health_recovery_retries</p> | <p>Sets the number of health check passes before the interface is considered healthy. This field is not used for a roaming template.</p>   |         |  |       |                 |   |  |         |   |         |        |   |  |
| <p>Web: Priority<br/>UCI: mobile.@roaming_template[0].priority<br/>Opt: priority</p>   | <p>Type the priority number. The higher the value, the higher the priority.</p> <table border="1" data-bbox="683 1462 1390 1529"> <tr> <td>0</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 0       |  | Range |                 |   |  |         |   |         |        |   |  |
| 0  |  |         |  |       |                 |   |  |         |   |         |        |   |  |
| Range  |  |         |  |       |                 |   |  |         |   |         |        |   |  |
| <p>Web: Minimum ifup interval<br/>UCI: mobile.@roaming_template[0].ifup_retry_sec<br/>Opt: ifup_retry_sec</p>                          | <p>Specifies the interval in seconds before retrying the primary interface when pre-empt mode is enabled.</p> <table border="1" data-bbox="683 1597 1390 1664"> <tr> <td>300</td> <td>Retry primary interface every 300 seconds.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 300     | Retry primary interface every 300 seconds. | Range |                 |   |  |         |   |         |        |   |  |
| 300  | Retry primary interface every 300 seconds.   |         |  |       |                 |   |  |         |   |         |        |   |  |
| Range  |  |         |  |       |                 |   |  |         |   |         |        |   |  |
| <p>Web: Interface Start Timeout<br/>UCI: mobile.@roaming_template[0].ifup_timeout_sec<br/>Opt: ifup_timeout</p>                        | <p>Specifies the time in seconds for interface to start up. If it is not up after this period, it will be considered a fail It is recommended to configure a value greater than 120 seconds.</p> <table border="1" data-bbox="683 1753 1390 1821"> <tr> <td>40</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 40      |  | Range |                 |   |  |         |   |         |        |   |  |
| 40   |  |         |  |       |                 |   |  |         |   |         |        |   |  |
| Range  |  |         |  |       |                 |   |  |         |   |         |        |   |  |
| <p>Web: Signal Threshold (dBm)<br/>UCI: mobile.@roaming_template[0].signal_threshold<br/>Opt: signal_threshold</p>                     | <p>Specifies the minimum signal strength in dBm before considering if the interface fails signal health check. Uses the value stored for sig_dbm in mobile diagnostics.-115 dBm.</p> <table border="1" data-bbox="683 1910 1390 2000"> <tr> <td></td> <td>Disabled</td> </tr> <tr> <td>Range</td> <td>-46 to -115 dBm</td> </tr> </table>  |         | Disabled                                   | Range | -46 to -115 dBm |   |  |         |   |         |        |   |  |
|  | Disabled   |         |  |       |                 |   |  |         |   |         |        |   |  |
| Range  | -46 to -115 dBm  |         |  |       |                 |   |  |         |   |         |        |   |  |

Table 111: Information table for roaming interface template

When you have configured your settings, click **Save & Apply**.

### 27.2.11.1 Set multi-WAN operation

From the top menu, select **Network -> Multi-Wan**. The Multi-WAN page appears.

Figure 165: The multi-WAN page

In the Multi-WAN section click **Add**.

| Web Field/UCI/Package Option                                  | Description   |   |           |   |          |
|---|---|---|-----------|---|----------|
| Web: Enable<br>UCI: multiwan.config.enabled<br>Opt: enabled   | Enables multiwan.<br>Select this option.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0 | Disabled. | 1 | Enabled. |
| 0   | Disabled.   |   |           |   |          |
| 1   | Enabled.  |   |           |   |          |
| Web: Preempt<br>UCI: multiwan.config.preempt<br>Opt: pre-empt | Enables or disables pre-emption for multiwan. If enabled the router will keep trying to connect to a higher priority interface depending on timer set by ifup_retry_sec.<br>Leave this option unselected.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0 | Disabled. | 1 | Enabled. |
| 0   | Disabled.   |   |           |   |          |
| 1   | Enabled.  |   |           |   |          |
| Web: Alternate Mode<br>UCI: multiwan.config.alt<br>Opt: alt   | Enables or disables alternate mode for multiwan. If enabled the router will use an alternate interface after reboot.<br>Leave this option unselected.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0 | Disabled. | 1 | Enabled. |
| 0   | Disabled.   |   |           |   |          |
| 1   | Enabled.  |   |           |   |          |

Table 112: Information table for multi-WAN operation

## 27.3 Configuring via UCI

### 27.3.1 PMP + roaming: pre-empt enabled & disabled via UCI

#### 27.3.1.1 PMP interface configuration

The PMP interface is configured in the network package `/etc/config/network`. To view the network configuration file, enter:

```
root@VA_router:~# uci export network
package network

config interface 'loopback'
```

```

option ifname 'lo'
option proto 'static'
option ipaddr '127.0.0.1'
option netmask '255.0.0.0'

config interface 'lan'
option ifname 'eth0'
option proto 'static'
option ipaddr '192.168.100.1'
option netmask '255.255.255.0'

config interface '3g_s1_voda'
option auto '0'
option proto '3g'
option service_order 'auto lte umts gprs'
option apn 'testIE'
option username 'test'
option password 'test'
option sim '1'          option operator 'vodafone IE'

```

To view uci commands, enter:

```

root@VA_router:~# uci show network
network.loopback=interface
network.loopback.ifname=lo
network.loopback.proto=static
network.loopback.ipaddr=127.0.0.1
network.loopback.netmask=255.0.0.0
network.lan=interface
network.lan.ifname=eth0
network.lan.proto=static
network.lan.ipaddr=192.168.100.1
network.lan.netmask=255.255.255.0
network.3g_s1_voda=interface
network. 3g_s1_voda.auto=0
network. 3g_s1_voda.proto=3g
network. 3g_s1_voda.service_order='auto lte umts gprs'
network. 3g_s1_voda.apn=test IE

```

```
network. 3g_s1_voda.username=test
network. 3g_s1_voda.password=test
network. 3g_s1_voda.sim=1
network. 3g_s1_voda.operator=vodafone IE
```

### 27.3.1.2 Roaming interface configuration

The roaming interface configurations are stored in the mobile package /etc/config/mobile.

To view the mobile configuration file, enter: root@VA\_router:~# uci export mobile

```
config mobile 'main'
    option sms 'yes'
    option roaming_sim '1'
    option init_get_iccids 'no'
config caller
    option name 'Test'
    option number '*'
    option enabled 'yes'
    option respond 'yes'
config roaming_template
    option roaming_sim '1'
    option firewall_zone 'wan'
    option apn 'test IE'
    option username 'test'
    option password 'test'
    option service 'umts'
    option health_interval '4'
    option icmp_hosts 'disable'
    option timeout 'disable'
    option health_fail_retries '3'
    option signal_threshold '-95'
    option priority '5'
    option ifup_retry_sec '120'
    option ifup_timeout_sec '180'
    option defaultroute 'yes'
    option sort_sig_strength 'yes'
```

To view the uci command of package mobile, enter:

```
root@VA_router:~#uci show mobile
mobile.main=mobile
mobile.main.sms=yes
mobile.main.roaming_sim=1
mobile.main.init_get_iccids=no
mobile.@caller[0]=caller
mobile.@caller[0].name=Test
mobile.@caller[0].number=*
mobile.@caller[0].enabled=yes
mobile.@caller[0].respond=yes
mobile.@roaming_template[0]=roaming_template
mobile.@roaming_template[0].roaming_sim=1
mobile.@roaming_template[0].firewall_zone=wan
mobile.@roaming_template[0].apn=test IE
mobile.@roaming_template[0].username=test
mobile.@roaming_template[0].password=test
mobile.@roaming_template[0].service=umts
mobile.@roaming_template[0].health_interval=4
mobile.@roaming_template[0].icmp_hosts=disable
mobile.@roaming_template[0].timeout=disable
mobile.@roaming_template[0].health_fail_retries=3
mobile.@roaming_template[0].signal_threshold=-95
mobile.@roaming_template[0].priority=5
mobile.@roaming_template[0].ifup_retry_sec=120
mobile.@roaming_template[0].ifup_timeout_sec=180
mobile.@roaming_template[0].defaultroute=yes
mobile.@roaming_template[0].sort_sig_strength=yes
```

### 27.3.1.3 Multi-WAN configuration using UCI

The configuration file for package multiwan is stored on **/etc/config/multiwan**

To see configuration file of mobile package, enter:

```
root@VA_router:~# cat /etc/config/multiwan
config multiwan 'config'
    option enabled '1'
    option preempt '1'
```

```

config interface '3g_s1_voda'
    option health_fail_retries '3'
    option health_interval '3'
    option timeout '1'
    option icmp_hosts 'disable'
    option priority '10'
    option exclusive_group '3g'
    option signal_threshold '-95'
    option ifup_retry_sec '350'
    option ifup_timeout_sec '180'
    option manage_state '1'

```

To view the uci command of package multiwan, enter:

```

root@VA_router:~# uci show multiwan
multiwan.config=multiwan
multiwan.config.enabled=1
multiwan.config.preempt=1
multiwan.main_voda=interface
multiwan.main_voda.health_fail_retries=3
multiwan.main_voda.health_interval=3
multiwan.3g_s1_voda.timeout=1
multiwan.3g_s1_voda.icmp_hosts=disable
multiwan.3g_s1 main _voda.priority=10
multiwan.3g_s1_voda.exclusive_group=3g
multiwan.3g_s1_voda.signal_threshold=-95
multiwan.3g_s1_voda.ifup_retry_sec=350
multiwan.3g_s1_voda.ifup_timeout_sec=180
multiwan.3g_s1_voda.manage_state=1

```

The difference between PMP + roaming: pre-empt enabled and disabled is setting one option parameter. To disable pre-empt, enter:

```

uci set multiwan.config.preempt=0
uci commit

```

**Note:** available values are:

|   |          |
|---|----------|
| 0 | Disabled |
| 1 | Enabled  |

## 27.4 Configuring no PMP + roaming using UCI

The roaming interface configuration file is stored in the mobile package **/etc/config/mobile**. To view the mobile package, enter:

```
root@VA_router:~# uci export mobile

package mobile
config mobile 'main'
    option sms 'yes'
    option roaming_sim '1'
    option debug '1'

config caller
    option name 'Eval'
    option number '*'
    option enabled 'yes'
    option respond 'yes'

config roaming_template
    option roaming_sim '1'
    option firewall_zone 'wan'
    option apn 'test IE'
    option username 'test'
    option password 'test'
    option service 'umts'
    option health_fail_retries '2'
    option signal_threshold '-100'
    option priority '5'
    option ifup_timeout_sec '180'
    option defaultroute 'yes'
    option sort_sig_strength 'yes'
    option ifup_retry_sec '200'
    option health_interval '120'
    option icmp_hosts '172.31.4.129'
    option timeout '3'
    option health_recovery_retries '3'
```

To view the mobile package via uci commands, enter:

```
root@VA_router:~# uci show mobile
mobile.main=mobile
mobile.main.sms=yes
mobile.main.roaming_sim=1
mobile.main.debug=1
mobile.@caller[0]=caller
mobile.@caller[0].name=Eval
mobile.@caller[0].number=*
mobile.@caller[0].enabled=yes
mobile.@caller[0].respond=yes
mobile.@roaming_template[0]=roaming_template
mobile.@roaming_template[0].roaming_sim=1
mobile.@roaming_template[0].firewall_zone=wan
mobile.@roaming_template[0].apn=stream.co.uk
mobile.@roaming_template[0].username=default
mobile.@roaming_template[0].password=void
mobile.@roaming_template[0].service=umts
mobile.@roaming_template[0].health_fail_retries=2
mobile.@roaming_template[0].signal_threshold=-100
mobile.@roaming_template[0].priority=5
mobile.@roaming_template[0].ifup_timeout_sec=180
mobile.@roaming_template[0].defaultroute=yes
mobile.@roaming_template[0].sort_sig_strength=yes
mobile.@roaming_template[0].ifup_retry_sec=200
mobile.@roaming_template[0].health_interval=120
mobile.@roaming_template[0].icmp_hosts=172.31.4.129
mobile.@roaming_template[0].timeout=3
mobile.@roaming_template[0].health_recovery_retries=3
```

The multiwan package is stored on **/etc/config/multiwan**. To view the multiwan package, enter:

```
root@VA_router:~# uci export multiwan
package multiwan

config multiwan 'config'
    option enabled 'yes'
```



```

option preempt 'no'
option alt_mode 'no'
To see multiwan package via uci, enter:
root@VA_router:~# uci show multiwan
multiwan.config=multiwan
multiwan.config.enabled=yes
multiwan.config.preempt=no
multiwan.config.alt_mode=no

```

## 27.5 Automatic operator selection diagnostics via the web interface

### 27.5.1 Checking the status of the multiwan package

When interfaces are auto-created they are presented in the network and in the multiwan package.

To check interfaces created in the multiwan package, from the top menu, select **Network -> Multi-WAN**.

To check interfaces that have been created in the network package, from the top menu, select **Network -> Interfaces**.






| Interface Overview  |  |  |
|---|--|--|
| Network   | Status   | Actions  |
| <b>3G_S1_O2IR</b><br><br>3g-3g_s1_o2IR | RX: 0.00 B (0 Pkts.)<br>TX: 0.00 B (0 Pkts.)   | <input type="button" value="Connect"/> <input type="button" value="Stop"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> |
| <b>3G_S1_VODA</b><br><br>3g-3g_s1_voda | Uptime: 7h 31m 26s<br>RX: 62.00 B (8 Pkts.)<br>TX: 23.44 KB (329 Pkts.)<br>IPv4: 10.140.1.23/32  | <input type="button" value="Connect"/> <input type="button" value="Stop"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> |
| <b>WCLIENT</b><br><br>Client "0"       | MAC Address: 00:00:00:00:00:00<br>RX: 0.00 B (0 Pkts.)<br>TX: 0.00 B (0 Pkts.)   | <input type="button" value="Connect"/> <input type="button" value="Stop"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> |
| <b>LAN</b><br><br>eth0                 | Uptime: 7h 35m 24s<br>MAC Address: 00:E0:C8:10:1A:82<br>RX: 67.25 KB (502 Pkts.)<br>TX: 132.29 KB (157 Pkts.)<br>IPv4: 10.1.1.9/29                           | <input type="button" value="Connect"/> <input type="button" value="Stop"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> |
| <b>LOOPBACK</b><br><br>lo              | Uptime: 7h 35m 30s<br>MAC Address: 00:00:00:00:00:00<br>RX: 41.72 KB (516 Pkts.)<br>TX: 41.72 KB (516 Pkts.)<br>IPv4: 127.0.0.1/8<br>IPv6: 0:0:0:0:0:0:1/128 | <input type="button" value="Connect"/> <input type="button" value="Stop"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

Figure 166: The interface overview page

To check the status of the interface you are currently using, in the top menu, click **Status**. The Interface Status page appears.

Scroll down to the bottom of the page to view Multi-WAN Stats.

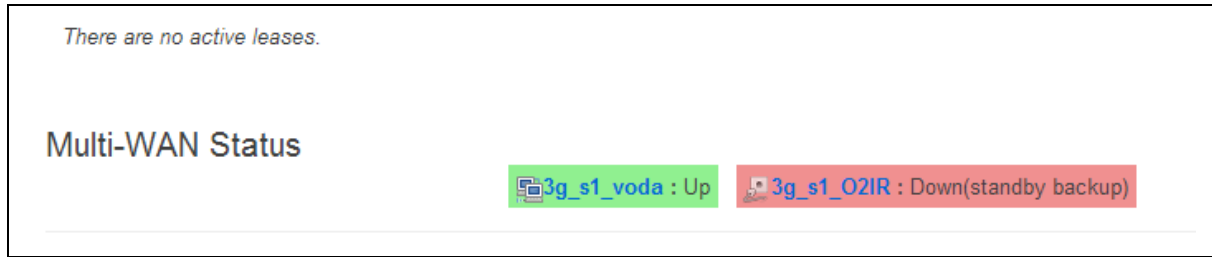


Figure 167: The status page: multi-WAN status section page

## 27.6 Automatic operator selection diagnostics via UCI

### 27.6.1 Check roaming interfaces discovered

Roaming interfaces discovered during roaming search are stored at **/var/const\_state/roaming**. This file contains a section for each discovered operator/service combination, along with signal strength, if tested. Time taken to scan is also available along with the time of scan and number of services found.

To check roaming interfaces discovered, enter

```
root@VA_router:~# cat /var/const_state/roaming
roaming.main2_voda_lte=service
roaming.main2_voda_lte.name=vodafone IE
roaming.main2_voda_lte.shortname=voda IE
roaming.main2_voda_lte.opnum=27201
roaming.main2_voda_lte.interface=main2_voda
roaming.main2_voda_lte.servicetype=7
roaming.main2_voda_lte.sim=2
roaming.main2_voda_lte.tested=0
roaming.main2_voda_lte.signalstrength=0
roaming.main2_voda_ums=service
roaming.main2_voda_ums.name=vodafone IE
roaming.main2_voda_ums.shortname=voda IE
roaming.main2_voda_ums.opnum=27201
roaming.main2_voda_ums.interface=main2_voda
roaming.main2_voda_ums.servicetype=2
roaming.main2_voda_ums.sim=2
roaming.main2_voda_ums.tested=1
roaming.main2_voda_ums.signalstrength=-79
roaming.main2_voda_gprs=service
roaming.main2_voda_gprs.name=vodafone IE
roaming.main2_voda_gprs.shortname=voda IE
```

```
roaming.main2_voda_gprs.opnum=27201
roaming.main2_voda_gprs.interface=main2_voda
roaming.main2_voda_gprs.servicetype=0
roaming.main2_voda_gprs.sim=2
roaming.main2_voda_gprs.tested=0
roaming.main2_voda_gprs.signalstrength=0
roaming.main2_o2IR_ums=service
roaming.main2_o2IR_ums.name=o2 IRL
roaming.main2_o2IR_ums.shortname=o2 - IRL
roaming.main2_o2IR_ums.opnum=27202
roaming.main2_o2IR_ums.interface=main2_o2IR
roaming.main2_o2IR_ums.servicetype=2
roaming.main2_o2IR_ums.sim=2
roaming.main2_o2IR_ums.tested=1
roaming.main2_o2IR_ums.signalstrength=-85
roaming.main2_o2IR_gprs=service
roaming.main2_o2IR_gprs.name=o2 IRL
roaming.main2_o2IR_gprs.shortname=o2 - IRL
roaming.main2_o2IR_gprs.opnum=27202
roaming.main2_o2IR_gprs.interface=main2_o2IR
roaming.main2_o2IR_gprs.servicetype=0
roaming.main2_o2IR_gprs.sim=2
roaming.main2_o2IR_gprs.tested=0
roaming.main2_o2IR_gprs.signalstrength=0
roaming.status=status
roaming.status.num_services=5
roaming.status.scan_update_time=Thu Feb 22 05:02:38 2018
roaming.status.scan_duration=185
```

Roaming operators are also stored in MIB `vaModemRoaming.mib`.

## 27.6.2 Check interfaces created in multiwan

To check interfaces created in the multiwan package, enter:

```
root@VA_router:~# cat /var/const_state/multiwan
multiwan.main2_3IRL=interface
multiwan.main2_3IRL.timeout=disable
multiwan.main2_3IRL.health_recovery_retries=5
multiwan.main2_3IRL.exclusive_group=3g
multiwan.main2_3IRL.manage_state=yes
multiwan.main2_3IRL.signal_threshold=-80
multiwan.main2_3IRL.ifup_timeout_sec=150
multiwan.main2_3IRL.icmp_hosts=disable
multiwan.main2_3IRL.health_interval=4
multiwan.main2_3IRL.priority=5
multiwan.main2_3IRL.ifup_retry_sec=120
multiwan.main2_3IRL.health_fail_retries=3
multiwan.main2_o2IR=interface
multiwan.main2_o2IR.timeout=disable
multiwan.main2_o2IR.health_recovery_retries=5
multiwan.main2_o2IR.exclusive_group=3g
multiwan.main2_o2IR.manage_state=yes
multiwan.main2_o2IR.signal_threshold=-80
multiwan.main2_o2IR.ifup_timeout_sec=150
multiwan.main2_o2IR.icmp_hosts=disable
multiwan.main2_o2IR.health_interval=4
multiwan.main2_o2IR.priority=5
multiwan.main2_o2IR.ifup_retry_sec=120
multiwan.main2_o2IR.health_fail_retries=3
```

## 27.6.3 Check interfaces created in network

To check interfaces created in the network package, enter:

```
root@VA_router:~# cat /var/const_state/network
network.main2_3IRL=interface
network.main2_3IRL.snmp_alias_ifindex=3
network.main2_3IRL.sim=2
network.main2_3IRL.defaultroute=yes
network.main2_3IRL.username=campen1
```

```
network.main2_3IRL.apn=vpn.amylan.co.uk
network.main2_3IRL.opformat=2
network.main2_3IRL.phy=1-1
network.main2_3IRL.roaming_sim=2
network.main2_3IRL.operator=27205
network.main2_3IRL.password=campen1
network.main2_3IRL.auto=no
network.main2_3IRL.service_order=auto
network.main2_3IRL.proto=3g
network.main2_o2IR=interface
network.main2_o2IR.snmp_alias_ifindex=3
network.main2_o2IR.sim=2
network.main2_o2IR.defaultroute=yes
network.main2_o2IR.username=campen1
network.main2_o2IR.apn=vpn.amylan.co.uk
network.main2_o2IR.opformat=2
network.main2_o2IR.phy=1-1
network.main2_o2IR.roaming_sim=2
network.main2_o2IR.operator=27202
network.main2_o2IR.password=campen1
network.main2_o2IR.auto=no
network.main2_o2IR.service_order=auto
network.main2_o2IR.proto=3g
```

#### 27.6.4 Check current interface

To check the SIM status of the interface you are currently using, enter:

```
root@VA_router:~# cat /var/const_state/mobile
mobile.3g_1_1=status
mobile.3g_1_1.sim2_iccid=89314404000075920976
mobile.3g_1_1.imei=866802020194140
mobile.3g_1_1.hw_rev=4534B04SIM7100E
mobile.3g_1_1.sim_select=yes
```

To check mobile status of the interface you are currently using, enter

```
root@VA_router:~# cat /var/state/mobile
mobile.3g_1_1=status
mobile.3g_1_1.auto_info=/tmp/3g_1-1.auto
mobile.3g_1_1.scan_update_time=Thu Feb 22 05:02:38 2018
mobile.3g_1_1.imsi=204043726930595
mobile.3g_1_1.imsi2=204043726930595
mobile.3g_1_1.lte_band=3
mobile.3g_1_1.last_error=no network service
mobile.3g_1_1.mcc=272
mobile.3g_1_1.last_error_time=2018-02-22 10:41:27
mobile.3g_1_1.lac=11
mobile.3g_1_1.cell=46542698
mobile.3g_1_1.mnc=05
mobile.3g_1_1.operator_code=27205
mobile.3g_1_1.operator_name=3 IRL DATA ONLY
mobile.3g_1_1.rscp_dbm=-86
mobile.3g_1_1.ecio_db=-8.5
mobile.3g_1_1.sig_dbm=-51
mobile.3g_1_1.temperature=37
mobile.3g_1_1.vam_state=connecting
mobile.3g_1_1.sim_slot=2
mobile.3g_1_1.sim_in=yes
mobile.3g_1_1.technology=UMTS
mobile.3g_1_1.registered=Roaming
mobile.3g_1_1.reg_code=5
mobile.3g_1_1.registered_pkt=Searching
mobile.3g_1_1.reg_code_pkt=2
```

## 28 Configuring Connection Watch (cwatch)

Connection Watch is a recovery feature to enable dynamic recovery of an interface. You can configure multiple instances of Connection Watch.

Connection Watch consists of the following configurable instances:

- Interface(s) to be monitored
- Failure periods
- Recovery actions

If no data is received over the monitored interface during the configured duration, then the recovery action is performed. If more than one interface is specified under a single Connection Watch, the recovery action will be performed only if no data is received on both of the interfaces for the defined period.

Currently three configurable periods and associated recovery actions can be defined. Recovery actions are prioritised based on their configured failure periods, the smallest failure period having the lowest priority. Lowest priority actions are repeated until the next highest priority action executes at which point it then stops leaving only the new action to execute at configured intervals.

Example:

- Failure time 1 = 1 hour; Failure action 1 = interface up
- Failure time 2 = 10 hours; Failure action 2 = interface restart
- Failure time 3 = 24 hours; Failure action 3 = reboot

In the above example action execution priorities are action 3 > action 2 > action 1. In the case of failure to detect incoming packets, action 1 is triggered first and is executed at intervals of one hour until action 2 is due. When action 2 is executed, action 1 gets disabled and thereafter only action 2 is executed every 10 hours until action 3 is due.

If the status of the interface is detected as 'up' at any stage then no subsequent failure action will occur and all failure timers are reset. In the case of any subsequent failure, all failure actions are re-enabled and the action sequence is repeated.

### 28.1 Configuration package used

| Package | Sections |
|---------|----------|
| cwatch  | watch    |

### 28.2 Configuring Connection Watch using the web interface

To configure Connection Watch using the web interface, select **Services - >Connection Watch**. The Connection Watch page appears.

If no Connection Watch configuration exists in the configuration file, first enter a name for the Connection Watch instance and select **Add**.

**Connection Watch**  
Configuration of Connection Watch.

Watch

*This section contains no values yet*

WATCH\_MOBILE

Figure 168: The add connection watch configuration page

**Connection Watch**  
Configuration of Connection Watch.

Watch

**WATCH\_MOBILE**

Enabled

Status **unknown**

Interfaces  LAN:  LAN1:  MOBILE1:  PPPoADSL:  loopback:

Failure Time for Action 1

Failure Action 1

Failure Grace Time 1  Interface activity will be ignored during the grace time

Failure Time for Action 2

Failure Action 2

Failure Grace Time 2  Interface activity will be ignored during the grace time

Failure Time for Action 3

Failure Action 3

Failure Grace Time 3  Interface activity will be ignored during the grace time

Figure 169: The connection watch configuration page



| Web Field/UCI/Package Option   | Description   |       |               |       |             |
|--|---|-------|---------------|-------|-------------|
| Web: Enabled<br>UCI: cwatch.@watch[0].enabled<br>Opt: enabled  | Enables a cwatch instance.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0     | Disabled.     | 1     | Enabled.    |
| 0  | Disabled.   |       |               |       |             |
| 1  | Enabled.  |       |               |       |             |
| Web: Interfaces<br>UCI: cwatch.@watch[0].test_ifaces<br>Opt: test_ifaces                             | Defines the interface name(s) to monitor. Multiple interfaces are delimited by space separator. Example:<br><pre>option test_ifaces 'WANADSL WANMOBILE'</pre> If multiple interfaces are defined the failure action will only be triggered if no traffic is received on all interfaces for the defined period.  |       |               |       |             |
| Web: Failure Time for Action 1<br>UCI: cwatch.@watch[0].failure_time_1<br>Opt: failure_time_1        | Defines a duration to monitor an interface for receive traffic. Duration can be specified in seconds, minutes, hours, days.<br><table border="1"> <tr> <td>1h</td> <td></td> </tr> <tr> <td>Range</td> <td>s; m; h; d;</td> </tr> </table>  | 1h    |               | Range | s; m; h; d; |
| 1h   |   |       |               |       |             |
| Range  | s; m; h; d;   |       |               |       |             |
| Web: Failure Action 1<br>UCI: cwatch.@watch[0].failure_action_1<br>Opt: failure_action_1             | Defines the failure action associated with failure_time_1. Example to force up interface:<br><pre>option failure_action_1 'ifup wan'</pre> <table border="1"> <tr> <td>blank</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | blank |               | Range |             |
| blank  |   |       |               |       |             |
| Range  |   |       |               |       |             |
| Web: Failure Grace Time 1<br>UCI: cwatch.@watch[0].failure_grace_time_1<br>Opt: failure_grace_time_1 | Defines a grace time during which interface activity will be ignored after 'Failure Action 1' is executed.<br>Connection Watch will assume the interface to be down during the grace period and will not reset the failure action timers even if packets are received during this grace time.<br>This can be used to overcome the situation where packets can be received after a failure action even though the interface eventually fails to connect.<br>For example, during a USB restart on a mobile interface, a small amount of packets can be registered as being received while a mobile connection is attempted but fails registration.<br><table border="1"> <tr> <td>0</td> <td>No grace time</td> </tr> <tr> <td>Range</td> <td>s; m; h; d;</td> </tr> </table> | 0     | No grace time | Range | s; m; h; d; |
| 0  | No grace time   |       |               |       |             |
| Range  | s; m; h; d;   |       |               |       |             |
| Web: Failure Time for Action 2<br>UCI: cwatch.@watch[0].failure_time_2<br>Opt: failure_time_2        | Defines a second duration to monitor an interface for receive traffic. Duration can be specified in seconds, minutes, hours, days.<br><table border="1"> <tr> <td>10h</td> <td></td> </tr> <tr> <td>Range</td> <td>s; m; h; d;</td> </tr> </table>  | 10h   |               | Range | s; m; h; d; |
| 10h  |   |       |               |       |             |
| Range  | s; m; h; d;   |       |               |       |             |
| Web: Failure Action 2<br>UCI: cwatch.@watch[0].failure_action_2<br>Opt: failure_action_2             | Defines the failure action associated with failure_time_2. Example to reset usb:<br><pre>option failure_action_1 '/etc/init.d/usb_startup restart'</pre> <table border="1"> <tr> <td>blank</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | blank |               | Range |             |
| blank  |   |       |               |       |             |
| Range  |   |       |               |       |             |
| Web: Failure Grace Time 2<br>UCI: cwatch.@watch[0].failure_grace_time_2<br>Opt: failure_grace_time_2 | Defines a grace time during which interface activity will be ignored after 'Failure Action 2' is executed.<br>Connection Watch will assume the interface to be down during the grace period and will not reset the failure action timers even if packets are received during this grace time.<br>This can be used to overcome the situation where packets can be received after a failure action even though the interface eventually fails to connect.<br>For example, during a USB restart on a mobile interface, a small amount of packets can be registered as being received while a mobile connection is attempted but fails registration.<br><table border="1"> <tr> <td>0</td> <td>No grace time</td> </tr> <tr> <td>Range</td> <td>s; m; h; d;</td> </tr> </table> | 0     | No grace time | Range | s; m; h; d; |
| 0  | No grace time   |       |               |       |             |
| Range  | s; m; h; d;   |       |               |       |             |

|   |   |       |               |       |             |
|---|---|-------|---------------|-------|-------------|
| <p>Web: Failure Time for Action 3<br/>UCI: cwatch.@watch[0].failure_time_3<br/>Opt: failure_time_3</p>            | <p>Defines a third duration to monitor an interface for receive traffic. Duration can be specified in seconds, minutes, hours, days.</p> <table border="1" data-bbox="683 280 1332 349"> <tr> <td>24h</td> <td></td> </tr> <tr> <td>Range</td> <td>s; m; h; d;</td> </tr> </table>  | 24h   |               | Range | s; m; h; d; |
| 24h   |   |       |               |       |             |
| Range   | s; m; h; d;   |       |               |       |             |
| <p>Web: Failure Action 3<br/>UCI: cwatch.@watch[0].failure_action_3<br/>Opt: failure_action_3</p>                 | <p>Defines the failure action associated with failure_time_3. Example to reset usb:<br/>option failure action 3 'reboot'</p> <table border="1" data-bbox="683 443 1332 510"> <tr> <td>blank</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | blank |               | Range |             |
| blank   |   |       |               |       |             |
| Range   |   |       |               |       |             |
| <p>Web: Failure Grace Time 3<br/>UCI:<br/>cwatch.@watch[0].failure_grace_time_3<br/>Opt: failure_grace_time_3</p> | <p>Defines a grace time during which interface activity will be ignored after 'Failure Action 3' is executed. Connection Watch will assume the interface to be down during the grace period and will not reset the failure action timers even if packets are received during this grace time. This can be used to overcome the situation where packets can be received after a failure action even though the interface eventually fails to connect. For example, during a USB restart on a mobile interface, a small amount of packets can be registered as being received while a mobile connection is attempted but fails registration.</p> <table border="1" data-bbox="683 831 1332 896"> <tr> <td>0</td> <td>No grace time</td> </tr> <tr> <td>Range</td> <td>s; m; h; d;</td> </tr> </table> | 0     | No grace time | Range | s; m; h; d; |
| 0   | No grace time   |       |               |       |             |
| Range   | s; m; h; d;   |       |               |       |             |

Table 113: Information table for cwatch section

## 28.3 Configuring cwatch using command line

By default, all cwatch instances are named 'watch', the cwatch instance is identified by @watch then the watch position in the package as a number. For example, for the first route in the package using UCI:

```
cwatch.@watch[0]=watch
cwatch.@watch[0].enabled=1
```

Or using package options:

```
config watch
    option enabled '1'
```

However, to better identify it, we recommend giving the cwatch instance a name. For example, a watch named 'WATCH\_MOBILE' will be cwatch.WATCH\_MOBILE.

To define a named cwatch instance using UCI, enter:

```
cwatch.WATCH_MOBILE=watch
cwatch.WATCH_MOBILE.enabled=1
```

To define a named cwatch instance using package options, enter:

```
config watch 'WATCH_MOBILE'
    option 'enabled' '1'
```

### 28.3.1 cwatch using UCI

```

root@VA_router:~# uci show cwatch
cwatch.WATCH_MOBILE=watch
cwatch.WATCH_MOBILE.enabled=1
cwatch.WATCH_MOBILE.test_ifaces=wan
cwatch.WATCH_MOBILE.failure_time_1=1h
cwatch.WATCH_MOBILE.failure_action_1=ifup wan
cwatch.WATCH_MOBILE.failure_time_2=10h
cwatch.WATCH_MOBILE.failure_action_2=/etc/init.d/usb_startup restart
cwatch.WATCH_MOBILE.failure_time_3=24h
cwatch.WATCH_MOBILE.failure_action_3=reboot

```

### 28.3.2 cwatch using package options

```

root@VA_router:~# uci export cwatch
package cwatch

config watch 'WATCH_MOBILE'
    option enabled '1'
    option test_ifaces wan
    option failure_time_1 '1h'
    option failure_action_1 'ifup wan'
    option failure_grace_time_1 `30s`
    option failure_time_2 '10h'
    option failure_action_2 '/etc/init.d/usb_startup restart'
    option failure_grace_time_2 `2m`
    option failure_time_3 '24h'
    option failure_action_3 'reboot'

```

## 28.4 cwatch diagnostics

### 28.4.1 Syslog

A syslog message will be generated when cwatch starts:

```
cwatch[x]: cwatch configuration OK. Entering main loop...
```

Syslog messages will be generated when the failure action is triggered:

```
cwatch[x]: Watch WATCH_MOBILE executed action 1 grace time [x]
```

```
cwatch[x]: Watch WATCH_MOBILE executed action 2 grace time [x]  
cwatch[x]: Watch WATCH_MOBILE executed action 3 grace time [x]
```

A syslog message will be generated if there is a problem with the configured cwatch instance.

```
cwatch[x]: Watch WATCH_MOBILE test_ifaces not defined. Watch ignored
```

## 29 Configuring DHCP server and DNS (Dnsmasq)

Dynamic Host Configuration Protocol (DHCP) server is responsible for assigning IP addresses to hosts. IP addresses can be given out on different interfaces and different subnets. You can manually configure lease time as well as setting static IP to host mappings.

Domain Name Server (DNS) is responsible for resolution of IP addresses to domain names on the internet.

Dnsmasq is the application which controls DHCP and DNS services. Dnsmasq has two sections; one to specify general DHCP and DNS settings and one or more DHCP pools to define DHCP operation on the desired network interface.

### 29.1 Configuration package used

| Package | Sections |
|---------|----------|
| dhcp    | dnsmasq  |
|         | dhcp     |
|         | host     |

### 29.2 Configuring DHCP and DNS using the web interface

In the top menu, select **Network -> DHCP and DNS**. The DHCP and DNS page appears. There are three sections: Server Settings, Active Leases, and Static Leases.

Status ▾ System ▾ Services ▾ Network ▾ Logout
AUTO REFRESH ON

## DHCP and DNS

Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

### Server Settings

General Settings
Resolv and Hosts Files
TFTP Settings
Advanced Settings

Domain required   Don't forward DNS-Requests without DNS-Name

Authoritative   This is the only DHCP in the local network

Interfaces  lan  lan2  loopback  wan  wan1

Select interfaces to be served by dnsmasq. If none selected dnsmasq will serve on all interfaces

Local server   Local domain specification. Names matching this domain are never forwarded and resolved from DHCP or hosts files only

Local domain   Local domain suffix appended to DHCP names and hosts file entries

Log queries   Write received DNS requests to syslog

DNS forwardings   List of DNS servers to forward requests to. To forward only specific domain requests use // syntax

Rebind protection   Discard upstream RFC1918 responses

Allow localhost   Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services

Domain whitelist   List of domains to allow RFC1918 responses for

### Active Leases

| Hostname                    | IPv4-Address | MAC-Address | Leasetime remaining |
|-----------------------------|--------------|-------------|---------------------|
| There are no active leases. |              |             |                     |

### Static Leases

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served. Use the Add Button to add a new lease entry. The MAC-Address identifies the host, the IPv4-Address specifies to the fixed address to use and the Hostname is assigned as symbolic name to the requesting host.

| Hostname                            | MAC-Address | IPv4-Address |
|-------------------------------------|-------------|--------------|
| This section contains no values yet |             |              |

Save & Apply
Save
Reset

Figure 170: The DHCP and DNS page

## 29.2.1 Dnsmasq: general settings

| Web Field/UCI/Package Option   | Description   |       |                              |       |           |
|--|---|-------|------------------------------|-------|-----------|
| Web: Domain required<br>UCI: dhcp.@dnsmasq[0].domainneeded<br>Opt: domainneeded                | Defines whether to forward DNS requests without a DNS name. Dnsmasq will never forward queries for plain names, without dots or domain parts, to upstream nameservers. If the name is not known from /etc/hosts or DHCP then a "not found" answer is returned. <table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table> | 1     | Enabled.                     | 0     | Disabled. |
| 1  | Enabled.  |       |                              |       |           |
| 0  | Disabled.   |       |                              |       |           |
| Web: Authoritative<br>UCI: dhcp.@dnsmasq[0].authoritative<br>Opt: authoritative                | Forces authoritative mode. This speeds up DHCP leasing. Used if this is the only server in the network. <table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table>  | 1     | Enabled.                     | 0     | Disabled. |
| 1  | Enabled.  |       |                              |       |           |
| 0  | Disabled.   |       |                              |       |           |
| Web: Interfaces<br>UCI: dhcp.@dnsmasq[0].interface<br>Opt: list interface                      | Defines the list of interfaces to be served by dnsmasq. If you do not select a specific interface, dnsmasq will serve on all interfaces. Configured interfaces are shown via the web GUI. <table border="1"> <tr> <td>Lan</td> <td>Serve only on LAN interface.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | Lan   | Serve only on LAN interface. | Range |           |
| Lan  | Serve only on LAN interface.  |       |                              |       |           |
| Range  |   |       |                              |       |           |
| Web: Local Server<br>UCI: dhcp.@dnsmasq[0].local<br>Opt: local                                 | Specifies the local domain. Names matching this domain are never forwarded and are resolved from DHCP or host files only. <table border="1"> <tr> <td>/lan/</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | /lan/ |                              | Range |           |
| /lan/  |   |       |                              |       |           |
| Range  |   |       |                              |       |           |
| Web: Local Domain<br>UCI: dhcp.@dnsmasq[0].domain<br>Opt: domain                               | Specifies local domain suffix appended to DHCP names and hosts file entries. <table border="1"> <tr> <td>lan</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | lan   |                              | Range |           |
| lan  |   |       |                              |       |           |
| Range  |   |       |                              |       |           |
| Web: Log Queries<br>UCI: dhcp.@dnsmasq[0].logqueries<br>Opt: logqueries                        | Writes received DNS requests to syslog. <table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0     | Disabled.                    | 1     | Enabled.  |
| 0  | Disabled.   |       |                              |       |           |
| 1  | Enabled.  |       |                              |       |           |
| Web: DNS Forwardings<br>UCI: dhcp.@dnsmasq[0].server<br>Opt: list server                       | List of DNS servers to forward requests to. To forward specific domain requests only, use // syntax. When using UCI, enter multiple servers with a space between them. <table border="1"> <tr> <td></td> <td>No DNS server configured.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  |       | No DNS server configured.    | Range |           |
|  | No DNS server configured.   |       |                              |       |           |
| Range  |   |       |                              |       |           |
| Web: Rebind Protection<br>UCI:<br>dhcp.@dnsmasq[0].rebind_protection<br>Opt: rebind_protection | Enables DNS rebind attack protection by discarding upstream RFC1918 responses. <table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0     | Disabled.                    | 1     | Enabled.  |
| 0  | Disabled.   |       |                              |       |           |
| 1  | Enabled.  |       |                              |       |           |
| Web: Allow Localhost<br>UCI: dhcp.@dnsmasq[0].rebind_localhost<br>Opt: rebind_localhost        | Defines whether to allow upstream responses in the 127.0.0.0/8 range. This is required for DNS-based blacklist services. Only takes effect if rebind protection is enabled. <table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0     | Disabled.                    | 1     | Enabled.  |
| 0  | Disabled.   |       |                              |       |           |
| 1  | Enabled.  |       |                              |       |           |
| Web: Domain Whitelist<br>UCI: dhcp.@dnsmasq[0].rebind_domain<br>Opt: list rebind_domain        | Defines the list of domains to allow RFC1918 responses to. Only takes effect if rebind protection is enabled. When using UCI multiple servers, enter the domains with a space between them. <table border="1"> <tr> <td></td> <td>No list configured.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   |       | No list configured.          | Range |           |
|  | No list configured.   |       |                              |       |           |
| Range  |   |       |                              |       |           |

**Table 114: Information table for general server settings**

## 29.2.2 Dnsmasq: resolv and host files

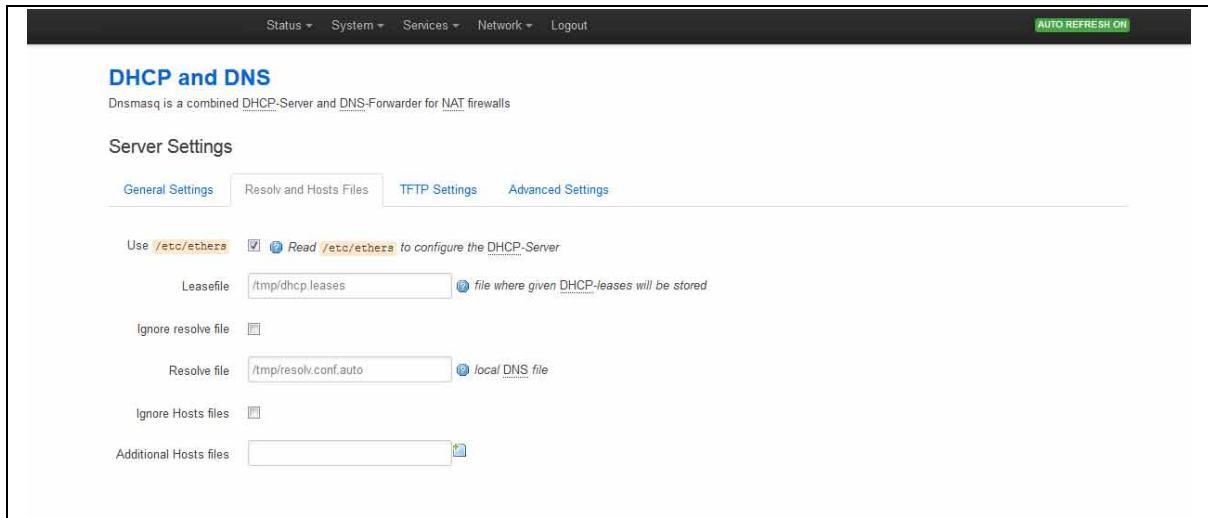


Figure 171: The resolv and host files section

| Web Field/UCI/Package Option  | Description   |                       |                                 |       |                          |
|---|---|-----------------------|---------------------------------|-------|--------------------------|
| Web: Use /etc/ethers<br>UCI: dhcp.@dnsmasq[0].readethers<br>Opt: readethers           | Defines whether static lease entries are read from /etc/ethers. <table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table>  | 1                     | Enabled.                        | 0     | Disabled.                |
| 1   | Enabled.  |                       |                                 |       |                          |
| 0   | Disabled.   |                       |                                 |       |                          |
| Web: Leasefile<br>UCI: dhcp.@dnsmasq[0].leasefile<br>Opt: leasefile                   | Defines the file where given DHCP leases will be stored. The DHCP lease file allows leases to be picked up again if dnsmasq is restarted. <table border="1"> <tr> <td>/tmp/dhcp.leases</td> <td>Store DHCP leases in this file.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table> | /tmp/dhcp.leases      | Store DHCP leases in this file. | Range |                          |
| /tmp/dhcp.leases  | Store DHCP leases in this file.   |                       |                                 |       |                          |
| Range   |   |                       |                                 |       |                          |
| Web: Ignore resolve file<br>UCI: dhcp.@dnsmasq[0].noresolv<br>Opt: noresolv           | Defines whether to use the local DNS file for resolving DNS. <table border="1"> <tr> <td>0</td> <td>Use local DNS file.</td> </tr> <tr> <td>1</td> <td>Ignore local DNS file.</td> </tr> </table>   | 0                     | Use local DNS file.             | 1     | Ignore local DNS file.   |
| 0   | Use local DNS file.   |                       |                                 |       |                          |
| 1   | Ignore local DNS file.  |                       |                                 |       |                          |
| Web: Resolve file<br>UCI: dhcp.@dnsmasq[0].resolvfile<br>Opt: resolvfile              | Defines the local DNS file. <table border="1"> <tr> <td>/tmp/resolv.conf.auto</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | /tmp/resolv.conf.auto |                                 | Range |                          |
| /tmp/resolv.conf.auto   |   |                       |                                 |       |                          |
| Range   |   |                       |                                 |       |                          |
| Web: Ignore Hosts files<br>UCI: dhcp.@dnsmasq[0].nohosts<br>Opt: nohosts              | Defines whether to use local host's files for resolving DNS. <table border="1"> <tr> <td>0</td> <td>Use local hosts file.</td> </tr> <tr> <td>1</td> <td>Ignore local hosts file.</td> </tr> </table>   | 0                     | Use local hosts file.           | 1     | Ignore local hosts file. |
| 0   | Use local hosts file.   |                       |                                 |       |                          |
| 1   | Ignore local hosts file.  |                       |                                 |       |                          |
| Web: Additional Hosts files<br>UCI: dhcp.@dnsmasq[0].addnhosts<br>Opt: list addnhosts | Defines local host's files. When using UCI multiple servers should be entered with a space between them.  |                       |                                 |       |                          |

Table 115: Information table for resolv and host files section



### 29.2.3 Dnsmasq: TFTP settings

Figure 172: The TFTP settings section

| Web Field/UCI/Package Option   | Description  |   |           |   |          |
|--|--|---|-----------|---|----------|
| Web: Enable TFTP server<br>UCI: dhcp.@dnsmasq[0].enable_tftp<br>Opt: enable_tftp | Enables the TFTP server.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0 | Disabled. | 1 | Enabled. |
| 0  | Disabled.  |   |           |   |          |
| 1  | Enabled.   |   |           |   |          |
| Web: TFTP server Root<br>UCI: dhcp.@dnsmasq[0].tftp_root<br>Opt: tftp_root       | Defines root directory for file served by TFTP.  |   |           |   |          |
| Web: Network boot image<br>UCI: dhcp.@dnsmasq[0].dhcp_boot<br>Opt: dhcp_boot     | Defines the filename of the boot image advertised to clients. This specifies BOOTP options, in most cases just the file name.            |   |           |   |          |

Table 116: Information table for TFTP settings

## 29.2.4 Dnsmasq: advanced settings

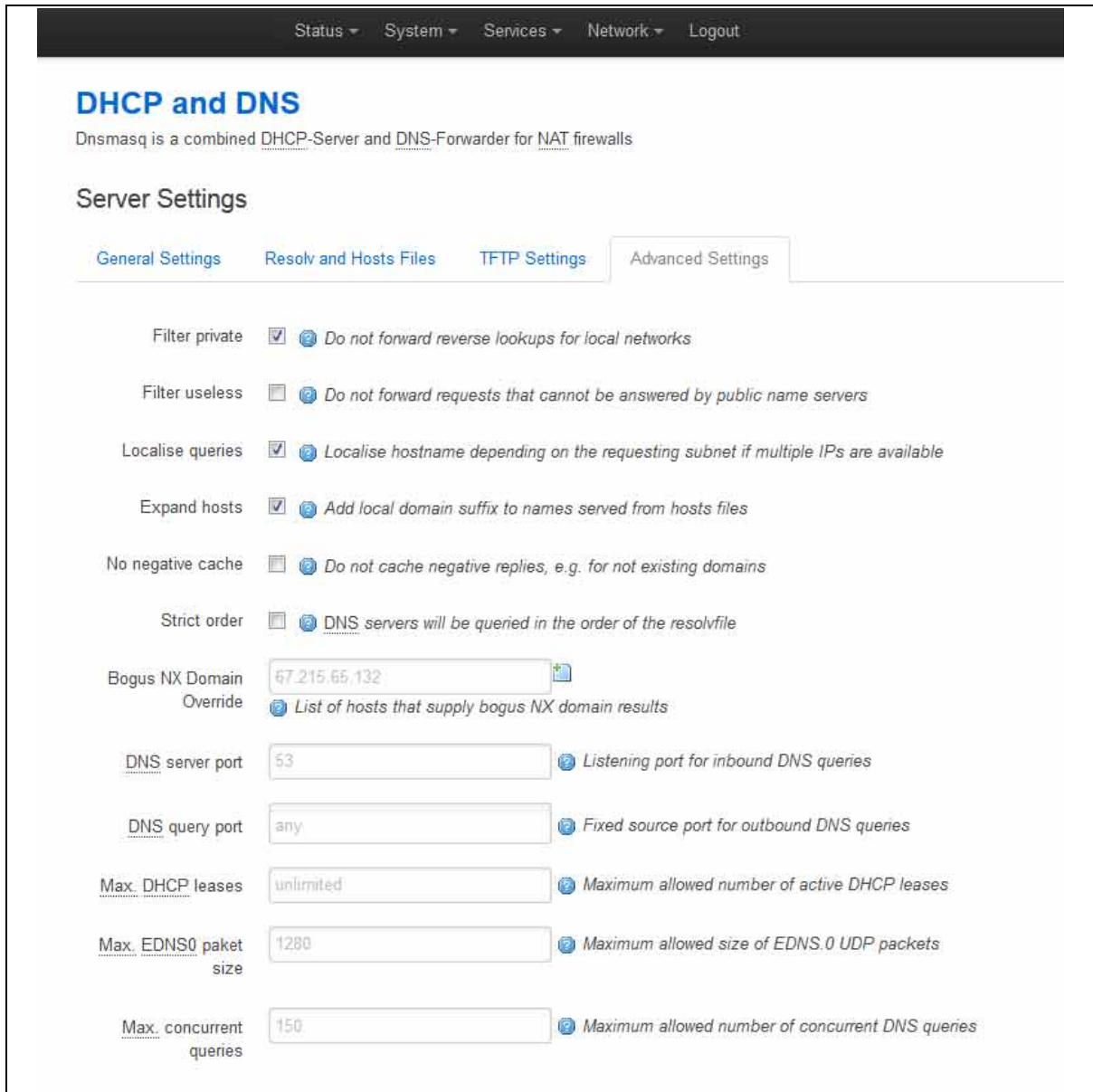


Figure 173: The advanced settings page

| Web Field/UCI/Package Option   | Description   |   |          |   |           |
|--|---|---|----------|---|-----------|
| Web: Filter private<br>UCI: dhcp.@dnsmasq[0].<br>Opt: boguspriv              | <p>Enables disallow option for forwarding reverse lookups for local networks. This rejects reverse lookups to private IP ranges where no corresponding entry exists in /etc/hosts.</p> <table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table> | 1 | Enabled. | 0 | Disabled. |
| 1  | Enabled.  |   |          |   |           |
| 0  | Disabled.   |   |          |   |           |
| Web: Filter useless<br>UCI: dhcp.@dnsmasq[0].filterwin2k<br>Opt: filterwin2k | <p>Enables disallow option for forwarding requests that cannot be answered by public name servers. Normally enabled for dial on demand interfaces.</p> <table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table>                                 | 1 | Enabled. | 0 | Disabled. |
| 1  | Enabled.  |   |          |   |           |
| 0  | Disabled.   |   |          |   |           |

|   |   |            |   |       |                |
|---|---|------------|---|-------|----------------|
| Web: Localise queries<br>UCI: dhcp.@dnsmasq[0].localise_queries<br>Opt: localise_queries        | Defines whether to use an IP address to match the incoming interface if multiple addresses are assigned to a host name in /etc/hosts.<br><table border="1"> <tr><td>1</td><td>Enabled.</td></tr> <tr><td>0</td><td>Disabled.</td></tr> </table> | 1          | Enabled.                                      | 0     | Disabled.      |
| 1   | Enabled.  |            |   |       |                |
| 0   | Disabled.   |            |   |       |                |
| Web: Expand hosts<br>UCI: dhcp.@dnsmasq[0].expandhosts<br>Opt: expandhosts                      | Adds a local domain suffix to names served from host files.<br><table border="1"> <tr><td>1</td><td>Enabled.</td></tr> <tr><td>0</td><td>Disabled.</td></tr> </table>   | 1          | Enabled.                                      | 0     | Disabled.      |
| 1   | Enabled.  |            |   |       |                |
| 0   | Disabled.   |            |   |       |                |
| Web: No negative cache<br>UCI: dhcp.@dnsmasq[0].nonegcache<br>Opt: nonegcache                   | Enable this to stop caching of negative replies. For example, non-existing domains.<br><table border="1"> <tr><td>1</td><td>Enabled.</td></tr> <tr><td>0</td><td>Disabled.</td></tr> </table>   | 1          | Enabled.                                      | 0     | Disabled.      |
| 1   | Enabled.  |            |   |       |                |
| 0   | Disabled.   |            |   |       |                |
| Web: Strict order<br>UCI: dhcp.@dnsmasq[0].strictorder<br>Opt: strictorder                      | Enable this to query DNS servers in the order of the resolve file.<br><table border="1"> <tr><td>1</td><td>Enabled.</td></tr> <tr><td>0</td><td>Disabled.</td></tr> </table>  | 1          | Enabled.                                      | 0     | Disabled.      |
| 1   | Enabled.  |            |   |       |                |
| 0   | Disabled.   |            |   |       |                |
| Web: Bogus NX Domain override<br>UCI: dhcp.@dnsmasq[0].bogusnxdomain<br>Opt: list bogusnxdomain | A list of hosts that supply bogus NX domain results. When using UCI multiple servers, enter the server names with a space between them.<br><table border="1"> <tr><td>Empty list</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>   | Empty list |   | Range |                |
| Empty list  |   |            |   |       |                |
| Range   |   |            |   |       |                |
| Web: DNS server port<br>UCI: dhcp.@dnsmasq[0].port<br>Opt: port                                 | Listening port for inbound DNS queries.<br><table border="1"> <tr><td>53</td><td>Set to <b>0</b> to disable DNS functionality.</td></tr> <tr><td>Range</td><td>0 - 65535</td></tr> </table>   | 53         | Set to <b>0</b> to disable DNS functionality. | Range | 0 - 65535      |
| 53  | Set to <b>0</b> to disable DNS functionality.   |            |   |       |                |
| Range   | 0 - 65535   |            |   |       |                |
| Web: DNS query port<br>UCI: dhcp.@dnsmasq[0].queryport<br>Opt: queryport                        | Defines fixed source port for outbound DNS queries.<br><table border="1"> <tr><td>any</td><td></td></tr> <tr><td>Range</td><td>any; 0 - 65535</td></tr> </table>  | any        |   | Range | any; 0 - 65535 |
| any   |   |            |   |       |                |
| Range   | any; 0 - 65535  |            |   |       |                |
| Web: Max DHCP leases<br>UCI: dhcp.@dnsmasq[0].dhcpleasemax<br>Opt:dhcpleasemax                  | Defines the maximum allowed number of active DHCP leases.<br><table border="1"> <tr><td>unlimited</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>  | unlimited  |   | Range |                |
| unlimited   |   |            |   |       |                |
| Range   |   |            |   |       |                |
| Web: Max EDNS0 packet size<br>UCI: dhcp.@dnsmasq[0].ednspacket_max<br>Opt: ednspacket_max       | Defines the maximum allowed size of EDNS.0 UDP packets in bytes.<br><table border="1"> <tr><td>1280</td><td>1280 bytes</td></tr> <tr><td>Range</td><td></td></tr> </table>  | 1280       | 1280 bytes                                    | Range |                |
| 1280  | 1280 bytes  |            |   |       |                |
| Range   |   |            |   |       |                |
| Web: Max concurrent queries<br>UCI: dhcp.@dnsmasq[0].dnsforwardmax<br>Opt: dnsforwardmax        | Maximum allowed number of concurrent DNS queries.<br><table border="1"> <tr><td>150</td><td>1280 bytes</td></tr> <tr><td>Range</td><td></td></tr> </table>  | 150        | 1280 bytes                                    | Range |                |
| 150   | 1280 bytes  |            |   |       |                |
| Range   |   |            |   |       |                |

**Table 117: Information table for advanced settings**

### 29.2.5 Active leases

This section displays all currently active leases.



**Figure 174: The active leases section**

| Web Field/UCI/Package Option                      | Description                             |
|---|---|
| Web: Hostname<br>UCI: n/a<br>Opt: n/a             | Displays the hostname of the client.    |
| Web: IPv4 Address<br>UCI: n/a<br>Opt: n/a         | Displays the IP address of the client.  |
| Web: MAC Address<br>UCI: n/a<br>Opt: n/a          | Displays the MAC address of the client. |
| Web: Lease time remaining<br>UCI: n/a<br>Opt: n/a | Displays the remaining lease time.      |

**Table 118: Information table for active leases section**

### 29.2.6 Static leases

Use static leases to assign fixed IP addresses and symbolic hostnames to DHCP clients. Static leases are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served. Click **Add** to add a new lease entry.

**Figure 175: The static leases section**

| Web Field/UCI/Package Option                           | Description  |   |          |   |           |
|--|--|---|----------|---|-----------|
| Web: Hostname<br>UCI: dhcp.@host[0].name<br>Opt: name  | Defines the optional symbolic name to assign to this static DHCP entry.<br><table border="1" style="width: 100%;"> <tr> <td style="width: 20px; text-align: center;">1</td> <td>Enabled.</td> </tr> <tr> <td style="width: 20px; text-align: center;">0</td> <td>Disabled.</td> </tr> </table> | 1 | Enabled. | 0 | Disabled. |
| 1  | Enabled.   |   |          |   |           |
| 0  | Disabled.  |   |          |   |           |
| Web: MAC Address<br>UCI: dhcp.@host[0].mac<br>Opt: mac | Defines the hardware address that identifies the host.   |   |          |   |           |
| Web: IPv4 Address<br>UCI: dhcp.@host[0].ip<br>Opt: ip  | The IPv4 address specifies the fixed address to use for this host.   |   |          |   |           |

**Table 119: Information table for static leases**

## 29.2.7 Configuring DHCP pools using the web

DHCP pools are configured via the interface configuration.

Select **Network -> Interfaces**. Choose the interface you want to add the DHCP pool to and select **Edit**. Scroll to **DHCP Server** section.

**Note:** this section is only available for interfaces with a static IP address.

To assign a DHCP Server to the interface, click **Setup DHCP Server**.



Figure 176: The DHCP Server settings section

The DHCP Server configuration options will appear. The DHCP Server is divided into two sub sections: General Setup and Advanced Settings.

### 29.2.7.1 DHCP server: general setup

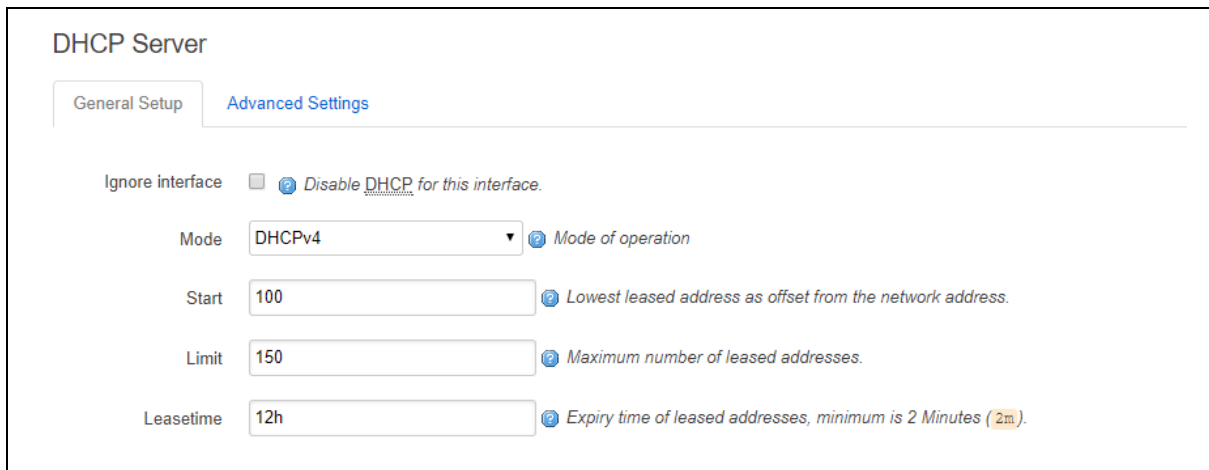


Figure 177: The DHCP server general setup section

| Web Field/UCI/Package Option                                      | Description   |   |           |   |          |
|---|---|---|-----------|---|----------|
| Web: Ignore interface<br>UCI: dhcp.@dhcp[x].ignore<br>Opt: ignore | Defines whether the DHCP pool should be enabled for this interface. If not specified for the DHCP pool then the default is disabled i.e. dhcp pool enabled. |   |           |   |          |
|   | <table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0 | Disabled. | 1 | Enabled. |
| 0   | Disabled.   |   |           |   |          |
| 1   | Enabled.  |   |           |   |          |

| <p>Web: Mode<br/>UCI: dhcp.@dhcp[x].mode<br/>Opt: mode</p>                | <p>Defines whether the DHCP pool should be enabled for this interface. If not specified for the DHCP pool then the default is disabled i.e. dhcp pool enabled.</p> <table border="1" data-bbox="683 277 1396 506"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>DHCPv4</td> <td>DHCP for IPv4</td> <td>ipv4</td> </tr> <tr> <td>DHCPv6</td> <td>DHCP for IPv6</td> <td>ipv6_dhcp</td> </tr> <tr> <td>IPv6 Router Advertisements</td> <td>IPv6 RA</td> <td>ipv6_ra</td> </tr> <tr> <td>DHCPv6 Prefix Delegation</td> <td>DHCPv6 prefix delegation</td> <td>ipv6_pd</td> </tr> </tbody> </table>   | Web       | Description   | UCI   | DHCPv4  | DHCP for IPv4 | ipv4 | DHCPv6 | DHCP for IPv6 | ipv6_dhcp | IPv6 Router Advertisements | IPv6 RA | ipv6_ra | DHCPv6 Prefix Delegation | DHCPv6 prefix delegation | ipv6_pd |
|---|---|-----------|---|-------|---------|---------------|------|--------|---------------|-----------|----------------------------|---------|---------|--------------------------|--------------------------|---------|
| Web   | Description   | UCI       |   |       |         |               |      |        |               |           |                            |         |         |                          |                          |         |
| DHCPv4  | DHCP for IPv4   | ipv4      |   |       |         |               |      |        |               |           |                            |         |         |                          |                          |         |
| DHCPv6  | DHCP for IPv6   | ipv6_dhcp |   |       |         |               |      |        |               |           |                            |         |         |                          |                          |         |
| IPv6 Router Advertisements  | IPv6 RA   | ipv6_ra   |   |       |         |               |      |        |               |           |                            |         |         |                          |                          |         |
| DHCPv6 Prefix Delegation  | DHCPv6 prefix delegation  | ipv6_pd   |   |       |         |               |      |        |               |           |                            |         |         |                          |                          |         |
| <p>Web: Start<br/>UCI: dhcp.@dhcp[x].start<br/>Opt: start</p>             | <p>Defines the offset from the network address for the start of the DHCP pool.<br/>Example: for network address 192.168.100.10/24, start=100, DHCP allocation pool will start at 192.168.100.100.<br/>For subnets greater than /24, it may be greater than 255 to span subnets. Alternatively, specify in IP address notation using the wildcard '0' where the octet is required to inherit bits from the interface IP address.<br/>Example: to define a DHCP scope starting from 10.1.20.0 on an interface with 10.1.0.0/16 address, set start to <b>0.0.20.1</b></p> <table border="1" data-bbox="683 797 1332 869"> <tr> <td>100</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table> | 100       |   | Range |         |               |      |        |               |           |                            |         |         |                          |                          |         |
| 100   |   |           |   |       |         |               |      |        |               |           |                            |         |         |                          |                          |         |
| Range   |   |           |   |       |         |               |      |        |               |           |                            |         |         |                          |                          |         |
| <p>Web: Limit<br/>UCI: dhcp.@dhcp[x].limit<br/>Opt: limit</p>             | <p>Defines the size of the address pool.<br/>Example: For network address 192.168.100.10/24, start=100, limit=150, DHCP allocation pool will be .100 to .249</p> <table border="1" data-bbox="683 965 1332 1061"> <tr> <td>150</td> <td>Limits DHCP allocation pool to 150 available address.</td> </tr> <tr> <td>Range</td> <td>0 - 255</td> </tr> </table>  | 150       | Limits DHCP allocation pool to 150 available address. | Range | 0 - 255 |               |      |        |               |           |                            |         |         |                          |                          |         |
| 150   | Limits DHCP allocation pool to 150 available address.   |           |   |       |         |               |      |        |               |           |                            |         |         |                          |                          |         |
| Range   | 0 - 255   |           |   |       |         |               |      |        |               |           |                            |         |         |                          |                          |         |
| <p>Web: Leasetime<br/>UCI: dhcp.@dhcp[x].leasetime<br/>Opt: leasetime</p> | <p>Defines the lease time of addresses handed out to clients, for example 12h or 30m.</p> <table border="1" data-bbox="683 1122 1332 1196"> <tr> <td>12h</td> <td>12 hours</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 12h       | 12 hours  | Range |         |               |      |        |               |           |                            |         |         |                          |                          |         |
| 12h   | 12 hours  |           |   |       |         |               |      |        |               |           |                            |         |         |                          |                          |         |
| Range   |   |           |   |       |         |               |      |        |               |           |                            |         |         |                          |                          |         |
| <p>Web: n/a<br/>UCI: dhcp.@dhcp[x].interface<br/>Opt: interface</p>       | <p>Defines the interface that is served by this DHCP pool. This must be one of the configured interfaces.<br/>When configured through the web UI this will be automatically populated with the interface name.</p>  |           |   |       |         |               |      |        |               |           |                            |         |         |                          |                          |         |

Table 120: Information table for DHCP server general setup page

### 29.2.7.2 DHCP server: advanced settings

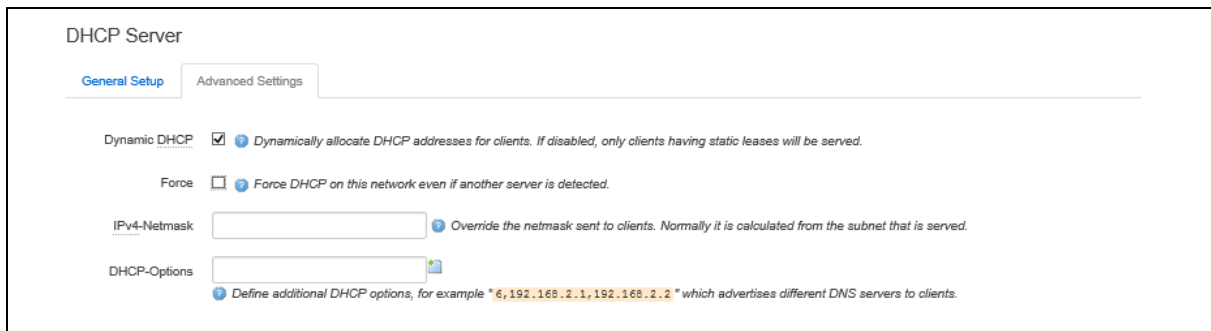


Figure 178: The DHCP server advanced settings section

| Web Field/UCI/Package Option   | Description   |   |                                    |        |   |
|--|---|---|------------------------------------|--------|---|
| Web: Dynamic DHCP<br>UCI: dhcp.@dhcp[x].dynamicdhcp<br>Opt: dynamicdhcp      | Defines whether to dynamically allocate DHCP leases.<br><table border="1"> <tr> <td>1</td> <td>Dynamically allocate leases.</td> </tr> <tr> <td>0</td> <td>Use /etc/ethers file for serving DHCP leases.</td> </tr> </table>  | 1 | Dynamically allocate leases.       | 0      | Use /etc/ethers file for serving DHCP leases. |
| 1  | Dynamically allocate leases.  |   |                                    |        |   |
| 0  | Use /etc/ethers file for serving DHCP leases.   |   |                                    |        |   |
| Web: Force<br>UCI: dhcp.@dhcp[x].force<br>Opt: force                         | Forces DHCP serving on the specified interface even if another DHCP server is detected on the same network segment.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0 | Disabled.                          | 1      | Enabled.                                      |
| 0  | Disabled.   |   |                                    |        |   |
| 1  | Enabled.  |   |                                    |        |   |
| Web: IPv4-Netmask<br>UCI: dhcp.@dhcp[x].netmask<br>Opt: netmask              | Defines a netmask sent to clients that overrides the netmask as calculated from the interface subnet.<br><table border="1"> <tr> <td></td> <td>Use netmask from interface subnet.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   |   | Use netmask from interface subnet. | Range  |   |
|  | Use netmask from interface subnet.  |   |                                    |        |   |
| Range  |   |   |                                    |        |   |
| Web: DHCP-Options<br>UCI: dhcp.@dhcp[x].dhcp_option<br>Opt: list dhcp_option | Defines additional options to be added for this dhcp pool.<br>For example, with 'list dhcp_option 26,1470' or 'list dhcp_option mtu, 1470' you can assign a specific MTU per DHCP pool. Your client must accept the MTU option for this to work. Options that contain multiple values should be separated by a comma.<br>Example: list dhcp_option 6,192.168.2.1,192.168.2.2<br><table border="1"> <tr> <td></td> <td>No options defined.</td> </tr> <tr> <td>Syntax</td> <td>Option_number, option_value</td> </tr> </table> |   | No options defined.                | Syntax | Option_number, option_value                   |
|  | No options defined.   |   |                                    |        |   |
| Syntax   | Option_number, option_value   |   |                                    |        |   |
| Web: n/a<br>UCI: dhcp.@dhcp[x].networkid<br>Opt: networkid                   | Assigns a network-id to all clients that obtain an IP address from this pool.<br><table border="1"> <tr> <td></td> <td>Use network from interface subnet.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   |   | Use network from interface subnet. | Range  |   |
|  | Use network from interface subnet.  |   |                                    |        |   |
| Range  |   |   |                                    |        |   |

Table 121: Information table for DHCP advanced settings page

## 29.3 Configuring DHCP and DNS using command line

Possible section types of the DHCP configuration file include Common Options (dnsmasq), DHCP Pools (dhcp) and Static Leases (host). Not all types may appear in the file and most of them are only needed for special configurations.

### 29.3.1 Dnsmasq using command line

The configuration section type **dnsmasq** determines values and options relevant to the overall operation of dnsmasq and the DHCP options on all interfaces served.

#### 29.3.1.1 Dnsmasq using UCI

```
root@VA_router:~# uci show dhcp
dhcp.@dnsmasq[0]=dnsmasq
dhcp.@dnsmasq[0].domainneeded=1
dhcp.@dnsmasq[0].boguspriv=1
dhcp.@dnsmasq[0].filterwin2k=0
dhcp.@dnsmasq[0].localise_queries=1
dhcp.@dnsmasq[0].logqueries=1
dhcp.@dnsmasq[0].rebind_protection=1
dhcp.@dnsmasq[0].rebind_localhost=1
```

```

dhcp.@dnsmasq[0].local=/lan/
dhcp.@dnsmasq[0].domain=lan
dhcp.@dnsmasq[0].expandhosts=1
dhcp.@dnsmasq[0].nonegcache=0
dhcp.@dnsmasq[0].authoritative=1
dhcp.@dnsmasq[0].readethers=1
dhcp.@dnsmasq[0].leasefile=/tmp/dhcp.leases
dhcp.@dnsmasq[0].noresolve=0
dhcp.@dnsmasq[0].resolvfile=/tmp/resolv.conf.auto
dhcp.@dnsmasq[0].nohosts=0
dhcp.@dnsmasq[0].addnhosts=hostfile1 hostfile2
dhcp.@dnsmasq[0].interface=lan
dhcp.@dnsmasq[0].server=1.1.1.1 2.2.2.2
dhcp.@dnsmasq[0].rebind domain=tes.domain
dhcp.@dnsmasq[0].enable_tftp=0
dhcp.@dnsmasq[0].tftp_root=/tmp/tftp
dhcp.@dnsmasq[0].dhcp_boot=boot.image
dhcp.@dnsmasq[0].nonegcache=0
dhcp.@dnsmasq[0].strictorder=0
dhcp.@dnsmasq[0].bogusnxdomain=1.1.1.1 2.2.2.2
dhcp.@dnsmasq[0].port=53
dhcp.@dnsmasq[0].dhcp_lease_max=150
dhcp.@dnsmasq[0].ednspacket_max=1280
dhcp.@dnsmasq[0].dnsforwardmax=150

```

### 29.3.1.2 Dnsmasq using package options

```

root@VA_router:~# uci show dhcp
config 'dnsmasq'
    option domainneeded '1'
        option rebind_protection '1'
        option rebind_localhost '1'
    option local '/lan/'
    option domain 'lan'
    option authoritative '1'
    option readethers '1'
    option leasefile '/tmp/dhcp.leases'
    list interface 'lan'

```



```

list server '1.2.3.4'
list server '4.5.6.7'
list rebind_domain 'test1.domain'
list rebind_domain 'tes2.domain'
option logqueries '1'
option resolvfile '/tmp/resolv1.conf.auto'
list addnhosts 'hosts1'
list addnhosts 'hosts2'
option enable_tftp '1'
option tftp_root '/tmp/tftp'
option dhcp_boot 'boot.image'
option filterwin2k '1'
option nonegcache '1'
option strictorder '1'
list bogusnxdomain '1.1.1.1 '
list bogusnxdomain '2.2.2.2'
option port '53'
option dhcp_lease_max '150'
option edns_packet_max '1280'
option dns_forward_max '150'

```

Options `local` and `domain` enable dnsmasq to serve entries in `/etc/hosts` as well as the DHCP client's names as if they were entered into the LAN DNS domain.

For options `domainneeded`, `boguspriv`, `localise_queries`, and `expandhosts` make sure that requests for these local host names (and the reverse lookup) never get forwarded to the upstream DNS servers.

### 29.3.2 Configuring static leases using command line

Static leases are configured under the `dhcp` package, stored at `/etc/config/dhcp`.

By default, all static leases instances are named `host`. The static lease is identified by `@host` then the static lease position in the package as a number. For example, for the first static lease in the package using UCI:

```

dhcp.@host[0]=dhcp
dhcp.@host[0].name=mypc

```

Or using package options:

```

config host
    option name 'mypc'

```

However, to better identify, it is recommended to give the static lease instance a name. For example, to create a static instance named mypc.

To define a named static lease instance using UCI, enter:

```
dhcp.mypc=host
dhcp.mypc.name=mypc
```

To define a named static lease instance using package options, enter:

```
config dhcp 'mypc'
    option name 'mypc'
```

The following example adds the fixed IP address 192.168.1.2 and the name "mypc" for a machine with the (Ethernet) hardware address 00:11:22:33:44:55.

### 29.3.2.1 Static leases using UCI

```
root@VA_router:~# uci show dhcp.mypc
dhcp.mypc=host
dhcp.mypc.ip=192.168.1.2
dhcp.mypc.mac=00:11:22:33:44:55
dhcp.mypc.name=mypc
```

### 29.3.2.2 Static leases using package options

```
root@VA_router:~# uci export dhcp
package dhcp
.....
config host 'mypc'
    option ip          '192.168.1.2'
    option mac         '00:11:22:33:44:55'
    option name        'mypc'
```

## 29.3.3 Configuring DHCP pools using command line

DHCP pools are configured under the dhcp package, stored at **/etc/config/dhcp**.

Sections of the type **dhcp** specify per interface lease pools and settings. Typically, there is at least one section of this type present in the **/etc/config/dhcp** file to cover the LAN interface.

You can disable a lease pool for a specific interface by specifying the ignore option in the corresponding section.

You can configure multiple dhcp pools.

By default, all dhcp pool instances are named 'dhcp'. The instance is identified by @dhcp then the dhcp pool position in the package as a number. For example, for the first dhcp pool in the package using UCI:

```
dhcp.@dhcp[0]=dhcp
dhcp.@dhcp[0].interface=LAN
```

Or using package options:

```
config dhcp
    option interface 'LAN'
```

However, to better identify, it is recommended to give the dhcp pool instance a name. For example, to create a dhcp pool instance named LAN.

To define a named dhcp pool instance using UCI, enter:

```
dhcp.LAN=dhcp
dhcp.LAN.interface=LAN
```

To define a named dhcp pool instance using package options, enter:

```
config dhcp 'LAN'
    option interface 'LAN'
```

### 29.3.3.1 Configuring DHCP pools using UCI

```
root@VA_router:~# uci show dhcp.LAN
dhcp.LAN=dhcp
dhcp.LAN.interface=lan
dhcp.LAN.start=100
dhcp.LAN.limit=150
dhcp.LAN.leasetime=12h
dhcp.LAN.ignore=0
```

### 29.3.3.2 Configuring DHCP pools using package options

```
root@VA_router:~# uci export dhcp
package dhcp
...
config 'dhcp' 'LAN'
    option 'interface'    'LAN'
    option 'start'        '100'
    option 'limit'        '150'
    option 'leasetime'    '12h'
    option ignore         0
```

## 30 Configuring DHCP client

This section describes how to configure an interface as a DHCP client. This section will only detail the configuration for DHCP client. For information on how to configure other interface options such as firewall zone, mapping of switch ports, etc, read the standard interface configuration document.

### 30.1 Configuration packages used

| Package | Sections  |
|---------|-----------|
| network | interface |

### 30.2 Configuring DHCP client using the web interface

DHCP client is configured under the interface configuration by setting the interface protocol to DHCP Client. To create and edit interfaces via the web interface, in the top menu, click **Network -> Interfaces**. The Interfaces overview page appears.

The screenshot shows the 'Interfaces' overview page in a network management web interface. The top navigation bar includes 'Status', 'System', 'Services', 'Network', and 'Logout'. The main content area is titled 'Interfaces' and 'Interface Overview'. It features a table with columns for 'Network' and 'Status'. A dropdown menu is open over the 'Network' column, listing various protocols and services. The table lists several interfaces, including LAN, LAN1, LOOPBACK, WAN, WAN1, and WAN2, each with associated statistics and actions (Connect, Stop, Edit, Delete). Below the table, there are sections for 'Port Map' and 'ATM Bridges'.

Figure 179: The interfaces overview page

There are three sections in the Interfaces page.

| Section            | Description  |
|--------------------|--|
| Interface Overview | Shows existing interfaces and their status. You can create new, and edit existing interfaces here.   |
| Port Map           | In this section you can map device ports to Ethernet interfaces. Ports are marked with capital letters starting with 'A'. Type in space-separated port character in the port map fields. |
| ATM Bridges        | ATM bridges expose encapsulated Ethernet in AAL5 connections as virtual Linux network interfaces, which can be used in conjunction with DHCP or PPP to dial into the provider network.   |

### 30.2.1 Editing an existing interface for DHCP client

To edit an existing interface, from the interface tabs at the top of the page, select the interface you wish to configure. Alternatively, click **Edit** in the interface's row.

### 30.2.2 Creating a new interface for DHCP client

To create a new interface, in the Interface Overview section, click **Add new interface**. The Create Interface page appears.

The screenshot shows the 'Create Interface' page in the VA\_router interface. The page has a navigation bar at the top with 'VA\_router', 'Status', 'System', 'Services', 'Network', and 'Logout'. The main heading is 'Create Interface'. Below the heading, there are several form fields and options:

- Name of the new interface:** A text input field containing 'LAN'. To the right, a tooltip indicates: 'The allowed characters are: A-Z, a-z, 0-9 and \_'.
- Protocol of the new interface:** A dropdown menu set to 'DHCP client'.
- Create a bridge over multiple interfaces:** An unchecked checkbox.
- Cover the following interface:** A list of radio buttons next to various Ethernet Adapters:
  - Ethernet Adapter: "eth0"
  - Ethernet Adapter: "eth1" (lan2)
  - Ethernet Adapter: "eth2"
  - Ethernet Adapter: "eth3"
  - Ethernet Adapter: "eth4"
  - Ethernet Adapter: "eth5"
  - Ethernet Adapter: "eth6"
  - Ethernet Adapter: "eth7"
  - Ethernet Adapter: "lo" (loopback)
  - Ethernet Adapter: "teql0"
  - Ethernet Adapter: "tunl0"
  - Custom Interface:
- Note:** A blue information icon followed by the text: 'Note: If you select an interface in this menu which is already a part of another network, it will be moved from that network to this network.'
- Buttons:** 'Back to Overview' and 'Submit' buttons at the bottom.

Figure 180: The create interface page

| Web Field/UCI/Package Option  | Description  |        |             |        |   |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |
|---|--|--------|-------------|--------|---|--|--------|-------------|---|------|-----------|-------------|-------|------------------------|---------------------------|--|----------------|-------------------------------------|--|-----|--|--|-----|--|--|------|-----------------------------|--|-----|-------------------------|--|-------|-------------------|--|---------|--------------|--|---------------------|---|--|
| Web: Name of the new interface<br>UCI: network.<if name><br>Opt: config interface         | Assigns a logical name to the interface. The network interface section will assign this name (<if name>).<br>Type the name of the new interface.<br>Allowed characters are A-Z, a-z, 0-9 and _   |        |             |        |   |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |
| Web: Protocol of the new interface<br>UCI: network.<if name>.proto<br>Opt: proto          | Specifies what protocol the interface will operate on. Select <b>DHCP Client</b> . <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Static</td> <td>Static configuration with fixed address and netmask.</td> <td>Static</td> </tr> <tr> <td>DHCP Client</td> <td>Address and netmask are assigned by DHCP.</td> <td>dhcp</td> </tr> <tr> <td>Unmanaged</td> <td>Unspecified</td> <td>Empty</td> </tr> <tr> <td>IPv6-in-IPv4 (RFC4213)</td> <td>Used with tunnel brokers.</td> <td></td> </tr> <tr> <td>IPv6-over-IPv4</td> <td>Stateless IPv6 over IPv4 transport.</td> <td></td> </tr> <tr> <td>GRE</td> <td>Generic Routing Encapsulation protocol</td> <td></td> </tr> <tr> <td>IOT</td> <td></td> <td></td> </tr> <tr> <td>L2TP</td> <td>Layer 2 Tunnelling Protocol</td> <td></td> </tr> <tr> <td>PPP</td> <td>Point to Point Protocol</td> <td></td> </tr> <tr> <td>PPPoE</td> <td>PPP over Ethernet</td> <td></td> </tr> <tr> <td>PPPoATM</td> <td>PPP over ATM</td> <td></td> </tr> <tr> <td>LTE/UMTS/GPRS/EV-DO</td> <td>CDMA, UMTS or GPRS connection using an AT-style 3G modem.</td> <td></td> </tr> </tbody> </table> | Option | Description | UCI    | Static  | Static configuration with fixed address and netmask. | Static | DHCP Client | Address and netmask are assigned by DHCP. | dhcp | Unmanaged | Unspecified | Empty | IPv6-in-IPv4 (RFC4213) | Used with tunnel brokers. |  | IPv6-over-IPv4 | Stateless IPv6 over IPv4 transport. |  | GRE | Generic Routing Encapsulation protocol |  | IOT |  |  | L2TP | Layer 2 Tunnelling Protocol |  | PPP | Point to Point Protocol |  | PPPoE | PPP over Ethernet |  | PPPoATM | PPP over ATM |  | LTE/UMTS/GPRS/EV-DO | CDMA, UMTS or GPRS connection using an AT-style 3G modem. |  |
| Option  | Description  | UCI    |             |        |   |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |
| Static  | Static configuration with fixed address and netmask.   | Static |             |        |   |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |
| DHCP Client   | Address and netmask are assigned by DHCP.  | dhcp   |             |        |   |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |
| Unmanaged   | Unspecified  | Empty  |             |        |   |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |
| IPv6-in-IPv4 (RFC4213)  | Used with tunnel brokers.  |        |             |        |   |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |
| IPv6-over-IPv4  | Stateless IPv6 over IPv4 transport.  |        |             |        |   |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |
| GRE   | Generic Routing Encapsulation protocol   |        |             |        |   |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |
| IOT   |  |        |             |        |   |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |
| L2TP  | Layer 2 Tunnelling Protocol  |        |             |        |   |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |
| PPP   | Point to Point Protocol  |        |             |        |   |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |
| PPPoE   | PPP over Ethernet  |        |             |        |   |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |
| PPPoATM   | PPP over ATM   |        |             |        |   |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |
| LTE/UMTS/GPRS/EV-DO   | CDMA, UMTS or GPRS connection using an AT-style 3G modem.  |        |             |        |   |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |
| Web: Create a bridge over multiple interfaces<br>UCI: network.<if name>.type<br>Opt: type | If you select this option, then the new logical interface created will act as a bridging interface between the chosen existing physical interfaces. <table border="1"> <tbody> <tr> <td>Empty</td> <td></td> </tr> <tr> <td>Bridge</td> <td>Configures a bridge over multiple interfaces.</td> </tr> </tbody> </table>   | Empty  |             | Bridge | Configures a bridge over multiple interfaces. |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |
| Empty   |  |        |             |        |   |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |
| Bridge  | Configures a bridge over multiple interfaces.  |        |             |        |   |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |
| Web: Cover the following interface<br>UCI: network.<if name>.ifname<br>Opt: ifname        | Physical interface name to assign to this logical interface. If creating a bridge over multiple interfaces select two interfaces to bridge. When using UCI, the interface names should be separated by a space e.g. option ifname 'eth2 eth3'.   |        |             |        |   |  |        |             |   |      |           |             |       |                        |                           |  |                |                                     |  |     |  |  |     |  |  |      |                             |  |     |                         |  |       |                   |  |         |              |  |                     |   |  |

**Table 122: Information table for the create new interface page**

Click **Submit**. The Interface configuration page appears. There are three sections:

| Section              | Description  |
|----------------------|--|
| Common Configuration | Configure the interface settings such as protocol, IP address, gateway, netmask, custom DNS servers, MTU and firewall configuration. |
| IP-Aliases           | Assign multiple IP addresses to the interface.   |
| DHCP Server          | Configure DHCP server settings for this interface.   |

### 30.2.3 Common configuration

The Common Configuration section has four sub-sections.

| Section           | Description   |
|-------------------|---|
| General Setup     | Configure the basic interface settings such as protocol, IP address, gateway, netmask, custom DNS servers.  |
| Advanced Settings | 'Bring up on boot', 'Monitor interface state', Override MAC address, Override MTU and 'Use gateway metric'. |
| Physical Settings | Bridge interfaces, VLAN PCP to SKB priority mapping.  |
| Firewall settings | Assign a firewall zone to the interface.  |

Only General Setup and Advanced Settings have DHCP client option configuration options

#### 30.2.3.1 Common configuration: general setup

The screenshot displays the 'Common Configuration' interface for the DHCP client protocol. It features four tabs: 'General Setup' (selected), 'Advanced Settings', 'Physical Settings', and 'Firewall Settings'. The 'Status' section shows the interface 'eth3' with a MAC address of '00:E0:C8:D3:18:20' and statistics for RX and TX. The 'Protocol' is set to 'DHCP client'. The 'Hostname to send when requesting DHCP' is 'VA\_router'. There are two unchecked checkboxes: 'Accept router advertisements' and 'Send router solicitations'.

Figure 181: The interface general setup configuration page for DHCP client protocol

| Web Field/UCI/Package Option   | Description  |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
|--|--|--------|---|--------|--|-------------|---|-----------|-------------|------------------------|---------------------------|----------------|-------------------------------------|-----|--|-----|--|------|------------------------------|-----|-------------------------|-------|-------------------|---------|--------------|---------------------|---|
| Web: Status  | Shows the current status of the interface.   |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| Web: Protocol<br>UCI: network.<if name>.proto<br>Opt: proto                                    | <p>Protocol type. The interface protocol may be one of the options shown below. The protocol selected in the previous step will be displayed as default but can be changed if required.</p> <p>Select <b>DHCP Client</b>.</p> <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Static</td> <td>Static configuration with fixed address and netmask.</td> </tr> <tr> <td>DHCP Client</td> <td>Address and netmask are assigned by DHCP.</td> </tr> <tr> <td>Unmanaged</td> <td>Unspecified</td> </tr> <tr> <td>IPv6-in-IPv4 (RFC4213)</td> <td>Used with tunnel brokers.</td> </tr> <tr> <td>IPv6-over-IPv4</td> <td>Stateless IPv6 over IPv4 transport.</td> </tr> <tr> <td>GRE</td> <td>Generic Routing Encapsulation protocol</td> </tr> <tr> <td>IOT</td> <td></td> </tr> <tr> <td>L2TP</td> <td>Layer 2 Tunnelling Protocol.</td> </tr> <tr> <td>PPP</td> <td>Point-to-Point protocol</td> </tr> <tr> <td>PPPoE</td> <td>PPP over Ethernet</td> </tr> <tr> <td>PPPoATM</td> <td>PPP over ATM</td> </tr> <tr> <td>LTE/UMTS/GPRS/EV-DO</td> <td>CDMA, UMTS or GPRS connection using an AT-style 3G modem.</td> </tr> </tbody> </table> | Option | Description                                 | Static | Static configuration with fixed address and netmask. | DHCP Client | Address and netmask are assigned by DHCP. | Unmanaged | Unspecified | IPv6-in-IPv4 (RFC4213) | Used with tunnel brokers. | IPv6-over-IPv4 | Stateless IPv6 over IPv4 transport. | GRE | Generic Routing Encapsulation protocol | IOT |  | L2TP | Layer 2 Tunnelling Protocol. | PPP | Point-to-Point protocol | PPPoE | PPP over Ethernet | PPPoATM | PPP over ATM | LTE/UMTS/GPRS/EV-DO | CDMA, UMTS or GPRS connection using an AT-style 3G modem. |
| Option   | Description  |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| Static   | Static configuration with fixed address and netmask.   |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| DHCP Client  | Address and netmask are assigned by DHCP.  |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| Unmanaged  | Unspecified  |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| IPv6-in-IPv4 (RFC4213)   | Used with tunnel brokers.  |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| IPv6-over-IPv4   | Stateless IPv6 over IPv4 transport.  |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| GRE  | Generic Routing Encapsulation protocol   |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| IOT  |  |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| L2TP   | Layer 2 Tunnelling Protocol.   |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| PPP  | Point-to-Point protocol  |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| PPPoE  | PPP over Ethernet  |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| PPPoATM  | PPP over ATM   |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| LTE/UMTS/GPRS/EV-DO  | CDMA, UMTS or GPRS connection using an AT-style 3G modem.  |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| Web: Hostname to send when requesting DHCP<br>UCI: network.<if name>.hostname<br>Opt: hostname | Defines the hostname to include in DHCP requests   |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| Web: Accept router advertisements<br>UCI: network.<if name>.accept_ra<br>Opt: accept_ra        | <p>Specifies whether to accept IPv6 Router Advertisements on this interface (optional).</p> <p><b>Note:</b> default is <b>1</b> if protocol is set to DHCP, otherwise the setting defaults to <b>0</b>.</p> <table border="1"> <tbody> <tr> <td>0</td> <td>Does not accept IPv6 router advertisements.</td> </tr> <tr> <td>1</td> <td>Accepts IPv6 router advertisements.</td> </tr> </tbody> </table>   | 0      | Does not accept IPv6 router advertisements. | 1      | Accepts IPv6 router advertisements.                  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| 0  | Does not accept IPv6 router advertisements.  |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| 1  | Accepts IPv6 router advertisements.  |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| Web: Send router solicitations<br>UCI: network.<if name>.send_rs<br>Opt: send_rs               | <p>Specifies whether to send router solicitations on this interface (optional).</p> <p><b>Note:</b> defaults to <b>1</b> for static protocol, otherwise the setting defaults to <b>0</b>.</p> <table border="1"> <tbody> <tr> <td>0</td> <td>Does not send router solicitations.</td> </tr> <tr> <td>1</td> <td>Sends router solicitations.</td> </tr> </tbody> </table>   | 0      | Does not send router solicitations.         | 1      | Sends router solicitations.                          |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| 0  | Does not send router solicitations.  |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |
| 1  | Sends router solicitations.  |        |   |        |  |             |   |           |             |                        |                           |                |                                     |     |  |     |  |      |                              |     |                         |       |                   |         |              |                     |   |

**Table 123: Information table for general setup configuration settings for DHCP client protocol**



### 30.2.3.2 Common configuration: advanced settings

**Common Configuration**

[General Setup](#) | 
 [Advanced Settings](#) | 
 [Physical Settings](#) | 
 [Firewall Settings](#)

---

Bring up on boot

Monitor interface state  This interface state would be reported to VA Monitor via keep-alive

Use broadcast flag  Required for certain ISPs, e.g. Charter with DOCSIS 3

Use default gateway  If unchecked, no default route is configured

Use DNS servers advertised by peer  If unchecked, the advertised DNS server addresses are ignored

Use gateway metric

Client ID to send when requesting DHCP

Vendor Class to send when requesting DHCP

Override MAC address

Override MTU

Dependant interfaces  ADSL:

LAN3:

**Figure 182: The interface advanced settings page for DHCP client protocol**

| Web Field/UCI/Package Option   | Description   |   |  |   |          |
|--|---|---|--|---|----------|
| Web: Bring up on boot<br>UCI: network.<if name>.auto<br>Opt: auto                  | Enables the interface to connect automatically on boot up.<br><table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0 | Disabled.                                | 1 | Enabled. |
| 0  | Disabled.   |   |  |   |          |
| 1  | Enabled.  |   |  |   |          |
| Web: Monitor interface state<br>UCI: network.<if name>.monitored<br>Opt: monitored | Enabled if the status of the interface is presented on the monitoring platform.<br><table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0 | Disabled.                                | 1 | Enabled. |
| 0  | Disabled.   |   |  |   |          |
| 1  | Enabled.  |   |  |   |          |
| Web: Use broadcast flag<br>UCI: network.<if name>.broadcast<br>Opt: broadcast      | Enables the broadcast flag in DHCP requests (required for certain ISPs).<br><table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0 | Disabled.                                | 1 | Enabled. |
| 0  | Disabled.   |   |  |   |          |
| 1  | Enabled.  |   |  |   |          |
| Web: Use default gateway<br>UCI: network.<if name>.gateway<br>Opt: gateway         | Defines whether to suppress the DHCP assigned default gateway. When disabled via web option, the gateway is set to 0.0.0.0.<br><table border="1" style="width: 100%;"> <tr> <td>0</td> <td>Disabled (option gateway set to 0.0.0.0)</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0 | Disabled (option gateway set to 0.0.0.0) | 1 | Enabled. |
| 0  | Disabled (option gateway set to 0.0.0.0)  |   |  |   |          |
| 1  | Enabled.  |   |  |   |          |
| Web: Use DNS servers advertised by peer<br>UCI: n/a<br>Opt: n/a                    | Defines whether to override DHCP assigned DNS servers with configured list of DNS servers. When unchecked allows configuration of custom DNS servers via web. There is no uci option set when checking or unchecking this option.   |   |  |   |          |

|   |   |       |  |       |                   |     |                  |      |               |      |               |
|---|---|-------|--|-------|-------------------|-----|------------------|------|---------------|------|---------------|
| <p>Web: Use custom DNS servers<br/>UCI: network.&lt;if name&gt;.dns<br/>Opt: dns</p>                              | <p>Defines whether to override DHCP assigned DNS servers with configured list of DNS servers.<br/>Multiple DNS Servers are separated by a space if using UCI.<br/>Example: <code>option dns '1.1.1.1 2.2.2.2'</code></p> <table border="1"> <tr> <td>0</td> <td>Disabled (option gateway set to 0.0.0.0)</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0     | Disabled (option gateway set to 0.0.0.0) | 1     | Enabled.          |     |                  |      |               |      |               |
| 0   | Disabled (option gateway set to 0.0.0.0)  |       |  |       |                   |     |                  |      |               |      |               |
| 1   | Enabled.  |       |  |       |                   |     |                  |      |               |      |               |
| <p>Web: Use gateway metric<br/>UCI: network.&lt;if name&gt;.metric<br/>Opt: metric</p>                            | <p>Specifies the default route metric to use for this interface.</p> <table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 0     | Disabled.                                | Range |                   |     |                  |      |               |      |               |
| 0   | Disabled.   |       |  |       |                   |     |                  |      |               |      |               |
| Range   |   |       |  |       |                   |     |                  |      |               |      |               |
| <p>Web: Client ID to send when requesting DHCP<br/>UCI: network.&lt;if name&gt;. clientid<br/>Opt: clientid</p>   | <p>Defines whether to override the client identifier in DHCP requests.</p> <table border="1"> <tr> <td>Blank</td> <td>Do not override.</td> </tr> <tr> <td>Range</td> <td>Override.</td> </tr> </table>   | Blank | Do not override.                         | Range | Override.         |     |                  |      |               |      |               |
| Blank   | Do not override.  |       |  |       |                   |     |                  |      |               |      |               |
| Range   | Override.   |       |  |       |                   |     |                  |      |               |      |               |
| <p>Web: Vendor Class to send when requesting DHCP<br/>UCI: network.&lt;if name&gt;.vendorid<br/>Opt: vendorid</p> | <p>Defines whether to override the vendor class in DHCP requests.</p> <table border="1"> <tr> <td>Blank</td> <td>Do not override.</td> </tr> <tr> <td>Range</td> <td>Override.</td> </tr> </table>  | Blank | Do not override.                         | Range | Override.         |     |                  |      |               |      |               |
| Blank   | Do not override.  |       |  |       |                   |     |                  |      |               |      |               |
| Range   | Override.   |       |  |       |                   |     |                  |      |               |      |               |
| <p>Web: Override MAC address<br/>UCI: network.&lt;if name&gt;.macaddr<br/>Opt: macaddr</p>                        | <p>Overrides the MAC address assigned to this interface. Must be in the form: hh:hh:hh:hh:hh:hh, where h is a hexadecimal number.</p>   |       |  |       |                   |     |                  |      |               |      |               |
| <p>Web: Override MTU<br/>UCI: network.&lt;if name&gt;.mtu<br/>Opt: mtu</p>  | <p>Defines the value to override the default MTU on this interface.</p> <table border="1"> <tr> <td>1500</td> <td>1500 bytes</td> </tr> </table>  | 1500  | 1500 bytes                               |       |                   |     |                  |      |               |      |               |
| 1500  | 1500 bytes  |       |  |       |                   |     |                  |      |               |      |               |
| <p>Web: Dependant Interfaces<br/>UCI: network.[if_name].dependants<br/>Opt: dependants</p>                        | <p>Lists interfaces that are dependant on this parent interface. Dependant interfaces will go down when the parent interface is down and will start or restart when the parent interface starts. Separate multiple interfaces by a space when using UCI.<br/>Example: <code>option dependants 'PPPADSL MOBILE'</code><br/>This replaces the following previous options in child interfaces.</p> <table border="1"> <tr> <td>gre</td> <td>option local_interface</td> </tr> <tr> <td>lt2p</td> <td>option src_ipaddr</td> </tr> <tr> <td>iot</td> <td>option wan1 wan2</td> </tr> <tr> <td>6in4</td> <td>option ipaddr</td> </tr> <tr> <td>6to4</td> <td>option ipaddr</td> </tr> </table> | gre   | option local_interface                   | lt2p  | option src_ipaddr | iot | option wan1 wan2 | 6in4 | option ipaddr | 6to4 | option ipaddr |
| gre   | option local_interface  |       |  |       |                   |     |                  |      |               |      |               |
| lt2p  | option src_ipaddr   |       |  |       |                   |     |                  |      |               |      |               |
| iot   | option wan1 wan2  |       |  |       |                   |     |                  |      |               |      |               |
| 6in4  | option ipaddr   |       |  |       |                   |     |                  |      |               |      |               |
| 6to4  | option ipaddr   |       |  |       |                   |     |                  |      |               |      |               |
| <p>Web: SNMP Alias ifIndex<br/>UCI:<br/>network.@interface[X].snmp_alias_ifindex<br/>Opt: snmp_alias_ifindex</p>  | <p>Defines a static SNMP interface alias index for this interface, that can be polled using via the SNMP interface index (<code>snmp alias ifindex+1000</code>)</p> <table border="1"> <tr> <td>Blank</td> <td>No SNMP interface alias index</td> </tr> <tr> <td>Range</td> <td>0 - 4294966295</td> </tr> </table>  | Blank | No SNMP interface alias index            | Range | 0 - 4294966295    |     |                  |      |               |      |               |
| Blank   | No SNMP interface alias index   |       |  |       |                   |     |                  |      |               |      |               |
| Range   | 0 - 4294966295  |       |  |       |                   |     |                  |      |               |      |               |

Table 124: Information table for advanced settings for DHCP client protocol

## 30.3 Configuring DHCP client using command line

The configuration files for DHCP client are stored on `/etc/config/network`

### 30.3.1 DHCP client using UCI

```
root@VA_router:~# uci show network
...
network.DHCPCLIENTLAN=interface
network.DHCPCLIENTLAN.proto=dhcp
```

```

network.DHCPCLIENTLAN.ifname=eth3
network.DHCPCLIENTLAN.monitored=0
network.DHCPCLIENTLAN.broadcast=0
network.DHCPCLIENTLAN.accept_ra=1
network.DHCPCLIENTLAN.send_rs=0
network.DHCPCLIENTLAN.metric=1

```

### 30.3.2 DHCP client using package options

```

root@VA_router:~# uci export network
package network
.....
config interface 'DHCPCLIENTLAN'
    option proto 'dhcp'
    option ifname 'eth3'
    option monitored '0'
    option broadcast '0'
    option accept_ra '1'
    option send_rs '0'
    option metric '1'

```

## 30.4 DHCP client diagnostics

### 30.4.1 Interface status

To view the IP address of DHCP client interface, enter:

```

root@VA_router:~# ifconfig
3g-CDMA  Link encap:Point-to-Point Protocol
          inet addr:10.33.152.100  P-t-P:178.72.0.237  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1400  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:428 (428.0 B)  TX bytes:2986 (2.9 KiB)

eth0      Link encap:Ethernet  HWaddr 00:E0:C8:12:12:15
          inet addr:192.168.100.1  Bcast:192.168.100.255
          Mask:255.255.255.0
          inet6 addr: fe80::2e0:c8ff:fe12:1215/64 Scope:Link

```

```

UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:6645 errors:0 dropped:0 overruns:0 frame:0
TX packets:523 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:569453 (556.1 KiB)  TX bytes:77306 (75.4 KiB)

lo
  Link encap:Local Loopback
  inet addr:127.0.0.1  Mask:255.0.0.0
  inet6 addr: ::1/128 Scope:Host
  UP LOOPBACK RUNNING  MTU:16436  Metric:1
  RX packets:385585 errors:0 dropped:0 overruns:0 frame:0
  TX packets:385585 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:0
  RX bytes:43205140 (41.2 MiB)  TX bytes:43205140 (41.2 MiB)

```

To display a specific interface, enter:

```

root@VA_router:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:E0:C8:12:12:15
          inet addr:192.168.100.1  Bcast:192.168.100.255
Mask:255.255.255.0

          inet6 addr: fe80::2e0:c8ff:fe12:1215/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7710 errors:0 dropped:0 overruns:0 frame:0
          TX packets:535 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:647933 (632.7 KiB)  TX bytes:80978 (79.0 KiB)

```

### 30.4.2 ARP table status

To show the current ARP table of the router, enter:

```

root@GW7314:~# arp
? (10.67.253.141) at 30:30:41:30:43:36 [ether]  on eth8
? (10.47.48.1) at 0a:44:b2:06 [ether]  on gre-gre1

```

### 30.4.3 Route status

To show the current routing status, enter:

```
root@VA_router:~# route -n
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
192.168.100.0    *                255.255.255.0  U        0      0      0 eth0
```

**Note:** a route will only be displayed in the routing table when the interface is up.

## 31 Configuring DHCP forwarding

This section describes how to configure the router to forward DHCP requests from an interface to a network DHCP server.

### 31.1 Configuration packages used

| Package  | Sections |
|----------|----------|
| dhcp_fwd | dhcpfwd  |

### 31.2 Configuring DHCP forwarding using the web interface

To configure DHCP forwarding using the web interface, in the top menu, click **Network -> DHCP-Forwarder**.

The DHCP forwarder page appears. The web GUI creates a dhcpfwd section called main so this will be used in the uci examples below.

Figure 183: The DHCP forwarder configuration page

| Web Field/UCI/Package Option   | Description  |   |                                   |   |                            |
|--|--|---|-----------------------------------|---|----------------------------|
| Web: Enabled<br>UCI: dhcp_fwd.main.enabled<br>Opt: enabled                           | Defines whether DHCP forwarding is enabled or disabled. <table border="1" style="margin-left: 20px;"> <tr> <td>0</td> <td>Do not send router solicitations.</td> </tr> <tr> <td>1</td> <td>Send router solicitations.</td> </tr> </table>  | 0 | Do not send router solicitations. | 1 | Send router solicitations. |
| 0  | Do not send router solicitations.  |   |                                   |   |                            |
| 1  | Send router solicitations.   |   |                                   |   |                            |
| Web: Interfaces<br>UCI: dhcp_fwd.main.listen_interface<br>Opt: list listen_interface | Defines a list of the source interface name(s) to forward DHCP messages from. Multiple interface_name(s) are entered using uci set and uci add_list commands. Example:<br><pre>uci set dhcp_fwd.main.listen_interface=LAN1 uci add_list dhcp_fwd.main.listen_interface=LAN2</pre> or using a list of options via package options<br><pre>list listen_interface 'LAN1' list listen_interface 'LAN2'</pre> |   |                                   |   |                            |
| Web: DHCP Servers<br>UCI: dhcp_fwd.main.server<br>Opt: list server                   | Defines a list of the network DHCP servers to forward DHCP messages to. Multiple interface_name(s) are entered using uci set and uci add_list commands. Example:<br><pre>uci set dhcp_fwd.main.server=1.1.1.1 uci add_list dhcp_fwd.main.main.server=2.2.2.2</pre> or using a list of options via package options<br><pre>list server '1.1.1.1' list server '2.2.2.2'</pre>                              |   |                                   |   |                            |

Table 125: Information table for the DHCP forwarder section

### 31.3 Configuring DHCP forwarding using command line

The configuration files for DHCP client are stored in `/etc/config/dhcp_fwd`

#### 31.3.1 DHCP forwarding using UCI

```
root@VA_router:~# uci show dhcp_fwd
dhcp_fwd.main=dhcpfwd
dhcp_fwd.main.enabled=1
dhcp_fwd.main.listen_interface=LAN3 lan2
dhcp_fwd.main.server=1.1.1.1
```

#### 31.3.2 DHCP forwarding using package options

```
root@VA_router:~# uci export dhcp_fwd
package dhcp_fwd

config dhcpfwd 'main'
    option enabled '1'
    list listen_interface 'LAN3'
    list listen_interface 'lan2'
    list server '1.1.1.1'
```

## 31.4 DHCP forwarding over IPsec

DHCP messages are forwarded over the WAN interface using the IP address of the WAN interface as the source IP for the transmitted packet. This means that when forwarding over an IPsec tunnel a source NAT firewall rule is required to change the source IP to match an IPsec connection rule.

### 31.4.1 Configuration packages used

| Package  | Sections |
|----------|----------|
| firewall | redirect |

### 31.4.2 Configuring source NAT for DHCP forwarding over IPsec

To enter a source NAT rule, browse to **Network -> Firewall**. Select **Traffic Rules** tab. The Firewall - Traffic Rules page appears. Configure a source NAT rule that changes the source IP for UDP destination port 67 from the required LAN.

For more information on configuring a source NAT rule, read the 'Configuring Firewall' section of the User Manual.

Figure 184: The firewall – traffic rules configuration page



| Web Field/UCI/Package Option  | Description  |
|---|--|
| Web: Name<br>UCI: firewall.@redirect[X].name<br>Opt: name                     | Defines a name for the source NAT rule.  |
| Web: Source Zone<br>UCI: firewall.@redirect[X].src<br>Opt: src                | Defines the source interface for the source NAT rule.<br>Select <b>the interface where the DHCP requests are originating</b> .                 |
| Web: Destination Zone<br>UCI: firewall.@redirect[X].dest<br>Opt: dest         | Defines destination interface for the source NAT rule.<br>Select <b>the interface where the DHCP requests are intended to be transmitted</b> . |
| Web: To source IP<br>UCI: firewall.@redirect[X].src_dip<br>Opt: src_dip       | Defines the IP address to rewrite matched traffic source IP.<br>Select <b>the source IP address to match the required IPsec rule</b> .         |
| Web: To source port<br>UCI: firewall.@redirect[X].src_dport<br>Opt: src_dport | Defines the port number to rewrite matched traffic source port number.<br><b>Leave empty.</b>  |

Table 126: Information table for the source NAT configuration

### Firewall - Traffic Rules - SNAT DHCPMessages

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled

Name

Protocol  You may specify multiple by selecting "-- custom --" and then entering protocols separated by space.

Source zone  lan: lan: lan2:  wan: main2\_voda: wan:

Source MAC address

Source IP address

Source port  Match incoming traffic originating from the given source port or port range on the client host.

Destination zone  lan: lan: lan2:  wan: main2\_voda: wan:

Destination IP address

Destination port  Match forwarded traffic to the given destination port or port range.

SNAT IP address  Rewrite matched traffic to the given address.

SNAT port  Rewrite matched traffic to the given source port. May be left empty to only rewrite the IP address.

Extra arguments  Passes additional arguments to iptables. Use with care!

Figure 185: The firewall – traffic rules – SNAT configuration page

| Web Field/UCI/Package Option   | Description   |         |             |     |               |                     |     |         |                             |         |     |                    |     |     |                    |     |      |                     |      |        |                       |  |
|--|---|---------|-------------|-----|---------------|---------------------|-----|---------|-----------------------------|---------|-----|--------------------|-----|-----|--------------------|-----|------|---------------------|------|--------|-----------------------|--|
| Web: Rule is enabled<br>UCI: firewall.@redirect[X].enabled<br>Opt: enabled | Defines whether source NAT rule is enabled.<br><table border="1"> <tr> <td>0</td> <td>Disabled</td> </tr> <tr> <td>1</td> <td>Enabled</td> </tr> </table>   | 0       | Disabled    | 1   | Enabled       |                     |     |         |                             |         |     |                    |     |     |                    |     |      |                     |      |        |                       |  |
| 0  | Disabled  |         |             |     |               |                     |     |         |                             |         |     |                    |     |     |                    |     |      |                     |      |        |                       |  |
| 1  | Enabled   |         |             |     |               |                     |     |         |                             |         |     |                    |     |     |                    |     |      |                     |      |        |                       |  |
| Web: Name<br>UCI: firewall.@redirect[X].name<br>Opt: name                  | Defines a name for the source NAT rule.   |         |             |     |               |                     |     |         |                             |         |     |                    |     |     |                    |     |      |                     |      |        |                       |  |
| Web: Protocol<br>UCI: firewall.@redirect[X].proto<br>Opt: proto            | Defines the protocol for the source NAT rule to match.<br>Select <b>UDP</b> .<br><table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>All protocols</td> <td>Match all protocols</td> <td>all</td> </tr> <tr> <td>TCP+UDP</td> <td>Match TCP and UDP protocols</td> <td>tcp upd</td> </tr> <tr> <td>TCP</td> <td>Match TCP protocol</td> <td>tcp</td> </tr> <tr> <td>UDP</td> <td>Match UDP protocol</td> <td>udp</td> </tr> <tr> <td>ICMP</td> <td>Match ICMP protocol</td> <td>icmp</td> </tr> <tr> <td>Custom</td> <td>Enter custom protocol</td> <td></td> </tr> </tbody> </table> | Option  | Description | UCI | All protocols | Match all protocols | all | TCP+UDP | Match TCP and UDP protocols | tcp upd | TCP | Match TCP protocol | tcp | UDP | Match UDP protocol | udp | ICMP | Match ICMP protocol | icmp | Custom | Enter custom protocol |  |
| Option   | Description   | UCI     |             |     |               |                     |     |         |                             |         |     |                    |     |     |                    |     |      |                     |      |        |                       |  |
| All protocols  | Match all protocols   | all     |             |     |               |                     |     |         |                             |         |     |                    |     |     |                    |     |      |                     |      |        |                       |  |
| TCP+UDP  | Match TCP and UDP protocols   | tcp upd |             |     |               |                     |     |         |                             |         |     |                    |     |     |                    |     |      |                     |      |        |                       |  |
| TCP  | Match TCP protocol  | tcp     |             |     |               |                     |     |         |                             |         |     |                    |     |     |                    |     |      |                     |      |        |                       |  |
| UDP  | Match UDP protocol  | udp     |             |     |               |                     |     |         |                             |         |     |                    |     |     |                    |     |      |                     |      |        |                       |  |
| ICMP   | Match ICMP protocol   | icmp    |             |     |               |                     |     |         |                             |         |     |                    |     |     |                    |     |      |                     |      |        |                       |  |
| Custom   | Enter custom protocol   |         |             |     |               |                     |     |         |                             |         |     |                    |     |     |                    |     |      |                     |      |        |                       |  |
| Web: Source Zone<br>UCI: firewall.@redirect[X].src<br>Opt: src             | Defines the source interface for the source NAT rule.<br>Select <b>the interface where the DHCP requests are originating</b> .  |         |             |     |               |                     |     |         |                             |         |     |                    |     |     |                    |     |      |                     |      |        |                       |  |
| Web: Destination Zone<br>UCI: firewall.@redirect[X].dest<br>Opt: dest      | Defines destination interface for the source NAT rule.<br>Select <b>the interface where the DHCP requests are intended to be transmitted</b> .  |         |             |     |               |                     |     |         |                             |         |     |                    |     |     |                    |     |      |                     |      |        |                       |  |
| Web: Destination port<br>UCI: firewall.@redirect[X].port<br>Opt: port      | Defines the destination port number to match.<br>Select <b>67</b> .   |         |             |     |               |                     |     |         |                             |         |     |                    |     |     |                    |     |      |                     |      |        |                       |  |
| Web: SNAT IP address<br>UCI: firewall.@redirect[X].src_dip<br>Opt: src_dip | Defines the IP address to rewrite matched traffic.<br>Select <b>the source IP address to match the required IPsec rule</b> .  |         |             |     |               |                     |     |         |                             |         |     |                    |     |     |                    |     |      |                     |      |        |                       |  |

Table 127: Information table for the advanced source NAT configuration

### 31.4.3 Configuring source NAT for DHCP forwarding over IPsec using command line

#### 31.4.3.1 Source NAT for DHCP forwarding over IPsec using UCI

```

root@VA_router:~# uci show firewall
.....
firewall.@redirect[0]=redirect
firewall.@redirect[0].target=SNAT
firewall.@redirect[0].src=lan
firewall.@redirect[0].dest=wan
firewall.@redirect[0].src_dip=192.168.100.1
firewall.@redirect[0].name=DHCPMessages
firewall.@redirect[0].proto=udp
firewall.@redirect[0].dest_port=67

```

### 31.4.3.2 Source NAT for DHCP forwarding over IPsec using package options

```
root@VA_router:~# uci export firewall
package firewall
.....
config redirect
    option target 'SNAT'
    option src 'lan'
    option dest 'wan'
    option src_dip '192.168.100.1'
    option name 'DHCPMessages'
    option proto 'udp'
    option dest_port '67'
```

## 31.5 DHCP forwarding diagnostics

### 31.5.1 Tracing DHCP packets

To trace DHCP packets on any interface on the router, enter:

```
root@VA_router:~# tcpdump -i any -n -p port 67 &
root@VA_router:~# tcpdump: verbose output suppressed, use -v or -vv for
full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535
bytes
16:39:20.666070 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request
from 00:e0:c8:13:02:3d, length 360
16:39:20.666166 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request
from 00:e0:c8:13:02:3d, length 360
```

To stop tracing enter **fg** (to bring tracing task to foreground), and then **<CTRL-C>** to stop the trace.

```
root@VA_router:~# fg
tcpdump -i any -n -p port 67
^C
33 packets captured
33 packets received by filter
0 packets dropped by kernel
```

```
16:39:20.666166 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request  
from 00:e0:c8:13:02:3d, length 360
```

### 31.5.2 ARP table status

To show the current ARP table of the router, enter **arp**

```
root@VA_router:~# arp  
? (10.67.253.141) at 30:30:41:30:43:36 [ether] on eth8  
? (10.47.48.1) at 0a:44:b2:06 [ether] on gre-gre1
```

## 32 Configuring Dynamic DNS

### 32.1 Overview

Dynamic DNS (DDNS) functionality on a Virtual Access router will dynamically perform DDNS updates to a server so it can associate an IP address with a correctly associated DNS name. Users can then contact a machine, router, device and so on with a DNS name rather than a dynamic IP address.

An account is required with the provider, and one or more domain names are associated with that account. A dynamic DNS client on the router monitors the public IP address associated with an interface and whenever the IP address changes, the client notifies the DNS provider to update the corresponding domain name.

When the DNS provider responds to queries for the domain name, it sets a low lifetime, typically a minute or two at most, on the response so that it is not cached. Updates to the domain name are thus visible throughout the whole internet with little delay.

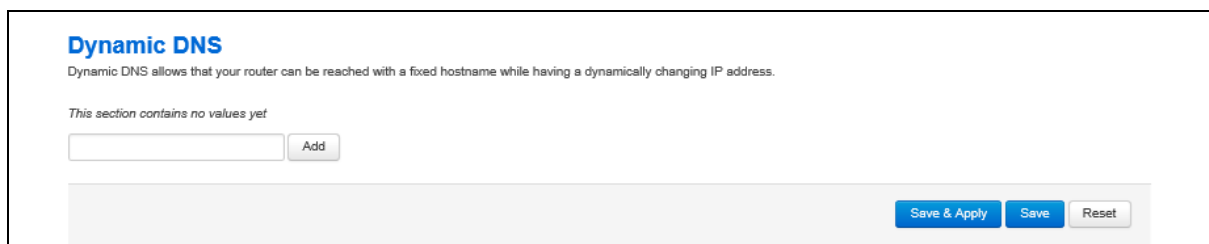
**Note:** most providers impose restrictions on how updates are handled: updating when no change of address occurred is considered abusive and may result in an account being blocked. Sometimes, addresses must be refreshed periodically, for example, once a month, to show that they are still in active use.

### 32.2 Configuration packages used

| Package | Sections |
|---------|----------|
| ddns    | service  |

### 32.3 Configuring Dynamic DNS using the web interface

In the top menu, select **Services -> Dynamic DNS**. The Dynamic DNS Configuration page appears.



**Dynamic DNS**  
Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

*This section contains no values yet*

**Figure 186: The Dynamic DNS configuration page**

Enter a text name that will be used for the dynamic DNS section in the configuration. Select **Add**. The Dynamic DNS configuration options appear.

### 32.3.1 Dynamic DNS settings

## Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

### DDNS1

Enable

Service -- custom --

Custom update-URL

Hostname

Username

Password

Source of IP address network

**Network** lan

Check for changed IP every

Check-time unit min

Force update every

Force-time unit h

Listen on  dialin:

**Figure 187: The dynamic DNS main settings page**

| Web Field/UCI/Package Option   | Description  |         |  |           |                                     |     |                              |
|--|--|---------|--|-----------|-------------------------------------|-----|------------------------------|
| Web: Enable<br>UCI: ddns.<name>.enabled<br>Opt: enabled                    | Enables a dynamic DNS entry on the router.<br><table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30px; text-align: center;">0</td> <td>Disabled.</td> </tr> <tr> <td style="text-align: center;">1</td> <td>Enabled</td> </tr> </table>   | 0       | Disabled.                                      | 1         | Enabled                             |     |                              |
| 0  | Disabled.  |         |  |           |                                     |     |                              |
| 1  | Enabled  |         |  |           |                                     |     |                              |
| Web: Service<br>UCI: ddns.<name>.service_name<br>Opt: service_name         | Defines the dynamic DNS provider.  |         |  |           |                                     |     |                              |
| Web: Customer update-URL<br>UCI: ddns.<name>.update_url<br>Opt: update_url | Defines the customer DNS provider.<br>Displayed when the service is set to custom in the web interface.  |         |  |           |                                     |     |                              |
| Web: Hostname<br>UCI: ddns.<name>.domain<br>Opt: domain                    | Defines the fully qualified domain name associated with this entry. This is the name to update with the new IP address as needed.  |         |  |           |                                     |     |                              |
| Web: Username<br>UCI: ddns.<name>.username<br>Opt: username                | Defines the user name to use for authenticating domain updates with the selected provider.   |         |  |           |                                     |     |                              |
| Web: Password<br>UCI: ddns.<name>.password<br>Opt: password                | Defines the password to use for authenticating domain name updates with the selected provider.   |         |  |           |                                     |     |                              |
| Web: Source of IP address<br>UCI: ddns.<name>.ip_source<br>Opt: ip_source  | Defines the type of interface whose IP needs to be updated.<br><table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30px; text-align: center;">network</td> <td>IP is associated with a network configuration.</td> </tr> <tr> <td style="text-align: center;">interface</td> <td>IP is associated with an interface.</td> </tr> <tr> <td style="text-align: center;">web</td> <td>IP is associated with a URL.</td> </tr> </table> | network | IP is associated with a network configuration. | interface | IP is associated with an interface. | web | IP is associated with a URL. |
| network  | IP is associated with a network configuration.   |         |  |           |                                     |     |                              |
| interface  | IP is associated with an interface.  |         |  |           |                                     |     |                              |
| web  | IP is associated with a URL.   |         |  |           |                                     |     |                              |

|   |   |         |           |       |         |
|---|---|---------|-----------|-------|---------|
| Web: Network<br>UCI: ddns.<name>.ip_network<br>Opt: ip_network                            | Defines the network whose IP needs to be updated.<br>Displayed when the Source of IP address option is set to network.<br>All the configured network interfaces will be shown.                                    |         |           |       |         |
| Web: Interface<br>UCI: ddns.<name>.ip_interface<br>Opt: ip_interface                      | Defines the interface whose IP needs to be updated.<br>Displayed when the Source of IP address option is set to interface.<br>All the configured interfaces will be shown.  |         |           |       |         |
| Web: URL<br>UCI: ddns.<name>.ip_url<br>Opt: ip_url  | Defines the URL where the IP downloaded from.<br>Displayed when the Source of IP address option is set to URL.  |         |           |       |         |
| Web: Check for changed IP every<br>UCI: ddns.<name>.check_interval<br>Opt: check_interval | Defines how often to check for an IP change. Used in conjunction with check_unit.<br><table border="1"> <tr> <td>10</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>                             | 10      |           | Range |         |
| 10  |   |         |           |       |         |
| Range   |   |         |           |       |         |
| Web: Check-time unit<br>UCI: ddns.<name>.check_unit<br>Opt: check_unit                    | Defines the time unit to use for check for an IP change. Used in conjunction with check_interval.<br><table border="1"> <tr> <td>Minutes</td> <td></td> </tr> <tr> <td>hours</td> <td></td> </tr> </table>        | Minutes |           | hours |         |
| Minutes   |   |         |           |       |         |
| hours   |   |         |           |       |         |
| Web: Force update every<br>UCI: ddns.<name>.force_interval<br>Opt: force_interval         | Defines how often to force an IP update to the provider. Used in conjunction with force_unit.<br><table border="1"> <tr> <td>72</td> <td>Disabled.</td> </tr> <tr> <td>Range</td> <td>Enabled</td> </tr> </table> | 72      | Disabled. | Range | Enabled |
| 72  | Disabled.   |         |           |       |         |
| Range   | Enabled   |         |           |       |         |
| Web: Force-time unit<br>UCI: ddns.<name>.force_unit<br>Opt: force_unit                    | Defines the time unit to use for check for an IP change. Used in conjunction with force_interval.<br><table border="1"> <tr> <td>Minutes</td> <td></td> </tr> <tr> <td>Hours</td> <td></td> </tr> </table>        | Minutes |           | Hours |         |
| Minutes   |   |         |           |       |         |
| Hours   |   |         |           |       |         |
| Web: Listen on<br>UCI: ddns.<name>.interface<br>Opt: interface                            | Defines the interface for ddns monitoring. Typically this will be the same as the interface whose IP is being updated – as defined ip_network or ip_interface.<br>All configured interfaces will be displayed.    |         |           |       |         |

Table 128: Information table for dynamic DNS settings

## 32.4 Dynamic DNS using UCI

Dynamic DNS uses the ddns package `/etc/config/ddns`

### 32.4.1 UCI commands for DDNS

```

root@VA_router:~# uci show ddns
ddns.ddns1=service
ddns.ddns1.enabled=1
ddns.ddns1.service_name=dyndns.org
ddns.ddns1.domain=fqdn_of_interface
ddns.ddns1.username=testusername
ddns.ddns1.password=testpassword
ddns.ddns1.ip_source=network
ddns.ddns1.ip_network=ds10
ddns.ddns1.check_interval=10

```

```
ddns.ddns1.check_unit=minutes
ddns.ddns1.force_interval=72
ddns.ddns1.force_unit=hours
ddns.ddns1.interface=ds10
Package options for DDNS
root@VA_router:~# uci export ddns
package ddns

config service 'ddns1'
    option enabled '1'
    option service_name 'dyndns.org'
    option domain 'fqdn_of_interface'
    option username 'test'
    option password 'test'
    option ip_source 'network'
    option ip_network 'ds10'
    option check_interval '10'
    option check_unit 'minutes'
    option force_interval '72'
    option force_unit 'hours'
    option interface 'ds10'
```



## 33 Configuring hostnames

### 33.1 Overview

Hostnames are human-readable names that identify a device connected to a network. There are several different ways in which hostnames can be configured and used on the router.

- Local host file records
- PTR records
- Static DHCP leases

### 33.2 Local host file records

The hosts file is an operating system file that maps hostnames to IP addresses. It is used preferentially to other name resolution methods such as DNS.

The hosts file contains lines of text consisting of an IP address in the first text field followed by one or more host names. Each field is separated by white space; tabs are often preferred for historical reasons, but spaces are also used. Comment lines may be included; they are indicated by an octothorpe (#) in the first position of such lines. Entirely blank lines in the file are ignored.

By default, the router's local host file contains:

```
127.0.0.1 localhost
::1 ip6-localhost ip6-loopback
```

The local host file is stored at **/etc/hosts**

#### 33.2.1 Configuration packages used

| Package | Sections |
|---------|----------|
| network | host     |

#### 33.2.2 Configuring local host files entries using the web interface

In the top menu, select **Network -> Interfaces**. The Interfaces configuration page appears.

Browse to **Host Records** section at the bottom of the page.

**Figure 188: The host records add page**

Select **Add**. Enter a hostname and IP address and select **Save & Apply**.

**Figure 189: The host records configuration page**

| Web Field/UCI/Package Option                                 | Description  |
|--|--|
| Web: Hostname<br>UCI: network.host.hostname<br>Opt: hostname | Defines the hostname.                                |
| Web: IP-Address<br>UCI: network.host.addr<br>Opt: addr       | Defines the IP address associated with the hostname. |

**Table 129: Information table for host records settings**

### 33.2.3 Local host records using command line

Local host records are configured in the host section of the network package **/etc/config/network**.

Multiple hosts can be configured.

By default, all host instances are named host and are identified by @host then the host position in the package as a number. For example, for the first host in the package using UCI:

```
network.@host[0]=host
network.@host[0].hostname=Device1
```

Or using package options:

```
config host
    option hostname 'Device1'
```

### 33.2.3.1 Local host records using uci

```
root@VA_router:~# uci show network
.....
network.@host[0]=host
network.@host[0].hostname=Device1
network.@host[0].addr=1.1.1.1
```

### 33.2.3.2 Local host records using package option

```
root@VA_router:~# uci export network
package network
.....
config host
    option hostname 'Device1'
    option addr '1.1.1.1'
```

## 33.2.4 Local host records diagnostics

### 33.2.4.1 Hosts file

Local host records are written to the local hosts file stored at **/etc/hosts**. To view the local hosts file, enter:

```
root@VA_router:~# cat /etc/hosts
127.0.0.1 localhost
::1 ip6-localhost ip6-loopback
1.1.1.1 Device1
```

## 33.3 PTR records

PTR records are used for reverse DNS.

The primary purpose for DNS is to map domains to IP addresses. A pointer record works in the opposite way; it associates an IP address with a domain name.

### 33.3.1 Configuration packages used

| Package | Sections |
|---------|----------|
| dhcp    | domain   |

### 33.3.2 Configuring PTR records using the web interface

In the top menu, select **Network -> Hostnames**. The Hostnames configuration page appears.

Figure 190: The hostnames add page

Select **Add**. Enter a hostname and IP address for the PTR record and select **Save & Apply**.

Figure 191: The hostnames configuration page

| Web Field/UCI/Package Option                        | Description   |
|---|---|
| Web: Hostname<br>UCI: dhcp.domain.name<br>Opt: name | Defines the domain name for the PTR record.             |
| Web: IP-Address<br>UCI: dhcp.domain.ip<br>Opt: ip   | Defines the IP address associated with the domain name. |

Table 130: Information table for hostnames settings

### 33.3.3 PTR records using command line

PTR records are configured in the **domain** section of the dhcp package.  
**/etc/config/dhcp.**

Multiple **domains** can be configured.

By default, all domain instances are named domain and are identified by @domain then the domain position in the package as a number. For example, for the first domain in the package using UCI:

```
dhcp.@domain[0]=domain
dhcp.@domain[0].name=Domain1
```

Or using package options:

```
config domain
    option name 'Domain1'
```

### 33.3.3.1 PTR records using uci

```
root@VA_router:~# uci show dhcp
.....
dhcp.@domain[0]=domain
dhcp.@domain[0].name=Domain1
dhcp.@domain[0].ip=2.2.2.2
```

### 33.3.3.2 PTR records using package option

```
root@VA_router:~# uci export dhcp
package dhcp
.....
config domain
    option name 'Domain1'
    option ip '2.2.2.2'
```

## 33.3.4 PTR records diagnostics

### 33.3.4.1 PTR records table

To view PTR records, enter:

```
root@VA_router:~# pgrep -fl dnsmasq
4724 /usr/sbin/dnsmasq -K -D -y -Z -b -E -s lan -S /lan/ -l
/tmp/dhcp.leases -r /tmp/resolv.conf.auto --stop-dns-rebind --rebind-
localhost-ok -A /Device1.lan/1.1.1.1 --ptr-record=1.1.1.1.in-
addr.arpa,Device1.lan -A /Device2.lan/2.2.2.2 --ptr-record=2.2.2.2.in-
addr.arpa,Device2.lan
```

## 33.4 Static leases

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients based on their MAC (hardware) address.

They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.

### 33.4.1 Configuration packages used

| Package | Sections |
|---------|----------|
| dhcp    | host     |

### 33.4.2 Configuring static leases using the web interface

In the top menu, select **Network -> DHCP and DNS**. The DHCP and DNS configuration page appears.

Browse to **Static leases** section.

**Figure 192: The static leases add page**

Select **Add**. Enter a hostname, MAC address and IP address for the static lease. Select **Save & Apply**.

**Figure 193: The static leases configuration page**

| Web Field/UCI/Package Option                       | Description   |
|--|---|
| Web: Hostname<br>UCI: dhcp.host.name<br>Opt: name  | Defines the symbolic hostname to assign.  |
| Web: MAC-Address<br>UCI: dhcp.host.mac<br>Opt: mac | Defines the MAC address for this host. MAC addresses should be entered in the format <code>aa:bb:cc:dd:ee:ff</code> |
| Web: IPv4-Address<br>UCI: dhcp.host.ip<br>Opt: ip  | Defines the IP address to be used for this host.  |

**Table 131: Information table for static leases settings**

### 33.4.3 Static leases using command line

Static leases are configured in the **host** section of the dhcp package `/etc/config/dhcp`.

Multiple **hosts** can be configured.

By default, all dhcp host instances are named host. It is identified by `@host` then the host position in the package as a number. For example, for the first host in the package using UCI:

```
dhcp.@host[0]=host
dhcp.@host[0].name=Host1
```

Or using package options:

```
config host
    option name 'Host1'
```

### 33.4.3.1 Static leases using uci

```
root@VA_router:~# uci show dhcp
.....
dhcp.@host[0]=host
dhcp.@host[0].name=Host1
dhcp.@host[0].mac=aa:bb:cc:dd:ee:ff
dhcp.@host[0].ip=4.4.4.4
```

### 33.4.3.2 Static leases using package option

```
root@VA_router:~# uci export dhcp
package dhcp
.....
config host
    option name 'Host1'
    option mac 'aa:bb:cc:dd:ee:ff'
    option ip '4.4.4.4'
```

## 34 Configuring firewall

The firewall itself is not required. It is a set of scripts which configure Netfilter. If preferred, you can use Netfilter directly to achieve the desired firewall behaviour.

**Note:** the UCI firewall exists to simplify configuring Netfilter for many scenarios, without requiring the knowledge to deal with the complexity of Netfilter.

The firewall configuration consists of several zones covering one or more interfaces. Permitted traffic flow between the zones is controlled by forwardings. Each zone can include multiple rules and redirects (port forwarding rules).

The Netfilter system is a chained processing filter where packets pass through various rules. The first rule that matches is executed often leading to another rule-chain until a packet hits either ACCEPT or DROP/REJECT.

Accepted packets pass through the firewall. Dropped packets are prohibited from passing. Rejected packets are also prohibited but an ICMP message is returned to the source host.

A minimal firewall configuration for a router usually consists of one 'defaults' section, at least two 'zones' (LAN and WAN) and one forwarding to allow traffic from LAN to WAN. Other sections that exist are 'redirects', 'rules' and 'includes'.

### 34.1 Configuration package used

| Package  | Sections |
|----------|----------|
| firewall |          |

### 34.2 Configuring firewall using the web interface

In the top menu, select **Network -> Firewall**. The Firewall page appears. It is divided into four sections:

| Section               | Description  |
|-----------------------|--|
| General Zone Settings | Defines the firewall zones, both global and specific.  |
| Port Forwards         | Port Forwards are also known as Redirects. This section creates the redirects using DNAT (Destination Network Address Translation) with Netfilter. |
| Traffic Rules         | Defines rules to allow or restrict access to specific ports, hosts or protocols.   |

#### 34.2.1 Firewall: zone settings

The Zone settings section is divided into two:

| Section          | Description   |
|------------------|---|
| General Settings | Defines the global firewall settings that do not belong to any specific zones.  |
| Zones            | The zones section groups one or more interfaces and serves as a source or destination for forwardings, rules and redirects. Masquerading (NAT) of outgoing traffic is controlled on a per-zone basis. |



### 34.2.1.1 Firewall general settings

The General Settings page, or defaults section declares global firewall settings that do not belong to any specific zones. These default rules take effect last and more specific rules take effect first.

Figure 194: The firewall zone general settings page

| Web Field/UCI/Package Option   | Description   |        |   |        |   |      |  |
|--|---|--------|---|--------|---|------|--|
| Web: Enable SYN-flood protection<br>UCI: firewall.defaults.syn_flood<br>Opt: syn_flood | Enables SYN flood protection.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0      | Disabled.                                   | 1      | Enabled.  |      |  |
| 0  | Disabled.   |        |   |        |   |      |  |
| 1  | Enabled.  |        |   |        |   |      |  |
| Web: Drop invalid packets<br>UCI: firewall.defaults.drop_invalid<br>Opt: drop_invalid  | Drops packets not matching any active connection.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0      | Disabled.                                   | 1      | Enabled.  |      |  |
| 0  | Disabled.   |        |   |        |   |      |  |
| 1  | Enabled.  |        |   |        |   |      |  |
| Web: Input<br>UCI: firewall.defaults.input<br>Opt: input                               | Default policy for the Input chain.<br><table border="1"> <tr> <td>Accept</td> <td>Accepted packets pass through the firewall.</td> </tr> <tr> <td>Reject</td> <td>Rejected packets are blocked by the firewall and ICMP message is returned to the source host.</td> </tr> <tr> <td>Drop</td> <td>Dropped packets are blocked by the firewall.</td> </tr> </table>   | Accept | Accepted packets pass through the firewall. | Reject | Rejected packets are blocked by the firewall and ICMP message is returned to the source host. | Drop | Dropped packets are blocked by the firewall. |
| Accept   | Accepted packets pass through the firewall.   |        |   |        |   |      |  |
| Reject   | Rejected packets are blocked by the firewall and ICMP message is returned to the source host.   |        |   |        |   |      |  |
| Drop   | Dropped packets are blocked by the firewall.  |        |   |        |   |      |  |
| Web: Output<br>UCI: firewall.defaults.output<br>Opt: output                            | Default policy for the Output chain.<br><table border="1"> <tr> <td>Accept</td> <td>Accepted packets pass through the firewall.</td> </tr> <tr> <td>Reject</td> <td>Rejected packets are blocked by the firewall and ICMP message is returned to the source host.</td> </tr> <tr> <td>Drop</td> <td>Dropped packets are blocked by the firewall.</td> </tr> </table>  | Accept | Accepted packets pass through the firewall. | Reject | Rejected packets are blocked by the firewall and ICMP message is returned to the source host. | Drop | Dropped packets are blocked by the firewall. |
| Accept   | Accepted packets pass through the firewall.   |        |   |        |   |      |  |
| Reject   | Rejected packets are blocked by the firewall and ICMP message is returned to the source host.   |        |   |        |   |      |  |
| Drop   | Dropped packets are blocked by the firewall.  |        |   |        |   |      |  |
| Web: Forward<br>UCI: firewall.defaults.forward<br>Opt: forward                         | Default policy for the Forward chain.<br><table border="1"> <tr> <td>Accept</td> <td>Accepted packets pass through the firewall.</td> </tr> <tr> <td>Reject</td> <td>Rejected packets are blocked by the firewall and ICMP message is returned to the source host.</td> </tr> <tr> <td>Drop</td> <td>Dropped packets are blocked by the firewall.</td> </tr> </table> | Accept | Accepted packets pass through the firewall. | Reject | Rejected packets are blocked by the firewall and ICMP message is returned to the source host. | Drop | Dropped packets are blocked by the firewall. |
| Accept   | Accepted packets pass through the firewall.   |        |   |        |   |      |  |
| Reject   | Rejected packets are blocked by the firewall and ICMP message is returned to the source host.   |        |   |        |   |      |  |
| Drop   | Dropped packets are blocked by the firewall.  |        |   |        |   |      |  |

Table 132: Information table for general zone general settings page

### 34.2.1.2 Firewall zones

The Zones section groups one or more interfaces and serves as a source or destination for forwardings, rules and redirects. Masquerading (NAT) of outgoing traffic is controlled on a per-zone basis. To view a zone's settings, click **Edit**.

The number of concurrent dynamic/static NAT entries of any kind (NAT/PAT/DNAT/SNAT) is not limited in any way by software; the only hardware limitation is the amount of RAM installed on the device.

### 34.2.1.3 Firewall zone: general settings

The screenshot shows the 'Firewall - Zone Settings - Zone "lan"' configuration page. It has tabs for 'General Settings' (selected) and 'Advanced Settings'. The 'General Settings' section includes:

- Name: lan
- Input: accept
- Output: accept
- Forward: accept
- Masquerading:
- MSS clamping:
- Covered networks:
  - LAN1: (no interfaces attached)
  - LAN2: [icon]
  - LAN3: [icon]
  - MOBILE1: [icon]
  - PoAADSL: [icon]
  - loopback: [icon]

Figure 195: The firewall zone general settings

| Web Field/UCI/Package Option                                 | Description  |        |   |        |   |      |  |
|--|--|--------|---|--------|---|------|--|
| Web: name<br>UCI: firewall.<zone label>.name<br>Opt: name    | Sets the unique zone name. Maximum of 11 characters allowed.<br><b>Note:</b> the zone label is obtained by using the 'uci show firewall' command and is of the format '@zone[x]' where x is an integer starting at 0.  |        |   |        |   |      |  |
| Web: Input<br>UCI: firewall.<zone label>.input<br>Opt: input | Default policy for incoming zone traffic. Incoming traffic is traffic entering the router through an interface selected in the 'Covered Networks' option for this zone. <table border="1" data-bbox="683 1682 1331 1910"> <tbody> <tr> <td>Accept</td> <td>Accepted packets pass through the firewall.</td> </tr> <tr> <td>Reject</td> <td>Rejected packets are blocked by the firewall and ICMP message is returned to the source host.</td> </tr> <tr> <td>Drop</td> <td>Dropped packets are blocked by the firewall.</td> </tr> </tbody> </table> | Accept | Accepted packets pass through the firewall. | Reject | Rejected packets are blocked by the firewall and ICMP message is returned to the source host. | Drop | Dropped packets are blocked by the firewall. |
| Accept   | Accepted packets pass through the firewall.  |        |   |        |   |      |  |
| Reject   | Rejected packets are blocked by the firewall and ICMP message is returned to the source host.  |        |   |        |   |      |  |
| Drop   | Dropped packets are blocked by the firewall.   |        |   |        |   |      |  |

|  |   |        |   |        |   |      |  |
|--|---|--------|---|--------|---|------|--|
| <p>Web: Output<br/>UCI: firewall.&lt;zone label&gt;.output<br/>Opt: output</p>             | <p>Default policy for outgoing zone traffic. Outgoing traffic is traffic leaving the router through an interface selected in the 'Covered Networks' option for this zone.</p> <table border="1" data-bbox="683 293 1331 519"> <tr> <td data-bbox="683 293 831 360">Accept</td> <td data-bbox="837 293 1331 360">Accepted packets pass through the firewall.</td> </tr> <tr> <td data-bbox="683 369 831 459">Reject</td> <td data-bbox="837 369 1331 459">Rejected packets are blocked by the firewall and ICMP message is returned to the source host.</td> </tr> <tr> <td data-bbox="683 468 831 528">Drop</td> <td data-bbox="837 468 1331 528">Dropped packets are blocked by the firewall.</td> </tr> </table>        | Accept | Accepted packets pass through the firewall. | Reject | Rejected packets are blocked by the firewall and ICMP message is returned to the source host. | Drop | Dropped packets are blocked by the firewall. |
| Accept   | Accepted packets pass through the firewall.   |        |   |        |   |      |  |
| Reject   | Rejected packets are blocked by the firewall and ICMP message is returned to the source host.   |        |   |        |   |      |  |
| Drop   | Dropped packets are blocked by the firewall.  |        |   |        |   |      |  |
| <p>Web: Forward<br/>UCI: firewall.&lt;zone label&gt;.forward<br/>Opt: forward</p>          | <p>Default policy for internal zone traffic between interfaces. Forward rules for a zone describe what happens to traffic passing between different interfaces within that zone.</p> <table border="1" data-bbox="683 636 1331 862"> <tr> <td data-bbox="683 636 831 703">Accept</td> <td data-bbox="837 636 1331 703">Accepted packets pass through the firewall.</td> </tr> <tr> <td data-bbox="683 712 831 801">Reject</td> <td data-bbox="837 712 1331 801">Rejected packets are blocked by the firewall and ICMP message is returned to the source host.</td> </tr> <tr> <td data-bbox="683 810 831 864">Drop</td> <td data-bbox="837 810 1331 864">Dropped packets are blocked by the firewall.</td> </tr> </table> | Accept | Accepted packets pass through the firewall. | Reject | Rejected packets are blocked by the firewall and ICMP message is returned to the source host. | Drop | Dropped packets are blocked by the firewall. |
| Accept   | Accepted packets pass through the firewall.   |        |   |        |   |      |  |
| Reject   | Rejected packets are blocked by the firewall and ICMP message is returned to the source host.   |        |   |        |   |      |  |
| Drop   | Dropped packets are blocked by the firewall.  |        |   |        |   |      |  |
| <p>Web: Masquerading<br/>UCI: firewall.&lt;zone label&gt;.masq<br/>Opt: masq</p>           | <p>Specifies whether outgoing zone traffic should be masqueraded (NATTED). This is typically enabled on the wan zone.</p>   |        |   |        |   |      |  |
| <p>Web: MSS Clamping<br/>UCI: firewall.&lt;zone label&gt;.mtu_fix<br/>Opt: mtu_fix</p>     | <p>Enables MSS clamping for outgoing zone traffic. Subnets are allowed.</p> <table border="1" data-bbox="683 1048 1390 1128"> <tr> <td data-bbox="683 1048 831 1093">0</td> <td data-bbox="837 1048 1390 1093">Disabled.</td> </tr> <tr> <td data-bbox="683 1102 831 1128">1</td> <td data-bbox="837 1102 1390 1128">Enabled.</td> </tr> </table>   | 0      | Disabled.                                   | 1      | Enabled.  |      |  |
| 0  | Disabled.   |        |   |        |   |      |  |
| 1  | Enabled.  |        |   |        |   |      |  |
| <p>Web: Covered networks<br/>UCI: firewall.&lt;zone label&gt;.network<br/>Opt: network</p> | <p>Defines a list of interfaces attached to this zone, if omitted, the value of name is used by default.<br/><b>Note:</b> use the uci list syntax to edit this setting through UCI.</p>   |        |   |        |   |      |  |

**Table 133: Information table for firewall zone general settings**

### 34.2.1.4 Firewall zone: advanced settings

The screenshot shows the 'Firewall - Zone Settings - Zone "lan"' page. It has tabs for 'General Settings', 'Port Forwards', and 'Traffic Rules'. The 'Advanced Settings' tab is active. Below the title, there is a description of the zone settings. The settings are as follows:

- Restrict to address family: IPv4 and IPv6
- Restrict Masquerading to given source subnets: 0.0.0.0/0
- Restrict Masquerading to given destination subnets: 0.0.0.0/0
- Force connection tracking:
- Enable logging on this zone:
- Allow NAT Reflections:

Figure 196: Firewall zone advanced settings

| Web Field/UCI/Package Option   | Description   |        |                     |     |   |                    |     |           |           |      |           |           |      |
|--|---|--------|---------------------|-----|---|--------------------|-----|-----------|-----------|------|-----------|-----------|------|
| Web: Restrict to address family<br>UCI: firewall.<zone label>.family<br>Opt: family                                | Restricts zone to IPv4, IPv6 or both IPv4 and IPv6. <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>IPv4 and IPv6</td> <td>Any address family</td> <td>any</td> </tr> <tr> <td>IPv4 only</td> <td>IPv4 only</td> <td>ipv4</td> </tr> <tr> <td>IPv6 only</td> <td>IPv6 only</td> <td>Ipv6</td> </tr> </tbody> </table> | Option | Description         | UCI | IPv4 and IPv6                                     | Any address family | any | IPv4 only | IPv4 only | ipv4 | IPv6 only | IPv6 only | Ipv6 |
| Option   | Description   | UCI    |                     |     |   |                    |     |           |           |      |           |           |      |
| IPv4 and IPv6  | Any address family  | any    |                     |     |   |                    |     |           |           |      |           |           |      |
| IPv4 only  | IPv4 only   | ipv4   |                     |     |   |                    |     |           |           |      |           |           |      |
| IPv6 only  | IPv6 only   | Ipv6   |                     |     |   |                    |     |           |           |      |           |           |      |
| Web: Restrict Masquerading to given source subnets.<br>UCI: firewall.<zone label>.masq_src<br>Opt: masq_src        | Limits masquerading to the given source subnets. Negation is possible by prefixing the subnet with '!'. Multiple subnets are allowed.   |        |                     |     |   |                    |     |           |           |      |           |           |      |
| Web: Restrict Masquerading to given destination subnets.<br>UCI: firewall.<zone label>.masq_dest<br>Opt: masq_dest | Limits masquerading to the given destination subnets. Negation is possible by prefixing the subnet with '!'. Multiple subnets are allowed. Multiple IP addresses/subnets should be separated by a space, for example: option masq_dest '1.1.1.1 2.2.2.0/24'.  |        |                     |     |   |                    |     |           |           |      |           |           |      |
| Web: Force connection tracking<br>UCI: firewall.<zone label>.contrack<br>Opt: contrack                             | Forces connection tracking for this zone. <table border="1"> <tbody> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>If masquerading is used. Otherwise, default is 0.</td> </tr> </tbody> </table>  | 0      | Disabled.           | 1   | If masquerading is used. Otherwise, default is 0. |                    |     |           |           |      |           |           |      |
| 0  | Disabled.   |        |                     |     |   |                    |     |           |           |      |           |           |      |
| 1  | If masquerading is used. Otherwise, default is 0.   |        |                     |     |   |                    |     |           |           |      |           |           |      |
| Web: Enable logging on this zone<br>UCI: firewall.<zone label>.log<br>Opt: log                                     | Creates log rules for rejected and dropped traffic in this zone.  |        |                     |     |   |                    |     |           |           |      |           |           |      |
| Web: Allow NAT reflections<br>UCI: firewall.<zone label>.reflection<br>Opt: reflection                             | Enable/disable all NAT reflections for this zone.<br><b>Note:</b> for configs with a large number of firewall rules, disabling NAT reflection will speed up load of firewall rules on interface start. <table border="1"> <tbody> <tr> <td>0</td> <td>Disable reflection.</td> </tr> <tr> <td>1</td> <td>Enable reflection.</td> </tr> </tbody> </table>                                | 0      | Disable reflection. | 1   | Enable reflection.                                |                    |     |           |           |      |           |           |      |
| 0  | Disable reflection.   |        |                     |     |   |                    |     |           |           |      |           |           |      |
| 1  | Enable reflection.  |        |                     |     |   |                    |     |           |           |      |           |           |      |

|  |   |
|--|---|
| Web: n/a<br>UCI: firewall.<zone label>.log_limit<br>Opt: log_limit | Limits the amount of log messages per interval. |
|--|---|

**Table 134: Information table for firewall zone advanced settings**

### 34.2.1.5 Inter-zone forwarding

This section controls the traffic flow between zones. Selecting a source or destination zone generates a forwarding rule. Only one direction is covered by any forwarding rule. Hence for bidirectional traffic flow between two zones then two rules are required, with source and destination alternated.

**Figure 197: The inter-zone forwarding section**

| Web Field/UCI/Package Option  | Description  |
|---|--|
| Web: Allow forward to destination zones<br>UCI: firewall.<forwarding label>.dest<br>Opt: dest | Allows forward to other zones. Enter the current zone as the source.<br><br>Enabling this option puts two entries into the firewall file: destination and source.        |
| UCI firewall.<forwarding label>.src<br>Opt: src   |  |
| Web: Allow forward from source zones<br>UCI: firewall.<forwarding label>.dest<br>Opt: dest    | Allows forward from other zones. Enter the current zone as the destination.<br><br>Enabling this option puts two entries into the firewall file: destination and source. |
| UCI: firewall.<forwarding label>.src<br>Opt: src  |  |

**Table 135: Information table for inter-zone forwarding settings**

**Note:** the rules generated for forwarding traffic between zones relay connection tracking to be enabled on at least one of the source or destination zones. This can be enabled through the conntrack option or through masq.

## 34.2.2 Firewall port forwards

Port forwards are also known as redirects. This section creates the redirects using DNAT (Destination Network Address Translation) with Netfilter. The redirects are from the firewall zone labelled as wan to the firewall zone labelled as lan. These zones can refer to multiple external and internal interfaces as defined in the Firewall Zone settings.

To edit an existing port forward select **edit**.

To add a new port forward select **add**.

General Settings | Port Forwards | Traffic Rules

## Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

| Name  | Protocol | Source               | Via                          | Destination                                    | Enable                              | Sort  |
|-------|----------|----------------------|------------------------------|--|-------------------------------------|---|
| HTTPS | TCP      | From any host in wan | To any router IP at port 443 | Forward to IP 192.168.100.100, port 443 in lan | <input checked="" type="checkbox"/> | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

New port forward:

| Name  | Protocol  | External port        | Internal IP address  | Internal port        |
|---|-----------|----------------------|----------------------|----------------------|
| <input type="text" value="New port forward"/> | TCP+UDP ▼ | <input type="text"/> | <input type="text"/> | <input type="text"/> |

Figure 198: The firewall port forward page

| Web Field/UCI/Package Option   | Description   |         |                            |       |           |                                  |         |     |                         |     |     |                         |     |
|--|---|---------|----------------------------|-------|-----------|----------------------------------|---------|-----|-------------------------|-----|-----|-------------------------|-----|
| Web: name<br>UCI: firewall.<redirect label>.name<br>Opt: name                      | Sets the port forwarding name. For Web UI generated redirects the <redirect label> takes the form of @redirect[x], where x is an integer starting from 0.   |         |                            |       |           |                                  |         |     |                         |     |     |                         |     |
| Web: Protocol<br>UCI: firewall.<redirect label>.proto<br>Opt: proto                | Defines layer 4 protocol to match incoming traffic. <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>tcp+udp</td> <td>Match either TCP or UDP packets.</td> <td>tcp udp</td> </tr> <tr> <td>tcp</td> <td>Match TCP packets only.</td> <td>tcp</td> </tr> <tr> <td>udp</td> <td>Match UDP packets only.</td> <td>udp</td> </tr> </tbody> </table> | Option  | Description                | UCI   | tcp+udp   | Match either TCP or UDP packets. | tcp udp | tcp | Match TCP packets only. | tcp | udp | Match UDP packets only. | udp |
| Option   | Description   | UCI     |                            |       |           |                                  |         |     |                         |     |     |                         |     |
| tcp+udp  | Match either TCP or UDP packets.  | tcp udp |                            |       |           |                                  |         |     |                         |     |     |                         |     |
| tcp  | Match TCP packets only.   | tcp     |                            |       |           |                                  |         |     |                         |     |     |                         |     |
| udp  | Match UDP packets only.   | udp     |                            |       |           |                                  |         |     |                         |     |     |                         |     |
| Web: External port<br>UCI: firewall.<redirect label>.src_dport<br>Opt: src_dport   | Specifies the incoming TCP/UDP port or port range to match. This is the incoming destination port specified by the external host. Port ranges specified as start:stop, for example, 2001:2020. <table border="1"> <tbody> <tr> <td>Blank</td> <td>Match traffic to any port.</td> </tr> <tr> <td>Range</td> <td>1 - 65535</td> </tr> </tbody> </table>  | Blank   | Match traffic to any port. | Range | 1 - 65535 |                                  |         |     |                         |     |     |                         |     |
| Blank  | Match traffic to any port.  |         |                            |       |           |                                  |         |     |                         |     |     |                         |     |
| Range  | 1 - 65535   |         |                            |       |           |                                  |         |     |                         |     |     |                         |     |
| Web: Internal IP address<br>UCI: firewall.<redirect label>.dest_ip<br>Opt: dest_ip | Specifies the internal (LAN) IP address for the traffic to be redirected to.  |         |                            |       |           |                                  |         |     |                         |     |     |                         |     |
| Web: Internal port<br>UCI: firewall.<redirect label>.dest_port<br>Opt: dest_port   | Specifies the destination tcp/udp port for the redirect traffic.  |         |                            |       |           |                                  |         |     |                         |     |     |                         |     |

Table 136: Information table for firewall port forward settings

The defined redirects can be sorted into a specific order to be applied. More specific rules should be placed first.

After the redirect is created and saved, to make changes, click **Edit**. This will provide further options to change the source/destination zones; specify source MAC addresses and enable NAT loopback (reflection).

[General Settings](#) | [Port Forwards](#) | [Traffic Rules](#)

## Firewall - Port Forwards - (Unnamed Entry)

This page allows you to change advanced properties of the port forwarding entry. In most cases there is no need to modify those settings.

Rule is enabled

Name

Protocol

Source zone

lan: LAN1:  LAN2:  LAN3:

wan: MOBILE1:  PoAADSL:

Source MAC address

Only match incoming traffic from these MACs.

Source IP address

Only match incoming traffic from this IP or range.

Source port

Only match incoming traffic originating from the given source port or port range on the client host

External IP address

Only match incoming traffic directed at the given IP address.

External port

Match incoming traffic directed at the given destination port or port range on this host

Internal zone

lan: LAN1:  LAN2:  LAN3:

wan: MOBILE1:  PoAADSL:

Internal IP address

Redirect matched incoming traffic to the specified internal host

Internal port

Redirect matched incoming traffic to the given port on the internal host

Enable NAT Loopback

Extra arguments

Passes additional arguments to iptables. Use with care!

Figure 199: The firewall port forwards edits page

| Web Field/UCI/Package Option   | Description   |         |             |     |          |                                  |         |     |                         |     |     |                         |     |
|--|---|---------|-------------|-----|----------|----------------------------------|---------|-----|-------------------------|-----|-----|-------------------------|-----|
| Web: Rule is enabled<br>UCI: firewall.<redirect label>.enabled<br>Opt: enabled | Specifies if this redirect should be enabled or disabled. <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">0</td> <td style="width: 60px;">Disabled.</td> </tr> <tr> <td style="text-align: center;">1</td> <td>Enabled.</td> </tr> </table>  | 0       | Disabled.   | 1   | Enabled. |                                  |         |     |                         |     |     |                         |     |
| 0  | Disabled.   |         |             |     |          |                                  |         |     |                         |     |     |                         |     |
| 1  | Enabled.  |         |             |     |          |                                  |         |     |                         |     |     |                         |     |
| Web: name<br>UCI: firewall.<redirect label>.name<br>Opt: name                  | Sets the port forwarding name. For Web UI generated redirects the <redirect label> takes the form of @redirect[x], where x is an integer starting from 0.   |         |             |     |          |                                  |         |     |                         |     |     |                         |     |
| Web: Protocol<br>UCI: firewall.<redirect label>.proto<br>Opt: proto            | Defines layer 4 protocol to match incoming traffic. <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Option</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>tcp+udp</td> <td>Match either TCP or UDP packets.</td> <td>tcp udp</td> </tr> <tr> <td>tcp</td> <td>Match TCP packets only.</td> <td>tcp</td> </tr> <tr> <td>udp</td> <td>Match UDP packets only.</td> <td>udp</td> </tr> </tbody> </table> | Option  | Description | UCI | tcp+udp  | Match either TCP or UDP packets. | tcp udp | tcp | Match TCP packets only. | tcp | udp | Match UDP packets only. | udp |
| Option   | Description   | UCI     |             |     |          |                                  |         |     |                         |     |     |                         |     |
| tcp+udp  | Match either TCP or UDP packets.  | tcp udp |             |     |          |                                  |         |     |                         |     |     |                         |     |
| tcp  | Match TCP packets only.   | tcp     |             |     |          |                                  |         |     |                         |     |     |                         |     |
| udp  | Match UDP packets only.   | udp     |             |     |          |                                  |         |     |                         |     |     |                         |     |
| Web: Source zone<br>UCI: firewall.<redirect label>.src<br>Opt: src             | Specifies the traffic source zone. It must refer to one of the defined zone names. When using the web interface, this is set to WAN initially.  |         |             |     |          |                                  |         |     |                         |     |     |                         |     |

|   |   |       |                                     |       |                     |
|---|---|-------|-------------------------------------|-------|---------------------|
| <p>Web: Source MAC address<br/>UCI: firewall.&lt;redirect label&gt;.src_mac<br/>Opt: list src_mac</p>   | <p>Defines the list of source MAC addresses that this redirect will match.</p> <p>Format: aa:bb:cc:dd:ee:ff</p> <p>Multiple RIP interfaces are entered using <code>uci set</code> and <code>uci add_list</code> commands. Example:</p> <pre>uci set firewall.@redirect[0].src_mac=aa:bb:cc:dd:ee:ff uci add_list firewall.@redirect[0].src_mac=12:34:56:78:90:12</pre> <p>or using a list of options via package options</p> <pre>list network 'aa:bb:cc:dd:ee:ff' list network '12:34:56:78:90:12'</pre>                         |       |                                     |       |                     |
| <p>Web: Source IP address<br/>UCI: firewall.&lt;redirect label&gt;.src_ip<br/>Opt: src_ip</p>           | <p>Defines a source IP address that this redirect will match.</p> <table border="1"> <tr> <td>Blank</td> <td>Match traffic from any source IP.</td> </tr> <tr> <td>Range</td> <td>A.B.C.D/mask.</td> </tr> </table>   | Blank | Match traffic from any source IP.   | Range | A.B.C.D/mask.       |
| Blank   | Match traffic from any source IP.   |       |                                     |       |                     |
| Range   | A.B.C.D/mask.   |       |                                     |       |                     |
| <p>Web: Source port<br/>UCI: firewall.&lt;redirect label&gt;.src_port<br/>Opt: src_port</p>             | <p>Defines a source IP port that this redirect will match. You can enter multiple ports, using a space separator.</p> <p>*For example: option src_port '22 23'</p> <p>*see note below on use with options src_dport and dest_port</p> <table border="1"> <tr> <td>Blank</td> <td>Match traffic from any source port.</td> </tr> <tr> <td>Range</td> <td>1 - 65535</td> </tr> </table>   | Blank | Match traffic from any source port. | Range | 1 - 65535           |
| Blank   | Match traffic from any source port.   |       |                                     |       |                     |
| Range   | 1 - 65535   |       |                                     |       |                     |
| <p>Web: External port<br/>UCI: firewall.&lt;redirect label&gt;.src_dport<br/>Opt: src_dport</p>         | <p>Specifies the incoming TCP/UDP port or port range to match. This is the incoming destination port specified by the external host. Port ranges specified in format start:stop, for example, 2001:2020.</p> <p>You can enter multiple ports, using a space separator.</p> <p>*For example: option src_dport '22 23'</p> <p>*see note below on use with options src_port and dest_port</p> <table border="1"> <tr> <td>Blank</td> <td>Match traffic to any port.</td> </tr> <tr> <td>Range</td> <td>1 - 65535</td> </tr> </table> | Blank | Match traffic to any port.          | Range | 1 - 65535           |
| Blank   | Match traffic to any port.  |       |                                     |       |                     |
| Range   | 1 - 65535   |       |                                     |       |                     |
| <p>Web: Internal zone<br/>UCI: firewall.&lt;redirect label&gt;.dest<br/>Opt: dest</p>                   | <p>Specifies the traffic destination zone, must refer to one of the defined zone names.</p>   |       |                                     |       |                     |
| <p>Web: Internal IP address<br/>UCI: firewall.&lt;redirect label&gt;.dest_ip<br/>Opt: dest_ip</p>       | <p>Specifies the internal (LAN) IP address for the traffic to be redirected to.</p>   |       |                                     |       |                     |
| <p>Web: Internal port<br/>UCI: firewall.&lt;redirect label&gt;.dest_port<br/>Opt: dest_port</p>         | <p>Specifies the destination tcp/udp port for the redirect traffic. You can enter multiple ports, using a space separator.</p> <p>*For example: option dest_port '22 23'</p> <p>*See note below table on use with options src_port and src_dport.</p>   |       |                                     |       |                     |
| <p>Web: Enable NAT Loopback<br/>UCI: firewall.&lt;redirect label&gt;.reflection<br/>Opt: reflection</p> | <p>Enable or disable NAT reflection for this redirect.</p> <table border="1"> <tr> <td>0</td> <td>Reflection disabled.</td> </tr> <tr> <td>1</td> <td>Reflection enabled.</td> </tr> </table>   | 0     | Reflection disabled.                | 1     | Reflection enabled. |
| 0   | Reflection disabled.  |       |                                     |       |                     |
| 1   | Reflection enabled.   |       |                                     |       |                     |
| <p>Web: Extra arguments<br/>UCI: firewall.&lt;redirect label&gt;.extra<br/>Opt: extra</p>               | <p>Passes extra arguments to IP tables. This is useful to specify additional match options, like <code>-m policy --dir in</code> for IPsec. The arguments are entered as text strings.</p>  |       |                                     |       |                     |

**Table 137: Information table for port forward edits fields**



**\*Note:** redirect rule options `src_port` and `src_dport/dest_port` accept space-separated lists of ports. If `src_port` is a list, then `src_dport/dst_port` cannot be, to avoid ambiguity.

If `src_dport/dest_port` are lists of different lengths, then the missing values of the shorter list default to the corresponding port in the other list. For example, if configuration file is:

```
option src_dport '21 22 23'
option dest_port '21 22 23 24'
```

then the firmware will interpret the values as:

```
option src_dport '21 22 23 24'
option dest_port '21 22 23 24'
```

### 34.2.3 Firewall traffic rules

Rules can be defined to allow or restrict access to specific ports, hosts or protocols.

The screenshot shows the 'Firewall - Traffic Rules - (Unnamed Rule)' configuration page. The page has tabs for 'General Settings', 'Port Forwards', and 'Traffic Rules'. The main title is 'Firewall - Traffic Rules - (Unnamed Rule)' and a subtitle reads 'This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.'

The configuration options are as follows:

- Rule is enabled:
- Name:
- Restrict to address family:
- Protocol:
- Match ICMP type:
- Source zone:
  - Any zone
  - lan: LAN1: LAN2: LAN3:
  - wan: MOBILE1: PoAADS1:
- Source MAC address:
- Source address:
- Source port:
- Destination zone:
  - Device (input)
  - Any zone (forward)
  - lan: LAN1: LAN2: LAN3:
  - wan: MOBILE1: PoAADS1:
- Destination address:
- Destination port:
- Action:
- Extra arguments:  Passes additional arguments to iptables. Use with care!

Figure 200: The firewall traffic rules page

| Web Field/UCI/Package Option  | Description   |         |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
|---|---|---------|-------------------|-----|------------------|--|---------|-----------|--------------------------|------|-----------|--------------------------|------|------|---------------------------|------|--------|--------------------------------------|--|
| Web: Rule is enabled<br>UCI: firewall.<rule label>.enabled<br>Opt: enabled          | Enables or disables traffic rule. <table border="1"> <tr> <td>0</td> <td>Rule is disabled.</td> </tr> <tr> <td>1</td> <td>Rule is enabled.</td> </tr> </table>  | 0       | Rule is disabled. | 1   | Rule is enabled. |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| 0   | Rule is disabled.   |         |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| 1   | Rule is enabled.  |         |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| Web: Name<br>UCI: firewall.<rule label>.name<br>Opt: name                           | Select a descriptive name limited to less than 11 characters. No spaces are allowed in the naming convention.   |         |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| Web: Restrict to address family<br>UCI: firewall.<rule label>.family<br>Opt: family | Restrict to protocol family. <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>IPv4 and IPv6</td> <td>Traffic rule applies to any address family</td> <td>any</td> </tr> <tr> <td>IPv4 only</td> <td>IPv4 only</td> <td>ipv4</td> </tr> <tr> <td>IPv6 only</td> <td>IPv6 only</td> <td>ipv6</td> </tr> </tbody> </table>  | Option  | Description       | UCI | IPv4 and IPv6    | Traffic rule applies to any address family | any     | IPv4 only | IPv4 only                | ipv4 | IPv6 only | IPv6 only                | ipv6 |      |                           |      |        |                                      |  |
| Option  | Description   | UCI     |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| IPv4 and IPv6   | Traffic rule applies to any address family  | any     |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| IPv4 only   | IPv4 only   | ipv4    |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| IPv6 only   | IPv6 only   | ipv6    |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| Web: Protocol<br>UCI: firewall.<rule label>.proto<br>Opt: proto                     | Matches incoming traffic using the given protocol. <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>TCP+UDP</td> <td>Applies rule to TCP and UDP only</td> <td>tcp udp</td> </tr> <tr> <td>TCP</td> <td>Applies rule to TCP only</td> <td>tcp</td> </tr> <tr> <td>UDP</td> <td>Applies rule to UDP only</td> <td>udp</td> </tr> <tr> <td>ICMP</td> <td>Applies rule to ICMP only</td> <td>icmp</td> </tr> <tr> <td>custom</td> <td>Specify protocol from /etc/protocols</td> <td></td> </tr> </tbody> </table> | Option  | Description       | UCI | TCP+UDP          | Applies rule to TCP and UDP only           | tcp udp | TCP       | Applies rule to TCP only | tcp  | UDP       | Applies rule to UDP only | udp  | ICMP | Applies rule to ICMP only | icmp | custom | Specify protocol from /etc/protocols |  |
| Option  | Description   | UCI     |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| TCP+UDP   | Applies rule to TCP and UDP only  | tcp udp |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| TCP   | Applies rule to TCP only  | tcp     |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| UDP   | Applies rule to UDP only  | udp     |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| ICMP  | Applies rule to ICMP only   | icmp    |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| custom  | Specify protocol from /etc/protocols  |         |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| Web: Match ICMP type<br>UCI: firewall.<rule label>.icmp_type<br>Opt: icmp_type      | Match specific icmp types.<br>This option is only valid when ICMP is selected as the protocol. ICMP types can be listed as either type names or type numbers.<br><b>Note:</b> for a full list of valid ICMP type names, see the ICMP Options table below.   |         |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| Web: Source zone<br>UCI: firewall.<rule label>.src<br>Opt: src                      | Specifies the traffic source zone, must refer to one of the defined zone names. For typical port forwards, this is usually WAN.   |         |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| Web: Source MAC address<br>UCI: firewall.<rule label>.src_mac<br>Opt: src_mac       | Matches incoming traffic from the specified MAC address.<br>The MAC address must be entered in the following format:<br>aa:bb:cc:dd:ee:ff:<br>To only match the first portion of the MAC address append /prefix to the option value, where prefix defines the bits from the start of the MAC to match on.<br>Example:<br>option src_mac 00:E0:C8:12:34:56/24<br>will match on all packets with prefix 00:E0:C8.   |         |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| Web: Source address<br>UCI: firewall.<rule label>.src_ip<br>Opt: src_ip             | Matches incoming traffic from the specified source IP address.  |         |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| Web: Source port<br>UCI: firewall.<rule label>.src_port<br>Opt: src_port            | Matches incoming traffic originating from the given source port or port range on the client host.   |         |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| Web: Destination zone<br>UCI: firewall.<rule label>.dest<br>Opt: dest               | Specifies the traffic destination zone. Must refer to one of the defined zone names.  |         |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |
| Web: Destination address<br>UCI: firewall.<rule label>.dest_ip<br>Opt: dest_ip      | For DNAT, redirects matched incoming traffic to the specified internal host.<br>For SNAT, matches traffic directed at the given address.  |         |                   |     |                  |  |         |           |                          |      |           |                          |      |      |                           |      |        |                                      |  |

| <p>Web: Destination port<br/>UCI: firewall.&lt;rule label&gt;.dest_port<br/>Opt: dest_port</p> | <p>For DNAT, redirects matched incoming traffic to the given port on the internal host.<br/>For SNAT, matches traffic directed at the given ports.</p>  |         |             |     |      |                       |      |        |                        |        |        |                         |        |             |   |         |
|--|---|---------|-------------|-----|------|-----------------------|------|--------|------------------------|--------|--------|-------------------------|--------|-------------|---|---------|
| <p>Web: Action<br/>UCI: firewall.&lt;rule label&gt;.target<br/>Opt: target</p>                 | <p>Action to take when rule is matched.</p> <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>drop</td> <td>Drop matching traffic</td> <td>DROP</td> </tr> <tr> <td>accept</td> <td>Allow matching traffic</td> <td>ACCEPT</td> </tr> <tr> <td>reject</td> <td>Reject matching traffic</td> <td>REJECT</td> </tr> <tr> <td>don't track</td> <td>Disable connection tracking for the rule. See the 'Connection tracking' section below for more information.</td> <td>NOTRACK</td> </tr> </tbody> </table> | Option  | Description | UCI | drop | Drop matching traffic | DROP | accept | Allow matching traffic | ACCEPT | reject | Reject matching traffic | REJECT | don't track | Disable connection tracking for the rule. See the 'Connection tracking' section below for more information. | NOTRACK |
| Option   | Description   | UCI     |             |     |      |                       |      |        |                        |        |        |                         |        |             |   |         |
| drop   | Drop matching traffic   | DROP    |             |     |      |                       |      |        |                        |        |        |                         |        |             |   |         |
| accept   | Allow matching traffic  | ACCEPT  |             |     |      |                       |      |        |                        |        |        |                         |        |             |   |         |
| reject   | Reject matching traffic   | REJECT  |             |     |      |                       |      |        |                        |        |        |                         |        |             |   |         |
| don't track  | Disable connection tracking for the rule. See the 'Connection tracking' section below for more information.   | NOTRACK |             |     |      |                       |      |        |                        |        |        |                         |        |             |   |         |
| <p>Web: Extra arguments<br/>UCI: firewall.&lt;rule label&gt;.extra<br/>Opt: extra</p>          | <p>Passes extra arguments to IP tables. This is useful to specify additional match options, like -m policy --dir in for IPsec.</p>  |         |             |     |      |                       |      |        |                        |        |        |                         |        |             |   |         |
| <p>Web: n/a<br/>UCI: firewall.&lt;rule label&gt;.reflection<br/>Opt: reflection</p>            | <p>Disables NAT reflection for this redirect if set to 0. Applicable to DNAT targets.</p>   |         |             |     |      |                       |      |        |                        |        |        |                         |        |             |   |         |
| <p>Web: n/a<br/>UCI: firewall.&lt;rule label&gt;.limit<br/>Opt: limit</p>                      | <p>Sets maximum average matching rate; specified as a number, with an optional /second, /minute, /hour or /day suffix. Example: 3/hour.</p>   |         |             |     |      |                       |      |        |                        |        |        |                         |        |             |   |         |
| <p>Web: n/a<br/>UCI: firewall.&lt;rule label&gt;.limit_burst<br/>Opt: limit_burst</p>          | <p>Sets maximum initial number of packets to match. This number gets recharged by one every time the limit specified above is not reached, up to this number.</p>   |         |             |     |      |                       |      |        |                        |        |        |                         |        |             |   |         |
| <p>Web: n/a<br/>UCI: firewall.&lt;rule label&gt;.recent<br/>Opt: recent</p>                    | <p>Sets number of allowed connections within specified time. This command takes two values e.g. recent=2 120 will allow 2 connections within 120 seconds.</p>   |         |             |     |      |                       |      |        |                        |        |        |                         |        |             |   |         |

**Table 138: Information table for firewall traffic rules**

| ICMP Options              | ICMP Options        | ICMP Options            | ICMP Options               |
|---------------------------|---------------------|-------------------------|----------------------------|
| address-mask-reply        | host-redirect       | pong                    | time-exceeded              |
| address-mask-request      | host-unknown        | port-unreachable        | timestamp-reply            |
| any                       | host-unreachable    | precedence-cutoff       | timestamp-request          |
| communication-prohibited  | ip-header-bad       | protocol-unreachable    | TOS-host-redirect          |
| destination-unreachable   | network-prohibited  | redirect                | TOS-host-unreachable       |
| echo-reply                | network-redirect    | required-option-missing | TOS-network-redirect       |
| echo-request              | network-unknown     | router-advertisement    | TOS-network-unreachable    |
| fragmentation-needed      | network-unreachable | router-solicitation     | ttl-exceeded               |
| host-precedence-violation | parameter-problem   | source-quench           | ttl-zero-during-reassembly |
| host-prohibited           | ping                | source-route-failed     | ttl-zero-during-transit    |

**Table 139: Information table for match ICMP type drop-down menu**

## 34.3 Configuring firewall using UCI

Firewall is configured under the firewall package `/etc/config/firewall`.

There are six config sections: `defaults`, `zone`, `forwarding`, `redirect`, `rule` and `include`.

You can configure multiple `zone`, `forwarding` and `redirect` sections.

### 34.3.1 Firewall general settings

To set general (default) settings, enter:

```
uci add firewall defaults
uci set firewall.@defaults[0].syn_flood=1
uci set firewall.@defaults[0].drop_invalid=1
uci set firewall.@defaults[0].input=ACCEPT
uci set firewall.@defaults[0].output=ACCEPT
uci set firewall.@defaults[0].forward=ACCEPT
```

**Note:** this command is only required if there is no `defaults` section.

### 34.3.2 Firewall zone settings

By default, all firewall zone instances are named `zone`, instances are identified by `@zone` then the zone position in the package as a number. For example, for the first zone in the package using UCI, enter:

```
firewall.@zone[0]=zone
firewall.@zone[0].name=lan
```

Or using package options:

```
config zone
    option name 'lan'
```

To set up a firewall zone, enter:

```
uci add firewall zone
uci set firewall.@zone[1].name=lan
uci set firewall.@zone[1].input=ACCEPT
uci set firewall.@zone[1].output=ACCEPT
uci set firewall.@zone[1].forward=ACCEPT
uci set firewall.@zone[1].network=lan1 wifi_client
uci set firewall.@zone[1].family=any
uci set firewall.@zone[1].masq_src=10.0.0.0/24
uci set firewall.@zone[1].masq_dest=20.0.0.0/24
```

```
uci set firewall.@zone[1].contrack=1
uci set firewall.@zone[1].masq=1
uci set firewall.@zone[1].mtu_fix=1
uci set firewall.@zone[1].log=1
uci set firewall.@zone[1].log_limit=5
```

### 34.3.3 Inter-zone forwarding

By default, all inter-zone instances are named 'forwarding'; instances are identified by @forwarding then the forwarding position in the package as a number. For example, for the first forwarding in the package using UCI, enter:

```
firewall.@forwarding[0]=forwarding
firewall.@forwarding[0].src=lan
```

Or using package options:

```
config forwarding
    option src 'lan'
```

To enable forwarding of traffic from WAN to LAN, enter:

```
uci add firewall forwarding
uci set firewall.@forwarding[1].dest=wan
uci set firewall.@forwarding[1].src=lan
```

### 34.3.4 Firewall port forwards

By default, all port forward instances are named 'redirect'; instances are identified by @redirect then the redirect position in the package as a number. For example, for the first redirect in the package using UCI, enter:

```
firewall.@redirect[0]=redirect
firewall.@redirect[0].name=Forward
```

Or using package options:

```
config redirect
    option name 'Forward'
```

To set port forwarding rules, enter:

```
uci add firewall redirect
uci set firewall.@redirect[1].name=Forward
```

```
uci set firewall.@redirect[1].proto=tcp
uci set firewall.@redirect[1].src=wan # <- zone names
uci set firewall.@redirect[1].dest=lan # <- zone names
uci set firewall.@redirect[1].src_dport=2001
uci set firewall.@redirect[1].dest_ip=192.168.0.100
uci set firewall.@redirect[1].dest_port=2005
uci set firewall.@redirect[1].enabled=1
```

### 34.3.5 Firewall traffic rules

By default, all traffic rule instances are named rule, instances are identified by @rule then the rule position in the package as a number. For example, for the first rule in the package using UCI, enter:

```
firewall.@rule[0]=rule
firewall.@rule[0].enabled=1
```

Or using package options:

```
config rule
    option enabled '1'
```

To set traffic rules, enter:

```
uci add firewall rule
uci set firewall.@rule[1].enabled=1
uci set firewall.@rule[1].name=Allow_ICMP
uci set firewall.@rule[1].family=any
uci set firewall.@rule[1].proto=ICMP
uci set firewall.@rule[1].icmp_type=any
uci set firewall.@rule[1].src=wan
uci set firewall.@rule[1].src_mac=ff:ff:ff:ff:ff:ff
uci set firewall.@rule[1].src_port=
uci set firewall.@rule[1].dest=lan
uci set firewall.@rule[1].dest_port=
uci set firewall.@rule[1].dest_ip=192.168.100.1
uci set firewall.@rule[1].target=ACCEPT
uci set firewall.@rule[1].extra=
uci set firewall.@rule[1].src_ip=8.8.8.8
uci set firewall.@rule[1].src_dip=9.9.9.9
```

```
uci set firewall.@rule[1].src_dport=68
uci set firewall.@rule[1].reflection=1
uci set firewall.@rule[1].limit=3/second
uci set firewall.@rule[1].limit_burst=30
```

### 34.3.5.1 Custom firewall scripts: includes

It is possible to include custom firewall scripts by specifying one or more include sections in the firewall configuration.

There is only one possible parameter for includes:

| Parameter | Description   |
|-----------|---|
| path      | Specifies a shell script to execute on boot or firewall restarts. |

Custom scripts are executed as shell scripts and are expected to contain iptables commands.

## 34.4 IPv6 notes

As described above, the option family is used for distinguishing between IPv4, IPv6 and both protocols. However, the family is inferred automatically if a specific IP address family is used. For example, if IPv6 addresses are used then the rule is automatically treated as IPv6 only rule.

```
config rule
    option src wan
    option src_ip fdca:f00:ba3::/64
    option target ACCEPT
```

Similarly, the following rule is automatically treated as IPv4 only.

```
config rule
    option src wan
    option dest_ip 88.77.66.55
    option target REJECT
```

Rules without IP addresses are automatically added to iptables and ip6tables, unless overridden by the family option. Redirect rules (port forwards) are always IPv4 since there is no IPv6 DNAT support at present.

## 34.5 Implications of DROP vs. REJECT

The decision whether to drop or to reject traffic should be done on a case-by-case basis. Many people see dropping traffic as a security advantage over rejecting it because it exposes less information to a hypothetical attacker. While dropping slightly increases

security, it can also complicate the debugging of network issues or cause unwanted side-effects on client programs.

If traffic is rejected, the router will respond with an icmp error message ("destination port unreachable") causing the connection attempt to fail immediately. This also means that for each connection attempt a certain amount of response traffic is generated. This can actually harm if the firewall is attacked with many simultaneous connection attempts, the resulting backfire of icmp responses can clog up all available upload and make the connection unusable (DoS).

When connection attempts are dropped the client is not aware of the blocking and will continue to re-transmit its packets until the connection eventually times out. Depending on the way the client software is implemented, this could result in frozen or hanging programs that need to wait until a timeout occurs before they're able to continue.

#### **DROP**

- less information is exposed
- less attack surface
- client software may not cope well with it (hangs until connection times out)
- may complicate network debugging (where was traffic dropped and why)

#### **REJECT**

- may expose information (like the IP at which traffic was actually blocked)
- client software can recover faster from rejected connection attempts
- network debugging easier (routing and firewall issues clearly distinguishable)

## **34.6 Connection tracking**

By default, the firewall will disable connection tracking for a zone if no masquerading is enabled. This is achieved by generating NOTRACK firewall rules matching all traffic passing via interfaces referenced by the firewall zone. The purpose of NOTRACK is to speed up routing and save memory by circumventing resource intensive connection tracking in cases where it is not needed. You can check if connection tracking is disabled by issuing `iptables -t raw -S`, it will list all rules, check for NOTRACK target.

NOTRACK will render certain iptables extensions unusable, for example the MASQUERADE target or the state match will not work.

If connection tracking is required, for example by custom rules in `/etc/firewall.user`, you must enable the `contrack` option in the corresponding zone to disable NOTRACK. It should appear as option `'contrack' '1'` in the right zone in `/etc/config/firewall`.



## 34.7 Firewall examples

### 34.7.1 Opening ports

The default configuration accepts all LAN traffic, but blocks all incoming WAN traffic on ports not currently used for connections or NAT. To open a port for a service, add a rule section:

```
config rule
    option src          wan
    option dest_port    22
    option target       ACCEPT
    option proto        tcp
```

This example enables machines on the internet to use SSH to access your router.

### 34.7.2 Forwarding ports (destination NAT/DNAT)

This example forwards http, but not HTTPS, traffic to the web server running on 192.168.1.10:

```
config redirect
    option src          wan
    option src_dport    80
    option proto        tcp
    option dest_ip      192.168.1.10
```

The next example forwards one arbitrary port that you define to a box running SSH behind the firewall in a more secure manner because it is not using default port 22.

```
config 'redirect'
    option 'name' 'ssh'
    option 'src' 'wan'
    option 'proto' 'tcpudp'
    option 'src_dport' '5555'
    option 'dest_ip' '192.168.1.100'
    option 'dest_port' '22'
    option 'target' 'DNAT'
    option 'dest' 'lan'
```

### 34.7.3 Source NAT (SNAT)

Source NAT changes an outgoing packet destined for the system so that it looks as though the system is the source of the packet.

Define source NAT for UDP and TCP traffic directed to port 123 originating from the host with the IP address 10.55.34.85. The source address is rewritten to 63.240.161.99.

```
config redirect
    option src          lan
    option dest         wan
    option src_ip       10.55.34.85
    option src_dip      63.240.161.99
    option dest_port    123
    option target       SNAT
```

When used alone, Source NAT is used to restrict a computer's access to the internet, but allows it to access a few services by manually forwarding what appear to be a few local services; for example, NTP to the internet. While DNAT hides the local network from the internet, SNAT hides the internet from the local network.

Source NAT and destination NAT are combined and used dynamically in IP masquerading to make computers with private (192.168.x.x, etc.) IP addresses appear on the internet with the system's public WAN IP address.

### 34.7.4 True destination port forwarding

This usage is similar to SNAT, but as the destination IP address is not changed, machines on the destination network need to be aware that they will receive and answer requests from a public IP address that is not necessarily theirs. Port forwarding in this fashion is typically used for load balancing.

```
config redirect
    option src          wan
    option src_dport    80
    option dest         lan
    option dest_port    80
    option proto        tcp
```

### 34.7.5 Block access to a specific host

The following rule blocks all connection attempts to the specified host address.

```
config rule
    option src          lan
    option dest         wan
```

```
option dest_ip      123.45.67.89
option target       REJECT
```

### 34.7.6 Block access to the internet using MAC

The following rule blocks all connection attempts from the client to the internet.

```
config rule
    option src        lan
    option dest       wan
    option src_mac    00:00:00:00:00:00
    option target     REJECT
```

### 34.7.7 Block access to the internet for specific IP on certain times

The following rule blocks all connection attempts to the internet from 192.168.1.27 on weekdays between 21:00pm and 09:00am.

```
config rule
    option src        lan
    option dest       wan
    option src_ip     192.168.1.27
    option extra      '-m time --weekdays Mon,Tue,Wed,Thu,Fri --
timestart 21:00 --timestop 09:00'
    option target     REJECT
```

### 34.7.8 Restricted forwarding rule

The example below creates a forward rule rejecting traffic from LAN to WAN on the ports 1000-1100.

```
config rule
    option src        lan
    option dest       wan
    option dest_port  1000-1100
    option proto      tcpudp
    option target     REJECT
```

### 34.7.9 Denial of service protection rule

The example below shows a sample configuration of SSH DoS attack where if more than two SSH connections are attempted within 120 seconds, every further connection will be dropped. You can configure this for any port number.

```

config rule 'sshattack'
    option src 'lan'
    option dest_port '22'
    option proto 'tcp'
    option recent '2 120'
    option target 'DROP'

```

### 34.7.10 IP spoofing prevention mechanism

Configure IP spoofing protection on a per interface basis in the `/etc/config/network` configuration file. The example below shows the `ipv4_rp_filter` option enabled on the `Vlan12` interface in the network file. When reverse path filtering mechanism is enabled, the router will check whether a receiving packet source address is routable.

If it is routable through the interface from which it came, then the machine will accept the packet.

If it is not routable through the interface from which it came, then the machine will drop that packet.

```

config interface 'Vlan12'
    option type 'bridge'
    option proto 'static'
    option monitored '0'
    option ipaddr '10.1.28.122'
    option netmask '255.255.0.0'
    option ifname 'eth1 eth3.12'
    option ipv4_rp_filter '1'

```

### 34.7.11 Simple DMZ rule

The following rule redirects all WAN ports for all protocols to the internal host `192.168.1.2`.

```

config redirect
    option src wan
    option proto all
    option dest_ip 192.168.1.2

```

### 34.7.12 Transparent proxy rule (external)

The following rule redirects all outgoing HTTP traffic from LAN through an external proxy at `192.168.1.100` listening on port `3128`. It assumes the router LAN address to be `192.168.1.1` - this is needed to masquerade redirected traffic towards the proxy.

```
config redirect
    option src          lan
    option proto        tcp
    option src_ip       !192.168.1.100
    option src_dport    80
    option dest_ip      192.168.1.100
    option dest_port    3128
    option target        DNAT

config redirect
    option dest         lan
    option proto        tcp
    option src_dip      192.168.1.1
    option dest_ip      192.168.1.100
    option dest_port    3128
    option target        SNAT
```

### 34.7.13 Transparent proxy rule (same host)

The rule below redirects all outgoing HTTP traffic from LAN through a proxy server listening at port 3128 on the router itself.

```
config redirect
    option src          lan
    option proto        tcp
    option src_dport    80
    option dest_port    3128
```

### 34.7.14 IPSec passthrough

This example enables proper forwarding of IPSec traffic through the WAN.

```
# AH protocol
config rule
    option src          wan
    option dest         lan
    option proto        ah
    option target        ACCEPT

# ESP protocol
config rule
```

```
option src          wan
option dest         lan
option proto        esp
option target       ACCEPT
```

For some configurations you also have to open port 500/UDP.

```
# ISAKMP protocol
config rule
    option src          wan
    option dest         lan
    option proto        udp
    option src_port     500
    option dest_port    500
    option target       ACCEPT
```

### 34.7.15 Manual iptables rules

You can specify traditional iptables rules, in the standard iptables UNIX command form, in an external file and included in the firewall config file. It is possible to use this process to include multiple files.

```
config include
    option path /etc/firewall.user

config include
    option path /etc/firewall.vpn
```

The syntax for the includes is Linux standard and therefore different from UCIs.

### 34.7.16 Firewall management

After a configuration change, to rebuild firewall rules, enter:

```
root@VA_router:~# /etc/init.d/firewall restart
```

Executing the following command will flush all rules and set the policies to ACCEPT on all standard chains:

```
root@VA_router:~# /etc/init.d/firewall stop
```

To manually start the firewall, enter:

```
root@VA_router:~# /etc/init.d/firewall start
```

To permanently disable the firewall, enter:

```
root@VA_router:/# /etc/init.d/firewall disable
```

**Note:** disable does not flush the rules, so you might be required to issue a stop before.

To enable the firewall again, enter:

```
root@VA_router:/# /etc/init.d/firewall enable
```

### 34.7.17 Debug generated rule set

It is possible to observe the iptables commands generated by the firewall programme. This is useful to track down iptables errors during firewall restarts or to verify the outcome of certain UCI rules.

To see the rules as they are executed, run the `fw` command with the `FW_TRACE` environment variable set to **1**:

```
root@VA_router:/# FW_TRACE=1 fw reload
```

To direct the output to a file for later inspection, enter:

```
root@VA_router:/# FW_TRACE=1 fw reload 2>/tmp/iptables.lo
```

## 35 Configuring IPsec

Internet Protocol Security (IPsec) is a protocol suite used to secure communications at IP level. Use IPsec to secure communications between two hosts or between two networks. Virtual Access routers implement IPsec using strongSwan software.

If you need to create an IPsec template for DMVPN, read the chapter 'Dynamic Multipoint Virtual Private Network (DMVPN)'.

The number of IPsec tunnels supported by Virtual Access' routers is not limited in any way by software; the only hardware limitation is the amount of RAM installed on the device.

### 35.1 Configuration package used

| Package    | Sections                        |
|------------|---------------------------------|
| strongswan | general<br>connection<br>secret |

### 35.2 Configuring IPsec using the web interface

To configure IPsec using the web interface, in the top menu, select **Services -> IPsec**. The strongSwan IPsec VPN page appears. There are three sections:

|                     |   |
|---------------------|---|
| Common Settings     | Control the overall behaviour of strongSwan. This behaviour is common across all tunnels. |
| Connection Settings | Together, these sections define the required parameters for a two-way IKEv1 tunnel.       |
| Secret Settings     |   |

#### 35.2.1 Configure common settings

The screenshot shows the 'strongSwan IPsec VPN' configuration page. The title is 'strongSwan IPsec VPN' with a subtitle 'Configuration of the strongSwan IPsec VPN system.' There is a 'Delete' button in the top right corner. The settings are as follows:

- Enable StrongSwan IPsec:**
- Strict CRL Policy:**  Defines if a fresh CRL must be available in order for the peer authentication based on RSA signatures to succeed. IKEv2 additionally recognizes 'furni' which reverts to 'yes' if at least one CRL URI is defined and to 'no' if no URI is known.
- Unique IDs:**  Whether a particular participant ID should be kept unique, with any new (automatically keyed) connection using an ID from a different IP address deemed to replace all old ones using that ID. Participant IDs normally are unique, so a new (automatically-keyed) connection using the same ID is almost invariably intended to replace an old one. The IKEv2 daemon also accepts the value 'replace' which is identical to 'yes' and the value 'keep' to reject new IKE SA setups and keep the duplicate established earlier.
- Cache CRLs:**  CRLs fetched via HTTP or LDAP will be cached.
- Disable Revocation (CRL and OCSP):**
- Send INITIAL CONTACT by default:**  Send INITIAL CONTACT notification when first connection attempt for all connections
- Debug:**

Figure 201: The common settings section



| Web Field/UCI/Package Option  | Description  |      |                                    |         |   |         |   |      |   |
|---|--|------|------------------------------------|---------|---|---------|---|------|---|
| Web: Enable strongswan<br>UCI: strongswan.general.enable<br>Opt: enabled                                | Enables or disables IPsec.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0    | Disabled.                          | 1       | Enabled.  |         |   |      |   |
| 0   | Disabled.  |      |                                    |         |   |         |   |      |   |
| 1   | Enabled.   |      |                                    |         |   |         |   |      |   |
| Web: Strict CRL Policy<br>UCI: strongswan.general.strictcrlpolicy<br>Opt: strictcrlpolicy               | Defines if a fresh CRL must be available for the peer authentication based on RSA signatures to succeed.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>ifuri</td> <td>The IKEv2 application additionally recognises the <code>ifuri</code> option which reverts to 'yes' if at least one CRL URI is defined and to 'no' if no URI is known.</td> </tr> </table>  | 0    | Disabled.                          | 1       | Enabled.  | ifuri   | The IKEv2 application additionally recognises the <code>ifuri</code> option which reverts to 'yes' if at least one CRL URI is defined and to 'no' if no URI is known. |      |   |
| 0   | Disabled.  |      |                                    |         |   |         |   |      |   |
| 1   | Enabled.   |      |                                    |         |   |         |   |      |   |
| ifuri   | The IKEv2 application additionally recognises the <code>ifuri</code> option which reverts to 'yes' if at least one CRL URI is defined and to 'no' if no URI is known.  |      |                                    |         |   |         |   |      |   |
| Web: Unique IDs<br>UCI: strongswan.general.uniqueids<br>Opt: uniqueids                                  | Defines whether a particular participant ID should be kept unique, with any new, automatically keyed, connection using an ID from a different IP address deemed to replace all old ones using that ID.<br>Participant IDs normally are unique, so a new, automatically-keyed, connection using the same ID is almost invariably intended to replace an old one.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>replace</td> <td>Identical to Yes.</td> </tr> <tr> <td>keep</td> <td>Rejects new IKE SA and keep the duplicate established earlier</td> </tr> </table> | 0    | Disabled.                          | 1       | Enabled.  | replace | Identical to Yes.   | keep | Rejects new IKE SA and keep the duplicate established earlier |
| 0   | Disabled.  |      |                                    |         |   |         |   |      |   |
| 1   | Enabled.   |      |                                    |         |   |         |   |      |   |
| replace   | Identical to Yes.  |      |                                    |         |   |         |   |      |   |
| keep  | Rejects new IKE SA and keep the duplicate established earlier  |      |                                    |         |   |         |   |      |   |
| Web: Cache CRLs<br>UCI: strongswan.general.cachecrls<br>Opt: cachecrls                                  | Certificate Revocation Lists (CRLs) fetched via HTTP or LDAP will be cached in <code>/etc/ipsec.d/crls/</code> under a unique file name derived from the certification authority's public key.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0    | Disabled.                          | 1       | Enabled.  |         |   |      |   |
| 0   | Disabled.  |      |                                    |         |   |         |   |      |   |
| 1   | Enabled.   |      |                                    |         |   |         |   |      |   |
| Web: Disable Revocation<br>UCI:<br>strongswan.general.revocation_disabled<br>Opt: revocation_disabled   | Defines whether disable CRL and OCSP checking for revoked certificates.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0    | Disabled.                          | 1       | Enabled.  |         |   |      |   |
| 0   | Disabled.  |      |                                    |         |   |         |   |      |   |
| 1   | Enabled.   |      |                                    |         |   |         |   |      |   |
| Web: Send INITIAL CONTACT by default<br>UCI: strongswan.general.initial_contact<br>Opt: initial_contact | Defines whether the first attempt to contact a remote peer by this strongswan instance sets the <code>initial_contact</code> flag, which should cause compliant peers to automatically bring down any previous sessions. This can also be enabled or disabled per connection.<br><table border="1"> <tr> <td>0</td> <td>Does not set initial contact flag.</td> </tr> <tr> <td>1</td> <td>Sets initial contact flag on first attempt.</td> </tr> </table>  | 0    | Does not set initial contact flag. | 1       | Sets initial contact flag on first attempt.   |         |   |      |   |
| 0   | Does not set initial contact flag.   |      |                                    |         |   |         |   |      |   |
| 1   | Sets initial contact flag on first attempt.  |      |                                    |         |   |         |   |      |   |
| Web: Debug<br>UCI: strongswan.general.debug<br>Opt: debug   | Enables debugging. This option is used for trouble shooting issues. It is not suitable for a production environment.<br><table border="1"> <tr> <td>None</td> <td>Debug disabled.</td> </tr> <tr> <td>Control</td> <td>Debug enabled. Shows generic control flow with errors and very basic auditing logs.</td> </tr> <tr> <td>All</td> <td>Debug enabled. Most verbose logging also includes sensitive information such as keys.</td> </tr> </table>  | None | Debug disabled.                    | Control | Debug enabled. Shows generic control flow with errors and very basic auditing logs. | All     | Debug enabled. Most verbose logging also includes sensitive information such as keys.   |      |   |
| None  | Debug disabled.  |      |                                    |         |   |         |   |      |   |
| Control   | Debug enabled. Shows generic control flow with errors and very basic auditing logs.  |      |                                    |         |   |         |   |      |   |
| All   | Debug enabled. Most verbose logging also includes sensitive information such as keys.  |      |                                    |         |   |         |   |      |   |

Table 140: Information table for IPsec common settings

## 35.2.2 Common settings: configure connection

Figure 202: The configuring IPsec settings

| Web Field/UCI/Package Option  | Description  |        |                              |           |                                 |      |   |        |                                   |        |   |
|---|--|--------|------------------------------|-----------|---------------------------------|------|---|--------|-----------------------------------|--------|---|
| Web: Enabled<br>UCI: strongswan.@connection[X].enabled<br>Opt: enable           | Enables or disables an IPsec connection.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0      | Disabled.                    | 1         | Enabled.                        |      |   |        |                                   |        |   |
| 0   | Disabled.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| 1   | Enabled.   |        |                              |           |                                 |      |   |        |                                   |        |   |
| Web: Aggressive<br>UCI: strongswan.@connection[X].aggressive<br>Opt: aggressive | Enables or disables IKE aggressive mode.<br><b>Note:</b> using aggressive mode along with PSK authentication is a less secure method than main mode and should be avoided.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0      | Disabled.                    | 1         | Enabled.                        |      |   |        |                                   |        |   |
| 0   | Disabled.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| 1   | Enabled.   |        |                              |           |                                 |      |   |        |                                   |        |   |
| Web: Name<br>UCI: strongswan.@connection[X].name<br>Opt: name                   | Specifies a name for the tunnel.   |        |                              |           |                                 |      |   |        |                                   |        |   |
| Web: Autostart Action<br>UCI: strongswan.@connection[X].auto<br>Opt: auto       | Specifies when the tunnel is initiated.<br><table border="1"> <tr> <td>start</td> <td>On start up.</td> </tr> <tr> <td>route</td> <td>When traffic routes this way.</td> </tr> <tr> <td>add</td> <td>Loads a connection without starting it.</td> </tr> <tr> <td>ignore</td> <td>Ignores the connection.</td> </tr> <tr> <td>always</td> <td>Actively retries to establish the tunnel if it went down.</td> </tr> </table> | start  | On start up.                 | route     | When traffic routes this way.   | add  | Loads a connection without starting it.           | ignore | Ignores the connection.           | always | Actively retries to establish the tunnel if it went down. |
| start   | On start up.   |        |                              |           |                                 |      |   |        |                                   |        |   |
| route   | When traffic routes this way.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| add   | Loads a connection without starting it.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| ignore  | Ignores the connection.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| always  | Actively retries to establish the tunnel if it went down.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| Web: Connection Type<br>UCI: strongswan.@connection[X].type<br>Opt: type        | Defines the type of IPsec connection.<br><table border="1"> <tr> <td>tunnel</td> <td>Connection uses tunnel mode.</td> </tr> <tr> <td>transport</td> <td>Connection uses transport mode.</td> </tr> <tr> <td>pass</td> <td>Connection does not perform any IPsec processing.</td> </tr> <tr> <td>drop</td> <td>Connection drops all the packets.</td> </tr> </table>   | tunnel | Connection uses tunnel mode. | transport | Connection uses transport mode. | pass | Connection does not perform any IPsec processing. | drop   | Connection drops all the packets. |        |   |
| tunnel  | Connection uses tunnel mode.   |        |                              |           |                                 |      |   |        |                                   |        |   |
| transport   | Connection uses transport mode.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| pass  | Connection does not perform any IPsec processing.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| drop  | Connection drops all the packets.  |        |                              |           |                                 |      |   |        |                                   |        |   |

Table 141: Information table for connection settings

### 35.2.3 Common settings: IP addressing

The screenshot shows the IPsec configuration interface with the following settings:

- Connection Type: tunnel
- Remote GW Address: 89.501.154.151 (Could be IP address or FQDN or "%any")
- Local Id: 182.162.206.1 (Leave blank to use default (local interface IP address))
- Remote Id: 89.501.154.151 (Leave blank to use default (remote gateway IP address))
- Local LAN IP Address: 192.156.206.1
- Local LAN IP Address Mask: 258.258.255.255
- Remote LAN IP Address: 172.255.255.255
- Remote LAN IP Address Mask: (empty)
- Local Protocol: (empty) (Restrict the traffic selector to a single protocol on the local side)
- Local Port: (empty) (Restrict the traffic selector to a single UDP/TCP port on the local side)
- Remote Protocol: (empty) (Restrict the traffic selector to a single protocol on the remote side)
- Remote Port: (empty) (Restrict the traffic selector to a single UDP/TCP port on the remote side)
- Authby: psk (How the two security gateways should authenticate each other.)
- XAuth identity: (empty) (Defines the identity/username the client uses to reply to an XAuth request. If not defined, the IKEv1 identity will be used as XAuth identity.)

Figure 203: The IP addressing settings

| Web Field/UCI/Package Option  | Description  |
|---|--|
| Web: Remote GW Address<br>UCI: strongswan.@connection[X].remoteaddress<br>Opt: remoteaddress          | Sets the public IP address of the remote peer.         |
| Web: Local ID<br>UCI: strongswan.@connection[X].localid<br>Opt: localid                               | Defines the local peer identifier.                     |
| Web: Remote ID<br>UCI: strongswan.@connection[X].remoteid<br>Opt: remoteid                            | Defines the remote peer identifier.                    |
| Web: Local LAN IP Address<br>UCI: strongswan.@connection[X].locallan<br>Opt: locallan                 | Defines the local IP of LAN.                           |
| Web: Local LAN IP Address Mask<br>UCI: strongswan.@connection[X].locallanmask<br>Opt: locallanmask    | Defines the subnet of local LAN.                       |
| Web: Remote LAN IP Address<br>UCI: strongswan.@connection[X].remotelan<br>Opt: remotelan              | Defines the IP address of LAN serviced by remote peer. |
| Web: Remote LAN IP Address Mask<br>UCI: strongswan.@connection[X].remotelanmask<br>Opt: remotelanmask | Defines the Subnet of remote LAN.                      |

|  |  |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
|--|--|--------|----------------------------|--------|-----------------------------|----------|------------------------------------|-----|------------------------|-------------|--|----------|--|-------|--|
| Web: Local Protocol<br>UCI: strongswan.@connection[X].localproto<br>Opt: localproto      | Restricts the connection to a single protocol on the local side.   |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| Web: Local Port<br>UCI: strongswan.@connection[X].localport<br>Opt: localport            | Restricts the connection to a single port on the local side.   |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| Web: Remote Protocol<br>UCI:<br>strongswan.@connection[X].remoteproto<br>Opt:remoteproto | Restricts the connection to a single protocol on the remote side.  |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| Web: Remote Port<br>UCI: strongswan.@connection[X].remoteport<br>Opt: remoteport         | Restricts the connection to a single port on the remote side.  |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| Web: Authby<br>UCI: strongswan.@connection[X].authby<br>Opt: authby                      | <p>Defines how the two secure gateways should authenticate.<br/><b>Note:</b> using aggressive mode along with PSK authentication is unsecure and should be avoided.</p> <table border="1"> <tr> <td>Pubkey</td> <td>For public key signatures.</td> </tr> <tr> <td>Rsasig</td> <td>For RSA digital signatures.</td> </tr> <tr> <td>ecdsasig</td> <td>For elliptic curve DSA signatures.</td> </tr> <tr> <td>Psk</td> <td>Using a preshared key.</td> </tr> <tr> <td>xauthrsasig</td> <td>Enables eXtended Authentication (XAuth) with addition to RSA signatures.</td> </tr> <tr> <td>xauthpsk</td> <td>Using extended authentication and preshared key.</td> </tr> <tr> <td>never</td> <td>Can be used if negotiation is never to be attempted or accepted (shunt connections).</td> </tr> </table> | Pubkey | For public key signatures. | Rsasig | For RSA digital signatures. | ecdsasig | For elliptic curve DSA signatures. | Psk | Using a preshared key. | xauthrsasig | Enables eXtended Authentication (XAuth) with addition to RSA signatures. | xauthpsk | Using extended authentication and preshared key. | never | Can be used if negotiation is never to be attempted or accepted (shunt connections). |
| Pubkey   | For public key signatures.   |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| Rsasig   | For RSA digital signatures.  |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| ecdsasig   | For elliptic curve DSA signatures.   |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| Psk  | Using a preshared key.   |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| xauthrsasig  | Enables eXtended Authentication (XAuth) with addition to RSA signatures.   |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| xauthpsk   | Using extended authentication and preshared key.   |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| never  | Can be used if negotiation is never to be attempted or accepted (shunt connections).   |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |

**Table 142: Information table for IP addressing settings**

## 35.2.4 Common settings: IPsec settings

VA\_router Status System Services Network Logout

08EGC8121829  
L18-18.00.74.000rc12  
image1/config1

XAuth identity  Defines the identity/username the client uses to reply to an XAuth request. If not defined, the IKEv1 identity will be used as XAuth identity.

Reauthenticate  Reauthenticate the peer at every rekeying of the IKE\_SA

IKE algorithm

ESP algorithm

WAN Interface

IKE life time  How long the keying channel of a connection should last before being renegotiated.

Key life  Synonym for lifetime. How long a particular instance of a connection (a set of encryption/authentication keys for user packets) should last, from successful negotiation to expiry.

Rekey margin  Synonym for margintime. How long before connection expiry or keying-channel expiry should attempts to negotiate a replacement begin.

Keying tries  How many attempts (a positive integer or %forever) should be made to negotiate a connection, or a replacement for one, before giving up (default 3). The value %forever means 'never give up'.

Restart delay  Delay termination of previous IKE SA and start of the next IKE SA of automatic connection. If 0 then random delay in the range of 1 to Rekey margin is used

DPD Action  Controls the use of the DPD protocol where R\_U\_THERE notification messages (IKEv1) or empty INFORMATIONAL messages (IKEv2) are periodically sent in order to check the liveliness of the IPsec peer. If no activity is detected, all connections with a dead peer are stopped and unrouted (clear), put in the hold state (hold) or restarted (restart). The default is none which disables the active sending of DPD messages.

DPD Delay  Defines the period time interval with which R\_U\_THERE messages/INFORMATIONAL exchanges are sent to the peer.

DPD Timeout  Defines the timeout interval, after which all connections to a peer are deleted in case of inactivity.

Inherit CHILD SA  Inherit CHILD SA when IKE SA is rekeyed

Send INITIAL CONTACT  Send INITIAL CONTACT notification when first connection attempt

Figure 204: The IPsec connections settings

| Web Field/UCI/Package Option  | Description   |
|---|---|
| Web: XAuth Identity<br>UCI: strongswan.@connection[X].xauth_identity<br>Opt: xauth_identity | Defines Xauth ID.   |
| Web: IKE Algorithm<br>UCI: strongswan.@connection[X].ike<br>Opt: ike                        | Specifies the IKE algorithm to use.<br>The format is: encAlgo   authAlgo   DHGroup<br>encAlgo:<br>3des<br>aes128<br>aes256<br>serpent<br>twofish<br>blowfish<br>authAlgo:<br>md5<br>sha<br>sha2<br>DHGroup:<br>modp1024<br>modp1536<br>modp2048<br>modp3072<br>modp4096<br>modp6144<br>modp8192<br>For example, a valid IKE algorithm is aes128-sha-modp1536. |

|  |   |    |  |          |                   |
|--|---|----|--|----------|-------------------|
| <p>Web: ESP algorithm<br/>UCI: strongswan.@connection[X].esp<br/>Opt: esp</p>                    | <p>Specifies the esp algorithm to use.<br/>The format is: encAlgo   authAlgo   DHGroup<br/>encAlgo:<br/>3des<br/>aes128<br/>aes256<br/>serpent<br/>twofish<br/>blowfish<br/>authAlgo:<br/>md5<br/>sha<br/>sha2<br/>DHGroup:<br/>modp1024<br/>modp1536<br/>modp2048<br/>modp3072<br/>modp4096<br/>modp6144<br/>modp8192<br/>For example, a valid encryption algorithm is:<br/>aes128-sha-modp1536.<br/>If no DH group is defined then PFS is disabled.</p>                     |    |  |          |                   |
| <p>Web: WAN Interface<br/>UCI: strongswan.@connection[X].waniface<br/>Opt: waniface</p>          | <p>This is a space-separated list of the WAN interfaces the router will use to establish a tunnel with the secure gateway.<br/>On the web, a list of the interface names is automatically generated. If you want to specify more than one interface use the "custom" value.<br/>Example: if you have a 3G WAN interface called 'wan' and a WAN ADSL interface called 'dsl' and wanted to use one of these interfaces for this IPSec connection, you would use: 'wan dsl'.</p> |    |  |          |                   |
| <p>Web: IKE Life Time<br/>UCI: strongswan.@connection[X].ikelifetime<br/>Opt: ikelifetime</p>    | <p>Specifies how long the keyring channel of a connection (ISAKMP or IKE SA) should last before being renegotiated.</p> <table border="1" data-bbox="719 1317 1399 1391"> <tr> <td>3h</td> <td></td> </tr> <tr> <td>Timespec</td> <td>1d, 3h, 25m, 10s.</td> </tr> </table>   | 3h |  | Timespec | 1d, 3h, 25m, 10s. |
| 3h   |   |    |  |          |                   |
| Timespec   | 1d, 3h, 25m, 10s.   |    |  |          |                   |
| <p>Web: Key Life<br/>UCI: strongswan.@connection[X].keylife<br/>Opt: keylife</p>                 | <p>Specifies how long a particular instance of a connection (a set of encryption/authentication keys for user packets) should last, from successful negotiation to expiry.<br/>Normally, the connection is renegotiated (via the keyring channel) before it expires (see rekeymargin).</p> <table border="1" data-bbox="719 1536 1399 1608"> <tr> <td>1h</td> <td></td> </tr> <tr> <td>Timespec</td> <td>1d, 1h, 25m, 10s.</td> </tr> </table>                                | 1h |  | Timespec | 1d, 1h, 25m, 10s. |
| 1h   |   |    |  |          |                   |
| Timespec   | 1d, 1h, 25m, 10s.   |    |  |          |                   |
| <p>Web: Rekey Margin<br/>UCI:<br/>strongswan.@connection[X].rekeymargin<br/>Opt: rekeymargin</p> | <p>Specifies how long before connection expiry or keyring-channel expiry should attempt to negotiate a replacement begin.<br/>Relevant only locally, other end need not agree on it.</p> <table border="1" data-bbox="719 1727 1399 1794"> <tr> <td>9m</td> <td></td> </tr> <tr> <td>Timespec</td> <td>1d, 2h, 9m, 10s.</td> </tr> </table>   | 9m |  | Timespec | 1d, 2h, 9m, 10s.  |
| 9m   |   |    |  |          |                   |
| Timespec   | 1d, 2h, 9m, 10s.  |    |  |          |                   |

|  |   |      |  |          |  |      |  |         |  |
|--|---|------|--|----------|--|------|--|---------|--|
| <p>Web: Restart Delay<br/>UCI: strongswan.@connection[X].restartdelay<br/>Opt: restartdelay</p>                  | <p>Defines specific delay when re-establishing a connection. Previously if <code>close_action=restart</code>, then the new option <code>restartdelay</code> controls how many seconds it waits before attempting to re-establish the tunnel to allow the headend some time to tidy up. If not set, it defaults to zero, which means that the previous behaviour of choosing a random time interval in the range <code>0..RekeyMargin</code> seconds takes effect.</p> <p>Relevant only locally, other end need not agree on it.</p> <table border="1" data-bbox="719 456 1402 524"> <tr> <td>0</td> <td></td> </tr> <tr> <td>Timespec</td> <td>1d, 2h, 9m, 10s.</td> </tr> </table> | 0    |  | Timespec | 1d, 2h, 9m, 10s.   |      |  |         |  |
| 0  |   |      |  |          |  |      |  |         |  |
| Timespec   | 1d, 2h, 9m, 10s.  |      |  |          |  |      |  |         |  |
| <p>Web: Keying Tries<br/>UCI: strongswan.@connection[X].keyringtries<br/>Opt: keyringtries</p>                   | <p>Specifies how many attempts, for example, a positive integer or <code>%forever</code>, should be made to negotiate a connection, or a replacement for one, before giving up. The value <code>%forever</code> means 'never give up'. Relevant only locally, the other end need not agree on it.</p>   |      |  |          |  |      |  |         |  |
| <p>Web: DPD Action<br/>UCI: strongswan.@connection[X].dpdaction<br/>Opt: dpdaction</p>                           | <p>Defines DPD (Dead Peer Detection) action.</p> <table border="1" data-bbox="719 703 1402 898"> <tr> <td>None</td> <td>Disables DPD.</td> </tr> <tr> <td>Clear</td> <td>Clear down the tunnel if peer does not respond. Reconnect when traffic brings the tunnel up.</td> </tr> <tr> <td>Hold</td> <td>Clear down the tunnel and bring up as soon as the peer is available.</td> </tr> <tr> <td>Restart</td> <td>Restarts DPD when no activity is detected.</td> </tr> </table>  | None | Disables DPD.                              | Clear    | Clear down the tunnel if peer does not respond. Reconnect when traffic brings the tunnel up. | Hold | Clear down the tunnel and bring up as soon as the peer is available. | Restart | Restarts DPD when no activity is detected. |
| None   | Disables DPD.   |      |  |          |  |      |  |         |  |
| Clear  | Clear down the tunnel if peer does not respond. Reconnect when traffic brings the tunnel up.  |      |  |          |  |      |  |         |  |
| Hold   | Clear down the tunnel and bring up as soon as the peer is available.  |      |  |          |  |      |  |         |  |
| Restart  | Restarts DPD when no activity is detected.  |      |  |          |  |      |  |         |  |
| <p>Web: DPD Delay<br/>UCI: strongswan.@connection[X].dpddelay<br/>Opt: dpddelay</p>                              | <p>Defines the period time interval with which R_U_THERE messages and INFORMATIONAL exchanges are sent to the peer.</p> <p>These are only sent if no other traffic is received.</p> <table border="1" data-bbox="719 1016 1402 1088"> <tr> <td>30s</td> <td></td> </tr> <tr> <td>Timespec</td> <td>1d, 2h, 25m, 10s.</td> </tr> </table>  | 30s  |  | Timespec | 1d, 2h, 25m, 10s.  |      |  |         |  |
| 30s  |   |      |  |          |  |      |  |         |  |
| Timespec   | 1d, 2h, 25m, 10s.   |      |  |          |  |      |  |         |  |
| <p>Web: DPD Timeout<br/>UCI: strongswan.@connection[X].dpdtimeout<br/>Opt: dpdtimeout</p>                        | <p>Defines the timeout interval, after which all connections to a peer are deleted in case of inactivity.</p> <table border="1" data-bbox="719 1151 1402 1223"> <tr> <td>150s</td> <td></td> </tr> <tr> <td>Timespec</td> <td>1d, 2h, 25m, 10s.</td> </tr> </table>   | 150s |  | Timespec | 1d, 2h, 25m, 10s.  |      |  |         |  |
| 150s   |   |      |  |          |  |      |  |         |  |
| Timespec   | 1d, 2h, 25m, 10s.   |      |  |          |  |      |  |         |  |
| <p>Web: Inherit CHILD SA<br/>UCI:<br/>strongswan.@connection[X].inherit_child<br/>Opt: inherit_child</p>         | <p>Defines whether the existing phase two IPSEC SA is maintained through IKE rekey for this tunnel. This is normally set to match the behaviour on the IPSEC headend.</p> <table border="1" data-bbox="719 1308 1402 1379"> <tr> <td>0</td> <td>Delete the existing IPSEC SA on IKE rekey.</td> </tr> <tr> <td>1</td> <td>Maintain the existing IPSEC SA on IKE rekey.</td> </tr> </table>  | 0    | Delete the existing IPSEC SA on IKE rekey. | 1        | Maintain the existing IPSEC SA on IKE rekey.   |      |  |         |  |
| 0  | Delete the existing IPSEC SA on IKE rekey.  |      |  |          |  |      |  |         |  |
| 1  | Maintain the existing IPSEC SA on IKE rekey.  |      |  |          |  |      |  |         |  |
| <p>Web: Send INITIAL CONTACT<br/>UCI:<br/>strongswan.@connection[X].initial_contact<br/>Opt: initial_contact</p> | <p>Defines whether the first attempt to contact a remote peer by this strongswan instance sets the <code>initial_contact</code> flag which should cause compliant peers to automatically bring down any previous sessions.</p> <table border="1" data-bbox="719 1487 1402 1556"> <tr> <td>0</td> <td>Do not set initial contact flag.</td> </tr> <tr> <td>1</td> <td>Set initial contact flag on first attempt.</td> </tr> </table>   | 0    | Do not set initial contact flag.           | 1        | Set initial contact flag on first attempt.   |      |  |         |  |
| 0  | Do not set initial contact flag.  |      |  |          |  |      |  |         |  |
| 1  | Set initial contact flag on first attempt.  |      |  |          |  |      |  |         |  |

**Table 143: Information table for IPsec connections settings**

## 35.2.5 Configure secret settings

Each tunnel requires settings to configure how the local end point of the tunnel proves its identity to the remote end point.

Figure 205: IPSec secrets settings

| Web Field/UCI/Package Option   | Description  |     |                  |        |                       |        |                        |          |                               |       |                         |
|--|--|-----|------------------|--------|-----------------------|--------|------------------------|----------|-------------------------------|-------|-------------------------|
| Web: Enabled<br>UCI: strongswan.@secret[X].enabled<br>Opt: enabled                 | Defines whether this set of credentials is to be used or not.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0   | Disabled.        | 1      | Enabled.              |        |                        |          |                               |       |                         |
| 0  | Disabled.  |     |                  |        |                       |        |                        |          |                               |       |                         |
| 1  | Enabled.   |     |                  |        |                       |        |                        |          |                               |       |                         |
| Web: ID selector<br>UCI: strongswan.@secret[X].idtype<br>Opt: idtype               | Defines whether IP address or userfqdn is used.  |     |                  |        |                       |        |                        |          |                               |       |                         |
| Web: ID selector<br>UCI: strongswan.@secret[X].localaddress<br>Opt: localaddress   | Defines the local address this secret applies to.  |     |                  |        |                       |        |                        |          |                               |       |                         |
| Web: ID selector<br>UCI: strongswan.@secret[X].remoteaddress<br>Opt: remoteaddress | Defines the remote address this secret applies to.   |     |                  |        |                       |        |                        |          |                               |       |                         |
| Web: N/A<br>UCI: strongswan.@secret[X].userfqdn<br>Opt: userfqdn                   | FQDN or Xauth name used of Extended Authentication. This must match xauth_identity from the configuration connection section.  |     |                  |        |                       |        |                        |          |                               |       |                         |
| Web: Secret Type<br>UCI: strongswan.@secret[X].secrettype<br>Opt: secrettype       | Specifies the authentication mechanism to be used by the two peers.<br><table border="1"> <tr> <td>Psk</td> <td>Preshared secret</td> </tr> <tr> <td>Pubkey</td> <td>Public key signatures</td> </tr> <tr> <td>Rsasig</td> <td>RSA digital signatures</td> </tr> <tr> <td>Ecdsasig</td> <td>Elliptic Curve DSA signatures</td> </tr> <tr> <td>Xauth</td> <td>Extended authentication</td> </tr> </table> | Psk | Preshared secret | Pubkey | Public key signatures | Rsasig | RSA digital signatures | Ecdsasig | Elliptic Curve DSA signatures | Xauth | Extended authentication |
| Psk  | Preshared secret   |     |                  |        |                       |        |                        |          |                               |       |                         |
| Pubkey   | Public key signatures  |     |                  |        |                       |        |                        |          |                               |       |                         |
| Rsasig   | RSA digital signatures   |     |                  |        |                       |        |                        |          |                               |       |                         |
| Ecdsasig   | Elliptic Curve DSA signatures  |     |                  |        |                       |        |                        |          |                               |       |                         |
| Xauth  | Extended authentication  |     |                  |        |                       |        |                        |          |                               |       |                         |
| Web: Secret<br>UCI: strongswan.@secret[X].secret<br>Opt: secret                    | Defines the secret.  |     |                  |        |                       |        |                        |          |                               |       |                         |

Table 144: Information table for IPSec secrets settings



## 35.3 Configuring IPsec using UCI

### 35.3.1 Common settings

```
# Commands
touch /etc/config/strongswan
uci set strongswan.general=general
uci set strongswan.general.enabled=yes
uci set strongswan.general.strictcrpolicyno
uci set strongswan.general.uniqueids=yes
uci set strongswan.general.cachecrs=no
uci set strongswan.general.debug=none
uci set strongswan.general.initial_contact=0
uci commit
```

This will create the following output:

```
config general 'general'
    option enabled 'yes'
    option strictcrpolicyno 'no'
    option uniqueids 'yes'
    option cachecrs 'no'
    option debug 'none'
    option initial_contact '0'
```

### 35.3.2 Connection settings

**Note:** Xauth is not supported in IKEv2.

```
touch /etc/config/strongswan
uci add strongswan connection
uci set strongswan.@connection[0].ikelifetime=3h
uci set strongswan.@connection[0].keylife=1h
uci set strongswan.@connection[0].rekeymargin=9m
uci set strongswan.@connection[0].keyingtries=3
uci set strongswan.@connection[0].restartdelay=0
uci set strongswan.@connection[0].dpdaction=none
uci set strongswan.@connection[0].dpddelay=30s
uci set strongswan.@connection[0].dpdtimeout=150s
uci set strongswan.@connection[0].enabled=yes
```

```
uci set strongswan.@connection[0].name=3G_Backup
uci set strongswan.@connection[0].auto=start
uci set strongswan.@connection[0].type=tunnel
uci set strongswan.@connection[0].remoteaddress=100.100.100.100
uci set strongswan.@connection[0].localid=192.168.209.1
uci set strongswan.@connection[0].remoteid=100.100.100.100
uci set strongswan.@connection[0].locallan=192.168.209.1
uci set strongswan.@connection[0].locallanmask=255.255.255.255
uci set strongswan.@connection[0].remotelan=172.19.101.3
uci set strongswan.@connection[0].remotelanmask=255.255.255.255
uci set strongswan.@connection[0].authby=xauthpsk
uci set strongswan.@connection[0].xauth_identity=testxauth
uci set strongswan.@connection[0].ike=3des-md5-modp1024
uci set strongswan.@connection[0].esp=3des-md5
uci set strongswan.@connection[0].waniface=wan
uci set strongswan.@connection[0].inherit_child=0
uci set strongswan.@connection[0].initial_contact=0
uci commit
```

This will create the following output:

```
config connection
    option ikelifetime '3h'
    option keylife '1h'
    option rekeymargin '9m'
    option keyingtries '3'
    option restartdelay '0'
    option dpdaction 'none'
    option dpddelay '30s'
    option dpdtimeout '150s'
    option enabled 'yes'
    option name '3G_Backup'
    option auto 'start'
    option type 'tunnel'
    option remoteaddress '100.100.100.100 '
    option localid '192.168.209.1'
    option remoteid '100.100.100.100 '
    option locallan '192.168.209.1'
```

```

option locallanmask '255.255.255.255'
option remotelan '172.19.101.3'
option remotelanmask '255.255.255.255'
option authby 'xauthpsk'
option xauth_identity 'testxauth'
option ike '3des-md5-modp1024'
option esp '3des-md5'
option waniface 'wan'
option inherit_child '0'
option initial_contact '0'

```

### 35.3.3 Shunt connection

If the remote LAN network is 0.0.0.0/0 then all traffic generated on the local LAN will be sent via the IPsec tunnel. This includes the traffic destined to the router's IP address. To avoid this situation you must include an additional config connection section.

```

# Commands
touch /etc/config/strongswan
uci add strongswan connection
uci set strongswan.@connection[1].name=local
uci set strongswan.@connection[1].enabled=yes
uci set strongswan.@connection[1].locallan=10.1.1.1
uci set strongswan.@connection[1].locallanmask=255.255.255.255
uci set strongswan.@connection[1].remotelan=10.1.1.0
uci set strongswan.@connection[1].remotelanmask=255.255.255.0
uci set strongswan.@connection[1].type=pass
uci set strongswan.@connection[1].auto=route
uci commit

```

This will create the following output:

```

config connection
    option name 'local'
    option enabled 'yes'
    option locallan '10.1.1.1'
    option locallanmask '255.255.255.255'
    option remotelan '10.1.1.0'
    option remotelanmask '255.255.255.0'
    option type 'pass'
    option auto 'route'

```

Traffic originated on `remotelan` and destined to `locallan` address is excluded from VPN IPSec policy.

### 35.3.4 Secret settings

Each tunnel also requires settings for how the local end point of the tunnel proves its identity to the remote end point.

A sample secret section, which could be used with the connection section in 'Connection Settings', is shown below.

```
# Commands to add a secret for psk auth
touch /etc/config/strongswan
uci add strongswan secret
uci set strongswan.@secret[0].enabled=yes
uci set strongswan.@secret[0].localaddress=192.168.209.1
uci set strongswan.@secret[0].remoteaddress= 100.100.100.100
uci set strongswan.@secret[0].secrettype=psk
uci set strongswan.@secret[0].secret=secret
uci commit
```

This will create the following output:

```
config secret
    option enabled 'yes'
    option localaddress '192.168.209.1'
    option remoteaddress '100.100.100.100 '
    option secrettype 'psk'
    option secret 'secret'
```

If `xauth` is defined as the authentication method then you must include an additional `config secret` section, as shown in the example below.

```
# Commands to add a secret for xauth auth
touch /etc/config/strongswan
uci add strongswan secret
uci set strongswan.@secret[1].enabled=yes
uci set strongswan.@secret[1].idtype=userfqdn
uci set strongswan.@secret[1].userfqdn=testxauth
uci set strongswan.@secret[1].remoteaddress=100.100.100.100
uci set strongswan.@secret[1].secret=xauth
uci set strongswan.@secret[1].secrettype=XAUTH
uci commit
```

This will create the following output:

```
config secret
    option enabled 'yes'
    option idtype 'userfqdn'
    option userfqdn 'testxauth'
    option remoteaddress '100.100.100.100'
    option secret 'xauth'
    option secrettype 'XAUTH'
```

## 35.4 Configuring an IPsec template for DMVPN via the web interface

To configure IPsec using the web interface, in the top menu, select **Services -> IPsec**. The strongSwan IPsec VPN page appears. There are three sections:

|                     |   |
|---------------------|---|
| Common Settings     | Control the overall behaviour of strongSwan. This behaviour is common across all tunnels. |
| Connection Settings | Together, these sections define the required parameters for a two-way IKEv1 tunnel.       |
| Secret Settings     |   |

### 35.4.1 Configure common settings

The screenshot shows the 'strongSwan IPsec VPN' configuration page. At the top, there are navigation links for 'Services', 'Network', and 'Logout', and a 'UNSAVED CHANGES' button. The main heading is 'strongSwan IPsec VPN' with a subtitle 'Configuration of the strongSwan IPsec VPN system.' and a 'Delete' button. The settings are as follows:

- Enable StrongSwan IPsec:** A checked checkbox.
- Strict CRL Policy:** A dropdown menu set to 'no'. A tooltip explains: 'Defines if a fresh CRL must be available in order for the peer authentication based on RSA signatures to succeed. IKEv2 additionally recognizes 'fun' which reverts to 'yes' if at least one CRL URI is defined and to 'no' if no URI is known.'
- Unique IDs:** A dropdown menu set to 'yes'. A tooltip explains: 'Whether a particular participant ID should be kept unique, with any new (automatically keyed) connection using an ID from a different IP address deemed to replace all old ones using that ID. Participant IDs normally are unique, so a new (automatically-keyed) connection using the same ID is almost invariably intended to replace an old one. The IKEv2 daemon also accepts the value 'replace' which is identical to 'yes' and the value 'keep' to reject new IKE SA setups and keep the duplicate established earlier.'
- Cache CRLs:** A checked checkbox. A tooltip explains: 'CRLs fetched via HTTP or LDAP will be cached.'
- Debug:** A dropdown menu set to 'none'.

Figure 206: The common settings section

| Web Field/UCI/Package Option  | Description   |      |                 |         |   |         |   |      |   |
|---|---|------|-----------------|---------|---|---------|---|------|---|
| Web: Enable strongswan<br>UCI: strongswan.general.enable<br>Opt: enabled                  | Enables or disables IPsec.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0    | Disabled.       | 1       | Enabled.  |         |   |      |   |
| 0   | Disabled.   |      |                 |         |   |         |   |      |   |
| 1   | Enabled.  |      |                 |         |   |         |   |      |   |
| Web: Strict CRL Policy<br>UCI: strongswan.general.strictcrlpolicy<br>Opt: strictcrlpolicy | Defines if a fresh CRL must be available for the peer authentication based on RSA signatures to succeed.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>ifuri</td> <td>The IKEv2 application additionally recognizes the <code>ifuri</code> option which reverts to 'yes' if at least one CRL URI is defined and to 'no' if no URI is known.</td> </tr> </table>   | 0    | Disabled.       | 1       | Enabled.  | ifuri   | The IKEv2 application additionally recognizes the <code>ifuri</code> option which reverts to 'yes' if at least one CRL URI is defined and to 'no' if no URI is known. |      |   |
| 0   | Disabled.   |      |                 |         |   |         |   |      |   |
| 1   | Enabled.  |      |                 |         |   |         |   |      |   |
| ifuri   | The IKEv2 application additionally recognizes the <code>ifuri</code> option which reverts to 'yes' if at least one CRL URI is defined and to 'no' if no URI is known.   |      |                 |         |   |         |   |      |   |
| Web: Unique IDs<br>UCI: strongswan.general.uniqueids<br>Opt: uniqueids                    | Defines whether a particular participant ID should be kept unique, with any new, automatically keyed, connection using an ID from a different IP address deemed to replace all old ones using that ID.<br>Participant IDs normally are unique, so a new, automatically-keyed, connection using the same ID is almost invariably intended to replace an old one.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>replace</td> <td>Identical to Yes</td> </tr> <tr> <td>keep</td> <td>Rejects new IKE SA and keep the duplicate established earlier</td> </tr> </table> | 0    | Disabled.       | 1       | Enabled.  | replace | Identical to Yes  | keep | Rejects new IKE SA and keep the duplicate established earlier |
| 0   | Disabled.   |      |                 |         |   |         |   |      |   |
| 1   | Enabled.  |      |                 |         |   |         |   |      |   |
| replace   | Identical to Yes  |      |                 |         |   |         |   |      |   |
| keep  | Rejects new IKE SA and keep the duplicate established earlier   |      |                 |         |   |         |   |      |   |
| Web: Cache CRLs<br>UCI: strongswan.general.cachecrls<br>Opt: cachecrls                    | Certificate Revocation Lists (CRLs) fetched via HTTP or LDAP will be cached in <code>/etc/ipsec.d/crls/</code> under a unique file name derived from the certification authority's public key.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0    | Disabled.       | 1       | Enabled.  |         |   |      |   |
| 0   | Disabled.   |      |                 |         |   |         |   |      |   |
| 1   | Enabled.  |      |                 |         |   |         |   |      |   |
| Web: Debug<br>UCI: strongswan.general.debug<br>Opt: debug                                 | Enable debugging. This option is used for trouble shooting issues. It is not suitable for a production environment.<br><table border="1"> <tr> <td>None</td> <td>Debug disabled.</td> </tr> <tr> <td>Control</td> <td>Debug enabled. Shows generic control flow with errors and very basic auditing logs.</td> </tr> <tr> <td>All</td> <td>Debug enabled. Most verbose logging also includes sensitive information such as keys.</td> </tr> </table>  | None | Debug disabled. | Control | Debug enabled. Shows generic control flow with errors and very basic auditing logs. | All     | Debug enabled. Most verbose logging also includes sensitive information such as keys.   |      |   |
| None  | Debug disabled.   |      |                 |         |   |         |   |      |   |
| Control   | Debug enabled. Shows generic control flow with errors and very basic auditing logs.   |      |                 |         |   |         |   |      |   |
| All   | Debug enabled. Most verbose logging also includes sensitive information such as keys.   |      |                 |         |   |         |   |      |   |

Table 145: Information table for IPsec common settings

## 35.4.2 Configure connection settings

Scroll down to view the connection settings section.

If you want to create a DMVPN, you do not need to configure all settings as the DMVPN will automatically create them using the template. Leave the following sections blank:

- Remote GW Address
- Local ID
- Remote Id
- Local LAN IP Address
- Local LAN IP Address Mask
- Remote LAN IP Address
- Remote LAN IP Address Mask

|                            |   |  |
|----------------------------|---|--|
| Enabled                    | <input checked="" type="checkbox"/>               |  |
| Aggressive Mode            | <input checked="" type="checkbox"/>               |  |
| Name                       | <input type="text" value="DMVPN_VDF"/>            |  |
| Autostart Action           | <input type="text" value="ignore"/>               | <small>Operation on startup. <b>add</b> loads a connection without starting it. <b>route</b> loads a connection and installs kernel traps. If traffic is detected between local and remote, a connection is established. <b>start</b> loads a connection and brings it up immediately. <b>ignore</b> do nothing</small>  |
| Connection Type            | <input type="text" value="transport"/>            |  |
| Remote GW Address          | <input type="text"/>                              | <small>Could be IP address or FQDN or %any'</small>  |
| Local Id                   | <input type="text"/>                              | <small>Leave blank to use default (local interface IP address)</small>   |
| Remote Id                  | <input type="text"/>                              | <small>Leave blank to use default (remote gateway IP address)</small>  |
| Local LAN IP Address       | <input type="text"/>                              |  |
| Local LAN IP Address Mask  | <input type="text"/>                              |  |
| Remote LAN IP Address      | <input type="text"/>                              |  |
| Remote LAN IP Address Mask | <input type="text"/>                              |  |
| Local Protocol             | <input type="text" value="gre"/>                  | <small>Restrict the traffic selector to a single protocol on the local side</small>  |
| Local Port                 | <input type="text"/>                              | <small>Restrict the traffic selector to a single UDP/TCP port on the local side</small>  |
| Remote Protocol            | <input type="text" value="gre"/>                  | <small>Restrict the traffic selector to a single protocol on the remote side</small>   |
| Remote Port                | <input type="text"/>                              | <small>Restrict the traffic selector to a single UDP/TCP port on the remote side</small>   |
| Authby                     | <input type="text" value="psk"/>                  | <small>How the two security gateways should authenticate each other.</small>   |
| XAuth identity             | <input type="text"/>                              | <small>Defines the identity/username the client uses to reply to an XAuth request. If not defined, the IKEv1 identity will be used as XAuth identity.</small>  |
| IKE algorithm              | <input type="text" value="aes128-sha1-modp1024"/> |  |
| ESP algorithm              | <input type="text" value="3des-md5"/>             |  |
| WAN Interface              | <input type="text" value="3GVDF"/>                |  |
| IKE life time              | <input type="text" value="3h"/>                   | <small>How long the keying channel of a connection should last before being renegotiated.</small>  |
| Key life                   | <input type="text" value="1h"/>                   | <small>Synonym for lifetime. How long a particular instance of a connection (a set of encryption/authentication keys for user packets) should last, from successful negotiation to expiry.</small>   |
| Rekey margin               | <input type="text" value="9m"/>                   | <small>Synonym for margintime. How long before connection expiry or keying-channel expiry should attempts to negotiate a replacement begin.</small>  |
| Keying tries               | <input type="text" value="3"/>                    | <small>How many attempts (a positive integer or %forever) should be made to negotiate a connection, or a replacement for one, before giving up (default 3). The value %forever means 'never give up'.</small>  |
| DPD Action                 | <input type="text" value="none"/>                 | <small>Controls the use of the DPD protocol where R_U_THERE notification messages (IKEv1) or empty INFORMATIONAL messages (IKEv2) are periodically sent in order to check the liveness of the IPsec peer. If no activity is detected, all connections with a dead peer are stopped and unrouted (clear), put in the hold state (hold) or restarted (restart). The default is none which disables the active sending of DPD messages.</small> |
| DPD Delay                  | <input type="text" value="30s"/>                  | <small>Defines the period time interval with which R_U_THERE messages/INFORMATIONAL exchanges are sent to the peer.</small>  |
| DPD Timeout                | <input type="text" value="30s"/>                  | <small>Defines the timeout interval, after which all connections to a peer are deleted in case of inactivity.</small>  |

Figure 207: The connections settings section

| Web Field/UCI/Package Option  | Description  |        |                              |           |                                 |      |   |        |                                   |        |   |
|---|--|--------|------------------------------|-----------|---------------------------------|------|---|--------|-----------------------------------|--------|---|
| Web: Enabled<br>UCI: strongswan.@connection[X].enabled<br>Opt: enable                                 | Enables or disables IPsec connection.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0      | Disabled.                    | 1         | Enabled.                        |      |   |        |                                   |        |   |
| 0   | Disabled.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| 1   | Enabled.   |        |                              |           |                                 |      |   |        |                                   |        |   |
| Web: Aggressive<br>UCI: strongswan.@connection[X].aggressive<br>Opt: aggressive                       | Enables or disables IKE aggressive mode.<br><b>Note:</b> using aggressive mode along with PSK authentication is less secure method than main mode and should be avoided.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0      | Disabled.                    | 1         | Enabled.                        |      |   |        |                                   |        |   |
| 0   | Disabled.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| 1   | Enabled.   |        |                              |           |                                 |      |   |        |                                   |        |   |
| Web: Name<br>UCI: strongswan.@connection[X].name<br>Opt: name   | Specifies a name for the tunnel.   |        |                              |           |                                 |      |   |        |                                   |        |   |
| Web: Autostart Action<br>UCI: strongswan.@connection[X].auto<br>Opt: auto                             | Specifies when the tunnel is initiated.<br><table border="1"> <tr> <td>start</td> <td>On start up.</td> </tr> <tr> <td>route</td> <td>When traffic routes this way.</td> </tr> <tr> <td>add</td> <td>Loads a connection without starting it.</td> </tr> <tr> <td>ignore</td> <td>Ignores the connection.</td> </tr> <tr> <td>always</td> <td>Actively retries to establish the tunnel if it went down.</td> </tr> </table> | start  | On start up.                 | route     | When traffic routes this way.   | add  | Loads a connection without starting it.           | ignore | Ignores the connection.           | always | Actively retries to establish the tunnel if it went down. |
| start   | On start up.   |        |                              |           |                                 |      |   |        |                                   |        |   |
| route   | When traffic routes this way.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| add   | Loads a connection without starting it.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| ignore  | Ignores the connection.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| always  | Actively retries to establish the tunnel if it went down.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| Web: Connection Type<br>UCI: strongswan.@connection[X].type<br>Opt: type                              | Defines the type of IPsec connection.<br><table border="1"> <tr> <td>tunnel</td> <td>Connection uses tunnel mode.</td> </tr> <tr> <td>transport</td> <td>Connection uses transport mode.</td> </tr> <tr> <td>pass</td> <td>Connection does not perform any IPsec processing.</td> </tr> <tr> <td>drop</td> <td>Connection drops all the packets.</td> </tr> </table>   | tunnel | Connection uses tunnel mode. | transport | Connection uses transport mode. | pass | Connection does not perform any IPsec processing. | drop   | Connection drops all the packets. |        |   |
| tunnel  | Connection uses tunnel mode.   |        |                              |           |                                 |      |   |        |                                   |        |   |
| transport   | Connection uses transport mode.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| pass  | Connection does not perform any IPsec processing.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| drop  | Connection drops all the packets.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| Web: Remote GW Address<br>UCI: strongswan.@connection[X].remoteaddress<br>Opt: remoteaddress          | Sets the public IP address of the remote peer.<br>Leave blank for DMVPN.   |        |                              |           |                                 |      |   |        |                                   |        |   |
| Web: Local ID<br>UCI: strongswan.@connection[X].localid<br>Opt: localid                               | Defines the local peer identifier.<br>Leave blank for DMVPN.   |        |                              |           |                                 |      |   |        |                                   |        |   |
| Web: Remote ID<br>UCI: strongswan.@connection[X].remoteid<br>Opt:remoteid                             | Defines the remote peer identifier.<br>Leave blank for DMVPN.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| Web: Local LAN IP Address<br>UCI: strongswan.@connection[X]. locallan<br>Opt: locallan                | Defines the local IP of LAN.<br>Leave blank for DMVPN.   |        |                              |           |                                 |      |   |        |                                   |        |   |
| Web: Local LAN IP Address Mask<br>UCI: strongswan.@connection[X]. locallanmask<br>Opt: locallanmask   | Defines the subnet of local LAN.<br>Leave blank for DMVPN.   |        |                              |           |                                 |      |   |        |                                   |        |   |
| Web: Remote LAN IP Address<br>UCI: strongswan.@connection[X]. remotelan<br>Opt:remotelan              | Defines the IP address of LAN serviced by remote peer.<br>Leave blank for DMVPN.   |        |                              |           |                                 |      |   |        |                                   |        |   |
| Web: Remote LAN IP Address Mask<br>UCI: strongswan.@connection[X]. remotelanmask<br>Opt:remotelanmask | Defines the Subnet of remote LAN.<br>Leave blank for DMVPN.  |        |                              |           |                                 |      |   |        |                                   |        |   |
| Web: Local Protocol<br>UCI: strongswan.@connection[X].localproto<br>Opt: localproto                   | Restricts the connection to a single protocol on the local side.   |        |                              |           |                                 |      |   |        |                                   |        |   |



|  |  |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
|--|--|--------|----------------------------|--------|-----------------------------|----------|------------------------------------|-----|------------------------|-------------|--|----------|--|-------|--|
| <p>Web: Local Port<br/>UCI: strongswan.@connection[X].localport<br/>Opt: localport</p>               | <p>Restricts the connection to a single port on the local side.</p>  |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| <p>Web: Remote Protocol<br/>UCI: strongswan.@connection[X].remoteproto<br/>Opt:remoteproto</p>       | <p>Restricts the connection to a single protocol on the remote side.</p>   |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| <p>Web: Remote Port<br/>UCI: strongswan.@connection[X].remoteport<br/>Opt: remoteport</p>            | <p>Restricts the connection to a single port on the remote side.</p>   |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| <p>Web: Authby<br/>UCI: strongswan.@connection[X].authby<br/>Opt: authby</p>                         | <p>Defines how the two secure gateways should authenticate.<br/><b>Note:</b> using aggressive mode along with PSK authentication is unsecure and should be avoided.</p> <table border="1"> <tr> <td>Pubkey</td> <td>For public key signatures.</td> </tr> <tr> <td>Rsasig</td> <td>For RSA digital signatures.</td> </tr> <tr> <td>ecdsasig</td> <td>For Elliptic Curve DSA signatures.</td> </tr> <tr> <td>Psk</td> <td>Using a preshared key.</td> </tr> <tr> <td>xauthrsasig</td> <td>Enables eXtended Authentication (XAuth) with addition to RSA signatures.</td> </tr> <tr> <td>xauthpsk</td> <td>Using extended authentication and preshared key.</td> </tr> <tr> <td>never</td> <td>Can be used if negotiation is never to be attempted or accepted (shunt connections).</td> </tr> </table> | Pubkey | For public key signatures. | Rsasig | For RSA digital signatures. | ecdsasig | For Elliptic Curve DSA signatures. | Psk | Using a preshared key. | xauthrsasig | Enables eXtended Authentication (XAuth) with addition to RSA signatures. | xauthpsk | Using extended authentication and preshared key. | never | Can be used if negotiation is never to be attempted or accepted (shunt connections). |
| Pubkey   | For public key signatures.   |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| Rsasig   | For RSA digital signatures.  |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| ecdsasig   | For Elliptic Curve DSA signatures.   |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| Psk  | Using a preshared key.   |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| xauthrsasig  | Enables eXtended Authentication (XAuth) with addition to RSA signatures.   |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| xauthpsk   | Using extended authentication and preshared key.   |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| never  | Can be used if negotiation is never to be attempted or accepted (shunt connections).   |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| <p>Web: XAuth Identity<br/>UCI: strongswan.@connection[X].xauth_identity<br/>Opt: xauth_identity</p> | <p>Defines Xauth ID.</p>   |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |
| <p>Web: IKE Algorithm<br/>UCI: strongswan.@connection[X].ike<br/>Opt: ike</p>                        | <p>Specifies the IKE algorithm to use.<br/>The format is: encAlgo   authAlgo   DHGroup:<br/>encAlgo:<br/>3des<br/>aes128<br/>aes256<br/>serpent<br/>twofish<br/>blowfish<br/>authAlgo:<br/>md5<br/>sha<br/>sha2<br/>DHGroup:<br/>modp1024<br/>modp1536<br/>modp2048<br/>modp3072<br/>modp4096<br/>modp6144<br/>modp8192<br/>For example, a valid IKE algorithm is: aes128-sha-modp1536.</p>  |        |                            |        |                             |          |                                    |     |                        |             |  |          |  |       |  |

|  |  |    |  |          |                   |
|--|--|----|--|----------|-------------------|
| <p>Web: ESP algorithm<br/>         UCI: strongswan.@connection[X].esp<br/>         Opt: esp</p>                                | <p>Specifies the esp algorithm to use.<br/>         The format is: encAlgo   authAlgo   DHGroup<br/>         encAlgo:<br/>         3des<br/>         aes128<br/>         aes256<br/>         serpent<br/>         twofish<br/>         blowfish<br/>         authAlgo:<br/>         md5<br/>         sha<br/>         sha2<br/>         DHGroup:<br/>         modp1024<br/>         modp1536<br/>         modp2048<br/>         modp3072<br/>         modp4096<br/>         modp6144<br/>         modp8192<br/>         For example, a valid encryption algorithm is:<br/>         aes128-sha-modp1536.<br/>         If no DH group is defined then PFS is disabled.</p> |    |  |          |                   |
| <p>Web: WAN Interface<br/>         UCI: strongswan.@connection[X].waniface<br/>         Opt: waniface</p>                      | <p>This is a space separated list of the WAN interfaces the router will use to establish a tunnel with the secure gateway.<br/>         On the web, a list of the interface names is automatically generated. If you want to specify more than one interface use the "custom" value.<br/>         Example: If you have a 3G WAN interface called 'wan' and a WAN ADSL interface called 'dsl' and wanted to use one of these interfaces for this IPsec connection, you would use: 'wan adsl'.</p>   |    |  |          |                   |
| <p>Web: IKE Life Time<br/>         UCI: strongswan.@connection[X].ikelifetime<br/>         Opt: ikelifetime</p>                | <p>Specifies how long the keyring channel of a connection (ISAKMP or IKE SA) should last before being renegotiated.</p> <table border="1" data-bbox="699 1294 1396 1368"> <tr> <td>3h</td> <td></td> </tr> <tr> <td>Timespec</td> <td>1d, 3h, 25m, 10s.</td> </tr> </table>  | 3h |  | Timespec | 1d, 3h, 25m, 10s. |
| 3h   |  |    |  |          |                   |
| Timespec   | 1d, 3h, 25m, 10s.  |    |  |          |                   |
| <p>Web: Key Life<br/>         UCI: strongswan.@connection[X].keylife<br/>         Opt: keylife</p>                             | <p>Specifies how long a particular instance of a connection (a set of encryption/authentication keys for user packets) should last, from successful negotiation to expiry.<br/>         Normally, the connection is renegotiated (via the keyring channel) before it expires (see rekeymargin).</p> <table border="1" data-bbox="699 1512 1396 1585"> <tr> <td>1h</td> <td></td> </tr> <tr> <td>Timespec</td> <td>1d, 1h, 25m, 10s.</td> </tr> </table>  | 1h |  | Timespec | 1d, 1h, 25m, 10s. |
| 1h   |  |    |  |          |                   |
| Timespec   | 1d, 1h, 25m, 10s.  |    |  |          |                   |
| <p>Web: Rekey Margin<br/>         UCI:<br/>         strongswan.@connection[X].rekeymargin<br/>         Opt: rekeymargin</p>    | <p>Specifies how long before connection expiry or keyring-channel expiry should attempt to negotiate a replacement begin.<br/>         Relevant only locally, other end need not agree on it.</p> <table border="1" data-bbox="699 1680 1396 1753"> <tr> <td>9m</td> <td></td> </tr> <tr> <td>Timespec</td> <td>1d, 2h, 9m, 10s.</td> </tr> </table>   | 9m |  | Timespec | 1d, 2h, 9m, 10s.  |
| 9m   |  |    |  |          |                   |
| Timespec   | 1d, 2h, 9m, 10s.   |    |  |          |                   |
| <p>Web: Keyring Tries<br/>         UCI:<br/>         strongswan.@connection[X].keyringtries<br/>         Opt: keyringtries</p> | <p>Specifies how many attempts, for example, a positive integer or %forever, should be made to negotiate a connection, or a replacement for one, before giving up. The value %forever means 'never give up'. Relevant only locally, other end need not agree on it.</p>  |    |  |          |                   |

|   |  |      |               |          |  |      |  |         |  |
|---|--|------|---------------|----------|--|------|--|---------|--|
| Web: DPD Action<br>UCI: strongswan.@connection[X].dpdaction<br>Opt: dpdaction       | Defines DPD (Dead Peer Detection) action. <table border="1"> <tr> <td>None</td> <td>Disables DPD.</td> </tr> <tr> <td>Clear</td> <td>Clear down the tunnel if the peer does not respond. Reconnect when traffic brings the tunnel up.</td> </tr> <tr> <td>Hold</td> <td>Clear down the tunnel and bring up as soon as the peer is available.</td> </tr> <tr> <td>Restart</td> <td>Restarts DPD when no activity is detected.</td> </tr> </table> | None | Disables DPD. | Clear    | Clear down the tunnel if the peer does not respond. Reconnect when traffic brings the tunnel up. | Hold | Clear down the tunnel and bring up as soon as the peer is available. | Restart | Restarts DPD when no activity is detected. |
| None  | Disables DPD.  |      |               |          |  |      |  |         |  |
| Clear   | Clear down the tunnel if the peer does not respond. Reconnect when traffic brings the tunnel up.   |      |               |          |  |      |  |         |  |
| Hold  | Clear down the tunnel and bring up as soon as the peer is available.   |      |               |          |  |      |  |         |  |
| Restart   | Restarts DPD when no activity is detected.   |      |               |          |  |      |  |         |  |
| Web: DPD Delay<br>UCI: strongswan.@connection[X].dpddelay<br>Opt: dpddelay          | Defines the period time interval with which R_U_THERE messages and INFORMATIONAL exchanges are sent to the peer. These are only sent if no other traffic is received. <table border="1"> <tr> <td>30s</td> <td></td> </tr> <tr> <td>Timespec</td> <td>1d, 2h, 25m, 10s.</td> </tr> </table>  | 30s  |               | Timespec | 1d, 2h, 25m, 10s.  |      |  |         |  |
| 30s   |  |      |               |          |  |      |  |         |  |
| Timespec  | 1d, 2h, 25m, 10s.  |      |               |          |  |      |  |         |  |
| Web: DPD Timeout<br>UCI:<br>strongswan.@connection[X].dpdtimeout<br>Opt: dpdtimeout | Defines the timeout interval, after which all connections to a peer are deleted in case of inactivity. <table border="1"> <tr> <td>150s</td> <td></td> </tr> <tr> <td>Timespec</td> <td>1d, 2h, 25m, 10s.</td> </tr> </table>  | 150s |               | Timespec | 1d, 2h, 25m, 10s.  |      |  |         |  |
| 150s  |  |      |               |          |  |      |  |         |  |
| Timespec  | 1d, 2h, 25m, 10s.  |      |               |          |  |      |  |         |  |

Table 146: Information table for IPsec connections settings

### 35.4.3 Configure secret settings

Each tunnel requires settings to configure how the local end point of the tunnel proves its identity to the remote end point.

Figure 208: IPsec secrets settings

| Web Field/UCI/Package Option   | Description  |   |           |   |          |
|--|--|---|-----------|---|----------|
| Web: Enabled<br>UCI: strongswan.@secret[X].enabled<br>Opt: enabled                 | Defines whether this set of credentials is to be used or not. <table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0 | Disabled. | 1 | Enabled. |
| 0  | Disabled.  |   |           |   |          |
| 1  | Enabled.   |   |           |   |          |
| Web: ID selector<br>UCI: strongswan.@secret[X].idtype<br>Opt: idtype               | Defines whether IP address or userfqdn is used.  |   |           |   |          |
| Web: ID selector<br>UCI: strongswan.@secret[X].localaddress<br>Opt: localaddress   | Defines the local address this secret applies to.  |   |           |   |          |
| Web: ID selector<br>UCI: strongswan.@secret[X].remoteaddress<br>Opt: remoteaddress | Defines the remote address this secret applies to.   |   |           |   |          |

|  |  |     |                  |        |                       |        |                        |          |                               |       |                         |
|--|--|-----|------------------|--------|-----------------------|--------|------------------------|----------|-------------------------------|-------|-------------------------|
| Web: N/A<br>UCI: strongswan.@secret[X].userfqnd<br>Opt: userfqnd             | FQDN or Xauth name used of Extended Authentication. This must match xauth_identity from the configuration connection section.  |     |                  |        |                       |        |                        |          |                               |       |                         |
| Web: Secret Type<br>UCI: strongswan.@secret[X].secrettype<br>Opt: secrettype | Specifies the authentication mechanism to be used by the two peers.<br><table border="1"> <tr> <td>Psk</td> <td>Preshared secret</td> </tr> <tr> <td>Pubkey</td> <td>Public key signatures</td> </tr> <tr> <td>Rsasig</td> <td>RSA digital signatures</td> </tr> <tr> <td>Ecdsasig</td> <td>Elliptic Curve DSA signatures</td> </tr> <tr> <td>Xauth</td> <td>Extended authentication</td> </tr> </table> | Psk | Preshared secret | Pubkey | Public key signatures | Rsasig | RSA digital signatures | Ecdsasig | Elliptic Curve DSA signatures | Xauth | Extended authentication |
| Psk  | Preshared secret   |     |                  |        |                       |        |                        |          |                               |       |                         |
| Pubkey   | Public key signatures  |     |                  |        |                       |        |                        |          |                               |       |                         |
| Rsasig   | RSA digital signatures   |     |                  |        |                       |        |                        |          |                               |       |                         |
| Ecdsasig   | Elliptic Curve DSA signatures  |     |                  |        |                       |        |                        |          |                               |       |                         |
| Xauth  | Extended authentication  |     |                  |        |                       |        |                        |          |                               |       |                         |
| Web: Secret<br>UCI: strongswan.@secret[X].secret<br>Opt: secret              | Defines the secret.  |     |                  |        |                       |        |                        |          |                               |       |                         |

Table 147: Information table for IPsec secret settings

## 35.5 Configuring an IPsec template to use with DMVPN

The following example shows how to configure an IPsec connection template to use with DMVPN.

```
# Commands
touch /etc/config/strongswan
uci set strongswan.general=general
uci set strongswan.general.enabled=yes
uci set strongswan.general.strictcrpolicy=no
uci set strongswan.general.uniqueids=yes
uci set strongswan.general.cachecrs=yes
uci set strongswan.general.nattraversal=yes
uci add strongswan connection
uci set strongswan.@connection[0].enabled=yes
uci set strongswan.@connection[0].name=dmvpn
uci set strongswan.@connection[0].type=transport
uci set strongswan.@connection[0].localproto=gre
uci set strongswan.@connection[0].remoteprototo=gre
uci set strongswan.@connection[0].ike=aes-sha1-modp1024
uci set strongswan.@connection[0].esp=aes128-sha1
uci set strongswan.@connection[0].waniface=lan4
uci set strongswan.@connection[0].auto=ignore
uci set strongswan.@connection[0].ikelifetime=28800s
uci set strongswan.@connection[0].keylife=300s
uci set strongswan.@connection[0].rekeymargin=30s
uci set strongswan.@connection[0].keyingtries=%forever
uci set strongswan.@connection[0].dpdaction=hold
```

```
uci set strongswan.@connection[0].dpddelay=30s
uci set strongswan.@connection[0].dpdtimeout=150s
uci add strongswan secret
uci set strongswan.@secret[0].enabled=yes
uci set strongswan.@secret[0].secrettype=psk
uci set strongswan.@secret[0].secret=secret
```

This will create package strongswan.

```
config general 'general'
option enabled 'yes'
option strictcrpolicys 'no'
option uniqueids 'yes'
option cachecrpls 'yes'
option nat traversal 'yes'
  config connection
option enabled 'yes'
option name 'dmvpn'
option type 'transport'
option localproto 'gre'
option remoteprotos 'gre'
option ike 'aes-sha1-modp1024'
option esp 'aes128-sha1'
option waniface 'lan4'
option auto 'ignore'
option ikelifetime '28800s'
option keylife '300s'
option rekeymargin '30s'
option keyingtries '%forever'
option dpdaction 'hold'
option dpddelay '30s'
option dpdtimeout '150s'
config secret
option enabled 'yes'
option secrettype 'psk'
option secret 'secret'
```

## 35.6 IPsec diagnostics using the web interface

### 35.6.1 IPsec status

In the top menu, click **Status -> IPsec**. The IPsec Connections page appears.

| IPsec Connections    |             |                |             |            |             |           |        |             |          |
|----------------------|-------------|----------------|-------------|------------|-------------|-----------|--------|-------------|----------|
| Name                 | IKE         |                |             |            |             | SA        |        |             |          |
|                      | Status      | Remote         | Established | Encryption | Integrity   | Status    | Policy | Data In/Out | Rekey in |
| dmvpn_213_233_148_2  | ESTABLISHED | 213.233.148.2  | 2 hours ago | 3DES_CBC   | HMAC_MD5_96 | INSTALLED |        |             |          |
| dmvpn_89_101_154_151 | ESTABLISHED | 89.101.154.151 | 2 hours ago | 3DES_CBC   | HMAC_MD5_96 | INSTALLED |        |             |          |

Figure 209: The IPsec connections page

In the Name column, the syntax contains the IPsec Name defined in package dmvpn and the remote IP address of the hub, or the spoke separated by an underscore; for example, dmvpn\_213.233.148.2.

## 35.7 IPsec diagnostics using UCI

### 35.7.1 IPsec configuration

To view IPsec configuration via UCI, enter:

```
root@VA_router:~# uci export strongswan
```

To restart strongSwan, enter:

```
root@VA_router:~# /etc/init.d/strongswan restart
```

### 35.7.2 IPsec status

### 35.7.3 To view IPsec status, enter:

```
root@VA_router:~# ipsec statusall
Security Associations (1 up, 0 connecting):
dmvpn_89_101_154_151[1]: ESTABLISHED 2 hours ago,
10.68.234.133[10.68.234.133]...89.101.154.151[89.101.154.151]
dmvpn_89_101_154_151{1}: REKEYING, TRANSPORT, expires in 55 seconds
dmvpn_89_101_154_151{1}: 10.68.234.133/32[gre] === 192.168./32[gre]
dmvpn_89_101_154_151{1}: INSTALLED, TRANSPORT, ESP in UDP SPIs: cca7b970_i
d874dc90_o
dmvpn_89_101_154_151{1}: 10.68.234.133/32[gre] === 89.101.154.151/32[gre]
```

To view a list of IPsec commands, enter:

```
root@VA_router:~# ipsec -help
```

## 36 Configuring SCEP (Simple Certificate Enrolment Protocol)

SCEP is a method for automatically obtaining x.509 certificates for IPsec validation. This protocol is commonly used in a Private Key Infrastructure (PKI).

The SCEP method has the following steps:

- Obtain a copy of the Certificate Authority (CA) certificate and validate it.
- Generate a Certificate Signing Request (CSR) and send it securely to the CA.
- Re-enrol as necessary to obtain a new certificate prior to the expiration of the current certificate.

This section only details the SCEP portion of an IPsec configuration. For more information on configuring general IPsec, read the chapter 'Configuring IPsec'.

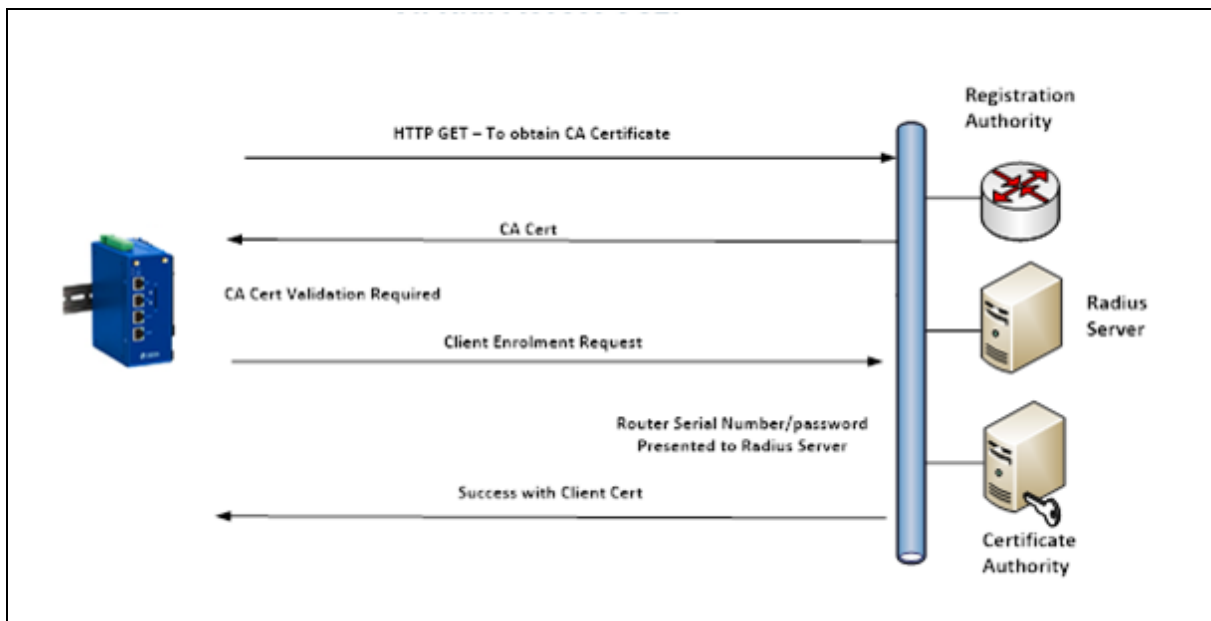


Figure 210: The SCEP process between router and PKI infrastructure

### 36.1 Configuration package used

| Package    | Sections  |
|------------|-----------|
| strongswan | scep_cert |

### 36.2 Configuring SCEP using the web interface

To define an automatically enrolled certificate, using SCEP, select **Services -> IPsec**. Scroll down to the SCEP Certificate section. Enter a name for the SCEP section and select **Add**.

## SCEP Certificate

SCEP works only on boot

*This section contains no values yet*

**Figure 211: Creating a SCEP certificate section name**

The SCEP certificate configuration section options appear.

### SCEPCERT

Enabled

Blocking  Don't start IPsec until certificate is received

SCEP URL  SCEP server URL

SCEP DN  Distinguished Name

SCEP Password

Certificate Path  Location to store certificate on the router (defaults to /etc/ipsec.d/certs/.pem)

Private Key Path  Location to store private key on the router (defaults to /etc/ipsec.d/private/.pem)

CA Certificate Path  Location to store CA certificate on the router

Minimal Renew Margin (in Hours)  Renew certificate not less than Minimal Renew Margin hours before expiration

Maximal Renew Margin (in Hours)  Renew certificate not more than Maximal Renew Margin hours before expiration

Minimal Retry Interval (in Seconds)  Minimal SCEP poll time

Maximal Retry Interval (in Seconds)  Maximal SCEP poll time

Private Key Length (in bits)

HTTP Method

PKCS#7 Encryption Algorithm

PKCS#7 Digest Algorithm

PKCS#10 Signature Algorithm

CA Implementation  Force certain CA implementation. Leave blank unless you know what you're doing

**Figure 212: The SCEP certificate section**



| Web Field/UCI/Package Option  | Description   |       |   |       |  |
|---|---|-------|---|-------|--|
| Web: Enabled<br>UCI: strongswan.@scep_cert[0].enabled<br>Opt: enabled                                       | Defines whether SCEP automatic enrolment is enabled.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0     | Disabled.   | 1     | Enabled.                                       |
| 0   | Disabled.   |       |   |       |  |
| 1   | Enabled.  |       |   |       |  |
| Web: Blocking<br>UCI: strongswan.@scep_cert[0].blocking<br>Opt: blocking                                    | Defines whether to wait until the certificate is received before starting IPsec.<br><table border="1"> <tr> <td>0</td> <td>Wait until the certificate is received before starting IPsec.</td> </tr> <tr> <td>1</td> <td>Do not wait until the certificate is received.</td> </tr> </table>  | 0     | Wait until the certificate is received before starting IPsec. | 1     | Do not wait until the certificate is received. |
| 0   | Wait until the certificate is received before starting IPsec.   |       |   |       |  |
| 1   | Do not wait until the certificate is received.  |       |   |       |  |
| Web: SCEP URL<br>UCI: strongswan.@scep_cert[0].url<br>Opt: url  | Defines the URL for the SCEP server.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> </table>   | Range |   |       |  |
| Range   |   |       |   |       |  |
| Web: SCEP DN<br>UCI: strongswan.@scep_cert[0].dn<br>Opt: dn   | Defines the Distinguished Name to use for new certificate.<br><b>Note:</b> substring %serial will be replaced with a router's serial number.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> </table>   | Range |   |       |  |
| Range   |   |       |   |       |  |
| Web: SCEP Password<br>UCI: strongswan.@scep_cert[0].scep_psk<br>Opt: scep_psk                               | Defines a SCEP password.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> </table>   | Range |   |       |  |
| Range   |   |       |   |       |  |
| Web: Certificate Path<br>UCI: strongswan.@scep_cert[0].cert_path<br>Opt: cert_path                          | Defines the filepath to store the certificate on the router (absolute or relative).<br><table border="1"> <tr> <td>Empty</td> <td>/etc/ipsec.d/certs/.pem</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | Empty | /etc/ipsec.d/certs/.pem                                       | Range |  |
| Empty   | /etc/ipsec.d/certs/.pem   |       |   |       |  |
| Range   |   |       |   |       |  |
| Web: Private Key Path<br>UCI: strongswan.@scep_cert[0].key_path<br>Opt: key_path                            | Defines the filepath to store the private key on the router (absolute or relative).<br><table border="1"> <tr> <td>Empty</td> <td>/etc/ipsec.d/private/.pem</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | Empty | /etc/ipsec.d/private/.pem                                     | Range |  |
| Empty   | /etc/ipsec.d/private/.pem   |       |   |       |  |
| Range   |   |       |   |       |  |
| Web: CA Certificate Path<br>UCI: strongswan.@scep_cert[0].cacert<br>Opt: cacert                             | Defines the filepath to store the CA certificate on the router (absolute or relative).<br><table border="1"> <tr> <td>Empty</td> <td>/etc/ipsec.d/cacerts/.pem</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | Empty | /etc/ipsec.d/cacerts/.pem                                     | Range |  |
| Empty   | /etc/ipsec.d/cacerts/.pem   |       |   |       |  |
| Range   |   |       |   |       |  |
| Web: Minimal Renewal Margin (Hours)<br>UCI:<br>strongswan.@scep_cert[0].minmargin_hrs<br>Opt: minmargin_hrs | Defines the minimum duration, in hours, from certificate expiration for renewal of certificate.<br><b>Note:</b> a random value between minimal and maximal renewal margin will be used.<br><table border="1"> <tr> <td>10</td> <td>10 hours</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 10    | 10 hours  | Range |  |
| 10  | 10 hours  |       |   |       |  |
| Range   |   |       |   |       |  |
| Web: Maximal Renewal Margin (Hours)<br>UCI:<br>strongswan.@scep_cert[0].maxmargin_hrs<br>Opt: maxmargin_hrs | Defines the maximum duration, in hours, from certificate expiration for renewal of certificate.<br><b>Note:</b> the retry interval will be set to a random value between minimal and maximal renewal margin.<br><table border="1"> <tr> <td>24</td> <td>24 hours</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 24    | 24 hours  | Range |  |
| 24  | 24 hours  |       |   |       |  |
| Range   |   |       |   |       |  |
| Web: Minimal Retry Interval (Seconds)<br>UCI: strongswan.@scep_cert[0].minretry<br>Opt: minretry            | Defines the minimal poll time, in seconds.<br><b>Note:</b> the retry interval will be set to a random value between minimal and maximal renewal margin. The retry interval is used when the server replies with PENDING status for initial request (also called manual mode).<br><table border="1"> <tr> <td>10</td> <td>10 seconds</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table> | 10    | 10 seconds  | Range |  |
| 10  | 10 seconds  |       |   |       |  |
| Range   |   |       |   |       |  |

| <p>Web: Maximal Retry Interval (Seconds)<br/>         UCI: strongswan.@scep_cert[0].maxretry<br/>         Opt: maxretry</p>                      | <p>Defines the maximal poll time, in seconds.<br/> <b>Note:</b> the retry interval will be set to a random value between minimal and maximal renewal margin. The retry interval is used when the server replies with <code>PENDING</code> status for initial request (also called <code>manual</code> mode).</p> <table border="1"> <tr> <td>100</td> <td>100 seconds</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>                          | 100    | 100 seconds | Range |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
|--|--|--------|-------------|-------|-----------|----------------------------------|-----------|--------------|--------------|------------|----------------------|--|--------|------|--|------|-----|--|-----|
| 100  | 100 seconds  |        |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| Range  |  |        |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| <p>Web: Private Key Length (in bits)<br/>         UCI: strongswan.@scep_cert[0].key_len<br/>         Opt: key_len</p>                            | <p>Defines the private key length.</p> <table border="1"> <tr> <td>2048</td> <td>2048 bits</td> </tr> <tr> <td>4096</td> <td>4096 bits</td> </tr> <tr> <td>6144</td> <td>6144 bits</td> </tr> <tr> <td>8192</td> <td>8192 bits</td> </tr> <tr> <td>--custom--</td> <td>Define custom length</td> </tr> </table>  | 2048   | 2048 bits   | 4096  | 4096 bits | 6144                             | 6144 bits | 8192         | 8192 bits    | --custom-- | Define custom length |  |        |      |  |      |     |  |     |
| 2048   | 2048 bits  |        |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| 4096   | 4096 bits  |        |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| 6144   | 6144 bits  |        |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| 8192   | 8192 bits  |        |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| --custom--   | Define custom length   |        |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| <p>Web: HTTP Method<br/>         UCI: strongswan.@scep_cert[0].method<br/>         Opt: method</p>   | <p>Defines the HTTP method used for client enrolment</p> <table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>GET</td> <td>HTTP GET</td> <td>get</td> </tr> <tr> <td>POST</td> <td>HTTP POST</td> <td>post</td> </tr> </tbody> </table>  | Web    | Description | UCI   | GET       | HTTP GET                         | get       | POST         | HTTP POST    | post       |                      |  |        |      |  |      |     |  |     |
| Web  | Description  | UCI    |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| GET  | HTTP GET   | get    |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| POST   | HTTP POST  | post   |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| <p>Web: PKCS#7 Encryption Algorithm<br/>         UCI:<br/>         strongswan.@scep_cert[0].pkcs7_enc_algo<br/>         Opt: pkcs7_enc_algo</p>  | <p>Defines the symmetric encryption algorithm to use.</p> <table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>aes256</td> <td></td> <td>aes256</td> </tr> <tr> <td>aes192</td> <td></td> <td>aes192</td> </tr> <tr> <td>aes128</td> <td></td> <td>aes128</td> </tr> <tr> <td>3des</td> <td></td> <td>3des</td> </tr> </tbody> </table>  | Web    | Description | UCI   | aes256    |                                  | aes256    | aes192       |              | aes192     | aes128               |  | aes128 | 3des |  | 3des |     |  |     |
| Web  | Description  | UCI    |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| aes256   |  | aes256 |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| aes192   |  | aes192 |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| aes128   |  | aes128 |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| 3des   |  | 3des   |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| <p>Web: PKCS#7 Digest Algorithm<br/>         UCI:<br/>         strongswan.@scep_cert[0].pkcs7_dgst_algo<br/>         Opt: pkcs7_dgst_algo</p>    | <p>Defines the hash algorithm for pkcs7 digest calculation.</p> <table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>sha512</td> <td></td> <td>sha512</td> </tr> <tr> <td>sha384</td> <td></td> <td>sha384</td> </tr> <tr> <td>sha256</td> <td></td> <td>sha256</td> </tr> <tr> <td>sha1</td> <td></td> <td>sha1</td> </tr> <tr> <td>md5</td> <td></td> <td>md5</td> </tr> </tbody> </table> | Web    | Description | UCI   | sha512    |                                  | sha512    | sha384       |              | sha384     | sha256               |  | sha256 | sha1 |  | sha1 | md5 |  | md5 |
| Web  | Description  | UCI    |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| sha512   |  | sha512 |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| sha384   |  | sha384 |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| sha256   |  | sha256 |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| sha1   |  | sha1   |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| md5  |  | md5    |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| <p>Web: PKCS#7 Signature Algorithm<br/>         UCI:<br/>         strongswan.@scep_cert[0].pkcs10_sig_algo<br/>         Opt: pkcs10_sig_algo</p> | <p>Defines the hash algorithm for pkcs10 signature.</p> <table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>sha512</td> <td></td> <td>sha512</td> </tr> <tr> <td>sha384</td> <td></td> <td>sha384</td> </tr> <tr> <td>sha256</td> <td></td> <td>sha256</td> </tr> <tr> <td>sha1</td> <td></td> <td>sha1</td> </tr> <tr> <td>md5</td> <td></td> <td>md5</td> </tr> </tbody> </table>         | Web    | Description | UCI   | sha512    |                                  | sha512    | sha384       |              | sha384     | sha256               |  | sha256 | sha1 |  | sha1 | md5 |  | md5 |
| Web  | Description  | UCI    |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| sha512   |  | sha512 |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| sha384   |  | sha384 |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| sha256   |  | sha256 |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| sha1   |  | sha1   |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| md5  |  | md5    |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| <p>Web: CA Implementation<br/>         UCI: strongswan.@scep_cert[0].caimpl<br/>         Opt: caimpl</p>   | <p>Defines the SCEP server implementation.</p> <table border="1"> <thead> <tr> <th>Web</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Empty</td> <td>Automatically deducted from URL.</td> <td></td> </tr> <tr> <td>Microsoft CA</td> <td>Microsoft CA</td> <td>ms</td> </tr> <tr> <td>EJB CA</td> <td>Enterprise Java Beans Certificate Authority.</td> <td>ejbca</td> </tr> </tbody> </table>                                | Web    | Description | UCI   | Empty     | Automatically deducted from URL. |           | Microsoft CA | Microsoft CA | ms         | EJB CA               | Enterprise Java Beans Certificate Authority. | ejbca  |      |  |      |     |  |     |
| Web  | Description  | UCI    |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| Empty  | Automatically deducted from URL.   |        |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| Microsoft CA   | Microsoft CA   | ms     |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |
| EJB CA   | Enterprise Java Beans Certificate Authority.   | ejbca  |             |       |           |                                  |           |              |              |            |                      |  |        |      |  |      |     |  |     |

Table 148: Information table for SCEP certificate settings

### 36.2.1 Configuring SCEP certificate using the command line

SCEP is configured using the `scep_cert` configuration section in the strongswan package `/etc/config/strongswan`.

You can configure multiple SCEP configuration sections.

By default, all SCEP certificate instances are named 'scep\_cert'. The SCEP certificate instance is identified by @scep\_cert then the SCEP certificate position in the package as a number. For example, for the first SCEP certificate in the package using UCI, enter:

```
strongswan.@scep_cert[0]=scep_cert
strongswan.@scep_cert[0].enabled=1
```

Or using package options, enter:

```
config scep_cert
    option enabled '1'
```

However, to better identify it, we recommend giving the SCEP certificate instance a name. For example, a SCEP certificate named 'SCEPCERT' will be strongswan.SCEPCERT.

To define a named SCEP certificate instance using UCI, enter:

```
strongswan.SCEPCERT=scep_cert
strongswan.SCEPCERT.enabled=1
```

To define a named SCEP certificate instance using package options, enter:

```
config scep_cert 'SCEPCERT'
    option 'enabled' '1'
```

### 36.2.1.1 SCEP certificate using UCI

```
root@VA_router:~# uci show strongswan
package strongswan
.....
strongswan.SCEPCERT=scep_cert
strongswan.SCEPCERT.enabled=1
strongswan.SCEPCERT.url=url
strongswan.SCEPCERT.dn=dn
strongswan.SCEPCERT.scep_psk=password
strongswan.SCEPCERT.cert_path=/etc/ipsec.d/certs/
strongswan.SCEPCERT.key_path=/etc/ipsec.d/private/
strongswan.SCEPCERT.cacert=/etc/ipsec.d/cacerts/
strongswan.SCEPCERT.minmargin_hrs=10
strongswan.SCEPCERT.maxmargin_hrs=240
strongswan.SCEPCERT.minretry=10
strongswan.SCEPCERT.maxretry=100
```

```
strongswan.SCEPCERT.key_len=2048
strongswan.SCEPCERT.method=get
strongswan.SCEPCERT.pkcs7_enc_algo=aes256
strongswan.SCEPCERT.pkcs7_dgst_algo=sha512
strongswan.SCEPCERT.pkcs10_sig_algo=sha512
strongswan.SCEPCERT.caimpl=ms
```

### 36.2.1.2 SCEP certificate using package options

```
root@VA_router:~# uci export strongswan
package strongswan
.....
config scep_cert 'SCEPCERT'
    option enabled '1'
    option url 'url'
    option dn 'dn'
    option scep_psk 'password'
    option cert_path '/etc/ipsec.d/certs/'
    option key_path '/etc/ipsec.d/private/'
    option cacert '/etc/ipsec.d/cacerts/'
    option minmargin_hrs '10'
    option maxmargin_hrs '240'
    option minretry '10'
    option maxretry '100'
    option key_len '2048'
    option method 'get'
    option pkcs7_enc_algo 'aes256'
    option pkcs7_dgst_algo 'sha512'
    option pkcs10_sig_algo 'sha512'
    option caimpl 'ms'
```

## 36.3 SCEP certificate diagnostics

### 36.3.1 Syslog

SCEP certificate status can be monitored via the system log. An example of SCEP syslog messages can be seen below

```
Aug 14 04:51:01 user.notice 00E0C81604BE ipsec: ca cert
'/etc/ipsec.d/cacerts/vaebjtest' expired or not yet downloaded
Aug 14 04:51:01 authpriv.info 00E0C81604BE scepclient[9146]: loaded
plugins: curl aes des sha1 sha2 md5 random x509 pkcs1 pkcs7 pem openssl gmp
Aug 14 04:51:01 authpriv.info 00E0C81604BE scepclient[9146]: building
CRED_CONTAINER - PKCS7 failed, tried 2 builders
Aug 14 04:51:01 authpriv.info 00E0C81604BE scepclient[9146]: unable to
parse PKCS#7, assuming plain CA cert
Aug 14 04:51:01 authpriv.info 00E0C81604BE scepclient[9146]: written ca
cert file '/etc/ipsec.d/cacerts/vaebjtest' (1200 bytes)
Aug 14 04:51:01 authpriv.info 00E0C81604BE ipsec_starter[9172]: Starting
strongSwan 5.0.2 IPsec [starter]...
Aug 14 04:51:01 daemon.info 00E0C81604BE ipsec: 00[DMN] Starting IKE charon
daemon (strongSwan 5.0.2, Linux 3.18.11, mips)
Aug 14 04:51:02 daemon.info 00E0C81604BE ipsec: 00[CFG] loading ca
certificates from '/etc/ipsec.d/cacerts'
Aug 14 04:51:02 daemon.info 00E0C81604BE ipsec: 00[CFG] loaded ca
certificate "CN=VAejbcaTestCA, O=VA, C=IE" from
'/etc/ipsec.d/cacerts/vaebjtest'
Aug 14 04:51:02 daemon.info 00E0C81604BE ipsec: 00[CFG] loading aa
certificates from '/etc/ipsec.d/aacerts'
Aug 14 04:51:02 daemon.info 00E0C81604BE ipsec: 00[CFG] loading ocspsigner
certificates from '/etc/ipsec.d/ocspcerts'
Aug 14 04:51:02 daemon.info 00E0C81604BE ipsec: 00[CFG] loading attribute
certificates from '/etc/ipsec.d/acerts'
Aug 14 04:51:02 daemon.info 00E0C81604BE ipsec: 00[CFG] loading crls from
'/etc/ipsec.d/crls'
Aug 14 04:51:02 daemon.info 00E0C81604BE ipsec: 00[CFG] loading secrets
from '/etc/ipsec.secrets'
Aug 14 04:51:02 daemon.info 00E0C81604BE ipsec: 00[CFG] loading secrets
from '/var/conf/ipsec.secrets'
Aug 14 04:51:02 daemon.info 00E0C81604BE ipsec: 00[CFG] loaded RSA
private key from '/etc/ipsec.d/private/ejb_cert.pem'
```

### 36.3.2 Strongswan process using UCI

The strongswan process has its own subset of commands.

```
root@VA_router:~# /etc/init.d/strongswan
Syntax: /etc/init.d/dsl_control [command]
```

Available commands:

```
start    Start the service
stop     Stop the service
restart  Restart the service
reload   Reload configuration files (or restart if that fails)
enable   Enable service autostart
disable  Disable service autostart
```

To restart strongswan, enter:

```
root@VA_router:~# /etc/init.d/strongswan restart
```

## 37 Dynamic Multipoint Virtual Private Network (DMVPN)

Dynamic Multipoint Virtual Private Network (DMVPN) is a scalable method of creating VPN IPsec networks. DMVPN is a suite of three protocols: NHRP, GRE and IPsec, used to dynamically create VPN tunnels between different endpoints in the network without having to pre-configure each device with VPN details of the rest of endpoints in the network.

### 37.1 Prerequisites for configuring DMVPN

Before configuring DMVPN, you must first configure:

- A GRE interface; read the previous chapter, 'Configuring GRE interfaces'
- An IPsec connection to use as a template; read the previous chapter, 'Configuring IPsec'.

### 37.2 Advantages of using DMVPN

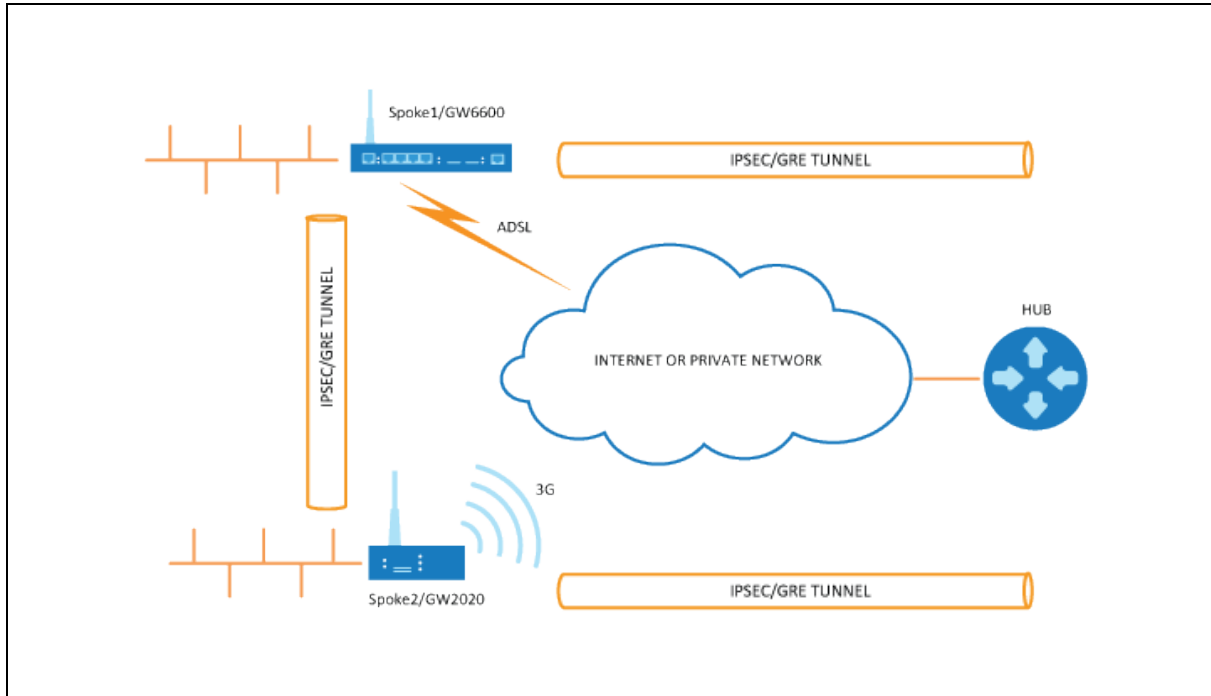
Using DMVPN eliminates the need of IPsec configuration to the physical interface. This reduces the number of lines of configuration required for a VPN development. For example, for a 1000-site deployment, DMVPN reduces the configuration effort at the hub from 3900 lines to 13.

- Adding new peers (spokes) to the VPN requires no changes at the hub.
- Better scalability of the network.
- Dynamic IP addresses can be used at the peers' site.
- Spokes can be connected in private or public network.
- NHRP NAT extension allows spoke-to-spoke tunnels to be built, even if one or more spokes is behind a Network Address Translation (NAT) device.
- New hubs can be added to the network to improve the performances and reliability.
- Ability to carry multicast and main routing protocols traffic (RIP, OSPF, BGP).
- DMVPN can be deployed using Activator: the Virtual Access automated provisioning system.
- Simplifies branch communications by enabling direct branch to branch connectivity.
- Simplifies configuration on the spoke routers. The same IPsec template configuration is used to create spoke-to-hub and spoke-to-spoke VPN IPsec tunnel.
- Improves business resiliency by preventing disruption of business-critical applications and services by incorporating routing with standards-based IPsec technology.

## 37.3 DMVPN scenarios

### 37.3.1 Scenario 1

Spoke1, spoke2 and a hub are in the same public or private network.



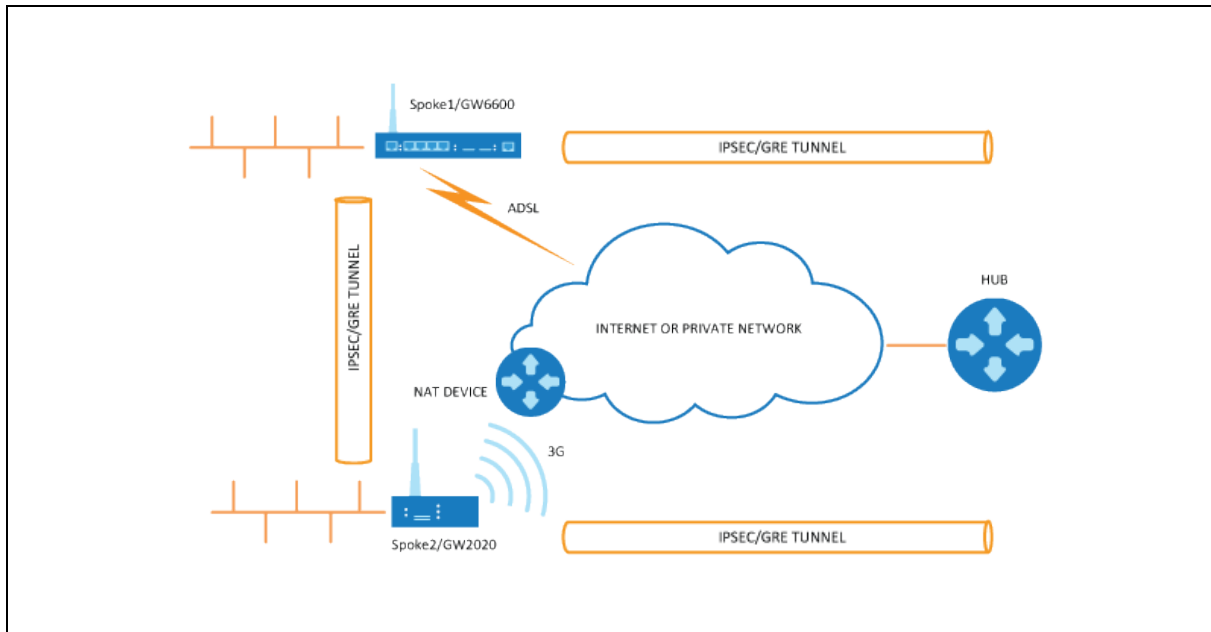
**Figure 213: Network diagram for DMVPN spoke to spoke**

- Spoke1 and spoke2 connect on their WAN interface: ADSL, 3G and initiate main mode IPsec in transport mode to the hub.
- After an IPsec tunnel is established, spokes register their NHRP membership with the hub.
- GRE tunnels come up.
- Hub caches the GRE tunnel and real IP addresses of each spoke.
- When spoke1 wants to talk to spoke2, it sends an NHRP resolution request to the hub.
- The hub checks its cache table and forwards that request to spoke2.
- Spoke2 caches spoke1's GRE and real IP address and sends an NHRP resolution reply via the hub.
- Spoke1 receives an NHRP resolution reply and updates its NHRP table with spoke2 information. Then it initiates VPN IPsec connection to spoke2.
- When an IPsec tunnel is established, spoke1 and spoke2 can send traffic directly to each other.



### 37.3.2 Scenario 2

Spoke1 is in a private (NAT-ed) network, spoke2 and hub are in public network.



**Figure 214: Network diagram for DMVPN spoke behind NAT**

- Spoke1 sends an NHRP registration request to the hub.
- Hub receives this request and compares the source tunnel address of the spoke with the source of the packet.
- Hub sends an NHRP registration reply with a NAT extension to spoke1.
- The NAT extension informs spoke1 that it is behind the NAT-ed device.
- Spoke1 registers its pre- and post-NAT address.
- When spoke1 wants to talk to spoke2, it sends an NHRP resolution request to the hub.
- Hub checks its cache table and forwards that request to spoke2.
- Spoke2 caches spoke1's GRE pre- and post-NAT IP address and sends an NHRP resolution reply via the hub.
- Spoke1 receives the NHRP resolution reply and updates its NHRP table with spoke2 information. It initiates a VPN IPsec connection to spoke2.
- When the IPsec tunnel is established, spoke1 and spoke2 can send traffic directly to each other.

**Note:** if an IPsec tunnel fails to be established between the spokes then packets between the spokes are sent via the hub.

## 37.4 Configuration packages used

| Package    | Sections   |
|------------|--|
| network    | For configuring GRE tunnels.                               |
| strongswan | For enabling and configuring the IPsec connection template |
| dmvpn      |  |

## 37.5 Configuring DMVPN using the web interface

The DMVPN section contains fields required to configure the parameters relative to the DMVPN Hub. These are used for DMVPN tunnels, such as GRE tunnels, GRE tunnel remote IP, DMVPN Hub IP and password.

### 37.5.1 DMVPN general settings

In the top menu, select **Network -> DMVPN**. The DMVPN page appears. There are two sections: General and DMVPN Hub Settings.

Figure 215: The DMVPN general section

| Web Field/UCI/Package Option  | Description  |   |           |   |          |
|---|--|---|-----------|---|----------|
| Web: Enable DMVPN<br>UCI: dmvpn.common.enabled<br>Opt: enable                                       | Enables DMVPN.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0 | Disabled. | 1 | Enabled. |
| 0   | Disabled.  |   |           |   |          |
| 1   | Enabled.   |   |           |   |          |
| Web: IPsec template connection<br>UCI: dmvpn.common.ipsec_template_name<br>Opt: ipsec_template_name | Selects the IPsec connection, defined in strongSwan, to be used as a template.   |   |           |   |          |

Table 149: Information table for DMVPN general settings

## 37.5.2 DMVPN hub settings

The screenshot shows the 'DMVPN Hub Settings' configuration page. It features a table with the following columns: GRE Interface, GRE Remote Endpoint IP Address, GRE Remote Endpoint Mask Length, DMVPN Hub IP Address, NHRP Authentication, NHRP Holding Time, Use as Default Route, Default Route Metric, and LED state Indication. The 'Use as Default Route' checkbox is checked. Below the table are 'Save & Apply', 'Save', and 'Reset' buttons.

Figure 216: The DMVPN hub settings

| Web Field/UCI/Package Option  | Description   |   |           |   |          |
|---|---|---|-----------|---|----------|
| Web: GRE Interface<br>UCI: dmvpn.@interface[X].gre_interface<br>Opt: gre_interface  | Specifies which GRE interface will be used with this DMVPN configuration.   |   |           |   |          |
| Web: GRE Remote Endpoint IP Address<br>UCI:<br>dmvpn.@interface[X].gre_endpoint_ip<br>Opt: gre_endpoint_ip                    | Configures the GRE IP address of the hub.   |   |           |   |          |
| Web: GRE Remote Endpoint Mask Length<br>UCI:<br>dmvpn.@interface[X].gre_endpoint_mask_length<br>Opt: gre_endpoint_mask_length | Configures the length of the mask of the GRE interface on the hub. For example if the mask is 255.255.0.0 the length will be 16.                            |   |           |   |          |
| Web: DMVPN Hub IP Address<br>UCI: dmvpn.@interface[X].nhs_ip<br>Opt: nhs_ip   | Configures the physical IP address for the DMVPN hub.   |   |           |   |          |
| Web: NHRP Authentication<br>UCI: dmvpn.@interface[X].cisco_auth<br>Opt: cisco_auth  | Enables authentication on NHRP. The password will be applied in plaintext to the outgoing NHRP packets. Maximum length is 8 characters.                     |   |           |   |          |
| Web: NHRP Holding Time<br>UCI: dmvpn.@interface[X].holding_time<br>Opt: holding_time  | Timeout for cached NHRP requests.   |   |           |   |          |
| Web: Use As Default Route<br>UCI : dmvpn.@interface[X].defaultroute<br>Opt: defaultroute                                      | Adds a default route into tunnel interface.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0 | Disabled. | 1 | Enabled. |
| 0   | Disabled.   |   |           |   |          |
| 1   | Enabled.  |   |           |   |          |
| Web: Default Route Metric<br>UCI:<br>dmvpn.@interface[X].defaultroutemetric<br>Opt: defaultroutemetric                        | Metric to use for the default route.  |   |           |   |          |
| Web: LED state indication<br>UCI: dmvpn.@interface[X].led<br>Opt: led   | LED to use for indicating if the VPN is up.   |   |           |   |          |

Table 150: Information table for DMVPN hub settings

## 37.5.3 Configuring an IPSec template for DMVPN using the web interface

Configuring an IPSec template is covered in the chapter 'Configuring IPSec'.

## 37.6 DMVPN diagnostics

In the top menu, click **Status -> IPSec**. The IPSec Connections page appears.

| IPsec Connections    |             |                |             |            |             |           |        |             |          |
|----------------------|-------------|----------------|-------------|------------|-------------|-----------|--------|-------------|----------|
| Name                 | IKE         |                |             |            |             | SA        |        |             |          |
|                      | Status      | Remote         | Established | Encryption | Integrity   | Status    | Policy | Data In/Out | Rekey in |
| dmvpn_213_233_148_2  | ESTABLISHED | 213.233.148.2  | 2 hours ago | 3DES_CBC   | HMAC_MD5_96 | INSTALLED |        |             |          |
| dmvpn_89_101_154_151 | ESTABLISHED | 89.101.154.151 | 2 hours ago | 3DES_CBC   | HMAC_MD5_96 | INSTALLED |        |             |          |

**Figure 217: The IPSec connections page**

In the Name column, the syntax contains the IPSec name defined in package dmvpn and the remote IP address of the hub, or the spoke separated by an underscore; for example, dmvpn\_213.233.148.2.

To check the status of DMVPN, in the top menu, click **Status -> DMVPN**.

| NBMA peers     |           |               |       |
|----------------|-----------|---------------|-------|
| NBMA Address   | Interface | Address       | Type  |
| 213.233.148.2  | GRE       | 11.11.11.3/32 | spoke |
| 89.101.154.151 | GRE       | 11.11.11.1/29 | hub   |

Powered by LuCI Trunk (trunk+svn8382) VIE-16.00.28 image1 config2

**Figure 218: The NBMA peers page**

To check DMVPN status, enter:

```

:~# opennhrpctl show
Status: ok
Interface: gre-GRE
Type: local
Protocol-Address: 11.11.11.7/32
Alias-Address: 11.11.11.3
Flags: up
Interface: gre-GRE
Type: local
Protocol-Address: 11.11.11.3/32
Flags: up
Interface: gre-GRE
Type: cached
Protocol-Address: 11.11.11.2/32
NBMA-Address: 178.237.115.129
NBMA-NAT-OA-Address: 172.20.38.129

```

```

Flags: used up
Expires-In: 0:18

Interface: gre-GRE
Type: static
Protocol-Address: 11.11.11.1/29
NBMA-Address: 89.101.154.151
Flags: up

```

| Interface           | Description   |  |
|---------------------|---|--|
| Type                | incomplete  | Resolution request sent.                 |
|                     | negative  | Negative cached.                         |
|                     | cached  | Received/relayed resolution reply.       |
|                     | shortcut_route  | Received/relayed resolution for route.   |
|                     | dynamic   | NHC resolution.                          |
|                     | dynamic_nhs   | Dynamic NHS from dns-map.                |
|                     | static  | Static mapping from config file.         |
|                     | dynamic_map   | Static dns-map from config file.         |
|                     | local_route   | Non-local destination, with local route. |
| local_addr          | Local destination (IP or off-NBMA subnet).  |  |
| Protocol Address    | Tunnel IP address   |  |
| NBMA-Address        | Pre-NAT IP address if NBMA-NAT-OA-Address is present or real address if NAT is not present. |  |
| NBMA-NAT-OA-Address | Post NAT IP address. This field is present when address is translated in the network.       |  |
| Flags               | up  | Can send all packets (registration ok).  |
|                     | unique  | Peer is unique.                          |
|                     | used  | Peer is kernel ARP table.                |
|                     | lower-up  | openhrp script executed successfully.    |
| Expires-In          | Expiration time.  |  |

**Table 151: Information table for DMVPN status**

You can check IPsec status using UCI commands.

```

root@VA-router:~# ipsec status
Security Associations (1 up, 0 connecting):
dmvpn_89_101_154_151[1]: ESTABLISHED 2 hours ago,
10.68.234.133[10.68.234.133]...89.101.154.151[89.101.154.151]
dmvpn_89_101_154_151{1}: REKEYING, TRANSPORT, expires in 55 seconds
dmvpn_89_101_154_151{1}: 10.68.234.133/32[gre] === 192.168./32[gre]
dmvpn_89_101_154_151{1}: INSTALLED, TRANSPORT, ESP in UDP SPIs: cca7b970_i
d874dc90_o
dmvpn_89_101_154_151{1}: 10.68.234.133/32[gre] === 89.101.154.151/32[gre]

```

You can check DMVPN status using UCI commands.

```
:~# opennhrpctl show
Status: ok

Interface: gre-GRE
Type: local
Protocol-Address: 11.11.11.7/32
Alias-Address: 11.11.11.3
Flags: up

Interface: gre-GRE
Type: local
Protocol-Address: 11.11.11.3/32
Flags: up
Interface: gre-GRE
Type: cached
Protocol-Address: 11.11.11.2/32
NBMA-Address: 178.237.115.129
NBMA-NAT-OA-Address: 172.20.38.129
Flags: used up
Expires-In: 0:18
Interface: gre-GRE
Type: static
Protocol-Address: 11.11.11.1/29

NBMA-Address: 89.101.154.151
Flags: up
```

## 38 Configuring multicasting using PIM and IGMP interfaces

### 38.1 Overview

IP multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to potentially thousands of corporate recipients. Applications that take advantage of multicast include video conferencing and corporate communications.

IP multicast delivers application source traffic to multiple receivers without burdening the source or the receivers while using a minimum of network bandwidth.

PIM (Protocol Independent Multicast) and IGMP (Internet Group Management Protocol) are protocols used to create multicasting networks within a regular IP network.

A multicast group is an arbitrary group of receivers that expresses an interest in receiving a particular data stream. The receivers (the designated multicast group) are interested in receiving a data stream from the source. They indicate this by sending an Internet Group Management Protocol (IGMP) host report to their closest router in the network. The routers are then responsible for delivering the data from the source to the receivers. The routers use Protocol Independent Multicast (PIM) between themselves to dynamically create a multicast distribution tree. The data stream will then be delivered only to the network segments that are in the path between the source and the receivers.

To summarise: PIM is used between routers while IGMP is used between a receiver and its router only. As a result, PIM must be enabled on all the interfaces on the route from the multicast source to the multicast client while IGMP must be enabled on the interface to the multicast client only.

### 38.2 Configuration package used

| Package | Sections          |
|---------|-------------------|
| pimd    | pimd<br>interface |

### 38.3 Configuring PIM and IGMP using the web interface

To configure PIM through the web interface, in the top menu, select **Network -> PIM**. The PIM page appears. To access the Global Settings, click **Add**.



Figure 219: The global settings interface

### 38.3.1 Global settings

| Web Field/UCI/Package Option  | Description   |   |           |   |          |
|---|---|---|-----------|---|----------|
| Web: PIM Enabled<br>UCI: pimd.pimd.enabled<br>Opt: enabled          | Globally enables PIM on the router.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0 | Disabled. | 1 | Enabled. |
| 0   | Disabled.   |   |           |   |          |
| 1   | Enabled.  |   |           |   |          |
| Web: SSM Ping Enabled<br>UCI: pimd.pimd.ssm pingd<br>Opt: ssm pingd | Enables answers to SSM pings.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>       | 0 | Disabled. | 1 | Enabled. |
| 0   | Disabled.   |   |           |   |          |
| 1   | Enabled.  |   |           |   |          |

Table 152: Information table for PIM global settings

### 38.3.2 Interfaces configuration

Figure 220: The interfaces configuration section

| Web Field/UCI/Package Option   | Description   |   |           |   |          |
|--|---|---|-----------|---|----------|
| Web: Enabled<br>UCI: pimd.interface[x].enabled<br>Opt: enabled       | Enables multicast management of the given interface by the PIM application.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0 | Disabled. | 1 | Enabled. |
| 0  | Disabled.   |   |           |   |          |
| 1  | Enabled.  |   |           |   |          |
| Web: Interface<br>UCI: pimd.interface[x].interface<br>Opt: interface | Selects the interface to apply PIM settings to.   |   |           |   |          |
| Web: Enable IGMP<br>UCI: pimd.interface[x].igmp<br>Opt: igmp         | Enable IGMP on given interface.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> <p><b>Note:</b> you must enable PIM SSM and/or IGMP depending on your requirements.<br/>ICMP must be enabled on the interface to the multicast client only.</p> | 0 | Disabled. | 1 | Enabled. |
| 0  | Disabled.   |   |           |   |          |
| 1  | Enabled.  |   |           |   |          |
| Web: Enable SSM<br>UCI: pimd.interface[x].ssm<br>Opt: ssm            | Enable SSM on given interface.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0 | Disabled. | 1 | Enabled. |
| 0  | Disabled.   |   |           |   |          |
| 1  | Enabled.  |   |           |   |          |

Table 153: Information table for interface settings

To save your configuration updates, click **Save & Apply**.



## 38.4 Configuring PIM and IGMP using UCI

You can configure PIM and IGMP through CLI using UCI.

The configuration file is stored on **/etc/config/pimd**

To view the configuration file, enter:

```
uci export pimd
root@VA_router:/etc/config1# uci export pimd
package pimd
config routing 'pimd'
    option enabled 'yes'

config interface
    option enabled 'yes'
    option interface 'lan'
    option ssm 'yes'
    option igmp 'yes'

config interface
    option enabled 'yes'
    option interface 'wan'
    option ssm 'yes'
    option igmp 'no'
```

Alternatively, enter:

```
uci show pimd
root@VA_router:/etc/config1# uci show pimd
pimd.pimd=routing
pimd.pimd.enabled=yes
pimd.@interface[0]=interface
pimd.@interface[0].enabled=yes
pimd.@interface[0].interface=lan
pimd.@interface[0].ssm=yes
pimd.@interface[0].igmp=yes
pimd.@interface[1]=interface
pimd.@interface[1].enabled=yes
pimd.@interface[1].interface=wan
```

```
pimd.@interface[1].ssm=yes  
pimd.@interface[1].igmp=no
```

To change any of the above values use `uci set` command.

## 39 QoS: VLAN 802.1Q PCP tagging

### 39.1 Configuring VLAN PCP tagging

Virtual Access routers have the capability to respect and set PCP priority values inside 802.1Q VLAN tagged frames. The following partial export of network configuration shows how to configure VLAN priorities for specific interfaces (VLANs).

```
root@VA_router:~# uci export network package network
config va_switch
    option eth0 'A E'
    option eth1 'B F'
    option eth2 'C G'
    option eth3 'D'
    option eth4 'H'

config interface 'VLAN_1'
    option type 'bridge'
    option proto 'static'
    option ipaddr '10.1.28.99'
    option netmask '255.255.0.0'
    option ifname 'eth0 eth4'

config interface 'VLAN_2'
    option type 'bridge'
    option proto 'static'
    option ipaddr '192.168.2.1'
    option netmask '255.255.255.0'
    option ifname 'eth1 eth4.2'
    option vlan_qos_map_ingress '1:1'
    option vlan_qos_map_egress '0:1'

config interface 'VLAN_3'
    option ifname 'eth2 eth4.3'
    option type 'bridge'
    option proto 'static'
    option ipaddr '192.168.3.1'
    option netmask '255.255.255.0'
```

```

option vlan_qos_map_ingress '3:3'
option vlan_qos_map_egress '0:3'

config interface 'VLAN_4'
option ifname 'eth3 eth4.4'
option type 'bridge'
option proto 'static'
option ipaddr '192.168.3.1'
option netmask '255.255.255.0'

option vlan_qos_map_ingress '5:5'
option vlan_qos_map_egress '0:5'

```

| UCI/Package Option  | Description   |
|---|---|
| UCI: network.<if name>.vlan_qos_map_ingress<br>Opt: list vlan_qos_map_ingress | VLAN priority code point to socket buffer mapping.<br>Example: network.<if name>. vlan_qos_map_ingress =1:1 |
| UCI: network.<if name>.vlan_qos_map_egress<br>Opt: list vlan_qos_map_egress   | Socket buffer to VLAN priority code point mapping.<br>Example: network.<if name>. vlan_qos_map_egress =0:1  |

The above sample configuration specifies that any frames on VLAN2, VLAN3 and VLAN4 will be processed or have their PCP value adjusted according to QoS values set.

#### VLAN1

- VLAN1 is an untagged VLAN so there are no 802.1Q tags on the frames.

#### VLAN2

- Any frames received on VLAN2 destined to VLAN2 with PCP priority of 1 will be forwarded without altering the priority; it will be still set to 1.
- Any frames received on VLAN2 destined to VLAN2 with a PCP priority set to 0 will have a priority of 1 set as they leave the router on VLAN2.

#### VLAN3

- Any frames received on VLAN3 destined to VLAN3 with a PCP priority of 3 will be forwarded without altering the priority; it will be still set to 3.
- Any frames received on VLAN3 destined to VLAN2 with PCP priority set to 0 will have a priority of 3 set as they leave the router on VLAN3.

#### VLAN4

- Any frames received on VLAN4 destined to VLAN2 with PCP priority of 5 will be forwarded without altering the priority; it will be still set to 5.
- Any frames received on VLAN4 destined to VLAN2 with PCP priority set to 0 will have a priority of 5 set as they leave the router on VLAN4.

Four queues are supported and are structured as follows:

- Queue 1: PCP values 0 and 1 - Default
- Queue 2: PCP values 2 and 3 - Normal
- Queue 3: PCP values 4 and 5 - High
- Queue 4: PCP values 6 and 7 - Express

Value 7 is the highest priority and 0 is the lowest. These queues prioritise 802.1Q tagged frames as they are received on the port, these are hardware defined.

When 802.1Q frames are received on the port they are processed according to the above queues on arrival, even if not defined in the configuration. Then if value `'vlan_qos_map_ingress'` is configured you can modify the PCP priority for egress if the frame was to be forwarded on another tagged interface.

When frames are received on an untagged VLAN interface configured with `'vlan_qos_map_egress'` and are destined to tagged interface, 802.1Q tag will be created with a default priority of 0 and then the priority will be set according to the PCP value specified as the frames leave port.

## 40 QoS: type of service

Virtual Access routers are capable of implementing quality of service configurations on a per interface basis, which allows traffic prioritisation based on type of service criteria parameters.

### 40.1 QoS configuration overview

A minimal QoS configuration usually consists of:

- One interface section
- Some rules allocating packets to at least two buckets
- Configuration of buckets

### 40.2 Configuration packages used

| Package | Sections   |
|---------|------------|
| qos     | interface  |
|         | classgroup |
|         | class      |
|         | classify   |

### 40.3 Configuring QoS using the web interface

Browse to the router's IP address and login.

Select **Network tab -> QoS**. The QoS page appears. From this page you can configure interfaces that QoS is applied to as well as classification rules.

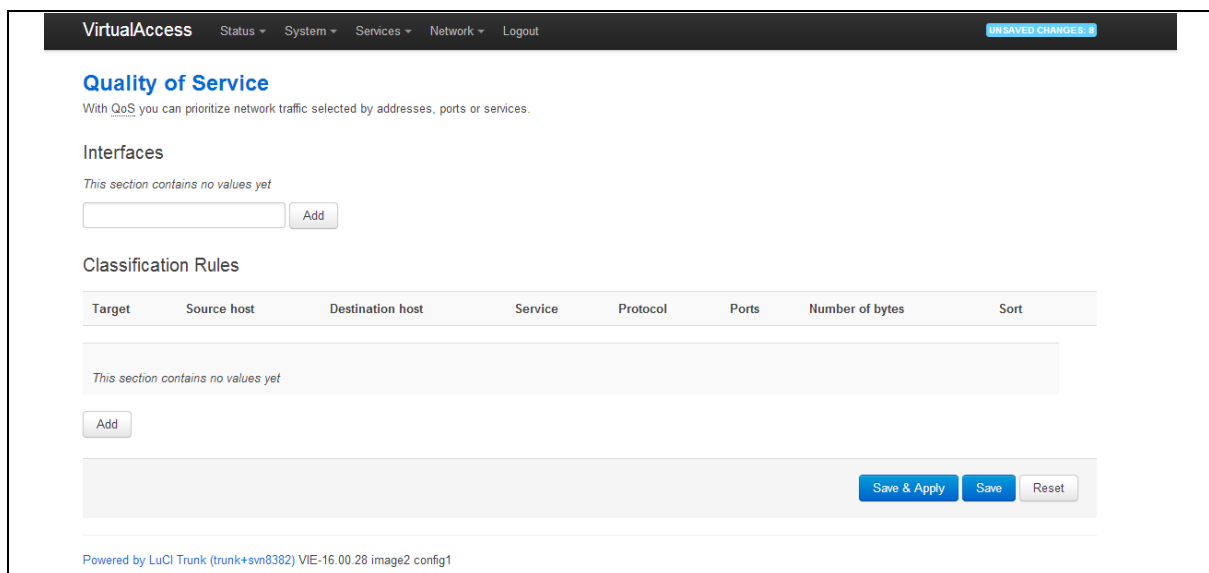


Figure 221: The quality of service page

To configure an interface, enter a relevant interface name and click **Add**. The Quality of Service page for that interface appears.

**Figure 222: The quality of service page for WAN interface**

Use the following parameters to configure the interface you have chosen. The name of the interfaces should match with the logical name given to the interface in the network configuration.

| Web Field/UCI/Package Option   | Description  |   |          |   |           |
|--|--|---|----------|---|-----------|
| Web: Enabled<br>UCI: qos.[interface].enabled<br>Opt: enabled                     | Enables or disables QoS interface.<br><table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table>         | 1 | Enabled. | 0 | Disabled. |
| 1  | Enabled.   |   |          |   |           |
| 0  | Disabled.  |   |          |   |           |
| Web: Classification group<br>UCI: qos. [interface].classgroup<br>Opt: classgroup | Creates a mapping before previously created classgroup and interface to which it should be assigned to.  |   |          |   |           |
| Web: Calculate overhead<br>UCI: qos. [interface].overhead<br>Opt: overhead       | Decreases upload and download ratio to prevent link saturation.  |   |          |   |           |
| Web: Half-duplex<br>UCI: qos [interface].halfduplex<br>Opt: halfduplex           | Enables or disables half-duplex operation.<br><table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table> | 1 | Enabled. | 0 | Disabled. |
| 1  | Enabled.   |   |          |   |           |
| 0  | Disabled.  |   |          |   |           |
| Web: Download speed<br>UCI: qos.[interface].download<br>Opt: download            | Download speed limit in kbits/sec.   |   |          |   |           |
| Web: Upload speed<br>UCI: qos.[interface].upload=2000<br>Opt:upload              | Upload speed limit in kbits/sec.   |   |          |   |           |

**Table 154: Information table for QoS page**

To add classification rules, click **Add**. The Classification Rules section appears. Configure each classification rule with the following parameters.

Figure 223: Parameters for classification rules

| Web Field/UCI/Package Option          | Description   |        |  |          |  |     |  |         |  |
|---------------------------------------|---|--------|--|----------|--|-----|--|---------|--|
| Web: Target<br>UCI:<br>Opt:           | Creates and configures selected target bucket.<br><table border="1"> <tr> <td>Normal</td> <td></td> </tr> <tr> <td>Priority</td> <td></td> </tr> <tr> <td>Low</td> <td></td> </tr> <tr> <td>Express</td> <td></td> </tr> </table> | Normal |  | Priority |  | Low |  | Express |  |
| Normal                                |   |        |  |          |  |     |  |         |  |
| Priority                              |   |        |  |          |  |     |  |         |  |
| Low                                   |   |        |  |          |  |     |  |         |  |
| Express                               |   |        |  |          |  |     |  |         |  |
| Web: Source host<br>UCI:<br>Opt:      | Source host.  |        |  |          |  |     |  |         |  |
| Web: Destination host<br>UCI:<br>Opt: | Destination host.   |        |  |          |  |     |  |         |  |
| Web: Service<br>UCI:<br>Opt:          | Selectable service.   |        |  |          |  |     |  |         |  |
| Web: Protocol<br>UCI:<br>Opt:         | Protocol to classify.   |        |  |          |  |     |  |         |  |
| Web: Ports<br>UCI:<br>Opt:            | Upload speed kbits/sec.   |        |  |          |  |     |  |         |  |
| Web: Number of bytes<br>UCI:<br>Opt:  | Number of bytes for bucket.   |        |  |          |  |     |  |         |  |

Table 155: Information table for classification rules

## 40.4 Configuring QoS using UCI

You can also configure QoS using UCI. The configuration file is stored on:

**/etc/config/qos**

### 40.4.1 Interface

Defines the interface on which configured QoS settings will take place.

Each interface can have its own buffer. The interface section declares global characteristics of the connection on which the specified interface is communicating. The following options are defined within this section:



```

config interface 'ADSL'
  option classgroup 'Default'
  option enabled '1'
  option overhead '1'
  option halfduplex '0'
  option download '900'
  option upload '245'

```

| Web Field/UCI/Package Option   | Description  |   |          |   |           |
|--|--|---|----------|---|-----------|
| Web: Enabled<br>UCI: qos.[interface].enabled<br>Opt: enabled                     | Enables or disables QoS interface.<br><table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table>         | 1 | Enabled. | 0 | Disabled. |
| 1  | Enabled.   |   |          |   |           |
| 0  | Disabled.  |   |          |   |           |
| Web: Classification group<br>UCI: qos. [interface].classgroup<br>Opt: classgroup | Creates a mapping before previously created classgroup and interface to which it should be assigned to.  |   |          |   |           |
| Web: Calculate overhead<br>UCI: qos. [interface].overhead<br>Opt: overhead       | Decrease upload and download ratio to prevent link saturation.   |   |          |   |           |
| Web: Half-duplex<br>UCI: qos [interface].halfduplex<br>Opt: halfduplex           | Enables or disables half-duplex operation.<br><table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table> | 1 | Enabled. | 0 | Disabled. |
| 1  | Enabled.   |   |          |   |           |
| 0  | Disabled.  |   |          |   |           |
| Web: Download speed<br>UCI: qos.[interface].download<br>Opt: download            | Download speed limit in kbits/sec.   |   |          |   |           |
| Web: Upload speed<br>UCI: qos.[interface].upload=2000<br>Opt:upload              | Upload speed limit in kbits/sec.   |   |          |   |           |

## 40.4.2 Classgroup

As there is more than one interface you can have more than one classgroup.

```

config classgroup 'Default'
  option classes 'Express Normal'
  option default 'Normal'

```

| UCI/Package Option                                      | Description  |
|---|--|
| UCI: qos.Default=classgroup<br>Opt: Default             | Specifies name of classgroup.  |
| UCI: qos.Default.classes=Express Normal<br>Opt: classes | Specifies the list of names of classes which should be part of classgroup. |
| qos.Default.default=Normal<br>Opt: default              | Defines which class is considered default.                                 |

### 40.4.3 Classes

Each bucket has its own configuration.

```

config class 'Normal'
    option packetsize '1500'
    option avgrate '30'
    option priority '5'

config class 'Express'
    option packetsize '1000'
    option maxsize '800'
    option avgrate '50'
    option priority '10'
    option limitrate '10'

```

| UCI/Package Option                                  | Description   |
|---|---|
| UCI: qos.Normal=class<br>Opt: Normal                | Specifies class name.   |
| UCI: qos.Normal.packetsize=1500<br>Opt: packetsize  | Specifies packet size for the class in bytes.                             |
| UCI: qos.Normal.avgrate=30<br>Opt: avgrate          | Average rate for this class, value in % of bandwidth in %.                |
| UCI: qos.Normal.priority=5<br>Opt: priority         | Specifies priority for the class in %.                                    |
| UCI: qos.Express=class<br>Opt: Express              | Specifies class name.   |
| UCI: qos.Express.packetsize=1000<br>Opt: packetsize | Specifies packet size for the class in bytes.                             |
| UCI: qos.Express.maxsize=800<br>Opt: maxsize        | Specify max packet size in bytes.   |
| UCI: qos.Express.avgrate=50<br>Opt: avgrate         | Average rate for this class, value in % of bandwidth in %.                |
| UCI: qos.Express.priority=10<br>Opt: priority       | Specifies priority for the class in %.                                    |
| UCI: qos.Express.limitrate=10<br>Opt: limitrate     | Defines to how many % of the available bandwidth this class is capped to. |

### 40.4.4 Classify

Classifiers match the traffic for desired class.

```

config classify
    option target 'Express'
    option proto 'udp'

```

| UCI/Package Option                                  | Description             |
|---|-------------------------|
| UCI: qos.@classify[0]=classify<br>Opt: classify     | Part of classify rule.  |
| UCI: qos.@classify[0].target=Express<br>Opt: target | Specifies target class. |
| UCI: qos.@classify[0].proto=udp<br>Opt: proto       | Specifies protocol.     |

## 40.5 Example QoS configurations

```

config interface 'ADSL'
    option classgroup 'Default'
    option enabled '1'
    option overhead '1'
    option download '900'
    option upload '245'

config classgroup 'Default'
    option classes 'Express Normal'
    option default 'Normal'

config class 'Normal'
    option packetsize '1500'
    option avgrate '30'
    option priority '5'

config class 'Express'
    option packetsize '1000'
    option maxsize '800'
    option avgrate '50'
    option priority '10'
    option limitrate '10'

config classify
    option target 'Express'
    option proto 'udp'

```

## 41 Management configuration settings

This chapter contains the configuration sections and parameters required to manage and monitor your device using Activator and Monitor.

### 41.1 Activator

Activator is a Virtual Access proprietary provisioning system, where specific router configurations and firmware can be stored to allow central management and provisioning. Activator has two distinct roles in provisioning firmware and configuration files to a router.

- Autoload activation of firmware and configuration files on router boot up:
  - Autoload is generally used for router installation. In this scenario the router will initiate the request for firmware and configuration files when it boots up. The router is installed with a factory config that will allow it to contact Activator. The autoload feature controls the behaviour of the router in requesting firmware and configuration files; this includes when to start the Activation process and the specific files requested. The HTTP Client (uhttpd) contains information about the Activator server and the protocol used for activation.
- Deployment of firmware to routers after installation:
  - In this scenario, Activator initiates the process. This process, known as Active Updates, allows for central automatic deployment of firmware and configuration files. It is used when configuration or firmware changes need to be pushed to live routers.

### 41.2 Monitor

Monitor is a Virtual Access proprietary tool, based on SNMP protocol, to monitor wide networks of deployed routers. The router is configured to send information to Monitor, which is then stored and viewed centrally via the Monitor application. This includes features such as traffic light availability status, syslog and SLA monitoring.

### 41.3 Configuration packages used

| Package          | Sections |
|------------------|----------|
| autoload         | main     |
| httpclient       | default  |
| management_users | user     |

## 41.4 Autoload: boot up activation

Autoload configurations specify how the device should behave with respect to activation when it boots up. Autoload entries contain information about the specific files to be downloaded and the destination for the downloaded file. Standard autoload entry configurations to download are:

- A firmware file (\$\$.img)
- A configuration file (\$\$.ini)
- A .vas file (\$\$.vas). This file signals the end of the autoloaod sequence to Activator

Activator identifies the device using the serial number of the router. \$\$ syntax is used to denote the serial number of the router when requesting a file. The requested files are written to the alternate image or config segment.

You can change the settings either directly in the configuration file or via appropriate UCI set commands. It is normal procedure for autoload to be enabled in the router's factory settings and disabled in running configurations (config 1 and 2).

Autoload may already have been set at factory config level. If you wish to enable autoload services, proceed through the following steps.

## 41.5 Autoload packages

| Package  | Sections |
|----------|----------|
| autoload | main     |

### 41.5.1 Create a configuration file

In the top menu, select **Services -> Autoload**. The Autoload page has two sections: Basic Settings and Entries. Click **Add** to access configuration settings for each section.

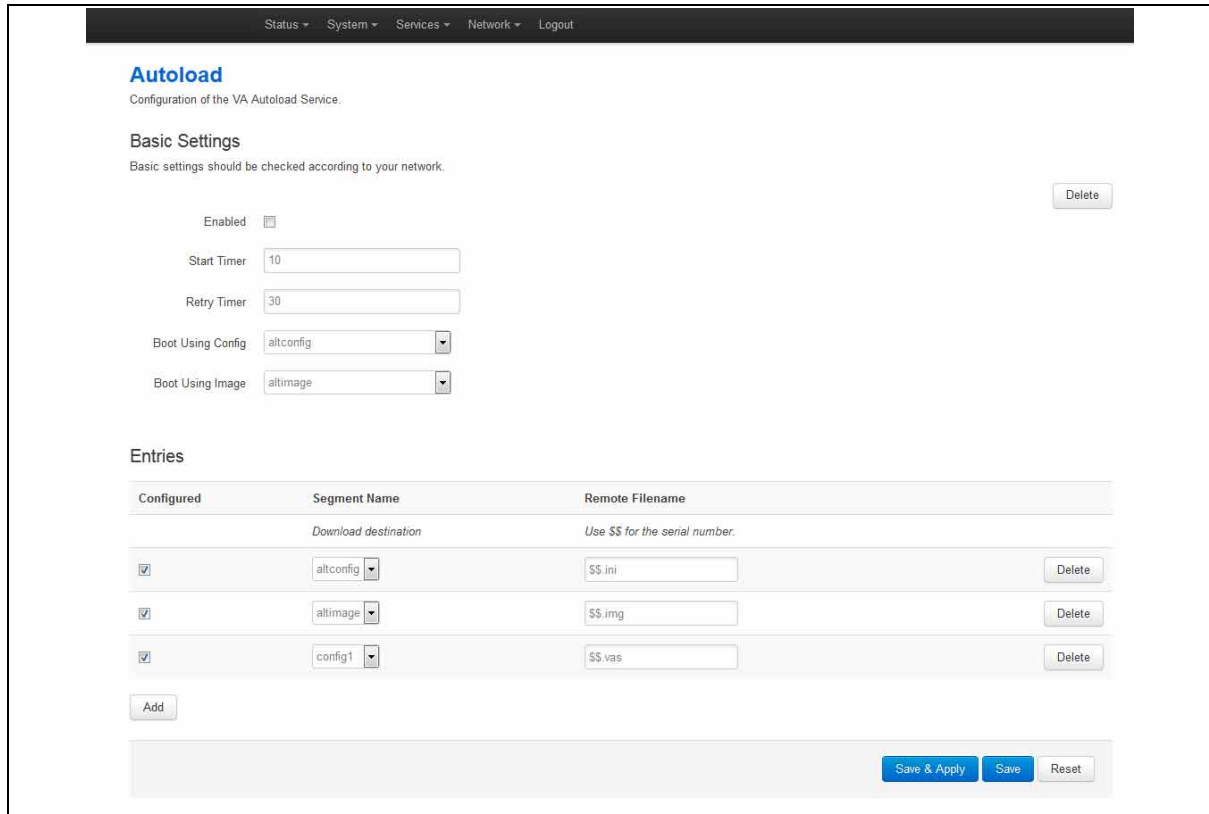


Figure 190: The autoload settings page

| Web Field/UCI/Package Option   | Description  |
|--|--|
| Basic settings   |  |
| Web: Enabled<br>UCI: autoload.main.enabled<br>Opt: Enabled             | Enables activation at system boot.<br>1 Enabled.<br>0 Disabled.  |
| Web: Start Timer<br>UCI: autoload.main.StartTimer<br>Opt: StartTimer   | Defines how long to wait after the boot up completes before starting activation.<br>10<br>Range 0-300 secs   |
| Web: Retry Timer<br>UCI: autoload.main.RetryTimer<br>Opt: RetryTimer   | Defines how many seconds to wait between retries if a download of a particular autoload entry fails.<br>30<br>Range 0-300 secs                                       |
| Web: N/A<br>UCI: autoload.main.NumberOfRetries<br>Opt: Numberofretries | Defines how many retries to attempt before failing the overall activation sequence, backing off and trying the whole activation sequence again.<br>5<br>Range        |
| Web: N/A<br>UCI: autoload.main.BackoffTimer<br>Opt: Backofftimer       | Defines how many minutes to back off for if a download and all retries fail. After the backoff period, the entire autoload sequence will start again.<br>15<br>Range |

|  |   |           |  |          |                       |          |                  |          |                       |
|--|---|-----------|--|----------|-----------------------|----------|------------------|----------|-----------------------|
| Web: Boot Using Config<br>UCI: autoload.main.BootUsingConfig<br>Opt: BootUsingConfig | Specifies which configuration to boot up with after the activation sequence.<br><table border="1"> <tr> <td>Altconfig</td> <td>Alternative configuration</td> </tr> <tr> <td>Config1</td> <td>Configuration 1</td> </tr> <tr> <td>Config2</td> <td>Configuration 2</td> </tr> <tr> <td>Factconf</td> <td>Factory configuration</td> </tr> </table>      | Altconfig | Alternative configuration                | Config1  | Configuration 1       | Config2  | Configuration 2  | Factconf | Factory configuration |
| Altconfig  | Alternative configuration   |           |  |          |                       |          |                  |          |                       |
| Config1  | Configuration 1   |           |  |          |                       |          |                  |          |                       |
| Config2  | Configuration 2   |           |  |          |                       |          |                  |          |                       |
| Factconf   | Factory configuration   |           |  |          |                       |          |                  |          |                       |
| Web: Boot Using Image<br>UCI: autoload.main.BootUsingImage<br>Opt: BootUsingImage    | Specifies which image to boot up with after the activation sequence completes successfully.<br><table border="1"> <tr> <td>Altimage</td> <td>Alternative image</td> </tr> <tr> <td>Image 1</td> <td>image 1</td> </tr> <tr> <td>Image 2</td> <td>image 2</td> </tr> </table>  | Altimage  | Alternative image                        | Image 1  | image 1               | Image 2  | image 2          |          |                       |
| Altimage   | Alternative image   |           |  |          |                       |          |                  |          |                       |
| Image 1  | image 1   |           |  |          |                       |          |                  |          |                       |
| Image 2  | image 2   |           |  |          |                       |          |                  |          |                       |
| Entries  |   |           |  |          |                       |          |                  |          |                       |
| Web: Configured<br>UCI: autoload.@entry[x].Configured<br>Opt: Configured             | Enables the autoload sequence to process this entry.<br><table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table>  | 1         | Enabled.                                 | 0        | Disabled.             |          |                  |          |                       |
| 1  | Enabled.  |           |  |          |                       |          |                  |          |                       |
| 0  | Disabled.   |           |  |          |                       |          |                  |          |                       |
| Web: Segment Name<br>UCI: autoload.@entry[x].SegmentName<br>Opt: SegmentName         | Defines where the downloaded file should be stored:<br>(config1   config2   altconfig   image1   image2   altimage).<br>Typically only altconfig and altimage are used.   |           |  |          |                       |          |                  |          |                       |
| Web: RemoteFilename<br>UCI: autoload.@entry[x].RemoteFilename<br>Opt: RemoteFilename | Defines the name of the file to be downloaded from Activator.<br><table border="1"> <tr> <td>\$\$ .vas</td> <td>Notifies activator sequence is complete.</td> </tr> <tr> <td>\$\$ ini</td> <td>Request configuration</td> </tr> <tr> <td>\$\$ img</td> <td>Request firmware</td> </tr> </table> <p>Note: \$\$ .vas should always be requested last.</p> | \$\$ .vas | Notifies activator sequence is complete. | \$\$ ini | Request configuration | \$\$ img | Request firmware |          |                       |
| \$\$ .vas  | Notifies activator sequence is complete.  |           |  |          |                       |          |                  |          |                       |
| \$\$ ini   | Request configuration   |           |  |          |                       |          |                  |          |                       |
| \$\$ img   | Request firmware  |           |  |          |                       |          |                  |          |                       |

Table 132: Information table for autoload

## 41.6 Autoload using UCI

```

root@VA_router:/# uci show autoload
autoload.main=core
autoload.main.Enabled=yes
autoload.main.StartTimer=10
autoload.main.RetryTimer=30
autoload.main.NumberOfRetries=5
autoload.main.BackoffTimer=15
autoload.main.BootUsingConfig=altconfig
autoload.main.BootUsingImage=altimage
autoload.@entry[0]=entry
autoload.@entry[0].Configured=yes
autoload.@entry[0].SegmentName=altconfig
autoload.@entry[0].RemoteFilename=$$.ini
autoload.@entry[1]=entry
autoload.@entry[1].Configured=yes
autoload.@entry[1].SegmentName=altimage
autoload.@entry[1].RemoteFilename=$$.img

```

```
autoload.@entry[2]=entry
autoload.@entry[2].Configured=yes
autoload.@entry[2].SegmentName=config1
autoload.@entry[2].RemoteFilename=$$.vas
Autoload using package options
root@VA_router:/# uci export autoload
package 'autoload'

config 'core' 'main'
    option 'Enabled' "yes"
    option 'StartTimer' "10"
    option 'RetryTimer' "30"
    option 'NumberOfRetries' "5"
    option 'BackoffTimer' "15"
    option 'BootUsingConfig' "altconfig"
    option 'BootUsingImage' "altimage"

config 'entry'
    option 'Configured' "yes"
    option 'SegmentName' "altconfig"
    option 'RemoteFilename' "\$\$.ini"

config 'entry'
    option 'Configured' "yes"
    option 'SegmentName' "altimage"
    option 'RemoteFilename' "\$\$.img"

config 'entry'
    option 'Configured' "yes"
    option 'SegmentName' "config1"
    option 'RemoteFilename' "\$\$.vas"
```

## 41.7 HTTP Client: configuring activation using the web interface

This section contains the settings for the HTTP Client used during activation and active updates of the device.

The httpclient core section configures the basic functionality of the module used for retrieving files from Activator during the activation process.



### 41.7.1 HTTP Client configuraton packages

| Package    | Sections |
|------------|----------|
| Httpclient | default  |

### 41.7.2 Web configuration

To configure HTTP Client for Activator, in the top menu, click **Services -> HTTP Client**. The HTTP Client page has two sections: Basic Settings and Advanced Settings.

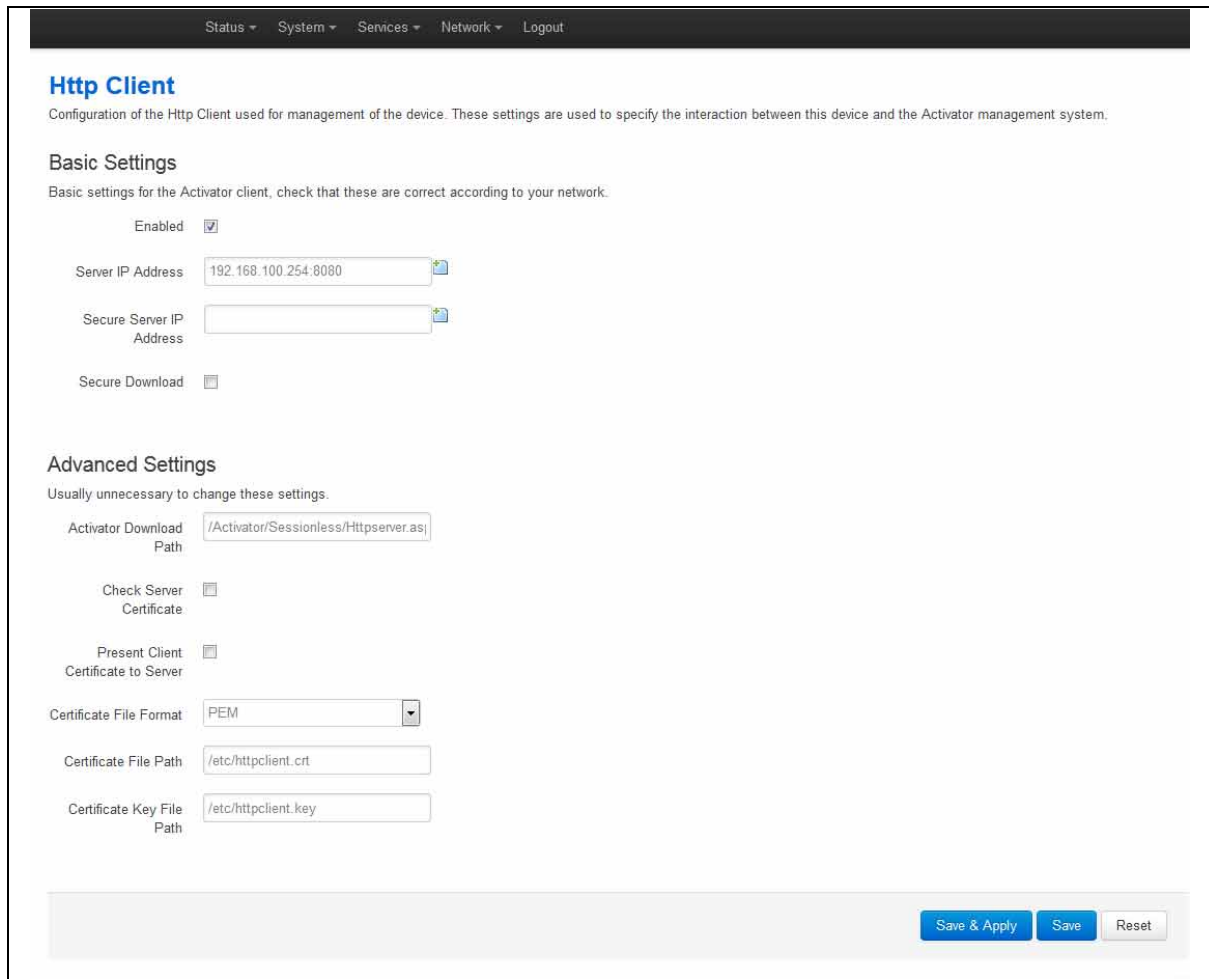


Figure 191: The HTTP client page

| Web Field/UCI/Package Option  | Description   |   |          |   |           |
|---|---|---|----------|---|-----------|
| Basic settings  |   |   |          |   |           |
| Web: Enabled<br>UCI: httpclient.default.enabled<br>Opt: Enabled   | Enables the HTTP client.<br><table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table>  | 1 | Enabled. | 0 | Disabled. |
| 1   | Enabled.  |   |          |   |           |
| 0   | Disabled.   |   |          |   |           |
| Web: Server IP Address<br>UCI: httpclient.default.Fileserver<br>Opt: list Fileserver                    | Specifies the address of Activator that uses http port 80. This can be an IP address or FQDN. The syntax should be x.x.x.x:80 or FQDN:80. Multiple servers should be separated by a space using UCI.      |   |          |   |           |
| Web: Secure Server IP Address<br>UCI: httpclient.default.SecureFileServer<br>Opt: list SecureFileServer | Specifies the address of Secure Activator that uses port 443. This can be an IP address or FQDN. The syntax should be x.x.x.x:443 or FQDN:443. Multiple servers should be separated by a space using UCI. |   |          |   |           |

|   |  |                                       |                               |            |                          |
|---|--|---------------------------------------|-------------------------------|------------|--------------------------|
| <p>Web: Secure Download<br/>UCI: httpclient.default.SecureDownload<br/>Opt: SecureDownload</p>  | <p>Enables Secure Download (port 443).</p> <table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table>  | 1                                     | Enabled.                      | 0          | Disabled.                |
| 1   | Enabled.   |                                       |                               |            |                          |
| 0   | Disabled.  |                                       |                               |            |                          |
| <p>Advanced settings</p>  |  |                                       |                               |            |                          |
| <p>Web: ActivatorDownloadPath<br/>UCI: httpclient.default.ActivatorDownloadPath<br/>Opt: ActivatorDownloadPath</p>                          | <p>Specifies the URL on Activator to which the client should send requests.</p> <table border="1"> <tr> <td>/Activator/Sessionless/Httpserver.asp</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | /Activator/Sessionless/Httpserver.asp |                               | Range      |                          |
| /Activator/Sessionless/Httpserver.asp   |  |                                       |                               |            |                          |
| Range   |  |                                       |                               |            |                          |
| <p>Web: Check Server Certificate<br/>UCI: httpclient.default.ValidateServerCertificateEnabled<br/>Opt: ValidateServerCertificateEnabled</p> | <p>Checks for the certificates presence and validity.</p> <table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table>   | 1                                     | Enabled.                      | 0          | Disabled.                |
| 1   | Enabled.   |                                       |                               |            |                          |
| 0   | Disabled.  |                                       |                               |            |                          |
| <p>Web: Present Client Certificate to Server<br/>UCI: httpclient.default.PresentCertificateEnabled<br/>Opt: PresentCertificateEnabled</p>   | <p>Specifies if the client presents its certificate to the server to identify itself.</p> <table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table>   | 1                                     | Enabled.                      | 0          | Disabled.                |
| 1   | Enabled.   |                                       |                               |            |                          |
| 0   | Disabled.  |                                       |                               |            |                          |
| <p>Web: CertificateFile Format<br/>UCI: httpclient.default.CertificateFormat<br/>Opt: CertificateFormat</p>                                 | <p>Specifies the value the client expects to see in the specified field in the server certificate.</p> <table border="1"> <tr> <td>PEM</td> <td></td> </tr> <tr> <td>DER</td> <td></td> </tr> </table>   | PEM                                   |                               | DER        |                          |
| PEM   |  |                                       |                               |            |                          |
| DER   |  |                                       |                               |            |                          |
| <p>Web: Certificate File Path<br/>UCI: httpclient.default.CertificateFile<br/>Opt: CertificateFile</p>                                      | <p>Defines the directory/location of the certificate.</p> <table border="1"> <tr> <td>/etc/httpclient.crt</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | /etc/httpclient.crt                   |                               | Range      |                          |
| /etc/httpclient.crt   |  |                                       |                               |            |                          |
| Range   |  |                                       |                               |            |                          |
| <p>Web: Certificate Key File Path<br/>UCI: httpclient.default.CertificateKey<br/>Opt: CertificateKey</p>                                    | <p>Specifies the directory/location of the certificate key.</p> <table border="1"> <tr> <td>/etc/httpclient.key</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | /etc/httpclient.key                   |                               | Range      |                          |
| /etc/httpclient.key   |  |                                       |                               |            |                          |
| Range   |  |                                       |                               |            |                          |
| <p>Web: N/A<br/>UCI: httpclient.default.ActivatorChunkyDownloadPath<br/>Opt: ActivatorChunkyDownloadPath</p>                                | <p>Enables partial download activations and active updates.<br/>The default value is:<br/><code>httpclient.default.ActivatorChunkyDownloadPath=/activator/partial/download</code><br/>The URL, on Activator, to which the client should send requests for chunky image download.</p> |                                       |                               |            |                          |
| <p>Web: N/A<br/>UCI: httpclient.default.ChunkSize<br/>Opt: ChunkSize</p>  | <p>Specifies the size of each packet payload.</p> <table border="1"> <tr> <td>100k</td> <td>100K bytes</td> </tr> <tr> <td>1-infinite</td> <td>Available values</td> </tr> </table>  | 100k                                  | 100K bytes                    | 1-infinite | Available values         |
| 100k  | 100K bytes   |                                       |                               |            |                          |
| 1-infinite  | Available values   |                                       |                               |            |                          |
| <p>Web: N/A<br/>UCI: httpclient.default.RateLimit<br/>Opt: RateLimit</p>  | <p>Throttle activation/active updates traffic received by device to specified limit.</p> <table border="1"> <tr> <td>None</td> <td>By default there is no limit.</td> </tr> <tr> <td>1-infinite</td> <td>Available values in kbps</td> </tr> </table>                                | None                                  | By default there is no limit. | 1-infinite | Available values in kbps |
| None  | By default there is no limit.  |                                       |                               |            |                          |
| 1-infinite  | Available values in kbps   |                                       |                               |            |                          |
| <p>Web: N/A<br/>UCI: httpclient.default.CAFile<br/>Opt: CAFile</p>  | <p>Defines the path to the certificate authority file stored on the router.</p>  |                                       |                               |            |                          |
| <p>Web: N/A<br/>UCI: httpclient.default.IgnoreServerCertificateStatus<br/>Opt: IgnoreServerCertificateStatus</p>                            | <p>Defines whether to skip the status check on the server certificate.</p> <table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table>  | 1                                     | Enabled.                      | 0          | Disabled.                |
| 1   | Enabled.   |                                       |                               |            |                          |
| 0   | Disabled.  |                                       |                               |            |                          |

**Table 133: Information table for HTTP client**

## 41.8 Httpclient: Activator configuration using UCI

```
root@VA_router:~# uci show httpclient
httpclient.default=core
httpclient.default.Enabled=yes
httpclient.default.FileServer=10.1.83.36:80 10.1.83.37:80
httpclient.default.SecureFileServer=10.1.83.36:443 10.1.83.37:443
httpclient.default.ActivatorDownloadPath=/Activator/Sessionless/Httpserver.
asp
httpclient.default.SecureDownload=no
httpclient.default.PresentCertificateEnabled=no
httpclient.default.ValidateServerCertificateEnabled=no
httpclient.default.CertificateFile=/etc/httpclient.crt
httpclient.default.CertificateFormat=PEM
httpclient.default.CertificateKey=/etc/httpclient.key
httpclient.default.ActivatorChunkyDownloadPath=/activator/partial/download
httpclient.default.ChunkSize=100k
httpclient.default.RateLimit=2
httpclient.default.CAFile='/'
httpclient.default.IgnoreServerCertificateStatus=0
```

## 41.9 Httpclient: Activator configuration using package options

```
root@VA_router:~# uci export httpclient
package httpclient

config core 'default'
    option Enabled 'yes'
    list FileServer '1.1.1.1:80'
    list FileServer '1.1.1.2:80'
    listSecureFileServer '1.1.1.1:443'
    list SecureFileServer '1.1.1.2:443'
    option ActivatorDownloadPath '/Activator/Sessionless/Httpserver.asp'
    option SecureDownload 'no'
    option PresentCertificateEnabled 'no'
    option ValidateServerCertificateEnabled 'no'
    option CertificateFile '/etc/httpclient.crt'
    option CertificateFormat 'PEM'
```

```
option CertificateKey '/etc/httpclient.key'
option ActivatorChunkyDownloadPath '/activator/partial/download'
option ChunkSize '100k'
option RateLimit '2'
option CAFile '\\'
option IgnoreServerCertificateStatus '0'
```

## 41.10 User management using UCI

User management is not currently available using the web interface. You can configure the feature using UCI or Activator.

### 41.10.1 User management packages

| Package          | Sections |
|------------------|----------|
| management_users | Users    |

### 41.10.2 Configuring user management

You can create different users on the system by defining them in the user management configuration file. This gives users access to different services.

| Web Field/UCI/Package Option  | Description  |   |           |   |          |
|---|--|---|-----------|---|----------|
| General settings  |  |   |           |   |          |
| Web: n/a<br>UCI: management_users.@user[x].enabled<br>Opt: enable       | Enables/creates the user.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0 | Disabled. | 1 | Enabled. |
| 0   | Disabled.  |   |           |   |          |
| 1   | Enabled.   |   |           |   |          |
| Web: n/a<br>UCI:<br>management_users.@user[x].username<br>Opt: username | Specifies the user's username.   |   |           |   |          |
| Web: n/a<br>UCI:<br>management_users.@user[x].password<br>Opt: password | Specifies the user's password. When entering the user password enter in plain text using the password option. After reboot the password is displayed encrypted via the CLI using the hashpassword option.<br>UCI: management_users.@user[x].hashpassword<br>Opt: hashpassword.<br><b>Note:</b> a SRP user password will be displayed using the srphash option. |   |           |   |          |
| Web: n/a<br>UCI: management_users.@user[x].webuser<br>Opt: webuser      | Specifies web access permissions for the user.<br><b>Note:</b> webuser will only work if linuxuser is set to <b>Enabled</b> .<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0 | Disabled. | 1 | Enabled. |
| 0   | Disabled.  |   |           |   |          |
| 1   | Enabled.   |   |           |   |          |
| Web: n/a<br>UCI:<br>management_users.@user[x].chapuser<br>Opt: chapuser | Specifies CHAP access permissions for the PPP connection.<br><b>Note:</b> chapuser will only work if linux user is set to <b>no</b> .<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0 | Disabled. | 1 | Enabled. |
| 0   | Disabled.  |   |           |   |          |
| 1   | Enabled.   |   |           |   |          |
| Web: n/a<br>UCI: management_users.@user[x].papuser<br>Opt: papuser      | Specifies PAP access permissions for the PPP connection.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0 | Disabled. | 1 | Enabled. |
| 0   | Disabled.  |   |           |   |          |
| 1   | Enabled.   |   |           |   |          |

|  |  |   |           |   |          |
|--|--|---|-----------|---|----------|
| Web: n/a<br>UCI: management_users.@user[x].srpuser<br>Opt: srpuser | Specifies SRP access permissions for the PPP connection.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | 0 | Disabled. | 1 | Enabled. |
| 0  | Disabled.  |   |           |   |          |
| 1  | Enabled.   |   |           |   |          |
| Web: n/a<br>UCI: management_users.@user[x].smsuser<br>Opt: smsuser | Specifies SMS access permissions for the user.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>           | 0 | Disabled. | 1 | Enabled. |
| 0  | Disabled.  |   |           |   |          |
| 1  | Enabled.   |   |           |   |          |
| Web: n/a<br>UCI: linuxuser<br>Opt: linuxuser                       | Specifies linuxuser access permissions for the user.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>     | 0 | Disabled. | 1 | Enabled. |
| 0  | Disabled.  |   |           |   |          |
| 1  | Enabled.   |   |           |   |          |
| Web: n/a<br>UCI: List allowed_pages<br>Opt: list allowed_pages     | Specifies which pages the user can view. Multiple pages should be entered using a space to separate if using UCI.  |   |           |   |          |

**Table 134: Information table for config user commands**

**Note:**

- webuser will only work if linuxuser is set to **yes**
- chapuser will only work if linuxuser is set to **no**

When a new user is created on the system and given web access, you will no longer be able to login to the router web interface with the default root user details. The user must use their new user login details.

## 41.11 Configuring the management user password using UCI

The user password is displayed encrypted via the CLI using the hashpassword option.

```
root@VA_router:~# uci show management_users
management_users.@user[0].username=test
management_users.@user[0].hashpassword=$1$XVzDHHPQ$SKK4geFonctihuffMjS4U0
```

If you are changing the password via the UCI, enter the new password in plain text using the password option.

```
root@VA_router:~# uci set management_users.@user[0].password=newpassword
root@VA_router:~# uci commit
```

The new password will take effect after reboot and will now be displayed in encrypted format through the hashpassword option.

## 41.12 Configuring management user password using package options

The root password is displayed encrypted via CLI using the hashpassword option.

```
root@VA_router:~# uci export management_users
package management_users

config user
    option hashpassword '$1$wRYYiJOz$EeHN.GQcxXhRgNPVbqxVw'
```

If you are changing the password using UCI, enter the new password in plain text using the password option.

```
package management_users

config user
    option hashpassword '$1$wRYYiJOz$EeHN.GQcxXhRgNPVbqxVw'
    option password 'newpassword'
```

The new password will take effect after reboot and will now be displayed in encrypted format via the hashpassword option.

## 41.13 User management using UCI

```
root@VA_router:~# uci show management_users
management_users.@user[0]=user
management_users.@user[0].enabled=1
management_users.@user[0].username=test
management_users.@user[0].hashpassword=$1$XVzDHHPQ$SKK4geFonctihuffMjS4U0
management_users.@user[0].webuser=1
management_users.@user[0].linuxuser=1
management_users.@user[0].papuser=0
management_users.@user[0].chapuser=0
management_users.@user[0].srpuser=0
management_users.@user[0].smsuser=0
```

## 41.14 User management using package options

```
root@VA_router:~# uci export management_users

package management_users

config user
```

```
option enabled '1'  
option username 'test'  
option hashpassword '$1$XVzDHHPQ$SKK4geFonctihuffMjS4U0'  
option webuser '1'  
option linuxuser '1'  
option papuser '0'  
option chapuser '0'  
option srpuser '0'  
option smsuser '0'
```

## 41.15 Configuring user access to specific web pages

To specify particular pages a user can view, add the list `allowed_pages`. Examples are:

```
list allowed_pages '/admin/status'
```

The user can view admin status page only.

```
List allowed_pages '/admin/system/flashops'
```

The user can view flash operation page only.

To specify monitor widgets only, enter:

```
listallowed_pages 'monitor/<widgetname>'
```

Example widget names are: dhcp, arp, 3gstats, interfaces, memory, multiwan, network, openvpn, routes, system, ipsec, dmvpn, tserverd.

## 42 Configuring Monitor

### 42.1 Introduction

Virtual Access monitoring system (Monitor) is a secure portal that provides:

- Centralised monitoring of devices
- Device status
- GPS location
- Syslog reporting
- Real time diagnostics
- Email notification
- Advanced statistics
- Dashboard graph reporting

You must configure each router in the network to send the required information to Monitor. This chapter explains how to configure the different information that can be sent to Monitor, including the required router configuration for:

- Reporting device status to Monitor
- Reporting GPS location to Monitor
- Reporting syslog to Monitor
- Configuration of interface statistics collection (ISAD)

For detailed information on operating Monitor, read the 'Virtual Access Monitor User Manual'.

### 42.2 Reporting device status to Monitor

To allow Monitor to track the IP address and ongoing presence of a device, a keepalive heartbeat SNMP trap is sent from the router. The router is capable of sending SNMP in version 1, 2c and 3.

The SNMP keepalive heartbeat sends basic information on interface status but can also be configured to contain more detailed information such as GPS location.

The basic heartbeat configuration consists of two parts:

- enabling the heartbeat keepalive
- enabling the interface(s) to be monitored

#### 42.2.1 Configuration package used

| Package | Sections  |
|---------|-----------|
| monitor | keepalive |
| network | interface |



## 42.2.2 Configuring keepalive heartbeat using the web interface

Select **Services -> Monitor**. The Monitor Keepalive & ISAD page appears.

The keepalive heartbeat is configured under the **Basic Settings** section.

A single instance keepalive can be configured to multiple monitor address using the same reference, heartbeat interval and other options. Or alternatively multiple keepalive instances can be configured with unique options.

Figure 226: The Monitor & ISAD keepalive page

### 42.2.2.1 Basic settings

| Web Field/UCI/Package Option  | Description  |   |                          |       |                 |   |                |
|---|--|---|--------------------------|-------|-----------------|---|----------------|
| Web: Enabled<br>UCI: monitor.@keepalive[0].enabled<br>Opt: Enabled                              | Enables Monitor to send heartbeats to the router.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0 | Disabled.                | 1     | Enabled.        |   |                |
| 0   | Disabled.  |   |                          |       |                 |   |                |
| 1   | Enabled.   |   |                          |       |                 |   |                |
| Web: Dev Reference<br>UCI:<br>monitor.@keepalive[0].dev_reference<br>Opt: dev_reference         | Sets a unique identification for this device known to Monitor.   |   |                          |       |                 |   |                |
| Web: Monitor Address<br>UCI: monitor.@keepalive[0].monitor_ip<br>Opt: list monitor_ip           | Defines the IP address of Monitor. It is possible to specify multiple addresses to which SNMP heartbeat traps will be sent. To configure via UCI use a space separator. Example:<br>monitor.@keepalive[0].monitor_ip=1.1.1.1 2.2.2.2 |   |                          |       |                 |   |                |
| Web: Monitor Heartbeat Interval<br>UCI: monitor.@keepalive[0].interval_min<br>Opt: interval_min | Specifies the interval, in minutes, at which traps are sent.<br><table border="1"> <tr> <td>1</td> <td>Trap set every 1 minute.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 1 | Trap set every 1 minute. | Range |                 |   |                |
| 1   | Trap set every 1 minute.   |   |                          |       |                 |   |                |
| Range   |  |   |                          |       |                 |   |                |
| Web: SNMP Protocol Version<br>UCI:<br>monitor.@keepalive[0].snmp_version<br>Opt: snmp_version   | Specifies what SNMP version is sent to remote manager.<br><table border="1"> <tr> <td>1</td> <td>snmp version 1</td> </tr> <tr> <td>2c</td> <td>SNMP version 2c</td> </tr> <tr> <td>3</td> <td>SNMP version 3</td> </tr> </table>    | 1 | snmp version 1           | 2c    | SNMP version 2c | 3 | SNMP version 3 |
| 1   | snmp version 1   |   |                          |       |                 |   |                |
| 2c  | SNMP version 2c  |   |                          |       |                 |   |                |
| 3   | SNMP version 3   |   |                          |       |                 |   |                |

Table 159: Information table for Monitor & ISAD basic configuration

The figure below shows options that are relevant only if you have selected SNMP version 3.

|                           |                      |
|---------------------------|----------------------|
| SNMP Protocol Version     | 3                    |
| User Name                 | <input type="text"/> |
| Authentication Protocol   | SHA                  |
| Authentication Password   | <input type="text"/> |
| Privacy Protocol          | AES                  |
| Privacy Password          | <input type="text"/> |
| SNMPv3 Context            | <input type="text"/> |
| SNMPv3 Context Engine ID  | <input type="text"/> |
| SNMPv3 Security Engine ID | <input type="text"/> |

**Figure 227: The Monitor & ISAD keepalive page for SNMP v3**

| Web Field/UCI/Package Option   | Description  |       |                |        |                                 |     |                                 |
|--|--|-------|----------------|--------|---------------------------------|-----|---------------------------------|
| Web: User Name<br>UCI: monitor.@keepalive[0].snmp_uname<br>Opt: snmp_uname                               | Specifies user name.<br><table border="1"> <tr> <td>Blank</td> <td>Default value</td> </tr> <tr> <td>String</td> <td></td> </tr> </table>  | Blank | Default value  | String |                                 |     |                                 |
| Blank  | Default value  |       |                |        |                                 |     |                                 |
| String   |  |       |                |        |                                 |     |                                 |
| Web: Authentication Password<br>UCI:<br>monitor.@keepalive[0].snmp_auth_pass<br>Opt: snmp_auth_pass      | Specifies snmpv3 authentication password.  |       |                |        |                                 |     |                                 |
| Web: Authentication Protocol<br>UCI:<br>monitor.@keepalive[0].snmp_auth_proto<br>Opt: snmp_auth_proto    | Specifies snmpv3 authentication protocol.<br><table border="1"> <tr> <td>Blank</td> <td>Default value.</td> </tr> <tr> <td>MD5</td> <td>MD5 as authentication protocol.</td> </tr> <tr> <td>SHA</td> <td>SHA as authentication protocol.</td> </tr> </table> | Blank | Default value. | MD5    | MD5 as authentication protocol. | SHA | SHA as authentication protocol. |
| Blank  | Default value.   |       |                |        |                                 |     |                                 |
| MD5  | MD5 as authentication protocol.  |       |                |        |                                 |     |                                 |
| SHA  | SHA as authentication protocol.  |       |                |        |                                 |     |                                 |
| Web: Privacy Protocol<br>UCI:<br>monitor.@keepalive[0].snmp_priv_proto<br>Opt: snmp_priv_proto           | Specifies snmpv3 privacy protocol.<br><table border="1"> <tr> <td>Blank</td> <td>Default value.</td> </tr> <tr> <td>AES</td> <td>AES as privacy protocol.</td> </tr> <tr> <td>DES</td> <td>MD5 as privacy protocol.</td> </tr> </table>                      | Blank | Default value. | AES    | AES as privacy protocol.        | DES | MD5 as privacy protocol.        |
| Blank  | Default value.   |       |                |        |                                 |     |                                 |
| AES  | AES as privacy protocol.   |       |                |        |                                 |     |                                 |
| DES  | MD5 as privacy protocol.   |       |                |        |                                 |     |                                 |
| Web: Privacy Password<br>UCI:<br>monitor.@keepalive[0].snmp_priv_pass<br>Opt: snmp_priv_pass             | Specifies snmpv3 privacy password.   |       |                |        |                                 |     |                                 |
| Web: SNMPv3 Context<br>UCI:<br>monitor.@keepalive[0].snmp_context<br>Opt: snmp_context                   | Specifies snmpv3 context name.   |       |                |        |                                 |     |                                 |
| Web: SNMPv3 Context Engine ID<br>UCI:<br>monitor.@keepalive[0].snmp_context_eid<br>Opt: snmp_context_eid | Specifies snmpv3 context engine ID.  |       |                |        |                                 |     |                                 |

|   |                                      |
|---|--------------------------------------|
| Web: SNMPv3 Security Engine ID<br>UCI:<br>monitor.@keepalive[0].snmp_sec_eid<br>Opt: snmp_sec_eid | Specifies snmpv3 security engine ID. |
|---|--------------------------------------|

**Table 160: Information table for SNMP v3 reporting device commands**

### 42.2.3 Configuring keepalive heartbeat using command line

Keepalive is configured under the monitor package.

By default, all keepalive instances are named 'keepalive', instances are identified by @keepalive then the keepalive position in the package as a number. For example, for the first keepalive in the package using UCI:

```
monitor.@keepalive[0]=keepalive
monitor.@ keepalive[0].enabled=1
```

Or using package options:

```
config keepalive
    option enabled '1'
```

However, to better identify, it is recommended to give the keepalive instance a name. For example, to create a keepalive instance named keepalivev1.

To define a named keepalive instance using UCI, enter:

```
monitor.keepalivev1=keepalive
monitor.keepalivev1.enable=1
```

To define a named keepalive instance using package options, enter:

```
config keepalive 'keepalivev1'
    option enabled '1'
```

### 42.2.4 Keepalive using UCI

```
root@VA_router:~# uci show monitor
monitor.keepalivev1=keepalive
monitor.keepalivev1enabled=1
monitor.keepalivev1.interval_min=1
monitor.keepalivev1.dev_reference=router1
monitor.keepalivev1.monitor_ip=10.1.83.36
monitor.keepalivev1.snmp_version=1
monitor.keepalivev2=keepalive
```

```
monitor.keepalived2.enable=1
monitor.keepalived2.interval_min=1
monitor.keepalived2.monitor_ip=172.16.250.100
monitor.keepalived2.dev_reference=TEST
monitor.keepalived2.snmp_version=2c
monitor.keepalived3=keepalive
monitor.keepalived3.enable=1
monitor.keepalived3.interval_min=1
monitor.keepalived3.monitor_ip=172.16.250.101
monitor.keepalived3.dev_reference=TEST
monitor.keepalived3.snmp_version=3
monitor.keepalived3.snmp_uname=TEST
monitor.keepalived3.snmp_auth_pass=vasecret
monitor.keepalived3.snmp_auth_proto=MD5
monitor.keepalived3.snmp_priv_pass=vasecret
monitor.keepalived3.snmp_priv_proto=DES
```

### 42.2.5 Keepalive using package options

```
root@VA_router:~# uci export monitor
package 'monitor'

config keepalive 'keepalive1'
    option enabled '1'
    option interval_min '1'
    option dev_reference 'router1'
    option enabled 'yes'
    list monitor_ip '10.1.83.36'

config keepalive 'keepalive2'
    option enable '1'
    option interval_min '1'
    list monitor_ip '172.16.250.100'
    option dev_reference 'TEST'
    option snmp_version '2c'

config keepalive 'keepalive3'
```

```

option enable '1'
option interval_min '1'
list monitor_ip '172.16.250.101'
option dev_reference 'TEST'
option snmp_version '3'
option snmp_uname 'TEST'
option snmp_auth_pass 'vasecret'
option snmp_auth_proto 'MD5'
option snmp_priv_pass 'vasecret'
option snmp_priv_proto 'DES'

```

## 42.2.6 Enabling interface status in keepalive heartbeat via web interface

The keepalive heartbeat can send information on multiple interfaces. To send an interface status to Monitor, select **Network -> Interfaces**, then under the required interface select **Edit**. Under **Advanced Settings** enable the Monitor interface state option.

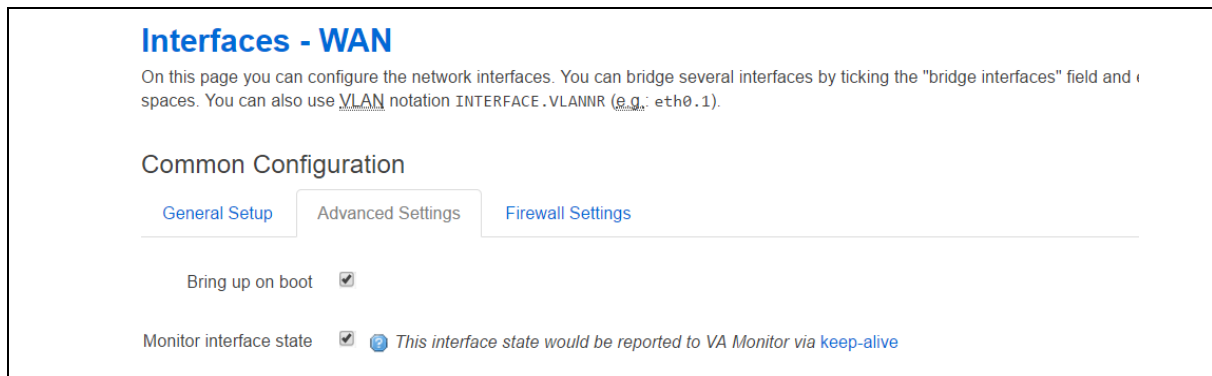


Figure 228: The interface common configuration page

| Web Field/UCI/Package Option   | Description   |
|--|---|
| Web: Monitor interface state<br>UCI: network.@interface[0].monitored<br>Opt: monitored | Enables interface status to be sent in the heartbeat trap to Monitor. |
|  | 0 Disabled.   |
|  | 1 Enabled.  |

Table 161: Information table for enabling interface status command

## 42.2.7 Enabling interface status using command line

Interface status is configured under the network package.

### 42.2.7.1 Enable interface status using UCI

```
root@VA_router:~# uci show network
network.@interface[0]=interface
.....
network.@interface[0].monitored=1
.....
```

### 42.2.7.2 Enable interface status using package option

```
root@VA_router:~# uci export network
package network
config interface 'WAN'
.....
option monitored '1'
.....
```

## 42.3 Reporting GPS location to Monitor

To allow Monitor to display a router GPS location, you can configure the GPS coordinates to be sent in the heartbeat keepalive from the router.

GPS location is only available in supported hardware models.

Ensure monitor keepalive heartbeat is correctly configured as in section 42.2 above.

### 42.3.1 Configuration package used

| Package | Sections |
|---------|----------|
| gpsd    | gpsd     |

### 42.3.2 Configuring GPS location via the web interface

Select **Services** -> **GPS**. The GPS configuration page appears.

The web interface configures a gpsd section named core.



Figure 229: The GPS configuration page

| Web Field/UCI/Package Option                                 | Description   |
|--|---|
| Web: Enable GPS<br>UCI: monitor.core.enabled<br>Opt: enabled | Enables GPS coordinates to be sent in the heartbeat keepalive to Monitor. |
|  | 0 Disabled.   |
|  | 1 Enabled.  |

Table 162: Information table for reporting GPS commands

### 42.3.3 Configuring GPS using command line

GPS location is configured under the gpsd package.

#### 42.3.3.1 GPS using UCI

```
root@VA_router:~# uci show gpsd
gpsd.core=gpsd
gpsd.core.enabled=1
```

#### 42.3.3.2 GPS using package options

```
root@VA_router:~# uci export gpsd
package gpsd
config gpsd 'core'
    option enabled '1'
```

### 42.3.4 GPS diagnostics

To view information on GPS coordinates via the web interface, select **Status -> GPS Information**.

Figure 230: The GPS status page

To view GPS coordinates via command line, enter:

```
root@VA_router:~# gpspeek
Fix: 3D,1495467700,53.342529,-6.241236,27.700000,202.600000,0.000000,0.000000
```

## 42.4 Reporting syslog to Monitor

### 42.4.1 Configuration package used

| Package | Sections |
|---------|----------|
| system  | main     |

### 42.4.2 Configuring syslog to Monitor via the web interface

Monitor can display syslog events sent from the router. To configure the router to send syslog events, select **System -> System -> Logging** and set **External system log server** to the Monitor IP. You can also configure the syslog server port if required.

All syslog events are sent to the syslog server.

Figure 231: The system properties page

| Web Field/UCI/Package Option  | Description   |
|---|---|
| Web: External system log server<br>UCI: system.main.log_ip<br>Opt: log_ip     | Defines the external syslog server IP address.                                  |
| Web: External system log server<br>UCI: system.main.log_port<br>Opt: log_port | Defines the external syslog server destination port number for syslog messages. |
|   | 514   |
|   | Range   |

Table 163: Information table for syslog properties commands

### 42.4.3 Configuring syslog events to Monitor using command line

Syslog is configured under the system package.

#### 42.4.3.1 Syslog events to Monitor using UCI

```
root@VA_router:~# uci show system
system.main=system
.....
system.main.log_ip=1.1.1.1
system.main.log_port=514
```



### 42.4.3.2 Syslog events to Monitor using package options

```

root@VA_router:~# uci export system
package system

config system 'main'
.....
    option log_ip '1.1.1.1'
    option log_port '514'

```

## 42.5 Configuring ISAD

ISAD is a system for collecting interface stats to be displayed on Monitor.

The following section explains how to configure interface statistics collection (iSAD). Statistical data is collected in bins with each bin containing interface transmit and receive packets/bytes/errors for a period. Signal strength and also temperature parameters are also stored in the bins. Bins are uploaded to Monitor periodically.

**Note:** ensure monitor keepalive heartbeat and interface status is correctly configured as in section 42.2 above. Interfaces should have `option monitored` enabled as part of the collection.

ISAD replaces the deprecated SLA feature.

### 42.5.1 Configuration package used

| Package | Sections        |
|---------|-----------------|
| monitor | interface_stats |

### 42.5.2 Configuring ISAD using the web interface

Select **Services -> Monitor**. The Monitor Keepalive & ISAD page appears. ISAD is configured under the **Interface Stats** section.



The screenshot shows the 'Interface Stats' configuration page. It includes the following elements:

- Enabled:** A checkbox that is currently unchecked.
- Bin Period:** A text input field containing the value '1h'.
- Maximum Number of Bins:** A text input field containing the value '24'.

Figure 232: The Monitor keepalive & ISAD interface stats page

| Web Field/UCI/Package Option  | Description   |       |                          |       |          |
|---|---|-------|--------------------------|-------|----------|
| Web: Enabled<br>UCI: monitor.stats.enabled=1<br>Opt: enabled                            | Enables ISAD.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0     | Disabled.                | 1     | Enabled. |
| 0   | Disabled.   |       |                          |       |          |
| 1   | Enabled.  |       |                          |       |          |
| Web: Bin Period<br>UCI: monitor.stats.bin_period<br>Opt: time                           | Specifies how long to collect data for one bin.<br>Specifies the interval, in minutes, at which traps are sent.<br><table border="1"> <tr> <td>1h</td> <td>Bin collected for 1 hour</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table> | 1h    | Bin collected for 1 hour | Range |          |
| 1h  | Bin collected for 1 hour  |       |                          |       |          |
| Range   |   |       |                          |       |          |
| Web: Maximum Number of Bins<br>UCI: monitor.stats.bin_cache_size<br>Opt: bin_cache_size | Specifies the maximum number of bins to store.<br><table border="1"> <tr> <td>Empty</td> <td>24</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | Empty | 24                       | Range |          |
| Empty   | 24  |       |                          |       |          |
| Range   |   |       |                          |       |          |

**Table 164: Information table for ISAD Monitor keepalive & ISAD interface stats section**

### 42.5.3 Configuring ISAD using the command line

ISAD is configured under the monitor package.

#### 42.5.3.1 ISAD using UCI

```
root@VA_router:~# uci show monitor
monitor.keepalivev1=keepalive
monitor.keepalivev1.enabled=1
monitor.keepalivev1.interval_min=1
monitor.keepalivev1.dev_reference=router1
monitor.keepalivev1.monitor_ip=10.1.83.36
monitor.keepalivev1.snmp_version=1
monitor.stats=interface_stats
monitor.stats.enabled=1
monitor.stats.bin_period=1h
monitor.stats.bin_cache_size=24
```

#### 42.5.3.2 ISAD using package options

```
root@VA_router:~# uci export monitor
package monitor

config keepalive 'keepalivev1'
    option interval_min '1'
    option enabled '1'
    list monitor_ip '10.1.83.36'
    option dev_reference 'router1'

config interface_stats 'stats'
    option enabled '1'
```

```
option bin_period '1h'
option bin_cache_size '24'
```

## 42.5.4 ISAD diagnostics

### 42.5.4.1 Checking process

To check to see if ISAD is running, enter:

```
root@VA_router:~# pgrep -fl isad
5303 /usr/sbin/isad -b 60 -s 10 -c 200 -u /var/state /var/const_state
```

### 42.5.4.2 Checking bin statistics

To check if stats are being collected, enter:

```
root@VA_router:~# cat /var/state/monitor
monitor.bin_0=isad
monitor.bin_0.end_ts=85020
monitor.bin_0.start_ts=84960
monitor.bin_1=isad
monitor.bin_1.end_ts=85080
monitor.bin_1.start_ts=85020
monitor.bin_2=isad
monitor.bin_2.end_ts=85140
monitor.bin_2.start_ts=85080
```

## 42.5.5 ISAD operation

The bin statistics stored on the router must be periodically pushed statistics to Monitor. This is normally done centrally when statistics are enabled on Monitor. Monitor contacts each router and auto-generates a script that will automatically schedule the upload of the bin statistics.

However, if Monitor cannot access the router WAN IP, you must do this manually on each router using a UDS script. An example is shown below where the bins are uploaded every hour to a Monitor server IP 89.101.154.154 using TFTP.

```
package uds

config script 'isb_upload_scr'
    option enabled '1'
    option exec_type 'periodic'
    option period '1h'
    list text '/usr/sbin/isb_upload.lua 89.101.154.154:69'
```

## 42.6 Speedtest reporting

To assist in determining WAN line speed characteristics the router can be configured to:

- Implement a Discard Protocol (RFC863)
- Implement a Character Generation Protocol (RFC864)

Note: A central client is required to generate the speedtest traffic and produce the measurement reports.

Configuration is not currently available via the web UI.

| Web Field/UCI/Package Option   | Description  |
|--|--|
| Web: n/a<br>UCI: monitor.speedtest.discard_enabled<br>Opt: discard_enabled   | Enables listening on TCP port 9 and discarding all received data.                                      |
|  | 0 Disabled.  |
|  | 1 Enabled.   |
| Web: n/a<br>UCI: monitor.speedtest.charngen_enabled<br>Opt: charngen_enabled | Enables listening on TCP port 19 and streaming data to the connected client at maximum possible speed. |
|  | 0 Disabled.  |
|  | 1 Enabled.   |

Table 165: Information table for monitor speedtest configuration options

### 42.6.1 Configuring speedtest via the command line

Speedtest options are configured in the speedtest configuration section of the monitor package.

#### 42.6.1.1 Speedtest using UCI

```
root@VA_router:~# uci show monitor
...
monitor.speedtest=speedtest
monitor.speedtest.discard_enabled
monitor.speedtest.charngen_enabled
```

#### 42.6.1.2 Speedtest using package options

```
root@VA_router:~# uci export monitor
package monitor
...
config speedtest
    option discard_enabled '0'
    option charngen_enabled '0'
```

## 43 Configuring SNMP

SNMP (Simple Network Management Protocol) is an internet-standard protocol for managing devices on IP networks. SNMP exposes management data in the form of a hierarchy of variables in a MIB (Management Information Base). These variables can be queried individually, or in groups using their OIDs (Object Identifiers) defined in MIBs. In addition, information from the router can be pushed to a network management station in the form of SNMP traps.

### 43.1 Configuration package used

| Package | Sections |                |                   |                 |              |
|---------|----------|----------------|-------------------|-----------------|--------------|
| snmpd   | access   | exec           | inventory         | monitor_load    | system       |
|         | agent    | group          | inventory_iftable | monitor_memory  | trapreceiver |
|         | com2sec  | heartbeat      | monitor_disk      | monitor_process | usm_user     |
|         | constant | informreceiver | monitor_ioerror   | pass            | view         |

The SNMP application has several configuration sections:

|                  |   |
|------------------|---|
| System and Agent | Configures the SNMP agent.  |
| Com2Sec          | Maps SNMP community names into an arbitrary security name.  |
| Group            | Assigns community names and SNMP protocols to groups.   |
| View and Access  | Creates views and sub-views of the whole available SNMP tree and grants specific access to those views on a group by group basis. |
| usm_user         | Defines a user for SNMPv3 USM.  |
| Trap receiver    | Sets the address of a notification receiver that should be sent SNMPv1 TRAPs and SNMPv2c TRAP2s.                                  |
| Inform receiver  | Sets the address of a notification receiver that should be sent SNMPv2 INFORM notifications respectively.                         |

### 43.2 Configuring SNMP using the web interface

In the top menu, select **Services -> SNMP**. The SNMP Service page appears.

Figure 233: The SNMP service page

### 43.2.1 System and agent settings

| Web Field/UCI/Package Option   | Description   |   |           |   |          |
|--|---|---|-----------|---|----------|
| System settings  |   |   |           |   |          |
| Web: System Location<br>UCI: snmpd.system[0].sysLocation<br>Opt: sysLocation                             | Sets the system location, system contact or system name for the agent. This information is reported in the 'system' group in the mibII tree.  |   |           |   |          |
| Web: System Contact<br>UCI: snmpd.system[0].sysContact<br>Opt: sysContact                                |   |   |           |   |          |
| Web: System Name<br>UCI: snmpd.system[0].sysName<br>Opt: sysName   |   |   |           |   |          |
| Agent Settings   |   |   |           |   |          |
| Web: Agent Address<br>UCI: snmpd.agent[0].agentaddress<br>Opt: agentaddress                              | Specifies the address(es) and port(s) on which the agent should listen.<br>[(udp tcp):][address:]port [,...]<br>Example:<br>udp:127.0.0.1:161, tcp:161, localhost:9161  |   |           |   |          |
| Web: Enable Authentication Traps<br>UCI: snmpd.agent[0].authtrapeenabled<br>Opt: authtrapeenabled        | Enables or disables SNMP authentication trap. <table border="1" data-bbox="678 929 1391 1012"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> <b>Note:</b> this is the SNMP poll authentication trap you set when there is a community mismatch. | 0 | Disabled. | 1 | Enabled. |
| 0  | Disabled.   |   |           |   |          |
| 1  | Enabled.  |   |           |   |          |
| Web: Enable Link State Notification<br>UCI: snmpd.agent[0].link_updown_notify<br>Opt: link_updown_notify | Generates trap/info when interface goes up or down. When enabled, the router sends a trap notification link up or down. <table border="1" data-bbox="678 1146 1391 1229"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>                         | 0 | Disabled. | 1 | Enabled. |
| 0  | Disabled.   |   |           |   |          |
| 1  | Enabled.  |   |           |   |          |

**Table 166: Information table for system and agent settings**

### 43.2.2 Com2Sec settings

To access Com2Sec settings, scroll down the SNMP Services page.

Use the COM2Sec section to map SNMP community names into an arbitrary security name. Map community names into security names based on the community name and the source subnet. Use the first source/community combination that matches the incoming packet.

A community string is a password that is applied to a device to restrict both read-only and read-write access to the SNMP data on the device. These community strings should be chosen carefully to ensure they are not trivial. They should also be changed at regular intervals and in accordance with network security policies.

COM2SEC Settings

| Security Name | Source    | Community |        |
|---------------|-----------|-----------|--------|
| public        | default   | public    | Delete |
| private       | localhost | private   | Delete |

Add

Figure 234: The COM2Sec settings section

| Web Field/UCI/Package Option  | Description   |
|---|---|
| Web: Security Name<br>UCI: snmpd.com2sec[x].secname<br>Opt: secname | Specifies an arbitrary security name for the user.  |
| Web: Source<br>UCI: snmpd.com2sec[x].source<br>Opt: source          | A hostname, localhost or a subnet specified as a.b.c.d/mask or a.b.c.d/bits or 'default' for no restrictions. |
| Web: Community<br>UCI: snmpd.com2sec[x].community<br>Opt: community | Specifies the community string being presented in the request.  |

Table 167: Information table for Com2Sec settings

### 43.2.3 Group settings

Group settings assign community names and SNMP protocols to groups.

Group Settings

| Group       | Version | Security Name |        |
|-------------|---------|---------------|--------|
| public_v1   | v1      | ro            | Delete |
| public_v2c  | v2c     | ro            | Delete |
| public_usm  | usm     | ro            | Delete |
| private_v1  | v1      | rw            | Delete |
| private_v2c | v2c     | rw            | Delete |

Figure 235: The group settings section

| Web Field/UCI/Package Option                                      | Description  |    |         |     |         |     |         |     |                  |
|---|--|----|---------|-----|---------|-----|---------|-----|------------------|
| Web: Group<br>UCI: snmpd.group[x].group<br>Opt: group             | Specifies an arbitrary group name.   |    |         |     |         |     |         |     |                  |
| Web: Version<br>UCI: snmpd.group[x].version<br>Opt: version       | Specifies the SNMP version number being used in the request: v1, v2c and usm (User-based Security Module) are supported. <table border="1"> <tr> <td>v1</td> <td>SNMP v1</td> </tr> <tr> <td>v2v</td> <td>SNMP v2</td> </tr> <tr> <td>usm</td> <td>SNMP v3</td> </tr> <tr> <td>any</td> <td>Any SNMP version</td> </tr> </table> | v1 | SNMP v1 | v2v | SNMP v2 | usm | SNMP v3 | any | Any SNMP version |
| v1  | SNMP v1  |    |         |     |         |     |         |     |                  |
| v2v   | SNMP v2  |    |         |     |         |     |         |     |                  |
| usm   | SNMP v3  |    |         |     |         |     |         |     |                  |
| any   | Any SNMP version   |    |         |     |         |     |         |     |                  |
| Web: Security Name<br>UCI: snmpd.group[x].secname<br>Opt: secname | Specifies the already defined security name that is being included in this group.  |    |         |     |         |     |         |     |                  |

Table 168: Information table for group settings

#### 43.2.4 View settings

View settings define a named "view", which is a subset of the overall OID tree. This is most commonly a single subtree, but several view directives can be given with the same view name, to build up a more complex collection of OIDs.

The screenshot shows a web interface titled "View Settings". It features a table with three columns: "Name", "Type", and "OID". The first row contains the text "all" under "Name", "included" under "Type", and "1" under "OID". To the right of the "OID" field is a "Delete" button. Below the table, there is an "Add" button and a text input field.

Figure 236: The view settings section

| Web Field/UCI/Package Option                              | Description  |          |            |               |                  |
|---|--|----------|------------|---------------|------------------|
| Web: Name<br>UCI: snmpd.view[x].viewname<br>Opt: viewname | Specifies an arbitrary view name. Typically it describes what the view shows.  |          |            |               |                  |
| Web: Type<br>UCI: snmpd.view[x].type<br>Opt: type         | Specifies whether the view lists oids that are included in the view or lists oids to be excluded from the view; in which case all other oids are visible apart from those ones listed. <table border="1"> <tr> <td>included</td> <td></td> </tr> <tr> <td>excluded</td> <td></td> </tr> </table> | included |            | excluded      |                  |
| included  |  |          |            |               |                  |
| excluded  |  |          |            |               |                  |
| Web: OID<br>UCI: snmpd.view[x].oid<br>Opt: oid            | OID to be included in or excluded from the view. Only numerical representation is supported. <table border="1"> <tr> <td>1</td> <td>Everything</td> </tr> <tr> <td>1.3.6.1.2.1.2</td> <td>Interfaces table</td> </tr> </table>   | 1        | Everything | 1.3.6.1.2.1.2 | Interfaces table |
| 1   | Everything   |          |            |               |                  |
| 1.3.6.1.2.1.2   | Interfaces table   |          |            |               |                  |

Table 169: Information table for view settings



## 43.2.5 Access settings

Access settings map from a group of users/communities, in a specific context and with a particular SNMP version and minimum security level, to one of three views, depending on the request being processed.

The screenshot shows the 'Access Settings' configuration interface. It features a table with the following columns: group, context, version, level, prefix, read, write, and notify. There are two rows of settings: 'public\_access' and 'private\_access'. Each row contains dropdown menus for each column and a 'Delete' button. Below the table is an 'Add' button.

Figure 237: The access settings section

| Web Field/UCI/Package Option                                 | Description   |        |         |      |         |      |         |     |                  |
|--|---|--------|---------|------|---------|------|---------|-----|------------------|
| Web: Group<br>UCI: snmpd.access[x].group<br>Opt: group       | Specifies the group to which access is being granted.   |        |         |      |         |      |         |     |                  |
| Web: Context<br>UCI: snmpd.access[x].context<br>Opt: context | SNMPv3 request context is matched against the value according to the prefix below. For SNMP v1 and SNMP v2c, the context must be <b>none</b> .<br><table border="1"> <tr><td>none</td><td></td></tr> <tr><td>all</td><td></td></tr> </table>  | none   |         | all  |         |      |         |     |                  |
| none   |   |        |         |      |         |      |         |     |                  |
| all  |   |        |         |      |         |      |         |     |                  |
| Web: Version<br>UCI: snmpd.access[x].version<br>Opt: version | Specifies the SNMP version number being used in the request: any, v1, v2c and usm are supported.<br><table border="1"> <tr><td>v1</td><td>SNMP v1</td></tr> <tr><td>v2v</td><td>SNMP v2</td></tr> <tr><td>usm</td><td>SNMP v3</td></tr> <tr><td>any</td><td>Any SNMP version</td></tr> </table> | v1     | SNMP v1 | v2v  | SNMP v2 | usm  | SNMP v3 | any | Any SNMP version |
| v1   | SNMP v1   |        |         |      |         |      |         |     |                  |
| v2v  | SNMP v2   |        |         |      |         |      |         |     |                  |
| usm  | SNMP v3   |        |         |      |         |      |         |     |                  |
| any  | Any SNMP version  |        |         |      |         |      |         |     |                  |
| Web: Level<br>UCI: snmpd.access[x].level<br>Opt: level       | Specifies the security level. For SNMP v1 and SNMP v2c the level must be <b>noauth</b> .<br><table border="1"> <tr><td>noauth</td><td></td></tr> <tr><td>auth</td><td></td></tr> <tr><td>priv</td><td></td></tr> </table>   | noauth |         | auth |         | priv |         |     |                  |
| noauth   |   |        |         |      |         |      |         |     |                  |
| auth   |   |        |         |      |         |      |         |     |                  |
| priv   |   |        |         |      |         |      |         |     |                  |
| Web: Prefix<br>UCI: snmpd.access[x].prefix<br>Opt: prefix    | Specifies how the context should be matched against the context of the incoming pdu.<br><table border="1"> <tr><td>exact</td><td></td></tr> <tr><td>any</td><td></td></tr> <tr><td>all</td><td></td></tr> </table>  | exact  |         | any  |         | all  |         |     |                  |
| exact  |   |        |         |      |         |      |         |     |                  |
| any  |   |        |         |      |         |      |         |     |                  |
| all  |   |        |         |      |         |      |         |     |                  |
| Web: Read<br>UCI: snmpd.access[x].read<br>Opt: read          | Specifies the view to be used for read access.  |        |         |      |         |      |         |     |                  |
| Web: Write<br>UCI: snmpd.access[x].write<br>Opt: write       | Specifies the view to be used for write access.   |        |         |      |         |      |         |     |                  |
| Web: Notify<br>UCI: snmpd.access[x].notify<br>Opt: notify    | Specifies the view to be used for notify access.  |        |         |      |         |      |         |     |                  |

Table 170: Information table for access settings

## 43.2.6 Trap receiver

Trap receiver settings define a notification receiver that should be sent SNMPv1 TRAPs and SNMPv2c TRAP2.

| Host            | Port | Version | Community |
|-----------------|------|---------|-----------|
| 192.168.100.254 |      | v1      | public    |

Buttons: Add, Delete

**Figure 238: The trap receiver settings page**

| Web Field/UCI/Package Option   | Description   |       |  |     |  |
|--|---|-------|--|-----|--|
| Web: Host<br>UCI: snmpd.trapreceiver[x].host<br>Opt: host                | Host address. Can be either an IP address or an FQDN.   |       |  |     |  |
| Web: Port<br>UCI: snmpd.trapreceiver[x].port<br>Opt: port                | UDP port to be used for sending traps.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> <tr> <td>162</td> <td></td> </tr> </table> | Range |  | 162 |  |
| Range  |   |       |  |     |  |
| 162  |   |       |  |     |  |
| Web: Version<br>UCI: snmpd.trapreceiver[x].version<br>Opt: version       | SNMP version.<br><table border="1"> <tr> <td>v1</td> <td></td> </tr> <tr> <td>V2</td> <td></td> </tr> </table>                              | v1    |  | V2  |  |
| v1   |   |       |  |     |  |
| V2   |   |       |  |     |  |
| Web: Community<br>UCI: snmpd.trapreceiver[x].community<br>Opt: community | Community to use in trap messages for this host.  |       |  |     |  |

**Table 171: Information table for trap receiver settings**

## 43.2.7 Inform receiver

Inform receiver settings define a notification receiver that should be sent SNMPv2c INFORM notifications.

| Host                                 | Port | Community |
|--------------------------------------|------|-----------|
| This section contains no values yet. |      |           |

**Figure 239: The inform receiver settings page**

| Web Field/UCI/Package Option   | Description   |       |  |     |  |
|--|---|-------|--|-----|--|
| Web: Host<br>UCI: snmpd.informreceiver[x].host<br>Opt: host                | Host address. Can be either an IP address or an FQDN.   |       |  |     |  |
| Web: Port<br>UCI: snmpd.informreceiver[x].port<br>Opt: port                | UDP port to be used for sending traps.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> <tr> <td>162</td> <td></td> </tr> </table> | Range |  | 162 |  |
| Range  |   |       |  |     |  |
| 162  |   |       |  |     |  |
| Web: Community<br>UCI: snmpd.informreceiver[x].community<br>Opt: community | Community to use in inform messages for this host.  |       |  |     |  |

Table 172: Information table for trap receiver settings

### 43.2.8 USM user

Configure a user for for SNMPv3 USM (User Based Security Model).

Figure 240: The USM user settings page

| Web Field/UCI/Package Option  | Description   |     |  |     |  |
|---|---|-----|--|-----|--|
| Web: Username<br>UCI: snmpd.@usm_user[0].name<br>Opt: name                        | Defines a USM username.   |     |  |     |  |
| Web: Auth Protocol<br>UCI: snmpd.@usm_user[0].auth_protocol<br>Opt: auth_protocol | Defines the authentication protocol to use.<br><b>Note:</b> if omitted the user will be defined as <code>noauth</code> user.<br><table border="1"> <tr> <td>MD5</td> <td></td> </tr> <tr> <td>SHA</td> <td></td> </tr> </table> | MD5 |  | SHA |  |
| MD5   |   |     |  |     |  |
| SHA   |   |     |  |     |  |
| Web: Auth Password<br>UCI: snmpd.@usm_user[0].auth_password<br>Opt: auth_password | Defines the authentication password.<br><b>Note:</b> password must be at least 8 characters long.   |     |  |     |  |
| Web: Priv Protocol<br>UCI: snmpd.@usm_user[0].priv_protocol<br>Opt: priv_protocol | Defines the privacy protocol to use.<br><b>Note:</b> if omitted the user will be defined as <code>authNoPriv</code> user.<br><table border="1"> <tr> <td>MD5</td> <td></td> </tr> <tr> <td>SHA</td> <td></td> </tr> </table>    | MD5 |  | SHA |  |
| MD5   |   |     |  |     |  |
| SHA   |   |     |  |     |  |
| Web: Priv Password<br>UCI: snmpd.@usm_user[0].priv_password<br>Opt: priv_password | Defines the privacy password.<br><b>Note:</b> the password must be at least 8 characters long.  |     |  |     |  |
| Web: OID<br>UCI: snmpd.@usm_user[0].oid<br>Opt: oid                               | Defines the OID branch to restrict this user to. Similar to view restrictions in v1 and v2c   |     |  |     |  |

Table 173: Information table for USM user settings

## 43.3 Configuring SNMP using command line

SNMP is configured under the `snmpd` package. The configuration files are stored on `/etc/config/snmpd`.

### 43.3.1 System settings using UCI

```
root@VA_router:~# uci show snmpd
snmpd.system=system
snmpd.system.sysLocation=Office 123
snmpd.system.sysContact=Mr White
snmpd.system.sysName=Backup Access 4
snmpd.agent=agent
snmpd.agent.agentaddress=UDP:161
snmpd.agent.authtrapenabled=yes
snmpd.agent.link_updown_notify=yes
```

### 43.3.2 System settings using package options

```
root@VA_router:~# uci export snmpd
package snmpd
config 'system'
    option sysLocation 'Office 123'
    option sysContact 'Mr White'
    option sysName 'Backup Access 4'

config 'agent'
    option agentaddress 'UDP:161'
    option authtrapenabled '1'
    option link_updown_notify '1'
```

Another sample agent configuration shown below causes the agent to listen on UDP port 161, TCP port 161 and UDP port 9161 on only the interface associated with the localhost address.

```
config 'agent'
    option agentaddress 'UDP:161,tcp:161,localhost:9161'
```

### 43.3.3 com2sec settings

The following sample specifies that a request from any source using "public" as the community string will be dealt with using the security name "ro". However, any request

from the localhost itself using "private" as the community string will be dealt with using the security name "rw".

**Note:** the security names of "ro" and "rw" here are simply names – the fact of a security name having read only or read-write permissions is handled in the access section and dealt with at a group granularity.

#### 43.3.3.1 Com2sec using UCI

```
snmpd.c2s_1=com2sec
snmpd.c2s_1.source=default
snmpd.c2s_1.community=public
snmpd.c2s_1.secname=rw
snmpd.c2s_2=com2sec
snmpd.c2s_2.source=localhost
snmpd.c2s_2.community=private
snmpd.c2s_2.secname=ro
```

#### 43.3.3.2 Com2sec using package options

```
config 'com2sec' 'public'
    option secname 'ro'
    option source 'default'
    option community 'public'

config 'com2sec' 'private'
    option secname 'rw'
    option source 'localhost'
    option community 'private'
```

### 43.3.4 Group settings

The following example specifies that a request from the security name "ro" using snmp v1, v2c or USM (User Based Security Model for SNMPv3) are all mapped to the "public" group. Similarly, requests from the security name "rw" in all protocols are mapped to the "private" group.

#### 43.3.4.1 Group settings using UCI

```
snmpd.grp_1_v1=group
snmpd.grp_1_v1.version=v1
snmpd.grp_1_v1.group=public
snmpd.grp_1_v1.secname=ro
snmpd.grp_1_v2c=group
snmpd.grp_1_v2c.version=v2c
```

```
snmpd.grp_1_v2c.group=public
snmpd.grp_1_v2c.secname=ro
snmpd.grp_1_usm=group
snmpd.grp_1_usm.version=usm
snmpd.grp_1_usm.group=public
snmpd.grp_1_usm.secname=ro
snmpd.grp_1_access=access
snmpd.grp_1_access.context=none
snmpd.grp_1_access.version=any
snmpd.grp_1_access.level=noauth
snmpd.grp_1_access.prefix=exact
snmpd.grp_1_access.read=all
snmpd.grp_1_access.write=none
snmpd.grp_1_access.notify=none
snmpd.grp_1_access.group=public
snmpd.grp_2_v1=group
snmpd.grp_2_v1.version=v1
snmpd.grp_2_v1.group=public
snmpd.grp_2_v1.secname=ro
snmpd.grp_2_v2c=group
snmpd.grp_2_v2c.version=v2c
snmpd.grp_2_v2c.group=public
snmpd.grp_2_v2c.secname=ro
snmpd.grp_2_usm=group
snmpd.grp_2_usm.version=usm
snmpd.grp_2_usm.group=public
snmpd.grp_2_usm.secname=ro
snmpd.grp_2_access=access
snmpd.grp_2_access.context=none
snmpd.grp_2_access.version=any
snmpd.grp_2_access.level=noauth
snmpd.grp_2_access.prefix=exact
snmpd.grp_2_access.read=all
snmpd.grp_2_access.write=all
snmpd.grp_2_access.notify=all
snmpd.grp_2_access.group=public
```

### 43.3.4.2 Group settings using package options

```
config 'group' 'public_v1'
    option group 'public'
    option version 'v1'
    option secname 'ro'

config 'group' 'public_v2c'
    option group 'public'
    option version 'v2c'
    option secname 'ro'

config 'group' 'public_usm'
    option group 'public'
    option version 'usm'
    option secname 'ro'

config 'group' 'private_v1'
    option group 'private'
    option version 'v1'
    option secname 'rw'

config 'group' 'private_v2c'
    option group 'private'

    option version 'v2c'
    option secname 'rw'

config 'group' 'private_usm'
    option group 'private'
    option version 'usm'
    option secname 'rw'
```

### 43.3.5 View settings using UCI

The following example defines two views, one for the entire system and another for only mib2.

```
snmpd.all=view
snmpd.all.viewname=all
snmpd.all.oid=.1
```

```
snmpd.mib2=view
snmpd.mib2.viewname=mib2
snmpd.mib2.type=included
snmpd.mib2.oid=.iso.org.dod.Internet.mgmt.mib-2
```

### 43.3.5.1 View settings using package options

```
config 'view' 'all'
    option viewname 'all'
    option type 'included'
    option oid '.1'

config 'view' 'mib2'
    option viewname 'mib2'
    option type 'included'
    option oid '.iso.org.dod.Internet.mgmt.mib-2'
```

## 43.3.6 Access settings

The following example shows the “public” group being granted read access on the “all” view and the “private” group being granted read and write access on the “all” view. Although it is possible to write some settings using SNMP write permission, it is not recommended as any changes to the configuration made through an `snmpset` command may conflict with the UCI configuration. In this instance the changes will be overwritten by other processes and will not persist after a reboot.

### 43.3.6.1 Access using package options

```
config 'access' 'public_access'
    option group 'public'
    option context 'none'
    option version 'any'
    option level 'noauth'
    option prefix 'exact'
    option read 'all'
    option write 'none'
    option notify 'none'

config 'access' 'private_access'
    option group 'private'
    option context 'none'
    option version 'any'
```



```
option level 'noauth'
option prefix 'exact'
option read 'all'
option write 'all'
option notify 'all'
```

### 43.3.7 SNMP traps settings

By default, all SNMP trap instances are named `trapreceiver`, it is identified by `@trapreceiver` then the trap receiver position in the package as a number. For example, for the first trap receiver in the package using UCI:

```
snmpd.@trapreceiver[0]=trapreceiver
snmpd.@trapreceiver[0].host=1.1.1.1:161
```

Or using package options:

```
config trapreceiver
    option host '1.1.1.1:161'
```

However, to better identify it, it is recommended to give the trap receiver instance a name. For example, to create a trap receiver instance named `TrapRecv1`.

To define a named trap receiver instance using UCI, enter:

```
snmpd.TrapRecv1=TrapRecv1
snmpd.TrapRecv1.host=1.1.1.1:161
```

To define a named trap receiver instance using package options, enter:

```
config trapreceiver TrapRecv1
    option host '1.1.1.1:161'
```

#### 43.3.7.1 SNMP trap using UCI

```
snmpd.@trapreceiver[0]=trapreceiver
snmpd.@trapreceiver[0].host=1.1.1.1:161
snmpd.@trapreceiver[0].version=v1
snmpd.@trapreceiver[0].community=public
```

#### 43.3.7.2 SNMP trap using package options

```
# for SNMPv1 or v2c trap receivers
config trapreceiver
    option host 'IPADDR[:PORT]'
```

```
option version 'v1|v2c'
option community 'COMMUNITY STRING'
```

### 43.3.8 SNMP inform receiver settings

By default, all SNMP inform receiver instances are named 'informreceiver', it is identified by @informreceiver then the inform receiver position in the package as a number. For example, for the first inform receiver in the package using UCI:

```
snmpd.@informreceiver [0]=informreceiver
snmpd.@informreceiver [0].host=1.1.1.1
```

Or using package options:

```
config informreceiver
    option host '1.1.1.1'
```

However, to better identify it, it is recommended to give the inform receiver instance a name. For example, to create a inform receiver instance named InformRecv1.

To define a named trap receiver instance using UCI, enter:

```
snmpd.InformRecv1=InformRecv1
snmpd.InformRecv1.host=1.1.1.1
```

To define a named trap receiver instance using package options, enter:

```
config informreceiver InformRecv1
    option host '1.1.1.1'
```

#### 43.3.8.1 SNMP inform receiver using UCI

```
snmpd.@informreceiver[0]=informreceiver
snmpd.@informreceiver[0].host=1.1.1.1
snmpd.@informreceiver[0].port=67
snmpd.@informreceiver[0].community=private
```

#### 43.3.8.2 SNMP inform receiver using package options

```
config informreceiver
    option host '1.1.1.1'
    option port '67'
    option community 'private'
```

### 43.3.9 SNMP USM user settings

By default, all USM User instances are named 'usm\_user', it is identified by @usm\_user then the USM user position in the package as a number. For example, for the first USM User in the package using UCI:

```
snmpd.@usm_user[0]=usm_user
snmpd.@usm_user[0].name=username
```

Or using package options:

```
config usm_user
    option name 'username'
```

However, to better identify it, it is recommended to give the usm\_user instance a name. For example, to create a usm\_user instance named User1.

To define a named usm\_user instance using UCI, enter:

```
snmpd.User1=User1
snmpd.User1.name=username
```

To define a named usm\_user instance using package options, enter:

```
config usm_user 'User1'
    option name 'username'
```

#### 43.3.9.1 SNMP USM user using UCI

```
snmpd.@usm_user[0]=usm_user
snmpd.@usm_user[0].name=username
snmpd.@usm_user[0].auth_protocol=SHA
snmpd.@usm_user[0].auth_password=password
snmpd.@usm_user[0].priv_protocol=AES
snmpd.@usm_user[0].priv_password=password
snmpd.@usm_user[0].oid=1.2.3.4
```

#### 43.3.9.2 SNMP USM user using package options

```
config usm_user
    option name 'username'
    option auth_protocol 'SHA'
    option auth_password 'password'
    option priv_protocol 'AES'
    option priv_password 'aespassword'
    option oid '1.2.3.4'
```

## 43.4 Configuring SNMP interface alias with static SNMP index

A Linux interface index changes dynamically. This is not ideal for SNMP managers that require static interface indexes to be defined.

The network package interface section allows defining a static SNMP interface alias index for this interface.

An alias entry is created in the SNMP ifEntry table at index (snmp\_alias\_ifindex + 1000). This entry is a shadow of the real underlying Linux interface corresponding to the UCI definition. You may use any numbering scheme you wish; the alias values do not need to be consecutive.

### 43.4.1 Configuration package used

| Package | Sections  |
|---------|-----------|
| network | interface |

### 43.4.2 Configuring SNMP interface alias

To enter and SNMP alias for an interface, select **Network -> Interfaces -> Edit-> Common Configuration -> Advanced Settings**.

Enter a small index value for **SNMP Alias ifindex** that is unique to this interface. To retrieve SNMP statistics for this interface, configure the SNMP manager to poll (snmp\_alias\_ifindex + 1000). For example, if an interface is configured with an snmp\_alias\_ifindex of 11, then the SNMP manager should poll ifIndex=1011. The ifIndex will remain fixed regardless of how many times the underlying interface is added or removed.

If the Linux interface associated with the UCI entry is active when the alias index is polled, the normal ifEntry information for that interface is reported. Otherwise, a dummy entry is created with the same ifDescr, and its ifOper field set to **DOWN**.

**Note:** if you are using SIM roaming, where mobile interfaces are created dynamically, you need to specify a fixed snmp\_alias\_ifindex value and a fixed ifName value in the roaming template. All roaming entries will then map to the same Linux interface name and underlying device.

SNMP Alias ifindex  Alias ifindex SNMP agent. Alias indexes are present at 1000 offset. So setting 1 here will create snmp ifTable entry 1001.  
Useful when interface creates new linux interface on every startup (e.g. ppp interface). With this set the interface could be monitored via constant snmp agent interface table entry

**Figure 241: The interface SNMP alias ifindex field advanced settings page**

| UCI/Package Option   | Description  |       |                               |       |                |
|--|--|-------|-------------------------------|-------|----------------|
| Web: SNMP Alias ifindex<br>UCI:<br>network.@interface[X].snmp_alias_ifindex<br>Opt: snmp_alias_ifindex | Defines a static SNMP interface alias index for this interface that can be polled using via the SNMP interface index.<br>snmp alias ifindex+1000<br><table border="1"> <tr> <td>Blank</td> <td>No SNMP interface alias index</td> </tr> <tr> <td>Range</td> <td>0 - 4294966295</td> </tr> </table>   | Blank | No SNMP interface alias index | Range | 0 - 4294966295 |
| Blank  | No SNMP interface alias index  |       |                               |       |                |
| Range  | 0 - 4294966295   |       |                               |       |                |
| Web: n/a<br>UCI:<br>network.@interface[X].snmp_alias_ifdescr<br>Opt: snmp_alias_ifdescr                | Defines an alias name to be reported for the UCI name in the enterprise MIB for UCI interfaces, and in alias entries in the ifIndex table. If present, this option supercedes the default ifDescr value (usually the UCI interface name, or configured ifName).<br><table border="1"> <tr> <td>Blank</td> <td>No SNMP interface alias name</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table> | Blank | No SNMP interface alias name  | Range |                |
| Blank  | No SNMP interface alias name   |       |                               |       |                |
| Range  |  |       |                               |       |                |

Table 174: Information table for static SNMP alias interface

### 43.4.3 Configuring SNMP interface alias using the command line

SNMP interface alias is configured under the network package **/etc/config/network**

The following examples use an interface section named MOBILE.

#### 43.4.3.1 SNMP interface alias using UCI

```
root@VA_router:~# uci show network
network.MOBILE=interface
.....
network.MOBILE.snmp_alias_ifindex=11
network.MOBILE.snmp_alias_ifdescr=primary_mobile
.....
```

#### 43.4.3.2 SNMP interface alias using package options

```
root@VA_router:~# uci show network
config interface 'MOBILE'
.....
    option snmp_alias_ifindex '11'
    option snmp_alias_ifdescr 'primary_mobile'
.....
```

### 43.4.4 SNMP interface alias MIBS

| OID Name              | OID  |
|-----------------------|--|
| interface alias table | .1.3.6.1.2.1.2.2.1.1.                          |
| snmp_alias_ifindex    | .1.3.6.1.2.1.2.2.1.1.<snmp_alias_ifindex+1000> |
| snmp_alias_ifdescr    | 1.3.6.1.4.1.2078.3.2.66.1.1.<index>.{5,6}      |

## 43.5 Automatic SNMP traps

### 43.5.1 Last gasp

The router will automatically generate an SNMP trap when power loss is detected, and attempt to deliver to the configured trap receiver – ORK firmware family only.

Note: whether the hardware is able to deliver the last gasp trap depends on the hold up time on the particular hardware model and the network conditions.

| Event    | SNMP Trap format   |
|----------|--|
| Shutdown | { SNMPv1 { Trap(28) E:8072.4 192.168.100.1 enterpriseSpecific s=2 8382 } |

Table 175: Example format of last gasp trap

### 43.5.2 Cold start

On completion of system start up, the router will generate a cold start SNMP trap and deliver to the configured trap receiver.

| Event   | SNMP Trap format  |
|---------|---|
| Startup | { SNMPv1 { Trap(29) E:8072.3.2.10 192.168.100.1 coldStart 9 } } |

Table 176: Example format of cold start trap

## 43.6 SNMP diagnostics

### 43.6.1 SNMP process

To check the SNMP process is running correctly, enter:

```
root@VA_router:~# pgrep -fl snmpd
6970 /usr/sbin/snmpd -Lsd0-6 -p /var/run/snmpd.pid -m -c
/var/conf/snmpd.conf
```

### 43.6.2 SNMP port

To check that SNMP service is listening on the configured port, enter:

```
root@VA_router:~# netstat -pantu | grep snmp
udp    0 0 0.0.0.0:161  0.0.0.0:*          6970/snmpd
```

### 43.6.3 Retrieving SNMP values

SNMP values can be queried by an `snmpwalk` or `snmpget` command either locally or remotely.

#### 43.6.3.1 snmpwalk

To create an `snmpwalk` locally, enter `snmpwalk`. An example `snmpwalk` is shown below:

```
root@VA_router:~# snmpwalk -c public -v 1 localhost .1.3.6.1.2.1.1
```

```

iso.3.6.1.2.1.1.1.0 = STRING: "Virtual Access GWXXXX, SN# 00E0C812D1A0,
EDG-21.00.07.008"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.2078
iso.3.6.1.2.1.1.3.0 = Timeticks: (71816) 0:11:58.16
iso.3.6.1.2.1.1.4.0 = STRING: "info@virtualaccess.com"
iso.3.6.1.2.1.1.5.0 = STRING: "GWXXXX"
iso.3.6.1.2.1.1.6.0 = STRING: "UK"
iso.3.6.1.2.1.1.7.0 = INTEGER: 79
iso.3.6.1.2.1.1.8.0 = Timeticks: (60) 0:00:00.60
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.2.1.10.131
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (35) 0:00:00.35
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (38) 0:00:00.38
iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (38) 0:00:00.38
iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (38) 0:00:00.38
iso.3.6.1.2.1.1.9.1.4.8 = Timeticks: (38) 0:00:00.38
iso.3.6.1.2.1.1.9.1.4.9 = Timeticks: (60) 0:00:00.60
.....

```

### 43.6.3.2 snmpget

To create an `snmpget` command locally, enter:

```

root@VA_router:~# snmpget -c public -v 1 localhost .1.3.6.1.4.1.2078.3.14.2
iso.3.6.1.4.1.2078.3.14.2 = STRING: "EDG-21.00.07.008"

```

### 43.6.4 SNMP status

To see an overview including tx/rx packets and uptime of the SNMP process, enter:

```
root@VA_router:~# snmpstatus -c public -v 2c localhost
[UDP: [0.0.0.0]->[127.0.0.1]:161]=>[Virtual Access GWXXXX, SN#
00E0C812D1A0, EDG-21.00.07.008] Up: 0:17:05.87
Interfaces: 21, Recv/Trans packets: 47632/9130 | IP: 15045/8256
15 interfaces are down!
```



## 44 Event system

Virtual Access routers feature an event system. It allows you to forward Virtual Access specific router events to predefined targets for efficient control and management of devices.

This chapter explains how the event system works and how to configure it using UCI commands.

### 44.1 Configuration package used

| Package   | Section     |
|-----------|-------------|
| va_eventd | main        |
|           | forwarding  |
|           | target      |
|           | conn_tester |

### 44.2 Event system overview

#### 44.2.1 Implementation of the event system

The event system is implemented by the **va\_eventd** application.

The va\_eventd application defines three types of object:

|                    |  |
|--------------------|--|
| Forwardings        | Rules that define what kind of events should be generated. For example, you might want an event to be created when an IPSec tunnel comes up or down. |
| Targets            | Define the targets to send the event to. The event may be sent to a target via a syslog message, a snmp trap or email.                               |
| Connection testers | Define methods to test the target is reachable. IP connectivity to a server and link state may be checked prior to sending events.                   |

For example, if you want to configure an SNMP trap to be sent when an IPSec tunnel comes up, you will need to:

- Define a forwarding rule for IPSec tunnel up events.
- Set an SNMP manager as the target.
- Optionally use a connection tester to ensure the SNMP manager is reachable.

#### 44.2.2 Supported events

Events have a class, ID, name and a severity. These properties are used to fine tune which events to report.

**Note:** only VA events can be forwarded using the event system. A comprehensive table of events is available from the CLI by entering **'vae\_cli -d'**.

### 44.2.3 Supported targets

The table below describes the targets currently supported.

| Target | Description                         |
|--------|-------------------------------------|
| Syslog | Event sent to syslog server.        |
| Email  | Event sent via email.               |
| SNMP   | Event sent via SNMP trap.           |
| Exec   | Command executed when event occurs. |
| SMS    | Event sent via SMS.                 |
| File   | Events written to a file            |

**Table 177: Targets currently supported**

The attributes of a target vary significantly depending on its type.

### 44.2.4 Supported connection testers

The table below describes the methods to test a connection that are currently supported.

| Type | Description  |
|------|--|
| link | Checks if the interface used to reach the target is up.  |
| ping | Pings the target. And then assumes there is connectivity during a configurable amount of time. |

**Table 178: Event system - supported connection tester methods**

## 44.3 Configuring the event system using the web interface

To configure the event system, select **Services -> VA Event System**. The VA Event System page appears.

There are four sections in the VA Event System page.

| Section            | Description                                      |
|--------------------|--|
| Basic Settings     | Configures basic global event system parameters. |
| Connection Tester  | Configures the connection testers.               |
| Events Destination | Configures the event targets.                    |
| Event Filters      | Configures the forwarding rules.                 |

### 44.3.1 Basic settings

The screenshot shows the 'VA Event System' configuration page. Under the 'Basic Settings' section, there are three main settings:

- Enabled:** A checkbox that is checked.
- Queue File:** A text input field containing '/tmp/event\_buffer'. A tooltip explains: 'File to temporarily queue events if they could not be sent immediately. Use '/tmp' if persistence not required and '/root' if persistence is required'.
- Maximum Queue File Size:** A dropdown menu set to '128K'. A tooltip explains: 'Queue file will not grow larger than this size. If size is reached older events would be discarded'.

**Figure 242: The VA event system basic settings configuration page**

| Web Field/UCI/Package Option  | Description   |                   |                |       |          |
|---|---|-------------------|----------------|-------|----------|
| Web: Enabled<br>UCI: va_eventd.main.enabled<br>Opt: enabled                   | Enables VA Event System.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0                 | Disabled.      | 1     | Enabled. |
| 0   | Disabled.   |                   |                |       |          |
| 1   | Enabled.  |                   |                |       |          |
| Web: Enabled<br>UCI: va_eventd.main.event_queue_file<br>Opt: event_queue_file | Defines the file to temporarily queue events when they cannot be sent immediately.<br><b>Note:</b> Use /tmp path if persistence is not required and /root if persistence is required.<br><table border="1"> <tr> <td>/tmp/event_buffer</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table> | /tmp/event_buffer | Disabled.      | 1     | Enabled. |
| /tmp/event_buffer   | Disabled.   |                   |                |       |          |
| 1   | Enabled.  |                   |                |       |          |
| Web: Enabled<br>UCI: va_eventd.main.event_queue_size<br>Opt: event_queue_size | Defines the file size for the temporary queue. Older events are discarded once file size is reached.<br><table border="1"> <tr> <td>128K</td> <td>128 Kilobytes.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 128K              | 128 Kilobytes. | Range |          |
| 128K  | 128 Kilobytes.  |                   |                |       |          |
| Range   |   |                   |                |       |          |

Table 179: Information table for event system basic settings

### 44.3.2 Connection tester

A connection tester is used to verify the event destination before forwarding the event. Connection testers configure the uci `conn_tester` section rules. Multiple connection testers can be configured. There are two types of connection tester:

| Type        | Description  |
|-------------|--|
| <b>link</b> | Checks if the interface used to reach the target is up.  |
| <b>ping</b> | Pings the target. And then assumes there is connectivity during a configurable amount of time. |

Connection Tester Delete

Enabled

Connection Tester Name:

Type:

Ping Target:

Ping Source:

Ping Success Duration:  Every successful ping will allow uninterrupted event stream for the specified number of seconds

Figure 243: The VA event system connection tester configuration page

| Web Field/UCI/Package Option  | Description   |           |             |     |          |                          |      |      |   |      |
|---|---|-----------|-------------|-----|----------|--------------------------|------|------|---|------|
| Web: Enabled<br>UCI: va_eventd.@conn_tester[0].enabled<br>Opt: enabled          | Enables a connection tester.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0         | Disabled.   | 1   | Enabled. |                          |      |      |   |      |
| 0   | Disabled.   |           |             |     |          |                          |      |      |   |      |
| 1   | Enabled.  |           |             |     |          |                          |      |      |   |      |
| Web: Connection Tester Name<br>UCI: va_eventd.@conn_tester[0].name<br>Opt: name | Defines the connection tester name.<br>This is used when configuring a connection tester for an event destination.  |           |             |     |          |                          |      |      |   |      |
| Web: Type<br>UCI: va_eventd.@conn_tester[0].type<br>Opt: type                   | Defines the connection tester type.<br><table border="1"> <thead> <tr> <th>Web Value</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Ping</td> <td>Verifies target by ping.</td> <td>ping</td> </tr> <tr> <td>Link</td> <td>Verifies target by checking routed interface is up.</td> <td>link</td> </tr> </tbody> </table> | Web Value | Description | UCI | Ping     | Verifies target by ping. | ping | Link | Verifies target by checking routed interface is up. | link |
| Web Value   | Description   | UCI       |             |     |          |                          |      |      |   |      |
| Ping  | Verifies target by ping.  | ping      |             |     |          |                          |      |      |   |      |
| Link  | Verifies target by checking routed interface is up.   | link      |             |     |          |                          |      |      |   |      |

|   |   |      |                              |       |  |
|---|---|------|------------------------------|-------|--|
| Web: Ping Target<br>UCI:<br>va_eventd.@conn_tester[0].ping_dest_addr<br>Opt: ping_dest_addr                                 | Defines the IP address for the target ping.<br><b>Note:</b> only displayed if connection tester type is set to 'Ping'. <table border="1"> <tr><td> </td><td> </td></tr> <tr><td>Range</td><td> </td></tr> </table>  |      |                              | Range |  |
|   |   |      |                              |       |  |
| Range   |   |      |                              |       |  |
| Web: Ping Source<br>UCI:<br>va_eventd.@conn_tester[0].ping_source<br>Opt: ping_source                                       | Defines an interface or IP address to source the pings from.<br><b>Note:</b> only displayed if connection tester type is set to 'Ping'. <table border="1"> <tr><td>eth0</td><td>Use eth0 IP for ping source.</td></tr> <tr><td>Range</td><td> </td></tr> </table>                           | eth0 | Use eth0 IP for ping source. | Range |  |
| eth0  | Use eth0 IP for ping source.  |      |                              |       |  |
| Range   |   |      |                              |       |  |
| Web: Ping Success Duration<br>UCI:<br>va_eventd.@conn_tester[0].ping_success_duration_sec<br>Opt: ping_success_duration_sec | Defines the duration, in seconds, for which a successful ping defines a connection tester as up.<br><b>Note:</b> only displayed if connection tester type is set to 'Ping'. <table border="1"> <tr><td>60</td><td> </td></tr> <tr><td>Range</td><td> </td></tr> </table>                    | 60   |                              | Range |  |
| 60  |   |      |                              |       |  |
| Range   |   |      |                              |       |  |
| Web: Link Interface<br>UCI:<br>va_eventd.@conn_tester[0].link_iface<br>Opt: link_iface                                      | Defines the interface to monitor when the connection tester type is set to 'link'. Configured interfaces are listed.<br><b>Note:</b> only displayed if connection tester type is set to 'Link'. <table border="1"> <tr><td> </td><td> </td></tr> <tr><td>Range</td><td> </td></tr> </table> |      |                              | Range |  |
|   |   |      |                              |       |  |
| Range   |   |      |                              |       |  |

**Table 180: Information table for event system connection tester settings**

### 44.3.3 Event destination

An event destination is the target for the event. Event destinations configure the uci `target` section rules. Multiple event destinations can be configured. There are currently six configurable event destinations.

| Target Type | Description                         |
|-------------|-------------------------------------|
| Syslog      | Event sent to syslog server.        |
| Email       | Event sent via email.               |
| SNMP        | Event sent via SNMP trap.           |
| Execute     | Command executed when event occurs. |
| SMS         | Event sent via SMS.                 |
| File        | Event written to a file             |

The available configuration options differ depending on the event destination type.

#### 44.3.3.1 Syslog target

When a syslog target receives an event, it sends it to the configured syslog server.

**Figure 244: The VA event system syslog event destination configuration page**

| Web Field/UCI/Package Option   | Description  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
|--|--|-----------|---|-------|----------|--|--------|-----------|--|----------|-------|--|-------|---------|--|------|-----|--|-----|------|-------------|------|
| Web: Enabled<br>UCI: va_eventd.@target[0].enabled<br>Opt: enabled                        | Enables an event destination. This is used in the event filters section.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0         | Disabled.                                     | 1     | Enabled. |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| 0  | Disabled.  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| 1  | Enabled.   |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| Web: Destination name<br>UCI: va_eventd.@target[0].name<br>Opt: name                     | Defines a name for the event destination.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> </table>   | Range     |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| Range  |  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| Web: Type<br>UCI: va_eventd.@target[0].type<br>Opt: type                                 | Defines the event destination type. For syslog server choose <b>Syslog</b> .<br><table border="1"> <thead> <tr> <th>Web Value</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Syslog</td> <td></td> <td>syslog</td> </tr> <tr> <td>SNMP Trap</td> <td></td> <td>snmptrap</td> </tr> <tr> <td>Email</td> <td></td> <td>email</td> </tr> <tr> <td>Execute</td> <td></td> <td>exec</td> </tr> <tr> <td>SMS</td> <td></td> <td>sms</td> </tr> <tr> <td>File</td> <td>File target</td> <td>file</td> </tr> </tbody> </table> | Web Value | Description                                   | UCI   | Syslog   |  | syslog | SNMP Trap |  | snmptrap | Email |  | email | Execute |  | exec | SMS |  | sms | File | File target | file |
| Web Value  | Description  | UCI       |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| Syslog   |  | syslog    |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| SNMP Trap  |  | snmptrap  |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| Email  |  | email     |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| Execute  |  | exec      |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| SMS  |  | sms       |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| File   | File target  | file      |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| Web: Connection Tester Name<br>UCI: va_eventd.@target[0].conn_tester<br>Opt: conn_tester | Defines the connection tester (if any) to use to verify the syslog target.<br><table border="1"> <tr> <td>None</td> <td>No connection tester. UCI option not present.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | None      | No connection tester. UCI option not present. | Range |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| None   | No connection tester. UCI option not present.  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| Range  |  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| Web: Destination Address<br>UCI: va_eventd.@target[0].target_addr<br>Opt: target_addr    | Defines the syslog target IP/FQDN and port.<br><table border="1"> <tr> <td>Range</td> <td>a.b.c.d:port or fqdn:port</td> </tr> </table>  | Range     | a.b.c.d:port or fqdn:port                     |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| Range  | a.b.c.d:port or fqdn:port  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| Web: Syslog Over TCP<br>UCI: va_eventd.@target[0].tcp_syslog<br>Opt: tcp_syslog          | Defines whether to use TCP for delivery of the syslog event.<br><table border="1"> <tr> <td>0</td> <td>Use UDP</td> </tr> <tr> <td>1</td> <td>Use TCP</td> </tr> </table>  | 0         | Use UDP                                       | 1     | Use TCP  |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| 0  | Use UDP  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| 1  | Use TCP  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| Web: Message Template<br>UCI: va_eventd.@target[0].template<br>Opt: template             | Defines the message template to use for the event. In general, this should be left empty.<br>See the section on message templates below.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> </table>  | Range     |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| Range  |  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| Web: n/a<br>UCI: va_eventd.@target[0].facility<br>Opt: facility                          | Defines a custom facility to overwrite existing facility on syslog messages before delivery to syslog target.<br><table border="1"> <tr> <td>Range</td> <td>Does not overwrite existing facility.</td> </tr> </table>  | Range     | Does not overwrite existing facility.         |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| Range  | Does not overwrite existing facility.  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| Web: n/a<br>UCI: va_eventd.@target[0].severity<br>Opt: severity                          | Defines a custom severity to overwrite existing severity on syslog messages before delivery to syslog target.<br><table border="1"> <tr> <td>Range</td> <td>Does not overwrite existing severity.</td> </tr> </table>  | Range     | Does not overwrite existing severity.         |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |
| Range  | Does not overwrite existing severity.  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |             |      |

**Table 181: Information table for event system syslog event destination settings**

### 44.3.3.2 Email target

When an email target receives an event, it sends it to the configured email address.

[Delete](#)

Event Destination

Enabled

Destination Name

Type

Connection Tester Name

From

To

Subject Template  Template for email subject

Body Template  Template for email body. Safe to leave blank

SMTP Server Address

SMTP User Name

SMTP Password

Use TLS

Send Timeout

**Figure 245: The VA event system email event destination configuration page**

| Web Field/UCI/Package Option   | Description   |           |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
|--|---|-----------|---|-------|----------|---------------|--------|-----------|-------------|----------|-------|--------------|-------|---------|----------------|------|-----|------------|-----|------|-------------|------|
| Web: Enabled<br>UCI: va_eventd.@target[0].enabled<br>Opt: enabled                        | Enables an event destination.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0         | Disabled.                                     | 1     | Enabled. |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| 0  | Disabled.   |           |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| 1  | Enabled.  |           |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Web: Destination name<br>UCI: va_eventd.@target[0].name<br>Opt: name                     | Defines a name for the event destination.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> </table>  | Range     |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Range  |   |           |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Web: Type<br>UCI: va_eventd.@target[0].type<br>Opt: type                                 | Defines the event destination type. For an email server choose <b>Email</b> .<br><table border="1"> <thead> <tr> <th>Web Value</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Syslog</td> <td>Syslog target</td> <td>syslog</td> </tr> <tr> <td>SNMP Trap</td> <td>SNMP target</td> <td>snmptrap</td> </tr> <tr> <td>Email</td> <td>Email target</td> <td>email</td> </tr> <tr> <td>Execute</td> <td>Execute target</td> <td>exec</td> </tr> <tr> <td>SMS</td> <td>SMS target</td> <td>sms</td> </tr> <tr> <td>File</td> <td>File target</td> <td>file</td> </tr> </tbody> </table> | Web Value | Description                                   | UCI   | Syslog   | Syslog target | syslog | SNMP Trap | SNMP target | snmptrap | Email | Email target | email | Execute | Execute target | exec | SMS | SMS target | sms | File | File target | file |
| Web Value  | Description   | UCI       |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Syslog   | Syslog target   | syslog    |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| SNMP Trap  | SNMP target   | snmptrap  |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Email  | Email target  | email     |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Execute  | Execute target  | exec      |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| SMS  | SMS target  | sms       |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| File   | File target   | file      |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Web: Connection Tester Name<br>UCI: va_eventd.@target[0].conn_tester<br>Opt: conn_tester | Defines the connection tester (if any) to use to verify the email target.<br><table border="1"> <tr> <td>None</td> <td>No connection tester. UCI option not present.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | None      | No connection tester. UCI option not present. | Range |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| None   | No connection tester. UCI option not present.   |           |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Range  |   |           |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Web: From<br>UCI: va_eventd.@target[0].from<br>Opt: from                                 | Defines the 'from' address for the email.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> </table>  | Range     |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Range  |   |           |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Web: To<br>UCI: va_eventd.@target[0].to<br>Opt: to                                       | Defines the 'to' address for the email.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> </table>  | Range     |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Range  |   |           |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |

|   |  |    |  |       |                           |
|---|--|----|--|-------|---------------------------|
| Web: Subject Template<br>UCI:<br>va_eventd.@target[0].subject_template<br>Opt: subject_template | Defines subject template for the email. In general, this should be left empty. Example:<br>va_eventd.@target[0].subject_template="%{severityName} %{eventName}!!!"<br>See the section on message templates below. <table border="1"> <tr><td></td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>     |    |  | Range |                           |
|   |  |    |  |       |                           |
| Range   |  |    |  |       |                           |
| Web: Body Template<br>UCI:<br>va_eventd.@target[0].body_template<br>Opt: body_template          | Defines the email body template. In general, this should be left blank. Example:<br>va_eventd.@target[0].body_template="%{eventName} (%{class}.%{subclass}) happened!"<br>See the section on message templates below. <table border="1"> <tr><td></td><td></td></tr> <tr><td>Range</td><td></td></tr> </table> |    |  | Range |                           |
|   |  |    |  |       |                           |
| Range   |  |    |  |       |                           |
| Web: SMTP Server Address<br>UCI: va_eventd.@target[0].smtp_addr<br>Opt: smtp_addr               | Defines the email server address and port. <table border="1"> <tr><td></td><td></td></tr> <tr><td>Range</td><td>a.b.c.d:port or fqdn:port</td></tr> </table>   |    |  | Range | a.b.c.d:port or fqdn:port |
|   |  |    |  |       |                           |
| Range   | a.b.c.d:port or fqdn:port  |    |  |       |                           |
| Web: SMTP User Name<br>UCI: va_eventd.@target[0].smtp_user<br>Opt: smtp_user                    | Defines user name for SMTP authentication. <table border="1"> <tr><td></td><td></td></tr> <tr><td>Range</td><td>name@site.com</td></tr> </table>   |    |  | Range | name@site.com             |
|   |  |    |  |       |                           |
| Range   | name@site.com  |    |  |       |                           |
| Web: SMTP Password<br>UCI:<br>va_eventd.@target[0].smtp_password<br>Opt: smtp_password          | Defines the password for SMTP authentication. <table border="1"> <tr><td></td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>   |    |  | Range |                           |
|   |  |    |  |       |                           |
| Range   |  |    |  |       |                           |
| Web: Use TLS<br>UCI: va_eventd.@target[0].use_tls<br>Opt: use_tls                               | Enables TLS (Transport Layer Security) support. <table border="1"> <tr><td>0</td><td></td></tr> <tr><td>1</td><td></td></tr> </table>  | 0  |  | 1     |                           |
| 0   |  |    |  |       |                           |
| 1   |  |    |  |       |                           |
| Web: Send Timeout<br>UCI: va_eventd.@target[0].timeout_sec<br>Opt: timeout_sec                  | Defines the email send timeout in seconds. <table border="1"> <tr><td>10</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>  | 10 |  | Range |                           |
| 10  |  |    |  |       |                           |
| Range   |  |    |  |       |                           |
| Web: Use StartTLS<br>UCI: va_eventd.@target[0].tls_starttls<br>Opt: tls_starttls                | Enables StartTLS support for TLS.<br>(Only displayed when TLS is enabled) <table border="1"> <tr><td>0</td><td></td></tr> <tr><td>1</td><td></td></tr> </table>  | 0  |  | 1     |                           |
| 0   |  |    |  |       |                           |
| 1   |  |    |  |       |                           |
| Web: Force SSLv3<br>UCI: va_eventd.@target[0].tls_forcessl3<br>Opt: tls_forcessl3               | Enables force SSLv3 for TLS.<br>(Only displayed when TLS is enabled) <table border="1"> <tr><td>0</td><td></td></tr> <tr><td>1</td><td></td></tr> </table>   | 0  |  | 1     |                           |
| 0   |  |    |  |       |                           |
| 1   |  |    |  |       |                           |

**Table 182: Information table for event system email event destination settings**

### 44.3.3.3 SNMP target

When a SNMP target receives an event, it sends it in a trap to the configured SNMP manager.

**Event Destination** Delete

Enabled

Destination Name

Type

Connection Tester Name

Destination Address

Message Template  For Syslog and SNMP types message template has reasonable default so it is safe to leave blank

Agent Address

SNMP Protocol Version

Community

**Figure 246: The VA event system SNMP event destination configuration page**

| Web Field/UCI/Package Option  | Description  |           |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
|---|--|-----------|---|-------|-------------------------|---------------|--------|-----------|-------------|----------|-------|--------------|-------|---------|----------------|------|-----|------------|-----|------|-------------|------|
| Web: Enabled<br>UCI: va_eventd.@target[0].enabled<br>Opt: enabled                         | Enables an event destination.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0         | Disabled.                                     | 1     | Enabled.                |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| 0   | Disabled.  |           |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| 1   | Enabled.   |           |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Web: Destination name<br>UCI: va_eventd.@target[0].name<br>Opt: name                      | Defines a name for the event destination.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> </table>   | Range     |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Range   |  |           |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Web: Type<br>UCI: va_eventd.@target[0].type<br>Opt: type                                  | Defines the event destination type. For SNMP server, choose <b>SNMP Trap</b> .<br><table border="1"> <thead> <tr> <th>Web Value</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Syslog</td> <td>Syslog target</td> <td>syslog</td> </tr> <tr> <td>SNMP Trap</td> <td>SNMP target</td> <td>snmptrap</td> </tr> <tr> <td>Email</td> <td>Email target</td> <td>email</td> </tr> <tr> <td>Execute</td> <td>Execute target</td> <td>exec</td> </tr> <tr> <td>SMS</td> <td>SMS target</td> <td>sms</td> </tr> <tr> <td>File</td> <td>File target</td> <td>file</td> </tr> </tbody> </table> | Web Value | Description                                   | UCI   | Syslog                  | Syslog target | syslog | SNMP Trap | SNMP target | snmptrap | Email | Email target | email | Execute | Execute target | exec | SMS | SMS target | sms | File | File target | file |
| Web Value   | Description  | UCI       |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Syslog  | Syslog target  | syslog    |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| SNMP Trap   | SNMP target  | snmptrap  |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Email   | Email target   | email     |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Execute   | Execute target   | exec      |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| SMS   | SMS target   | sms       |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| File  | File target  | file      |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Web: Connection Tester Name<br>UCI: va_eventd.@target[0]. conn_tester<br>Opt: conn_tester | Defines the connection tester (if any) to use to verify the SNMP target.<br><table border="1"> <tr> <td>None</td> <td>No connection tester. UCI option not present.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | None      | No connection tester. UCI option not present. | Range |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| None  | No connection tester. UCI option not present.  |           |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Range   |  |           |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Web: Destination Address<br>UCI: va_eventd.@target[0]. target_addr<br>Opt: target_addr    | Defines the SNMP target IP/FQDN and port.<br><table border="1"> <tr> <td>Range</td> <td>a.b.c.d:port or fqdn:port</td> </tr> </table>  | Range     | a.b.c.d:port or fqdn:port                     |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Range   | a.b.c.d:port or fqdn:port  |           |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Web: Message Template<br>UCI: va_eventd.@target[0].template<br>Opt: template              | Defines the message template to use for the event. In general, this should be left empty. Example:<br><pre>va_eventd.@target[0].template="%{eventName} %{eventSpecificTemplate}"</pre> <p>See the section on message templates below.</p> <table border="1"> <tr> <td>Range</td> <td></td> </tr> </table>  | Range     |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Range   |  |           |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Web: Agent Address<br>UCI: va_eventd.@target[0]. agent_addr<br>Opt: agent_addr            | Defines the IP address to source the SNMP trap. (optional)<br><table border="1"> <tr> <td>localhost</td> <td>Local IP</td> </tr> <tr> <td>Range</td> <td>Localhost or IP address</td> </tr> </table>   | localhost | Local IP                                      | Range | Localhost or IP address |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| localhost   | Local IP   |           |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Range   | Localhost or IP address  |           |   |       |                         |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |



|   |   |   |        |       |         |     |        |
|---|---|---|--------|-------|---------|-----|--------|
| <p>Web: SNMP Protocol Version<br/>UCI: va_eventd.@target[0].snmp_version<br/>Opt: snmp_version</p>                | <p>Defines the SNMP version.</p> <table border="1"> <tr> <td>1</td> <td>SNMPv1</td> </tr> <tr> <td>2c</td> <td>SNMPv2c</td> </tr> <tr> <td>3</td> <td>SNMPv3</td> </tr> </table>  | 1 | SNMPv1 | 2c    | SNMPv2c | 3   | SNMPv3 |
| 1   | SNMPv1  |   |        |       |         |     |        |
| 2c  | SNMPv2c   |   |        |       |         |     |        |
| 3   | SNMPv3  |   |        |       |         |     |        |
| <p>Web: Community<br/>UCI: va_eventd.@target[0].community<br/>Opt: community</p>                                  | <p>Defines the community string for SNMPv1.</p> <table border="1"> <tr> <td></td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  |   |        | Range |         |     |        |
|   |   |   |        |       |         |     |        |
| Range   |   |   |        |       |         |     |        |
| <p>Web: Username<br/>UCI: va_eventd.@target[0].snmp_uname<br/>Opt: snmp_uname</p>                                 | <p>Defines the username for SNMPv3.<br/>Only displayed when SNMP protocol version is SNMPv3</p> <table border="1"> <tr> <td></td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  |   |        | Range |         |     |        |
|   |   |   |        |       |         |     |        |
| Range   |   |   |        |       |         |     |        |
| <p>Web: Authentication Protocol<br/>UCI:<br/>va_eventd.@target[0].snmp_auth_proto<br/>Opt: snmp_auth_proto</p>    | <p>Defines the SNMPv3 authentication protocol<br/>Only displayed when SNMP protocol version is SNMPv3.</p> <table border="1"> <tr> <td></td> <td></td> </tr> <tr> <td>MD5</td> <td></td> </tr> <tr> <td>SHA</td> <td></td> </tr> </table>               |   |        | MD5   |         | SHA |        |
|   |   |   |        |       |         |     |        |
| MD5   |   |   |        |       |         |     |        |
| SHA   |   |   |        |       |         |     |        |
| <p>Web: Authentication Password<br/>UCI:<br/>va_eventd.@target[0].snmp_auth_pass<br/>Opt: snmp_auth_pass</p>      | <p>Defines the SNMPv3 authentication password.<br/>Only displayed when SNMPv3 authentication protocol is configured.</p> <table border="1"> <tr> <td></td> <td></td> </tr> <tr> <td>MD5</td> <td></td> </tr> <tr> <td>SHA</td> <td></td> </tr> </table> |   |        | MD5   |         | SHA |        |
|   |   |   |        |       |         |     |        |
| MD5   |   |   |        |       |         |     |        |
| SHA   |   |   |        |       |         |     |        |
| <p>Web: Privacy Protocol<br/>UCI:<br/>va_eventd.@target[0].snmp_priv_proto<br/>Opt: snmp_priv_proto</p>           | <p>Defines the SNMPv3 privacy protocol.<br/>Only displayed when SNMP authentication protocol is configured.</p> <table border="1"> <tr> <td></td> <td></td> </tr> <tr> <td>DES</td> <td></td> </tr> <tr> <td>AES</td> <td></td> </tr> </table>          |   |        | DES   |         | AES |        |
|   |   |   |        |       |         |     |        |
| DES   |   |   |        |       |         |     |        |
| AES   |   |   |        |       |         |     |        |
| <p>Web: Privacy Password<br/>UCI:<br/>va_eventd.@target[0].snmp_priv_pass<br/>Opt: snmp_priv_pass</p>             | <p>Defines SNMPv3 privacy password.<br/>Only displayed when SNMP privacy protocol is configured.</p> <table border="1"> <tr> <td></td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   |   |        | Range |         |     |        |
|   |   |   |        |       |         |     |        |
| Range   |   |   |        |       |         |     |        |
| <p>Web: SNMPv3 Context<br/>UCI: va_eventd.@target[0].snmp_context<br/>Opt: snmp_context</p>                       | <p>Defines the SNMPv3 context.<br/>Only displayed when SNMP authentication protocol is configured.</p> <table border="1"> <tr> <td></td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   |   |        | Range |         |     |        |
|   |   |   |        |       |         |     |        |
| Range   |   |   |        |       |         |     |        |
| <p>Web: SNMPv3 Context Engine ID<br/>UCI:<br/>va_eventd.@target[0].snmp_context_eid<br/>Opt: snmp_context_eid</p> | <p>Defines the SNMPv3 context engine ID.<br/>Only displayed when SNMP authentication protocol is configured.</p> <table border="1"> <tr> <td></td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   |   |        | Range |         |     |        |
|   |   |   |        |       |         |     |        |
| Range   |   |   |        |       |         |     |        |
| <p>Web: SNMPv3 Security Engine ID<br/>UCI: va_eventd.@target[0].snmp_sec_eid<br/>Opt: snmp_sec_eid</p>            | <p>Defines the SNMPv3 security engine ID.<br/>Only displayed when SNMP authentication protocol is configured.</p> <table border="1"> <tr> <td></td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  |   |        | Range |         |     |        |
|   |   |   |        |       |         |     |        |
| Range   |   |   |        |       |         |     |        |

**Table 183: Information table for event system SNMP event destination settings**

### 44.3.3.4 Exec target

When an Execute target receives an event, it executes a shell command.

Event Destination Delete

Enabled

Destination Name

Type

Connection Tester Name

Command Template  Template for the command to be executed

**Figure 247: The VA event system exec event destination configuration page**

| Web Field/UCI/Package Option  | Description  |           |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
|---|--|-----------|---|-------|----------|---------------|--------|-----------|-------------|----------|-------|--------------|-------|---------|----------------|------|-----|------------|-----|------|-------------|------|
| Web: Enabled<br>UCI: va_eventd.@target[0].enabled<br>Opt: enabled                         | Enables an event destination.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0         | Disabled.                                     | 1     | Enabled. |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| 0   | Disabled.  |           |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| 1   | Enabled.   |           |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Web: Destination name<br>UCI: va_eventd.@target[0].name<br>Opt: name                      | Defines a name for the event destination.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> </table>   | Range     |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Range   |  |           |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Web: Type<br>UCI: va_eventd.@target[0].type<br>Opt: type                                  | Defines the event destination type. For shell command execution, choose <b>Execute</b> .<br><table border="1"> <thead> <tr> <th>Web Value</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Syslog</td> <td>Syslog target</td> <td>syslog</td> </tr> <tr> <td>SNMP Trap</td> <td>SNMP target</td> <td>snmptrap</td> </tr> <tr> <td>Email</td> <td>Email target</td> <td>email</td> </tr> <tr> <td>Execute</td> <td>Execute target</td> <td>exec</td> </tr> <tr> <td>SMS</td> <td>SMS target</td> <td>sms</td> </tr> <tr> <td>File</td> <td>File target</td> <td>file</td> </tr> </tbody> </table> | Web Value | Description                                   | UCI   | Syslog   | Syslog target | syslog | SNMP Trap | SNMP target | snmptrap | Email | Email target | email | Execute | Execute target | exec | SMS | SMS target | sms | File | File target | file |
| Web Value   | Description  | UCI       |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Syslog  | Syslog target  | syslog    |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| SNMP Trap   | SNMP target  | snmptrap  |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Email   | Email target   | email     |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Execute   | Execute target   | exec      |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| SMS   | SMS target   | sms       |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| File  | File target  | file      |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Web: Connection Tester Name<br>UCI: va_eventd.@target[0]. conn_tester<br>Opt: conn_tester | Defines the connection tester, if any, to use to verify the execute target.<br><table border="1"> <tr> <td>None</td> <td>No connection tester. UCI option not present.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | None      | No connection tester. UCI option not present. | Range |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| None  | No connection tester. UCI option not present.  |           |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Range   |  |           |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Web: Command Template<br>UCI: va_eventd.@target[0].cmd_template<br>Opt: cmd_template      | Defines the command template to use for the event.<br>Example to log a syslog message:<br>va_eventd.@target[0].cmd_template="logger -t eventer %e"<br>See the section on message templates below.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> </table>   | Range     |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |
| Range   |  |           |   |       |          |               |        |           |             |          |       |              |       |         |                |      |     |            |     |      |             |      |

**Table 184: Information table for event system execute event destination settings**

### 44.3.3.5 SMS target

When an SMS target receives an event, it sends an SMS message.

Event Destination Delete

Enabled

Destination Name

Type

Connection Tester Name

Message Template  For Syslog and SNMP types message template has reasonable default so it is safe to leave blank

Phone Number  Where text will be send

**Figure 248: The VA event system SMS event destination configuration page**

| Web Field/UCI/Package Option  | Description   |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
|---|---|-----------|---|-------|----------|--|--------|-----------|--|----------|-------|--|-------|---------|--|------|-----|--|-----|------|--|------|
| Web: Enabled<br>UCI: va_eventd.@target[0].enabled<br>Opt: enabled                         | Enables an event destination.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0         | Disabled.                                     | 1     | Enabled. |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| 0   | Disabled.   |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| 1   | Enabled.  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Web: Destination name<br>UCI: va_eventd.@target[0].name<br>Opt: name                      | Defines a name for the event destination.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> </table>  | Range     |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Range   |   |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Web: Type<br>UCI: va_eventd.@target[0].type<br>Opt: type                                  | Defines the event destination type. For SMS destination, choose <b>SMS</b> .<br><table border="1"> <thead> <tr> <th>Web Value</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Syslog</td> <td></td> <td>syslog</td> </tr> <tr> <td>SNMP Trap</td> <td></td> <td>snmptrap</td> </tr> <tr> <td>Email</td> <td></td> <td>email</td> </tr> <tr> <td>Execute</td> <td></td> <td>exec</td> </tr> <tr> <td>SMS</td> <td></td> <td>sms</td> </tr> <tr> <td>File</td> <td></td> <td>file</td> </tr> </tbody> </table> | Web Value | Description                                   | UCI   | Syslog   |  | syslog | SNMP Trap |  | snmptrap | Email |  | email | Execute |  | exec | SMS |  | sms | File |  | file |
| Web Value   | Description   | UCI       |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Syslog  |   | syslog    |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| SNMP Trap   |   | snmptrap  |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Email   |   | email     |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Execute   |   | exec      |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| SMS   |   | sms       |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| File  |   | file      |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Web: Connection Tester Name<br>UCI: va_eventd.@target[0]. conn_tester<br>Opt: conn_tester | Defines the connection tester, if any, to use to verify the SMS target.<br><table border="1"> <tr> <td>None</td> <td>No connection tester. UCI option not present.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | None      | No connection tester. UCI option not present. | Range |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| None  | No connection tester. UCI option not present.   |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Range   |   |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Web: Message Template<br>UCI: va_eventd.@target[0].template<br>Opt: template              | Defines the message template to use for the event. In general, this should be left empty. Example:<br>va_eventd.@target[0].template="%{eventName}"<br>See the section on message templates below.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> </table>  | Range     |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Range   |   |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Web: Phone Number<br>UCI: va_eventd.@target[0].callee<br>Opt: callee                      | Defines the phone number for sending SMS to.<br><table border="1"> <tr> <td>Range</td> <td></td> </tr> </table>   | Range     |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Range   |   |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |

**Table 185: Information table for event system SMS event destination settings**

### 44.3.3.6 File target

When file target receives an event, it logs to a file.

Event Destination Delete

Enabled

Destination Name

Type

Connection Tester Name

Message Template  For Syslog and SNMP types message template has reasonable default so it is safe to leave blank

File Name  File to store events

Max Size (KiB)  Maximum file size in KiB. Older events will be overwritten when reached

**Figure 249: The VA event system file event destination configuration page**

| Web Field/UCI/Package Option   | Description  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
|--|--|-----------|---|-------|----------|--|--------|-----------|--|----------|-------|--|-------|---------|--|------|-----|--|-----|------|--|------|
| Web: Enabled<br>UCI: va_eventd.@target[0].enabled<br>Opt: enabled                        | Enables an event destination.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0         | Disabled.                                     | 1     | Enabled. |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| 0  | Disabled.  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| 1  | Enabled.   |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Web: Destination Name<br>UCI: va_eventd.@target[0].name<br>Opt: name                     | Defines a name for the event destination.<br><table border="1"> <tr> <td></td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  |           |   | Range |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
|  |  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Range  |  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Web: Type<br>UCI: va_eventd.@target[0].type<br>Opt: type                                 | Defines the event destination type. For file choose <b>File</b> .<br><table border="1"> <thead> <tr> <th>Web Value</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Syslog</td> <td></td> <td>syslog</td> </tr> <tr> <td>SNMP Trap</td> <td></td> <td>snmptrap</td> </tr> <tr> <td>Email</td> <td></td> <td>email</td> </tr> <tr> <td>Execute</td> <td></td> <td>exec</td> </tr> <tr> <td>SMS</td> <td></td> <td>sms</td> </tr> <tr> <td>File</td> <td></td> <td>file</td> </tr> </tbody> </table> | Web Value | Description                                   | UCI   | Syslog   |  | syslog | SNMP Trap |  | snmptrap | Email |  | email | Execute |  | exec | SMS |  | sms | File |  | file |
| Web Value  | Description  | UCI       |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Syslog   |  | syslog    |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| SNMP Trap  |  | snmptrap  |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Email  |  | email     |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Execute  |  | exec      |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| SMS  |  | sms       |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| File   |  | file      |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Web: Connection Tester Name<br>UCI: va_eventd.@target[0].conn_tester<br>Opt: conn_tester | Defines the connection tester (if any) to use to verify the File target.<br><table border="1"> <tr> <td>None</td> <td>No connection tester. UCI option not present.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | None      | No connection tester. UCI option not present. | Range |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| None   | No connection tester. UCI option not present.  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Range  |  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Web: Message Template<br>UCI: va_eventd.@target[0].template<br>Opt: template             | Defines the message template to use for the event. In general, this should be left empty.<br>See the section on message templates below.<br><table border="1"> <tr> <td></td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   |           |   | Range |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
|  |  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Range  |  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Web: File Name<br>UCI: va_eventd.@target[0].file_name<br>Opt: file_name                  | Defines a file name for the event destination. Full path.<br><table border="1"> <tr> <td></td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  |           |   | Range |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
|  |  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Range  |  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Web: Max Size (KiB)<br>UCI: va_eventd.@target[0].max_size_kb<br>Opt: file_name           | Defines a file size in kilobits.<br><table border="1"> <tr> <td>2048</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>   | 2048      |   | Range |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| 2048   |  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |
| Range  |  |           |   |       |          |  |        |           |  |          |       |  |       |         |  |      |     |  |     |      |  |      |

**Table 186: Information table for event system file event destination settings**

### 44.3.4 Event filters

Event filters are used to classify the events to be sent to the event destination. Multiple event filters can be defined. Event filters configure the uci `forwarding` section rules.

Figure 250: The VA event system event filters configuration page

| Web Field/UCI/Package Option   | Description   |       |                  |      |          |        |  |         |  |       |  |          |  |       |  |           |                  |
|--|---|-------|------------------|------|----------|--------|--|---------|--|-------|--|----------|--|-------|--|-----------|------------------|
| Web: Enabled<br>UCI: <code>va_eventd.@forwarding[0].enabled</code><br>Opt: <code>enabled</code>            | Enables an event filter.<br><table border="1"> <tr> <td>1</td> <td>Disabled.</td> </tr> <tr> <td>0</td> <td>Enabled.</td> </tr> </table>  | 1     | Disabled.        | 0    | Enabled. |        |  |         |  |       |  |          |  |       |  |           |                  |
| 1  | Disabled.   |       |                  |      |          |        |  |         |  |       |  |          |  |       |  |           |                  |
| 0  | Enabled.  |       |                  |      |          |        |  |         |  |       |  |          |  |       |  |           |                  |
| Web: Class Name<br>UCI:<br><code>va_eventd.@forwarding[0].className</code><br>Opt: <code>className</code>  | Only match events with the given class name. Available class names are listed or can be viewed using the command <code>vae_cli -d</code>  |       |                  |      |          |        |  |         |  |       |  |          |  |       |  |           |                  |
| Web: Event Name<br>UCI:<br><code>va_eventd.@forwarding[0].eventName</code><br>Opt: <code>eventName</code>  | Only match events with the given event name. Available event names are listed. The event name is optional and can be omitted.   |       |                  |      |          |        |  |         |  |       |  |          |  |       |  |           |                  |
| Web: Minimum Severity<br>UCI: <code>va_eventd.@forwarding[0].severity</code><br>Opt: <code>severity</code> | Defines the minimum event severity. The minimum severity event is DEBUG. Events generated within the minimum and maximum event severity will be matched.<br>Minimum and maximum severity are specified in the one UCI option and entered using a dash (-) separator in the form minimum-maximum. Example:<br><code>va_eventd.@forwarding[0].severity=debug-error</code><br><table border="1"> <tr> <td>debug</td> <td>minimum severity</td> </tr> <tr> <td>info</td> <td></td> </tr> <tr> <td>notice</td> <td></td> </tr> <tr> <td>warning</td> <td></td> </tr> <tr> <td>error</td> <td></td> </tr> <tr> <td>critical</td> <td></td> </tr> <tr> <td>alert</td> <td></td> </tr> <tr> <td>emergency</td> <td>maximum severity</td> </tr> </table> | debug | minimum severity | info |          | notice |  | warning |  | error |  | critical |  | alert |  | emergency | maximum severity |
| debug  | minimum severity  |       |                  |      |          |        |  |         |  |       |  |          |  |       |  |           |                  |
| info   |   |       |                  |      |          |        |  |         |  |       |  |          |  |       |  |           |                  |
| notice   |   |       |                  |      |          |        |  |         |  |       |  |          |  |       |  |           |                  |
| warning  |   |       |                  |      |          |        |  |         |  |       |  |          |  |       |  |           |                  |
| error  |   |       |                  |      |          |        |  |         |  |       |  |          |  |       |  |           |                  |
| critical   |   |       |                  |      |          |        |  |         |  |       |  |          |  |       |  |           |                  |
| alert  |   |       |                  |      |          |        |  |         |  |       |  |          |  |       |  |           |                  |
| emergency  | maximum severity  |       |                  |      |          |        |  |         |  |       |  |          |  |       |  |           |                  |

|   |  |       |                  |      |  |        |  |         |  |       |  |          |  |       |  |           |                  |
|---|--|-------|------------------|------|--|--------|--|---------|--|-------|--|----------|--|-------|--|-----------|------------------|
| <p>Web: Maximum Severity<br/>UCI: va_eventd.@forwarding[0].severity<br/>Opt: severity</p> | <p>Defines the maximum event severity. The maximum event severity is EMERGENCY. Events generated within the minimum and maximum event severity will be matched.</p> <p>The UCI command for specifying minimum and maximum severity is the same and is entered with two parameters using a dash (-) separator minimum-maximum. Example:<br/>va_eventd.@forwarding[0].severity=debug-error</p> <table border="1" data-bbox="678 398 1394 678"> <tr> <td>debug</td> <td>minimum severity</td> </tr> <tr> <td>info</td> <td></td> </tr> <tr> <td>notice</td> <td></td> </tr> <tr> <td>warning</td> <td></td> </tr> <tr> <td>error</td> <td></td> </tr> <tr> <td>critical</td> <td></td> </tr> <tr> <td>alert</td> <td></td> </tr> <tr> <td>emergency</td> <td>maximum severity</td> </tr> </table> | debug | minimum severity | info |  | notice |  | warning |  | error |  | critical |  | alert |  | emergency | maximum severity |
| debug   | minimum severity   |       |                  |      |  |        |  |         |  |       |  |          |  |       |  |           |                  |
| info  |  |       |                  |      |  |        |  |         |  |       |  |          |  |       |  |           |                  |
| notice  |  |       |                  |      |  |        |  |         |  |       |  |          |  |       |  |           |                  |
| warning   |  |       |                  |      |  |        |  |         |  |       |  |          |  |       |  |           |                  |
| error   |  |       |                  |      |  |        |  |         |  |       |  |          |  |       |  |           |                  |
| critical  |  |       |                  |      |  |        |  |         |  |       |  |          |  |       |  |           |                  |
| alert   |  |       |                  |      |  |        |  |         |  |       |  |          |  |       |  |           |                  |
| emergency   | maximum severity   |       |                  |      |  |        |  |         |  |       |  |          |  |       |  |           |                  |
| <p>Web: Target<br/>UCI: va_eventd.@forwarding[0].target<br/>Opt: target</p>               | <p>Defines the event destination to forward the event to. All configured event destinations will be displayed.</p>   |       |                  |      |  |        |  |         |  |       |  |          |  |       |  |           |                  |

**Table 187: Information table for event system event filters settings**

## 44.4 Configuring the event system using command line

The event system configuration files are stored at **/etc/config/va\_eventd**

There are four config sections main, conn\_tester, target and forwarding.

You can configure multiple conn\_tester, target and forwarding sections.

By default, all conn\_tester instances are named conn\_tester, it is identified by @conn\_tester then the conn\_tester position in the package as a number. For example, for the first conn\_tester in the package using UCI:

```
va_eventd.@conn_tester[0]=conn_tester
va_eventd.@conn_tester[0].enabled=1
```

Or using package options, enter:

```
config conn_tester
    option enabled '1'
```

By default, all target instances are named target. The target instance is identified by @target then the target position in the package as a number. For example, for the first target in the package using UCI:

```
va_eventd.@target[0]=target
va_eventd.@target[0].enabled=1
```

Or using package options, enter:

```
config target
    option enabled '1'
```

By default, all forwarding instances are named forwarding. The forwarding instance is identified by @forwarding then the forwarding position in the package as a number. For example, for the first forwarding rule in the package using UCI:

```
va_eventd.@forwarding[0]=forwarding
va_eventd.@forwarding[0].enabled=1
```

Or using package options:

```
config forwarding
    option enabled '1'
```

#### 44.4.1 Event system using UCI

```
root@VA_router:~# uci show va_eventd
#Sample basic settings
va_eventd.main=va_eventd
va_eventd.main.event_queue_file=/tmp/event_buffer
va_eventd.main.event_queue_size=128K

#Sample SNMP
va_eventd.@conn_tester[0]=conn_tester
va_eventd.@conn_tester[0].type=ping
va_eventd.@conn_tester[0].ping_dest_addr=192.168.100.1
va_eventd.@conn_tester[0].ping_success_duration_sec=60
va_eventd.@conn_tester[0].name=SNMPTest
va_eventd.@conn_tester[0].ping_source=LAN1
va_eventd.@target[0]=target
va_eventd.@target[0].suppress_duplicate_forwardings=no
va_eventd.@target[0].type=snmp
va_eventd.@target[0].agent_addr=localhost
va_eventd.@target[0].name=SNMPTarget
va_eventd.@target[0].conn_tester=SNMPTest
va_eventd.@target[0].target_addr=192.168.100.126:68
va_eventd.@target[0].snmp_version=3
va_eventd.@target[0].snmp_uname=v3username
va_eventd.@target[0].snmp_auth_proto=MD5
va_eventd.@target[0].snmp_auth_pass=md5password
va_eventd.@target[0].snmp_priv_proto=AES
va_eventd.@target[0].snmp_priv_pass=aespassword
va_eventd.@target[0].snmp_context=v3context
```

```
va_eventd.@target[0].snmp_context_eid=v3contextID
va_eventd.@target[0].snmp_sec_eid=v3SecurityID
va_eventd.@forwarding[0]=forwarding
va_eventd.@forwarding[0].enabled=yes
va_eventd.@forwarding[0].className=mobile
va_eventd.@forwarding[0].target=SNMPTarget
va_eventd.@forwarding[0].eventName=LinkUp
va_eventd.@forwarding[0].severity=notice-notice

#Sample Syslog
va_eventd.@conn_tester[1]=conn_tester
va_eventd.@conn_tester[1].name=SyslogTest
va_eventd.@conn_tester[1].type=ping
va_eventd.@conn_tester[1].ping_dest_addr=192.168.100.2
va_eventd.@conn_tester[1].ping_source=LAN1
va_eventd.@conn_tester[1].ping_success_duration_sec=60
va_eventd.@target[1]=target
va_eventd.@target[1].name=SyslogTarget
va_eventd.@target[1].type=syslog
va_eventd.@target[1].conn_tester=SyslogTest
va_eventd.@target[1].target_addr=192.168.100.2:514
va_eventd.@target[1].tcp_syslog=0
va_eventd.@forwarding[1]=forwarding
va_eventd.@forwarding[1].enabled=yes
va_eventd.@forwarding[1].severity=debug-error
va_eventd.@forwarding[1].target=SyslogTarget

#Sample Email
va_eventd.@conn_tester[2]=conn_tester
va_eventd.@conn_tester[2].name=EmailTest
va_eventd.@conn_tester[2].type=link
va_eventd.@conn_tester[2].link_iface=PoAADSL
va_eventd.@target[2]=target
va_eventd.@target[2].timeout_sec=10
va_eventd.@target[2].name=EmailTarget
va_eventd.@target[2].type=email
va_eventd.@target[2].conn_tester=EmailTest
```



```
va_eventd.@target[2].from=from@example.com
va_eventd.@target[2].to=to@example.com
va_eventd.@target[2].subject_template=%{serial} %{severityName} %{eventName}!!!
va_eventd.@target[2].body_template=%{eventName} (%{class}.%{subclass})
happened!
va_eventd.@target[2].smtp_addr=192.168.100.3:25
va_eventd.@target[2].smtp_user=root
va_eventd.@target[2].smtp_password=admin
va_eventd.@target[2].use_tls=0
va_eventd.@target[2].tls_starttls=0
va_eventd.@target[2].tls_forcessl3=0
va_eventd.@forwarding[2]=forwarding
va_eventd.@forwarding[2].enabled=yes
va_eventd.@forwarding[2].className=power
va_eventd.@forwarding[2].eventName=IgnitionOff
va_eventd.@forwarding[2].severity=notice-notice
va_eventd.@forwarding[2].target=EmailTarget

#Sample SMS
va_eventd.@target[3]=target
va_eventd.@target[3].name=SMStarget
va_eventd.@forwarding[3].target=SMStarget
va_eventd.@target[3].type=sms
va_eventd.@target[3].template=%{serial} %{severityName} %{eventName}!!!
va_eventd.@target[3].callee=0123456789
va_eventd.@forwarding[3]=forwarding
va_eventd.@forwarding[3].enabled=yes
va_eventd.@forwarding[3].target=SMStarget
va_eventd.@forwarding[3].className=auth
va_eventd.@forwarding[3].eventName>LoginSSH
va_eventd.@forwarding[3].severity=notice-notice

#Sample Execute
va_eventd.@target[4]=target
va_eventd.@target[4].name=ExecTarget
va_eventd.@target[4].type=exec
```

```

va_eventd.@target[4].cmd_template=logger -t eventer %{eventName}
va_eventd.@forwarding[4]=forwarding
va_eventd.@forwarding[4].enabled=yes
va_eventd.@forwarding[4].target=ExecTarget
va_eventd.@forwarding[4].className=ppp
va_eventd.@forwarding[4].severity=debug-error

#Sample File
va_eventd.@target[5]=target
va_eventd.@target[5].name=FileTarget
va_eventd.@target[5].type=file
va_eventd.@target[5].file_name=\tmp\eventfile
va_eventd.@target[5].max_size_kb=1028
va_eventd.@forwarding[5]=forwarding
va_eventd.@forwarding[5].enabled=yes
va_eventd.@forwarding[5].target=FileTarget
va_eventd.@forwarding[5].severity=debug-error

```

#### 44.4.1.1 Event system using package options

```

root@VA_router:~# uci export va_eventd
package va_eventd

config va_eventd 'main'
    option event_queue_file '/tmp/event_buffer'
    option event_queue_size '128K'

# Sample SNMP
config conn_tester
    option type 'ping'
    option ping_dest_addr '192.168.100.1'
    option ping_success_duration_sec '60'
    option name 'SNMPTest'
    option ping_source 'LAN1'

config target
    option suppress_duplicate_forwardings 'no'
    option type 'snmp'

```

```
option agent_addr 'localhost'
option name 'SNMPTarget'
option conn_tester 'SNMPTest'
option target_addr '192.168.100.126:68'
option snmp_version '3'
option snmp_uname 'v3username'
option snmp_auth_proto 'MD5'
option snmp_auth_pass 'md5password'
option snmp_priv_proto 'AES'
option snmp_priv_pass 'aespassword'
option snmp_context 'v3context'
option snmp_context_eid 'v3contextID'
option snmp_sec_eid 'v3SecurityID'

config forwarding
option enabled 'yes'
option className 'mobile'
option severity 'notice-notice'
option target 'SNMPTarget'
option eventname 'LinkUp'

# Sample Syslog
config conn_tester
option name 'SyslogTest'
option type 'ping'
option ping_dest_addr '192.168.100.2'
option ping_source 'LAN1'
option ping_success_duration_sec '60'

config target
option name 'SyslogTarget'
option type 'syslog'
option conn_tester 'SyslogTest'
option target_addr '192.168.100.2:514'
option tcp_syslog '0'

config forwarding
```

```
option enabled 'yes'
option severity 'debug-error'
option target 'SyslogTarget'

# Sample Email
config conn_tester
    option name 'EmailTest'
    option type 'link'
    option link_iface 'PoAADSL'

config target
    option timeout_sec '10'
    option name 'EmailTarget'
    option type 'email'
    option conn_tester 'EmailTest'
    option from 'from@example.com'
    option to 'to@example.com'
    option subject_template '%{serial} %{severityName} %{eventName}!!!'
    option body_template '%{eventName} (%{class}:%{subclass})
happened!'
    option smtp_addr '192.168.100.3:25'
    option smtp_user 'root'
    option smtp_password 'admin'
    option use_tls 'no'
    option tls_starttls 'no'
    option tls_forcessl3 'no'

config forwarding
    option enabled 'yes'
    option target 'EmailTarget'
    option className 'power'
    option eventName 'IgnitionOff'
    option severity 'notice-notice'

# Sample SMS
config target
    option name 'SMStarget'
```

```
option type 'sms'
option template '%{serial} %{severityName} %{eventName}!!!'
option callee '0123456789'

config forwarding
option enabled 'yes'
option target 'SMSTarget'
option className 'auth'
option eventName 'LoginSSH'
option severity 'notice-notice'

# Sample Execute
config target
option name 'ExecTarget'
option type 'exec'
option cmd_template 'logger -t eventer %{eventName}'

config forwarding
option enabled 'yes'
option target 'ExecTarget'
option className 'ppp'
option severity 'debug-error'

# Sample File
config target
option name 'FileTarget'
option type 'file'
option file_name '\tmp\eventfile'
option max_size_kb '1028'

config forwarding
option enabled 'yes'
option target 'FileTarget'
option severity 'debug-error'
```

## 44.5 Event system diagnostics

### 44.5.1 Displaying VA events

To view a list of all available class names, events and severity levels, enter:

```
root@VA_router:~# vae_cli -d
```

The following is an example of the output from this command:

```
| Class      | ID  | Name                                     | Severity | Specific Template
| internal   | 1   | EventdConfigErr                         | error    |
| %{p1} %{p2}: %{p3} has bad value..
| internal   | 2   | EventdConfigWarn                        | warning  |
| %{p1} %{p2}: %{p3} has bad value..
| internal   | 3   | EventdConfigUnknown                     | informat | %{p1} %{p2}:
field '%{p3}' is no..

| internal   | 4   | EventdSystemErr                         | error    |
| %{p1} %{p2}: %{p3} %{p4} %{p5} %..
| internal   | 5   | EventdSystemWarn                        | error    |
| %{p1} %{p2}: %{p3} %{p4} %{p5} %..
| internal   | 6   | EventdUpAndRunning                      | informat |
| internal   | 7   | EventdStopped                           | warning  | %{p1}
| mobile     | 1   | SIMin                                    | notice   | SIM card #%{p1}inserted

| mobile     | 2   | SIMout                                    | notice   | SIM card #%{p1} removed
| mobile     | 3   | LinkUp                                    | notice   | 3g link %{p1} up using sim
#%{p2}..
| mobile     | 4   | LinkDown                                  | notice   | 3g link %{p1} down
| mobile     | 5   | SMSByPassword                            | notice   | Received SMS from %{p1} (by
pass..
| mobile     | 6   | SMSByCaller                              | notice   | Received SMS from %{p1}
(%{p2}):..
| mobile     | 7   | SMSFromUnknown                           | warning  | Received SMS from
unknown sender..
| mobile     | 8   | SMSSendSuccess                           | informat | SMS send success: %{p1}
| mobile     | 9   | SMSSendError                             | warning  | SMS send error: %{p1}
| mobile     | 10  | SMSSent                                   | notice   | Sent SMS
to %{p1}: %{p2}
| ethernet   | 1   | LinkUp                                    | notice   | Ethernet %{p1} up
| ethernet   | 2   | LinkDown                                  | notice   | Ethernet %{p1} down
| auth       | 2   | BadPasswordSSH                           | warning  | SSH login attempt
from %{p2}: ba..
| auth       | 3   | BadUserConsole                           | warning  | Console login attempt
on %{p1}: ..
```

```

| auth      | 4 | BadPasswordConsole | warning | Console login attempt
on %{p2}: ..
| auth      | 5 | BadUserTelnet      | warning | Telnet login attempt:
bad username
| auth      | 6 | BadPasswordTelnet  | warning | Telnet login attempt:
bad passwo..
| auth      | 7 | BadUserLuCI        | warning | LuCI login attempt: bad
username..
| auth      | 8 | BadPasswordLuCI    | warning | LuCI login attempt: bad
password..
| auth      | 9 | LoginSSH           | notice  | SSH login: user %{p2}
from %{p3}
| auth      | 10 | LogoffSSH          | notice  | SSH logoff: user %{p1}
due to "%..
| auth      | 11 | LoginConsole       | notice  | Console login:
user %{p1} on %{p2}
| auth      | 12 | LogoffConsole      | notice  | Console logoff on %{p1}
| auth      | 13 | LoginTelnet        | notice  | Telnet login:
user %{p1}
| auth      | 14 | LoginLuCI          | notice  | LuCI login: user %{p1}
| auth      | 15 | ConsoleCommand     | informat | %{p1}@%{p2} %{p3}
| auth      | 16 | LuCIAction         | informat
| %{p1}@%{p2} %{p3} %{p4} %{p5}
| ipsec     | 6 | IPsecInitIKE       | informat | IPsec IKE %{p1}
established
| ipsec     | 7 | IPsecInitSA        | informat | IPsec SA %{p1}
established
| ipsec     | 8 | IPsecCloseIKE      | informat | IPsec IKE %{p1} deleted
| ipsec     | 9 | IPsecCloseSA       | informat | IPsec SA %{p1} closed
| ipsec     | 10 | IPsecDPDTimeOut    | informat | IPsec IKE %{p1} DPD
timed out
| wifi      | 1 | WiFiConnectedToAP  | notice  | WiFi %{p1} connected to
AP %{p2}
| wifi      | 1 | WiFiConnectedToAP  | notice  | WiFi %{p1} connected to
AP %{p2}
| wifi      | 2 | WiFiDisconnectedFromAP | notice  | WiFi %{p1}
disconnected from AP
| wifi      | 2 | WiFiDisconnectedFromAP | notice  | WiFi %{p1}
disconnected from AP
| wifi      | 3 | WiFiStationAttached | notice  | WiFi
station %{p2} connected to ..
| wifi      | 3 | WiFiStationAttached | notice  | WiFi
station %{p2} connected to ..

```

```

| wifi      | 4 | WiFiStationDetached | notice | WiFi
station %{p2} disconnected ..
| wifi      | 4 | WiFiStationDetached | notice | WiFi
station %{p2} disconnected ..
| wifi      | 5 | WiFiStationAttachFailed | notice | WiFi
station %{p2} failed to con..
| wifi      | 5 | WiFiStationAttachFailed | notice | WiFi
station %{p2} failed to con..
| ppp       | 1 | LinkUp              | informat | PPP for
interface %{p2} (protoco..
| ppp       | 2 | LinkDown            | informat | PPP for
interface %{p2} (protoco..
| ppp       | 3 | ConnEstablished     | informat | PPP connection
for interface %{p..
| adsl      | 1 | LinkUp              | notice | ADSL trained.
Starting interface..
| adsl      | 2 | LinkDown            | notice | ADSL down.
Stopping interface %{}..
| adsl      | 3 | Silent              | debug   | ADSL silent
| adsl      | 4 | Training            | debug   | ADSL training
| adsl      | 5 | TrainingSuccess     | notice  | ADSL training
successful: data ..
| system    | 1 | BootSuccess         | informat | Success booting into %{p1}
| system    | 2 | DigitalInputChange  | notice  | Digital
Input %{p1} changed valu..
| ntp       | 1 | InitialSync         | notice  | Initial NTP sync:
time: %{p1}; o..
| ntp       | 2 | Adjust              | informat | NTP adjust by %{p1}
| ntp       | 3 | QueryTimeout        | warning | NTP query to %{p1} timed
out. Ne..
| ntp       | 4 | QueryFailed         | warning | NTP query failed: %{p1}

```



## 45 Configuring data usage monitor

### 45.1 Introduction

Virtual Access software provides support for monitoring of data usage on mobile interfaces and to disable if the monthly limit is exceeded. This allows an element of control over data usage for SIMs with a limited data plan.

**DISCLAIMER:** data usage statistics calculated by Virtual Access data usage feature are best estimates and may vary from the mobile carrier statistics that are used for billing. Virtual Access cannot be held liable for any fees charged by the carrier to the customer for their data usage. We recommend that the configured data usage is lower than the allowance and that traffic percentage alerts are used.

### 45.2 Configuration package used

| Package    | Sections |
|------------|----------|
| procrustes | limit    |

### 45.3 Configuring data usage using the web interface

Select **Services -> Data Usage**. The Data Usage page appears.

You can monitor interfaces as a collective group, so enter a name for the group and select **Add**. The examples below show a group name configured as 'wan'.

You can configure multiple groups.

**Procrustes**  
Monitor network traffic for interface groups and stop interfaces and blacklist sim cards if limits are reached

Interface Group

*This section contains no values yet*

wan

Figure 251: The data usage page

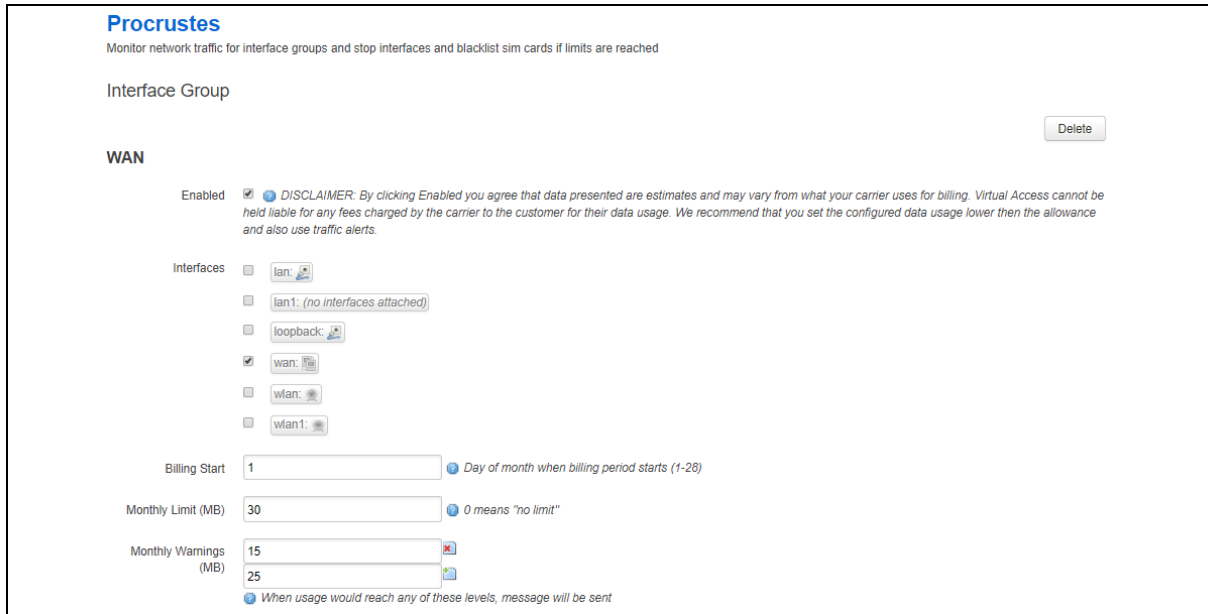


Figure 252: The data usage configuration page

| Web Field/UCI/Package Option   | Description   |   |                      |       |          |
|--|---|---|----------------------|-------|----------|
| Web: Enabled<br>UCI: procrustes.@limit[0].enabled<br>Opt: enabled  | Enable data usage monitor on this interface group.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0 | Disabled.            | 1     | Enabled. |
| 0  | Disabled.   |   |                      |       |          |
| 1  | Enabled.  |   |                      |       |          |
| Web: Billing Start<br>UCI:<br>procrustes.@limit[0].billing_period_start_day<br>Opt: billing_period_start_day     | Day of month on which the billing period starts.<br><table border="1"> <tr> <td>1</td> <td></td> </tr> <tr> <td>Range</td> <td>1 - 28</td> </tr> </table>   | 1 |                      | Range | 1 - 28   |
| 1  |   |   |                      |       |          |
| Range  | 1 - 28  |   |                      |       |          |
| Web: Interfaces<br>UCI: procrustes.@limit[0].interfaces<br>Opt: interfaces                                       | Monitor and apply limits to these interfaces as a group. Configure multiple interfaces via UCI using a space separator.<br>Example:<br>uci set procrustes.@limit[0].interfaces="lan wan"  |   |                      |       |          |
| Web: Monthly Limit (MB)<br>UCI:<br>procrustes.@limit[0].monthly_data_limit<br>Opt: monthly_data_limit            | Defines monthly data traffic limit in megabytes (MB). This is total RX and TX on the interface.<br><table border="1"> <tr> <td>0</td> <td>Zero means no limit.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 0 | Zero means no limit. | Range |          |
| 0  | Zero means no limit.  |   |                      |       |          |
| Range  |   |   |                      |       |          |
| Web: Monthly Warnings (MB)<br>UCI:<br>procrustes.@limit[0].monthly_warning_levels<br>Opt: monthly_warning_levels | Defines data usage limits for generating a log message and a VA event alert when used traffic reaches specified levels. Levels are specified in MB.<br>Set multiple limits via UCI using a space separator.<br>Example:<br>uci set procrustes.@limit[0].monthly_warning_levels="15 25"<br><table border="1"> <tr> <td>0</td> <td>Zero means no limit.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table> | 0 | Zero means no limit. | Range |          |
| 0  | Zero means no limit.  |   |                      |       |          |
| Range  |   |   |                      |       |          |

Table 188: Information table for data usage commands

### 45.3.1 Configuring data usage using command line

Data usage is configured under the **procrustes** package `/etc/config/procrustes`.

By default, all limit instances are named 'limit', and are identified by `@limit` followed by the limit position in the package as a number. For example, for the first limit in the package using UCI:

```
procrustes.@limit[0]=limit
procrustes.@limit[0].enabled=1
```

Or using package options, enter:

```
config limit
    option enabled '1'
```

However, to better identify instances, it is recommended to give the limit instance a name. For example, create a limit instance named MOBILE1.

To define a named limit instance using UCI, enter:

```
procrustes.@limit[0]=wan
procrustes.wan.enabled=1
```

To define a named limit instance using package options, enter:

```
config limit 'wan'
    option enabled '1'
```

The following examples show two limit groups wan and lan.

### 45.3.2 Procrustes using UCI

```
root@VA_router:~# uci show procrustes
procrustes.lan=limit
procrustes.lan.enabled=1
procrustes.lan.interfaces=LAN1
procrustes.lan.billing_period_start_day=1
procrustes.lan.monthly_data_limit=30
procrustes.lan.monthly_warning_levels=15 25
procrustes.wan=limit
procrustes.wan.enabled=1
procrustes.wan.interfaces=MOBILE1
procrustes.wan.billing_period_start_day=1
procrustes.wan.monthly_data_limit=30
procrustes.wan.monthly_warning_levels=15 25
```

### 45.3.3 Procrustes using package options

```

root@VA_router:~# uci export procrustes
package procrustes

config limit 'lan'
    option enabled '1'
    option interfaces 'LAN1'
    option billing_period_start_day '1'
    option monthly_data_limit '30'
    option monthly_warning_levels '15 25'

config limit 'wan'
    option enabled '1'
    option interfaces 'MOBILE1'
    option billing_period_start_day '1'
    option monthly_data_limit '30'
    option monthly_warning_levels '15 25'

```

## 45.4 Data usage status

Select **Status -> Overview**. The Status page appears.

To check current data usage, scroll to **Network -> Data Usage (MiB)** row.

Data usage is presented as progress bar.



Figure 253: The data usage status progress bar

## 45.5 Data usage diagnostics

### 45.5.1 Syslog events

The following events can be generated in logs by the data usage feature:

| Severity | Tag        | Text  |
|----------|------------|---|
| NOTICE   | procrustes | <if_group_name>: using counter 1404674 saved on 2017-09-30 16:26:57 |
| NOTICE   | procrustes | <if_group_name>: warning level 2097152 is reached                   |
| WARNING  | procrustes | <if_group_name>: hard limit 10485760 is reached                     |

|         |            |  |
|---------|------------|--|
| NOTICE  | procrustes | Data limit on SIM <iccid> exceeded and sim will be banned until the next month |
| ERROR   | procrustes | Could not get iccid for <ifname>   |
| DEBUG   | procrustes | Interface <ifname> is not up   |
| WARNING | procrustes | network.<ifname>.ifname is not defined   |
| NOTICE  | procrustes | <ifname>: reached billing start. Resetting...                                  |
| DEBUG   | procrustes | Saving current limit values  |
| NOTICE  | procrustes | <if_group_name>: not enabled   |
| WARNING | procrustes | <if_group_name>: defines no interfaces   |
| DEBUG   | procrustes | <if_group_name>: sim interface <ifname>  |
| ERROR   | procrustes | Daemonization failed   |
| ERROR   | procrustes | another procrustes is running. Exiting...                                      |
| NOTICE  | procrustes | No limits defined. Exiting...  |
| ERROR   | mobile     | SIM <iccid> is blacklisted, not establishing connection                        |

## 45.5.2 Viewing data usage

The router has monitoring application named **procrustatus.lua** that can be used for viewing data usage.

This application displays data statistics used for different interface groups, percentage of time left to next billing period start and percentage of data left for use before the interface will be shut down.

To view the application, enter the command `procrustes.lua`

```
root@VA_router:~# procrustatus.lua
  name      current/      max  time left  data left
  lan:      1404674/  10485760    1.03%    86.60%
  wan:      433436/   1048576    1.03%    58.66%
```

Alternatively, to check total data usage, enter:

```
root@VA_router:~# cat /var/state/procrustes
procrustes.lan.total_bytes=215780
procrustes.wan.total_bytes=433436
```

## 45.5.3 Additional debugging commands

Additional useful debug commands via the command line are described in the table below.

| Diagnostic Command                              | Description                             |
|---|---|
| <code>logread   grep procrustes</code>          | Shows logs related to "procrustes" only |
| <code>ls /root/procrustes/sim_blacklist/</code> | Shows list of blacklisted SIM iccids    |

## 46 Configuring terminal server

### 46.1 Overview

Terminal server is a background application whose main task is to forward data between TCP connections or UDP streams and asynchronous or synchronous serial ports.

The terminal server application serves up to four sessions simultaneously, one for each serial port, depending on the device. Each terminal server session has an IP endpoint and an associated specific serial port.

You can configure the IP endpoint of each terminal server session to be a:

- TCP server: each session is listening on a unique port.
- TCP client: the terminal server makes a TCP connection to external TCP server.
- UDP endpoint: the terminal server forwards data between a UDP stream and a serial port.

### 46.2 Configuration packages used

| Package | Sections |
|---------|----------|
| tservd  | main     |
|         | port     |

### 46.3 Configuring terminal server using the web interface

In the top menu, select **Services -> Terminal Server**. The Terminal Server Configuration page appears. You must configure two main sections:

- Main Settings are to enable the terminal server, syslog settings, and to enable log setting.
- The Port Settings section is for general port settings, serial settings such as port mode, port speed, parity stop bit and so on; and finally, network settings to configure the network side of the terminal server.

#### 46.3.1 Configure main settings

**Terminal Server**  
Configuration of the VA Terminal Server.

Main Settings

Enable  [enable terminal server](#)

Debug Enable  [enables detailed debug logging \(state transitions, data transfer etc\)](#)

Syslog severity

Log RX-TX  [enable logging data transfers](#)

**Figure 254: The terminal server main settings page**

| Web Field/UCI/Package Option   | Description  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
|--|--|---|-----------|---|----------|---|----------|---|-------|---|---------|---|--------|---|---------------|---|-------|
| Web: Enable<br>UCI: tserverd.main.enable<br>Opt: enable                            | Enables Terminal Server on the router.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0 | Disabled. | 1 | Enabled. |   |          |   |       |   |         |   |        |   |               |   |       |
| 0  | Disabled.  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 1  | Enabled.   |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| Web: Debug Enable<br>UCI: tserverd.main.debug_ev_enable<br>Opt: debug_ev_enable    | Enables detailed debug logging.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0 | Disabled. | 1 | Enabled. |   |          |   |       |   |         |   |        |   |               |   |       |
| 0  | Disabled.  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 1  | Enabled.   |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| Web: Syslog severity<br>UCI: tserverd.main.log_severity<br>Opt: log_severity       | Determines the syslog level. Events up to this priority will be logged.<br><table border="1"> <tr> <td>0</td> <td>Emergency</td> </tr> <tr> <td>1</td> <td>Alert</td> </tr> <tr> <td>2</td> <td>Critical</td> </tr> <tr> <td>3</td> <td>Error</td> </tr> <tr> <td>4</td> <td>Warning</td> </tr> <tr> <td>5</td> <td>Notice</td> </tr> <tr> <td>6</td> <td>Informational</td> </tr> <tr> <td>7</td> <td>Debug</td> </tr> </table> | 0 | Emergency | 1 | Alert    | 2 | Critical | 3 | Error | 4 | Warning | 5 | Notice | 6 | Informational | 7 | Debug |
| 0  | Emergency  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 1  | Alert  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 2  | Critical   |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 3  | Error  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 4  | Warning  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 5  | Notice   |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 6  | Informational  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 7  | Debug  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| Web: Log RX-TX<br>UCI: tserverd.main.debug_rx_tx_enable<br>Opt: debug_rx_tx_enable | Enables logging data transfers.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0 | Disabled. | 1 | Enabled. |   |          |   |       |   |         |   |        |   |               |   |       |
| 0  | Disabled.  |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 1  | Enabled.   |   |           |   |          |   |          |   |       |   |         |   |        |   |               |   |       |

Table 189: Information table for main settings

## 46.3.2 Configure port settings

The Port Settings section is divided into 3 sub-sections:

- General
- Serial
- Network

### 46.3.2.1 Port settings: general section

In this section you can configure general port settings. The settings are usually the same for the central and the remote site.

Port Settings

**PORT1**

General Serial Network

Enable  enable port

Network Forwarding Buffer Size  Forwarding buffer size (serial to network)

Network Forwarding Timeout (ms)  Forwarding timeout in milliseconds (serial to network)

Network Forwarding timer mode  Forwarding timer mode (serial to network)

Serial Forwarding Buffer Size  Forwarding buffer size (network to serial)

Serial Forwarding Timeout (ms)  Forwarding timeout in milliseconds (network to serial)

Serial Forwarding timer mode  Forwarding timer mode (network to serial)

Proxy mode  enable proxy mode

Disable remote client's local echo (Telnet option)

Telnet COM port control (RFC2217)

Enable HDLC Pseudowire over UDP (RFC4618)

Serial receive debug log size  bytes (0=disable)

Serial transmit debug log size  bytes (0=disable)

Figure 255: The general tab fields

| Web Field/UCI/Package Option   | Description  |      |  |       |                                |
|--|--|------|--|-------|--------------------------------|
| Web: Enable<br>UCI: tserverd.@port[0].enable<br>Opt: enable  | Enables terminal server port.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0    | Disabled.                                  | 1     | Enabled.                       |
| 0  | Disabled.  |      |  |       |                                |
| 1  | Enabled.   |      |  |       |                                |
| Web: Network Forwarding Buffer Size<br>UCI: tserverd.@port[0].fwd_buffer_size<br>Opt: fwd_buffer_size  | Forwarding buffer size in bytes (serial to network).<br><table border="1"> <tr> <td>256</td> <td>256 bytes</td> </tr> <tr> <td>Range</td> <td>0-2048</td> </tr> </table>   | 256  | 256 bytes                                  | Range | 0-2048                         |
| 256  | 256 bytes  |      |  |       |                                |
| Range  | 0-2048   |      |  |       |                                |
| Web: Network Forwarding Timeout(ms)<br>UCI: tserverd.@port[0].fwd_timeout<br>Opt: fwd_timeout          | Forwarding timeout in milliseconds (serial to network).<br><table border="1"> <tr> <td>30</td> <td>30 ms</td> </tr> <tr> <td>Range</td> <td>0-10000</td> </tr> </table>  | 30   | 30 ms                                      | Range | 0-10000                        |
| 30   | 30 ms  |      |  |       |                                |
| Range  | 0-10000  |      |  |       |                                |
| Web: Network Forwarding Timer Mode<br>UCI: tserverd.@port[0].fwd_timer_mode<br>Opt: fwd_timer_mode     | Forwarding timer mode (serial to network).<br><table border="1"> <tr> <td>Idle</td> <td>Timer is re-started on each received data.</td> </tr> <tr> <td>Aging</td> <td>Timer started on the first Rx.</td> </tr> </table>                   | Idle | Timer is re-started on each received data. | Aging | Timer started on the first Rx. |
| Idle   | Timer is re-started on each received data.   |      |  |       |                                |
| Aging  | Timer started on the first Rx.   |      |  |       |                                |
| Web: Serial Forwarding Buffer Size<br>UCI: tserverd.@port[0].sfwd_buffer_size<br>Opt: sfwd_buffer_size | Forwarding buffer size in bytes (network to serial).<br>Set to <b>0</b> to use maximum possible network Rx buffer size.<br><table border="1"> <tr> <td>0</td> <td>2048 bytes</td> </tr> <tr> <td>Range</td> <td>0-2048</td> </tr> </table> | 0    | 2048 bytes                                 | Range | 0-2048                         |
| 0  | 2048 bytes   |      |  |       |                                |
| Range  | 0-2048   |      |  |       |                                |
| Web: Serial Forwarding Timeout (ms)<br>UCI: tserverd.@port[0].sfwd_timeout<br>Opt: sfwd_timeout        | Forwarding timeout in milliseconds (network to serial).<br>Set to <b>0</b> to forward to serial immediately.<br><table border="1"> <tr> <td>20</td> <td>20 ms</td> </tr> <tr> <td>Range</td> <td>0-10000</td> </tr> </table>               | 20   | 20 ms                                      | Range | 0-10000                        |
| 20   | 20 ms  |      |  |       |                                |
| Range  | 0-10000  |      |  |       |                                |



|  |   |      |  |       |                                |
|--|---|------|--|-------|--------------------------------|
| <p>Web: Serial Forwarding Timer Mode<br/>UCI: tserverd.@port[0].sfwd_timer_mode<br/>Opt: sfwd_timer_mode</p>                 | <p>Forwarding timer mode (network to serial).</p> <table border="1" data-bbox="676 226 1396 300"> <tr> <td data-bbox="676 226 799 264">Idle</td> <td data-bbox="804 226 1396 264">Timer is restarted on each received data</td> </tr> <tr> <td data-bbox="676 264 799 300">Aging</td> <td data-bbox="804 264 1396 300">Timer started on the first Rx.</td> </tr> </table>   | Idle | Timer is restarted on each received data | Aging | Timer started on the first Rx. |
| Idle   | Timer is restarted on each received data  |      |  |       |                                |
| Aging  | Timer started on the first Rx.  |      |  |       |                                |
| <p>Web: Proxy Mode<br/>UCI: tserverd.@port[0].proxy_mode<br/>Opt: proxy_mode</p>   | <p>Defines if a special proxy mode should be configured to allow 'hijacking' of the terminal server. It allows a connection to be made from a remote location and redirect terminal server data temporarily for troubleshooting.</p> <p>When enabled, a TCP proxy server is started which listens for an incoming TCP connection from a remote peer. Once an incoming new TCP connection on the proxy server TCP port is accepted: The existing terminal server TCP client connection is disconnected.</p> <p>The terminal server automatically reconnects the TCP client side but this time to the local loopback address 127.0.0.1 and to the local proxies TCP port number.</p> <p>When the proxy server has both local and remote TCP sessions connected it simply forwards the data between the two connections, taking into account the flow control.</p> <p>When either side TCP socket closes, the main terminal server client reconnects to the normal IP destination and the server proxy returns to listening for another connection from the far end.</p> <table border="1" data-bbox="676 837 1396 909"> <tr> <td data-bbox="676 837 799 875">0</td> <td data-bbox="804 837 1396 875">Disabled.</td> </tr> <tr> <td data-bbox="676 875 799 909">1</td> <td data-bbox="804 875 1396 909">Enabled.</td> </tr> </table> | 0    | Disabled.                                | 1     | Enabled.                       |
| 0  | Disabled.   |      |  |       |                                |
| 1  | Enabled.  |      |  |       |                                |
| <p>Web: Disable Remote Client's Local Echo (Telnet option)<br/>UCI: tserverd.@port[0].disable_echo<br/>Opt: disable_echo</p> | <p>Set to <b>1</b> to send IAC WILL ECHO Telnet option to remote client forcing it to disable local echo. For server mode only.</p> <table border="1" data-bbox="676 969 1396 1043"> <tr> <td data-bbox="676 969 799 1008">0</td> <td data-bbox="804 969 1396 1008">Disabled.</td> </tr> <tr> <td data-bbox="676 1008 799 1043">1</td> <td data-bbox="804 1008 1396 1043">Enabled.</td> </tr> </table>  | 0    | Disabled.                                | 1     | Enabled.                       |
| 0  | Disabled.   |      |  |       |                                |
| 1  | Enabled.  |      |  |       |                                |
| <p>Web: Telnet COM Port Control<br/>UCI: tserverd.@port[0].com_port_control<br/>Opt: com_port_control</p>                    | <p>Set to <b>1</b> to enable support for Telnet COM port control (RFC2217).</p> <table border="1" data-bbox="676 1104 1396 1178"> <tr> <td data-bbox="676 1104 799 1142">0</td> <td data-bbox="804 1104 1396 1142">Disabled.</td> </tr> <tr> <td data-bbox="676 1142 799 1178">1</td> <td data-bbox="804 1142 1396 1178">Enabled.</td> </tr> </table>   | 0    | Disabled.                                | 1     | Enabled.                       |
| 0  | Disabled.   |      |  |       |                                |
| 1  | Enabled.  |      |  |       |                                |
| <p>Web: Enable HDLC Pseudowire over UDP (RFC4618)<br/>UCI: tserverd.@port[0].hdlc_pw_enabled<br/>Opt: hdlc_pw_enabled</p>    | <p>Set to <b>1</b> to enable HDLC pseudowire over UDP support based on RFC4618. Requires Transport Mode (udpmode) to be enabled.</p> <table border="1" data-bbox="676 1238 1396 1312"> <tr> <td data-bbox="676 1238 799 1276">0</td> <td data-bbox="804 1238 1396 1276">Disabled.</td> </tr> <tr> <td data-bbox="676 1276 799 1312">1</td> <td data-bbox="804 1276 1396 1312">Enabled.</td> </tr> </table>  | 0    | Disabled.                                | 1     | Enabled.                       |
| 0  | Disabled.   |      |  |       |                                |
| 1  | Enabled.  |      |  |       |                                |
| <p>Web: Serial Receive Debug Log Size<br/>UCI: tserverd.@port[0].serialRxLogSize<br/>Opt: serialRxLogSize</p>                | <p>Configures serial receive log size in bytes and enables receive data logging.</p> <table border="1" data-bbox="676 1373 1331 1447"> <tr> <td data-bbox="676 1373 799 1411">0</td> <td data-bbox="804 1373 1331 1411">Disabled.</td> </tr> <tr> <td data-bbox="676 1411 799 1447">1</td> <td data-bbox="804 1411 1331 1447">Enabled.</td> </tr> </table>  | 0    | Disabled.                                | 1     | Enabled.                       |
| 0  | Disabled.   |      |  |       |                                |
| 1  | Enabled.  |      |  |       |                                |
| <p>Web: Serial Transmit Debug Log Size<br/>UCI: tserverd.@port[0].serialTxLogSize<br/>Opt: serialTxLogSize</p>               | <p>Configures serial transmit log size in bytes and enables transmit data logging.</p> <table border="1" data-bbox="676 1507 1331 1581"> <tr> <td data-bbox="676 1507 799 1545">0</td> <td data-bbox="804 1507 1331 1545">Disabled.</td> </tr> <tr> <td data-bbox="676 1545 799 1581">1</td> <td data-bbox="804 1545 1331 1581">Enabled.</td> </tr> </table>  | 0    | Disabled.                                | 1     | Enabled.                       |
| 0  | Disabled.   |      |  |       |                                |
| 1  | Enabled.  |      |  |       |                                |

**Table 190: Information table for port settings section**

### 46.3.2.2 Port settings: serial section

In this section you can configure serial interface settings, such as port mode, port speed, parity stop bit and so on.

**Note:**

- The displayed settings vary depending on options selected.
- DTR <--> DSR signalling is not available on GW2028 router models.

The figure below shows the options available if you have selected RS232 mode.

**PORT1**

General Serial Network

Device: /dev/ttySC0 serial device name

Portmode: RS-232 serial interface mode

GPIO Control:  use GPIO pin to set the port mode

Speed (bps): 19200 asynchronous baud rate

Word size: 8 serial device word size in bits

Parity: Even serial device parity in bits

Stop bits: 1 serial device number of stop bits

Flow Control: NONE serial device flow control type

Auto RTS Invert:  invert RTS in auto-RTS mode

Keep serial port always open:  keep serial port always activated

RS232 Half Duplex:  enable RS232 half duplex mode for interfacing to external V.23 modem

RTS timeout: 30 RS232 half duplex mode RTS timeout in milliseconds

POST RTS timeout: 20 RS232 half duplex mode Post RTS timeout in milliseconds

Serial device idle timeout: 0 Serial device idle timeout in seconds

**Figure 256: The serial section fields (port mode RS232)**

The figure below shows the options available if you have selected RS485 mode.

**PORT2**

General Serial Network

Device: /dev/ttySC1 serial device name

Portmode: RS-485 Full Duplex serial interface mode

GPIO Control:  use GPIO pin to set the port mode

Speed (bps): 19200 asynchronous baud rate

Word size: 8 serial device word size in bits

Parity: None serial device parity in bits

Stop bits: 1 serial device number of stop bits

Flow Control: RTS/CTS serial device flow control type

RS485 termination:  enable RS485 line termination

Auto RTS Invert:  invert RTS in auto-RTS mode

Keep serial port always open:  keep serial port always activated

RTS timeout: 30 RS232 half duplex mode RTS timeout in milliseconds

POST RTS timeout: 20 RS232 half duplex mode Post RTS timeout in milliseconds

Serial device idle timeout: 0 Serial device idle timeout in seconds

**Figure 257: The serial section fields (port mode RS485)**

The figure below shows the options available if you have selected X.21 mode.

The screenshot shows the 'PORT1' configuration page with the 'Serial' tab selected. The 'Portmode' is set to 'X.21'. The 'Device' is '/dev/ttySC0'. The 'Keep serial port always open' checkbox is checked. The 'Synchronous mode' is 'HDLC'. The 'Synchronous rate' is '64000'. The 'DTR control mode' and 'RTS control mode' are both set to 'auto'. The 'RX data delay' and 'TX data delay' are both set to '0'. There are several checkboxes for 'Dual X.21 card' options, all of which are unchecked. A 'Delete' button is visible in the bottom right corner.

Figure 258: The serial section fields (port mode X.21)

| Web Field/UCI/Package Option                                       | Description   |             |               |             |  |             |                                |             |                                    |     |                                    |
|--|---|-------------|---------------|-------------|--|-------------|--------------------------------|-------------|------------------------------------|-----|------------------------------------|
| Web: Device<br>UCI: tservd.@port[0].devName<br>Opt: devName        | Serial device name.<br><table border="1"> <tr> <td>/dev/ttySC0</td> <td>serial port 1</td> </tr> <tr> <td>/dev/ttySC1</td> <td>serial port 2</td> </tr> <tr> <td>/dev/ttySC2</td> <td>serial port 3</td> </tr> <tr> <td>/dev/ttySC3</td> <td>serial port 4</td> </tr> </table>  | /dev/ttySC0 | serial port 1 | /dev/ttySC1 | serial port 2  | /dev/ttySC2 | serial port 3                  | /dev/ttySC3 | serial port 4                      |     |                                    |
| /dev/ttySC0  | serial port 1   |             |               |             |  |             |                                |             |                                    |     |                                    |
| /dev/ttySC1  | serial port 2   |             |               |             |  |             |                                |             |                                    |     |                                    |
| /dev/ttySC2  | serial port 3   |             |               |             |  |             |                                |             |                                    |     |                                    |
| /dev/ttySC3  | serial port 4   |             |               |             |  |             |                                |             |                                    |     |                                    |
| Web: Port mode<br>UCI: tservd.@port[0].port_mode<br>Opt: port_mode | Sets the serial interface mode.<br><table border="1"> <tr> <td>rs232</td> <td>RS232 mode.</td> </tr> <tr> <td>rs485hdx</td> <td>RS485 2-wire half-duplex mode in which the transmitter drives the RTS.</td> </tr> <tr> <td>rs485fdx</td> <td>RS485 4-wire full-duplex mode.</td> </tr> <tr> <td>v23</td> <td>Uses V.23 leased line card driver.</td> </tr> <tr> <td>x21</td> <td>Uses USB serial card in sync mode.</td> </tr> </table> | rs232       | RS232 mode.   | rs485hdx    | RS485 2-wire half-duplex mode in which the transmitter drives the RTS. | rs485fdx    | RS485 4-wire full-duplex mode. | v23         | Uses V.23 leased line card driver. | x21 | Uses USB serial card in sync mode. |
| rs232  | RS232 mode.   |             |               |             |  |             |                                |             |                                    |     |                                    |
| rs485hdx   | RS485 2-wire half-duplex mode in which the transmitter drives the RTS.  |             |               |             |  |             |                                |             |                                    |     |                                    |
| rs485fdx   | RS485 4-wire full-duplex mode.  |             |               |             |  |             |                                |             |                                    |     |                                    |
| v23  | Uses V.23 leased line card driver.  |             |               |             |  |             |                                |             |                                    |     |                                    |
| x21  | Uses USB serial card in sync mode.  |             |               |             |  |             |                                |             |                                    |     |                                    |

|   |  |      |   |       |  |   |          |   |       |
|---|--|------|---|-------|--|---|----------|---|-------|
| <p>Web: GPIO Control<br/>UCI: tservd.@port[1].serial_mode)gpio_control<br/>Opt: serial_mode_gpio_control</p>  | <p>Enables or disables software control of the port mode between RS232 and RS485. Applies only to port 1 (ttySC1) and not to port 0.<br/><b>Note:</b> the port mode is set with the option port mode described above.</p> <table border="1" data-bbox="683 338 1390 521"> <tr> <td data-bbox="683 338 858 434">0</td> <td data-bbox="858 338 1390 434">Port mode is configured by hardware settings and is not user configurable.<br/>Set to <b>0</b> for port 0.</td> </tr> <tr> <td data-bbox="683 434 858 521">1</td> <td data-bbox="858 434 1390 521">Enabled. Port mode is configurable by software settings. This is applicable to serial port 1 on devices that are capable of RS485.</td> </tr> </table> | 0    | Port mode is configured by hardware settings and is not user configurable.<br>Set to <b>0</b> for port 0. | 1     | Enabled. Port mode is configurable by software settings. This is applicable to serial port 1 on devices that are capable of RS485. |   |          |   |       |
| 0   | Port mode is configured by hardware settings and is not user configurable.<br>Set to <b>0</b> for port 0.  |      |   |       |  |   |          |   |       |
| 1   | Enabled. Port mode is configurable by software settings. This is applicable to serial port 1 on devices that are capable of RS485.   |      |   |       |  |   |          |   |       |
| <p>Web: Speed (bps)<br/>UCI: tservd.@port[0].speed<br/>Opt: speed</p>   | <p>Serial device speed in baud (bps).</p> <table border="1" data-bbox="683 555 1390 680"> <tr> <td data-bbox="683 555 858 591">9600</td> <td data-bbox="858 555 1390 591"></td> </tr> <tr> <td data-bbox="683 591 858 680">Range</td> <td data-bbox="858 591 1390 680">115200; 57600; 38400; 19200; 9600; 4800; 2400; 1800; 1200; 600; 300; 200; 150; 134; 110; 75; 50</td> </tr> </table>   | 9600 |   | Range | 115200; 57600; 38400; 19200; 9600; 4800; 2400; 1800; 1200; 600; 300; 200; 150; 134; 110; 75; 50                                    |   |          |   |       |
| 9600  |  |      |   |       |  |   |          |   |       |
| Range   | 115200; 57600; 38400; 19200; 9600; 4800; 2400; 1800; 1200; 600; 300; 200; 150; 134; 110; 75; 50  |      |   |       |  |   |          |   |       |
| <p>Web: Word size<br/>UCI: tservd.@port[0].wsize<br/>Opt: wsize</p>   | <p>Serial device word size.</p> <table border="1" data-bbox="683 714 1390 786"> <tr> <td data-bbox="683 714 858 750">8</td> <td data-bbox="858 714 1390 750"></td> </tr> <tr> <td data-bbox="683 750 858 786">Range</td> <td data-bbox="858 750 1390 786">5-8</td> </tr> </table>  | 8    |   | Range | 5-8  |   |          |   |       |
| 8   |  |      |   |       |  |   |          |   |       |
| Range   | 5-8  |      |   |       |  |   |          |   |       |
| <p>Web: Parity<br/>UCI: tservd.@port[0].parity<br/>Opt: parity</p>  | <p>Serial device parity.</p> <table border="1" data-bbox="683 819 1390 965"> <tr> <td data-bbox="683 819 858 855">0</td> <td data-bbox="858 819 1390 855">None</td> </tr> <tr> <td data-bbox="683 855 858 891">1</td> <td data-bbox="858 855 1390 891">Even</td> </tr> <tr> <td data-bbox="683 891 858 927">2</td> <td data-bbox="858 891 1390 927">Odd</td> </tr> <tr> <td data-bbox="683 927 858 965">3</td> <td data-bbox="858 927 1390 965">Space</td> </tr> </table>  | 0    | None  | 1     | Even   | 2 | Odd      | 3 | Space |
| 0   | None   |      |   |       |  |   |          |   |       |
| 1   | Even   |      |   |       |  |   |          |   |       |
| 2   | Odd  |      |   |       |  |   |          |   |       |
| 3   | Space  |      |   |       |  |   |          |   |       |
| <p>Web: Stop Bits<br/>UCI: tservd.@port[0].stops<br/>Opt: stops</p>   | <p>Serial device number of stop bits.</p> <table border="1" data-bbox="683 999 1390 1070"> <tr> <td data-bbox="683 999 858 1034">1</td> <td data-bbox="858 999 1390 1034"></td> </tr> <tr> <td data-bbox="683 1034 858 1070">Range</td> <td data-bbox="858 1034 1390 1070">1-2</td> </tr> </table>   | 1    |   | Range | 1-2  |   |          |   |       |
| 1   |  |      |   |       |  |   |          |   |       |
| Range   | 1-2  |      |   |       |  |   |          |   |       |
| <p>Web: Flow Control<br/>UCI: tservd.@port[0].fc_mode<br/>Opt: fc_mode</p>                                    | <p>Serial flow control mode.</p> <table border="1" data-bbox="683 1104 1390 1211"> <tr> <td data-bbox="683 1104 858 1140">0</td> <td data-bbox="858 1104 1390 1140">None</td> </tr> <tr> <td data-bbox="683 1140 858 1176">1</td> <td data-bbox="858 1140 1390 1176">RTS/CTS</td> </tr> <tr> <td data-bbox="683 1176 858 1211">2</td> <td data-bbox="858 1176 1390 1211">XON/XOFF</td> </tr> </table>  | 0    | None  | 1     | RTS/CTS  | 2 | XON/XOFF |   |       |
| 0   | None   |      |   |       |  |   |          |   |       |
| 1   | RTS/CTS  |      |   |       |  |   |          |   |       |
| 2   | XON/XOFF   |      |   |       |  |   |          |   |       |
| <p>Web: RS485 Termination<br/>UCI: tservd.@port[0].rs485_line_termination<br/>Opt: rs485_line_termination</p> | <p>Enables or disables RS485 termination. Applies only if port mode is set to RS485.</p> <table border="1" data-bbox="683 1267 1390 1346"> <tr> <td data-bbox="683 1267 858 1303">0</td> <td data-bbox="858 1267 1390 1303">Disabled.</td> </tr> <tr> <td data-bbox="683 1303 858 1346">1</td> <td data-bbox="858 1303 1390 1346">Enabled.</td> </tr> </table>   | 0    | Disabled.   | 1     | Enabled.   |   |          |   |       |
| 0   | Disabled.  |      |   |       |  |   |          |   |       |
| 1   | Enabled.   |      |   |       |  |   |          |   |       |
| <p>Web: Auto RTS Invert<br/>UCI: tservd.@port[0].rtsinvert<br/>Opt: rtsinvert</p>                             | <p>Invert RTS in auto-RTS mode, if port mode is set to RS485.</p> <table border="1" data-bbox="683 1379 1390 1451"> <tr> <td data-bbox="683 1379 858 1415">0</td> <td data-bbox="858 1379 1390 1415">Disabled.</td> </tr> <tr> <td data-bbox="683 1415 858 1451">1</td> <td data-bbox="858 1415 1390 1451">Enabled.</td> </tr> </table>  | 0    | Disabled.   | 1     | Enabled.   |   |          |   |       |
| 0   | Disabled.  |      |   |       |  |   |          |   |       |
| 1   | Enabled.   |      |   |       |  |   |          |   |       |
| <p>Web: Keep Serial Port Always Open<br/>UCI: tservd.@port[0].tty_always_open<br/>Opt: tty_always_open</p>    | <p>Keep serial port always open.</p> <table border="1" data-bbox="683 1485 1390 1556"> <tr> <td data-bbox="683 1485 858 1520">0</td> <td data-bbox="858 1485 1390 1520">Disabled.</td> </tr> <tr> <td data-bbox="683 1520 858 1556">1</td> <td data-bbox="858 1520 1390 1556">Enabled.</td> </tr> </table>   | 0    | Disabled.   | 1     | Enabled.   |   |          |   |       |
| 0   | Disabled.  |      |   |       |  |   |          |   |       |
| 1   | Enabled.   |      |   |       |  |   |          |   |       |
| <p>Web: RS232 Half Duplex<br/>UCI: tservd.@port[0].hd_mode<br/>Opt: hd_mode</p>                               | <p>Defines whether to enable special mode in the asynchronous serial driver for communication to an externally connected V.23 half-duplex modem. <b>Note:</b> this setting does not enable half-duplex mode in the serial hardware of the router.</p> <table border="1" data-bbox="683 1664 1390 1742"> <tr> <td data-bbox="683 1664 858 1700">0</td> <td data-bbox="858 1664 1390 1700">Full-duplex mode.</td> </tr> <tr> <td data-bbox="683 1700 858 1742">1</td> <td data-bbox="858 1700 1390 1742">Half-duplex mode.</td> </tr> </table>   | 0    | Full-duplex mode.   | 1     | Half-duplex mode.  |   |          |   |       |
| 0   | Full-duplex mode.  |      |   |       |  |   |          |   |       |
| 1   | Half-duplex mode.  |      |   |       |  |   |          |   |       |
| <p>Web: RTS Timeout<br/>UCI: tservd.@port[0].rts_timeout<br/>Opt: rts_timeout</p>                             | <p>In RS232 half-duplex mode, time in milliseconds between raising RTS and enabling the transmitter. For use with an externally connected V.23 modem.</p> <table border="1" data-bbox="683 1821 1390 1897"> <tr> <td data-bbox="683 1821 858 1856">30</td> <td data-bbox="858 1821 1390 1856">30ms</td> </tr> <tr> <td data-bbox="683 1856 858 1897">Range</td> <td data-bbox="858 1856 1390 1897"></td> </tr> </table>  | 30   | 30ms  | Range |  |   |          |   |       |
| 30  | 30ms   |      |   |       |  |   |          |   |       |
| Range   |  |      |   |       |  |   |          |   |       |

|   |  |       |   |        |   |     |                 |     |                                    |      |   |
|---|--|-------|---|--------|---|-----|-----------------|-----|------------------------------------|------|---|
| <p>Web: POST RTS Timeout<br/>UCI: tservd.@port[0].post_rts_timeout<br/>Opt: post_rts_timeout</p>        | <p>In RS232 half-duplex mode, sets the time in milliseconds between dropping RTS (transmission finished) and enabling the receiver. For use with externally connected V.23 modem.</p> <table border="1"> <tr> <td>20</td> <td>20 ms</td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>  | 20    | 20 ms   | Range  |   |     |                 |     |                                    |      |   |
| 20  | 20 ms  |       |   |        |   |     |                 |     |                                    |      |   |
| Range   |  |       |   |        |   |     |                 |     |                                    |      |   |
| <p>Web: Synchronous mode<br/>UCI: tservd.@port[0].sync mode<br/>Opt: sync mode</p>                      | <p>Defines synchronous frame mode. This setting is only displayed if an Atmel USB serial card is enabled.</p> <table border="1"> <tr> <td>hdlc</td> <td>HDLC frame mode.</td> </tr> <tr> <td>transp</td> <td>Transparent mode.</td> </tr> </table>   | hdlc  | HDLC frame mode.  | transp | Transparent mode.   |     |                 |     |                                    |      |   |
| hdlc  | HDLC frame mode.   |       |   |        |   |     |                 |     |                                    |      |   |
| transp  | Transparent mode.  |       |   |        |   |     |                 |     |                                    |      |   |
| <p>Web: Use CRC32<br/>UCI: tservd.@port[0].sync_crc32<br/>Opt: sync_crc32</p>                           | <p>Defines whether to use CRC32 or CRC16 in HDLC mode. This setting is only displayed if an Atmel USB serial card is enabled.</p> <table border="1"> <tr> <td>0</td> <td>Use CRC16.</td> </tr> <tr> <td>1</td> <td>Use CRC32.</td> </tr> </table>  | 0     | Use CRC16.  | 1      | Use CRC32.  |     |                 |     |                                    |      |   |
| 0   | Use CRC16.   |       |   |        |   |     |                 |     |                                    |      |   |
| 1   | Use CRC32.   |       |   |        |   |     |                 |     |                                    |      |   |
| <p>Web: DTR control mode<br/>UCI: tservd.@port[0].dtr_control_mode<br/>Opt: dtr_control_mode</p>        | <p>Defines DTR line control modes. This setting is only displayed if an Atmel USB serial card is enabled and port mode is X21.</p> <table border="1"> <tr> <td>auto</td> <td>DTR set to <b>On</b> when port is open; <b>Off</b> when the port is closed.</td> </tr> <tr> <td>on</td> <td>DTR always on.</td> </tr> <tr> <td>off</td> <td>DTR always off.</td> </tr> <tr> <td>app</td> <td>DTR controlled by the application.</td> </tr> <tr> <td>ontx</td> <td>In HDLC mode DTR is on during frame transmission.</td> </tr> </table> | auto  | DTR set to <b>On</b> when port is open; <b>Off</b> when the port is closed. | on     | DTR always on.  | off | DTR always off. | app | DTR controlled by the application. | ontx | In HDLC mode DTR is on during frame transmission. |
| auto  | DTR set to <b>On</b> when port is open; <b>Off</b> when the port is closed.  |       |   |        |   |     |                 |     |                                    |      |   |
| on  | DTR always on.   |       |   |        |   |     |                 |     |                                    |      |   |
| off   | DTR always off.  |       |   |        |   |     |                 |     |                                    |      |   |
| app   | DTR controlled by the application.   |       |   |        |   |     |                 |     |                                    |      |   |
| ontx  | In HDLC mode DTR is on during frame transmission.  |       |   |        |   |     |                 |     |                                    |      |   |
| <p>Web: RTS control mode<br/>UCI: tservd.@port[0].rts_control_mode<br/>Opt: rts_control_mode</p>        | <p>Defines RTS line control modes. Only displayed if an Atmel USB serial card is enabled and port mode is X21.</p> <table border="1"> <tr> <td>auto</td> <td>RTS set to <b>On</b> when port is open; <b>Off</b> when the port is closed.</td> </tr> <tr> <td>on</td> <td>RTS always on.</td> </tr> <tr> <td>off</td> <td>RTS always off.</td> </tr> <tr> <td>app</td> <td>RTS controlled by the application.</td> </tr> <tr> <td>ontx</td> <td>In HDLC mode RTS is on during frame transmission.</td> </tr> </table>                 | auto  | RTS set to <b>On</b> when port is open; <b>Off</b> when the port is closed. | on     | RTS always on.  | off | RTS always off. | app | RTS controlled by the application. | ontx | In HDLC mode RTS is on during frame transmission. |
| auto  | RTS set to <b>On</b> when port is open; <b>Off</b> when the port is closed.  |       |   |        |   |     |                 |     |                                    |      |   |
| on  | RTS always on.   |       |   |        |   |     |                 |     |                                    |      |   |
| off   | RTS always off.  |       |   |        |   |     |                 |     |                                    |      |   |
| app   | RTS controlled by the application.   |       |   |        |   |     |                 |     |                                    |      |   |
| ontx  | In HDLC mode RTS is on during frame transmission.  |       |   |        |   |     |                 |     |                                    |      |   |
| <p>Web: Synchronous rate<br/>UCI: tservd.@port[0].sync_speed<br/>Opt: sync_speed</p>                    | <p>Defines the synchronous speed in bps. Set to <b>0</b> for external clock. If not set to 0, an internal clock is used. This setting is only displayed if an Atmel USB serial card is enabled.</p> <table border="1"> <tr> <td>64000</td> <td>64 kbps</td> </tr> <tr> <td>Range</td> <td>2048000; 1024000; 768000; 512000; 384000; 256000; 128000; 19200; 9600</td> </tr> </table>  | 64000 | 64 kbps   | Range  | 2048000; 1024000; 768000; 512000; 384000; 256000; 128000; 19200; 9600 |     |                 |     |                                    |      |   |
| 64000   | 64 kbps  |       |   |        |   |     |                 |     |                                    |      |   |
| Range   | 2048000; 1024000; 768000; 512000; 384000; 256000; 128000; 19200; 9600  |       |   |        |   |     |                 |     |                                    |      |   |
| <p>Web: Invert receive clock<br/>UCI: tservd.@port[0].sync_invert_rxclk<br/>Opt: sync_invert_rxclk</p>  | <p>Defines receive clock inversion. Normal clock data is sampled on falling edge. Inverted clock data is sampled on rising edge. This setting is only displayed if an Atmel USB serial card is enabled.</p> <table border="1"> <tr> <td>0</td> <td>Normal.</td> </tr> <tr> <td>1</td> <td>Invert.</td> </tr> </table>  | 0     | Normal.   | 1      | Invert.   |     |                 |     |                                    |      |   |
| 0   | Normal.  |       |   |        |   |     |                 |     |                                    |      |   |
| 1   | Invert.  |       |   |        |   |     |                 |     |                                    |      |   |
| <p>Web: Invert transmit clock<br/>UCI: tservd.@port[0].sync_invert_txclk<br/>Opt: sync_invert_txclk</p> | <p>Defines transmit clock inversion. Normal clock data transmitted on falling edge. Inverted clock data transmitted on rising edge. Only displayed if an Atmel USB serial card is enabled.</p> <table border="1"> <tr> <td>0</td> <td>Normal.</td> </tr> <tr> <td>1</td> <td>Invert.</td> </tr> </table>   | 0     | Normal.   | 1      | Invert.   |     |                 |     |                                    |      |   |
| 0   | Normal.  |       |   |        |   |     |                 |     |                                    |      |   |
| 1   | Invert.  |       |   |        |   |     |                 |     |                                    |      |   |
| <p>Web: RX MSBF<br/>UCI: tservd.@port[0].sync_rx_msbf<br/>Opt: sync_rx_msbf</p>                         | <p>Defines whether most significant bit is received first. This setting is only displayed if an Atmel USB serial card is enabled.</p> <table border="1"> <tr> <td>0</td> <td>Receive least significant bit first.</td> </tr> <tr> <td>1</td> <td>Receive most significant bit first.</td> </tr> </table>   | 0     | Receive least significant bit first.  | 1      | Receive most significant bit first.                                   |     |                 |     |                                    |      |   |
| 0   | Receive least significant bit first.   |       |   |        |   |     |                 |     |                                    |      |   |
| 1   | Receive most significant bit first.  |       |   |        |   |     |                 |     |                                    |      |   |
| <p>Web: TX MSBF<br/>UCI: tservd.@port[0].sync_tx_msbf<br/>Opt: sync_tx_msbf</p>                         | <p>Defines whether most significant bit is transmitted first. This setting is only displayed if an Atmel USB serial card is enabled.</p> <table border="1"> <tr> <td>0</td> <td>Transmit least significant bit first.</td> </tr> <tr> <td>1</td> <td>Transmit most significant bit first.</td> </tr> </table>  | 0     | Transmit least significant bit first.                                       | 1      | Transmit most significant bit first.                                  |     |                 |     |                                    |      |   |
| 0   | Transmit least significant bit first.  |       |   |        |   |     |                 |     |                                    |      |   |
| 1   | Transmit most significant bit first.   |       |   |        |   |     |                 |     |                                    |      |   |

|   |  |     |                                  |       |                               |     |                           |       |         |
|---|--|-----|----------------------------------|-------|-------------------------------|-----|---------------------------|-------|---------|
| <p>Web: RX data delay<br/>UCI: tservd.@port[0].sync_rxdata_dly<br/>Opt: sync_rxdata_dly</p>                   | <p>Defines the number of bit positions to delay sampling data from the detecting clock edge. This setting is only displayed if an Atmel USB serial card is enabled.</p> <table border="1"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>  | 0   |                                  | Range |                               |     |                           |       |         |
| 0   |  |     |                                  |       |                               |     |                           |       |         |
| Range   |  |     |                                  |       |                               |     |                           |       |         |
| <p>Web: TX data delay<br/>UCI: tservd.@port[0].sync_txdata_dly<br/>Opt: sync_txdata_dly</p>                   | <p>Defines the number of bit positions to delay the output of data from the detecting clock edge. This setting is only displayed if an Atmel USB serial card is enabled.</p> <table border="1"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>   | 0   |                                  | Range |                               |     |                           |       |         |
| 0   |  |     |                                  |       |                               |     |                           |       |         |
| Range   |  |     |                                  |       |                               |     |                           |       |         |
| <p>Web: Dual X.21 card bit reverse<br/>UCI: tservd.@port[0].bit_reverse<br/>Opt: bit_reverse</p>              | <p>Enables bit reversal of all bits in 8 byte word during transmission.</p> <table border="1"> <tr><td>0</td><td>Normal.</td></tr> <tr><td>1</td><td>Reverse.</td></tr> </table>   | 0   | Normal.                          | 1     | Reverse.                      |     |                           |       |         |
| 0   | Normal.  |     |                                  |       |                               |     |                           |       |         |
| 1   | Reverse.   |     |                                  |       |                               |     |                           |       |         |
| <p>Web: Dual X.21 card DTE TT Invert<br/>UCI: tservd.@port[0].dte_tt_inv<br/>Opt: dte_tt_inv</p>              | <p>Enables X.21 TT clock signal inversion.</p> <table border="1"> <tr><td>0</td><td>Normal.</td></tr> <tr><td>1</td><td>Invert.</td></tr> </table>   | 0   | Normal.                          | 1     | Invert.                       |     |                           |       |         |
| 0   | Normal.  |     |                                  |       |                               |     |                           |       |         |
| 1   | Invert.  |     |                                  |       |                               |     |                           |       |         |
| <p>Web: Dual X.21 card DCE TCLK Invert<br/>UCI: tservd.@port[0].dce_tclk_inv<br/>Opt: dce_tclk_inv</p>        | <p>Enables X.21 DCE TCLK signal inversion.</p> <table border="1"> <tr><td>0</td><td>Normal.</td></tr> <tr><td>1</td><td>Invert.</td></tr> </table>   | 0   | Normal.                          | 1     | Invert.                       |     |                           |       |         |
| 0   | Normal.  |     |                                  |       |                               |     |                           |       |         |
| 1   | Invert.  |     |                                  |       |                               |     |                           |       |         |
| <p>Web: Dual X.21 card DCE RCLK Invert<br/>UCI: tservd.@port[0].dce_rclk_inv<br/>Opt: dce_rclk_inv</p>        | <p>Enables X.21 DCE RCLK signal inversion.</p> <table border="1"> <tr><td>0</td><td>Normal.</td></tr> <tr><td>1</td><td>Invert.</td></tr> </table>   | 0   | Normal.                          | 1     | Invert.                       |     |                           |       |         |
| 0   | Normal.  |     |                                  |       |                               |     |                           |       |         |
| 1   | Invert.  |     |                                  |       |                               |     |                           |       |         |
| <p>Web: Dual X.21 card CLK Invert<br/>UCI: tservd.@port[0].x21_clk_invert<br/>Opt: x21_clk_invert</p>         | <p>Enables X.21 DCE CLK signal inversion.</p> <table border="1"> <tr><td>0</td><td>Normal.</td></tr> <tr><td>1</td><td>Invert.</td></tr> </table>  | 0   | Normal.                          | 1     | Invert.                       |     |                           |       |         |
| 0   | Normal.  |     |                                  |       |                               |     |                           |       |         |
| 1   | Invert.  |     |                                  |       |                               |     |                           |       |         |
| <p>Web: Dual X.21 card RX data delay<br/>UCI: tservd.@port[0].x21_data_delay<br/>Opt: x21_data_delay</p>      | <p>Sets X.21 card RX data delay in number of bit positions.</p> <table border="1"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td>0 - 7</td></tr> </table>   | 0   |                                  | Range | 0 - 7                         |     |                           |       |         |
| 0   |  |     |                                  |       |                               |     |                           |       |         |
| Range   | 0 - 7  |     |                                  |       |                               |     |                           |       |         |
| <p>Web: n/a<br/>UCI: tservd.@port[0].sync_tx_idle<br/>Opt: sync_tx_idle</p>                                   | <p>Defines the value of idle character (decimal) to transmit in case of transmit underrun. In HDLC mode, this configures inter-frame fill.</p> <table border="1"> <tr><td>0</td><td>Transmit 0 (in HDLC mode)</td></tr> <tr><td>126</td><td>Transmit flags (in HDLC mode)</td></tr> <tr><td>255</td><td>Transmit 1 (in HDLC mode)</td></tr> <tr><td>Range</td><td>0 - 255</td></tr> </table> | 0   | Transmit 0 (in HDLC mode)        | 126   | Transmit flags (in HDLC mode) | 255 | Transmit 1 (in HDLC mode) | Range | 0 - 255 |
| 0   | Transmit 0 (in HDLC mode)  |     |                                  |       |                               |     |                           |       |         |
| 126   | Transmit flags (in HDLC mode)  |     |                                  |       |                               |     |                           |       |         |
| 255   | Transmit 1 (in HDLC mode)  |     |                                  |       |                               |     |                           |       |         |
| Range   | 0 - 255  |     |                                  |       |                               |     |                           |       |         |
| <p>Web: n/a<br/>UCI: tservd.@port[0].v23_inband_carrier_signalling<br/>Opt: v23_inband_carrier_signalling</p> | <p>Enables signalling of carrier by sending special characters.</p> <table border="1"> <tr><td>0</td><td>Disabled.</td></tr> <tr><td>1</td><td>Enabled.</td></tr> </table>   | 0   | Disabled.                        | 1     | Enabled.                      |     |                           |       |         |
| 0   | Disabled.  |     |                                  |       |                               |     |                           |       |         |
| 1   | Enabled.   |     |                                  |       |                               |     |                           |       |         |
| <p>Web: n/a<br/>UCI: tservd.@port[0].v23_inband_carrier_on_char<br/>Opt: v23_inband_carrier_on_char</p>       | <p>Defines the character decimal to signal remote carrier on.</p> <table border="1"> <tr><td>255</td><td></td></tr> <tr><td>Range</td><td>0 - 255</td></tr> </table>   | 255 |                                  | Range | 0 - 255                       |     |                           |       |         |
| 255   |  |     |                                  |       |                               |     |                           |       |         |
| Range   | 0 - 255  |     |                                  |       |                               |     |                           |       |         |
| <p>Web: n/a<br/>UCI: tservd.@port[0].v23_tx_gain<br/>Opt: v23_tx_gain</p>                                     | <p>Defines the transmit gain for v23 mode.</p> <table border="1"> <tr><td>2</td><td>Transmit samples multiplied by 2</td></tr> <tr><td>Range</td><td></td></tr> </table>   | 2   | Transmit samples multiplied by 2 | Range |                               |     |                           |       |         |
| 2   | Transmit samples multiplied by 2   |     |                                  |       |                               |     |                           |       |         |
| Range   |  |     |                                  |       |                               |     |                           |       |         |
| <p>Web: n/a<br/>UCI: tservd.@port[0].v23_rx_loss<br/>Opt: v23_rx_loss</p>                                     | <p>Defines the receive loss for v23 mode.</p> <table border="1"> <tr><td>1</td><td>Receive samples divided by 1.</td></tr> <tr><td>Range</td><td></td></tr> </table>   | 1   | Receive samples divided by 1.    | Range |                               |     |                           |       |         |
| 1   | Receive samples divided by 1.  |     |                                  |       |                               |     |                           |       |         |
| Range   |  |     |                                  |       |                               |     |                           |       |         |
| <p>Web: n/a<br/>UCI: tservd.@port[0].v23_rts_to_cts_delay<br/>Opt: v23_rts_to_cts_delay</p>                   | <p>Defines the v23 modem RTS to CTS delay in milliseconds.</p> <table border="1"> <tr><td>20</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>  | 20  |                                  | Range |                               |     |                           |       |         |
| 20  |  |     |                                  |       |                               |     |                           |       |         |
| Range   |  |     |                                  |       |                               |     |                           |       |         |

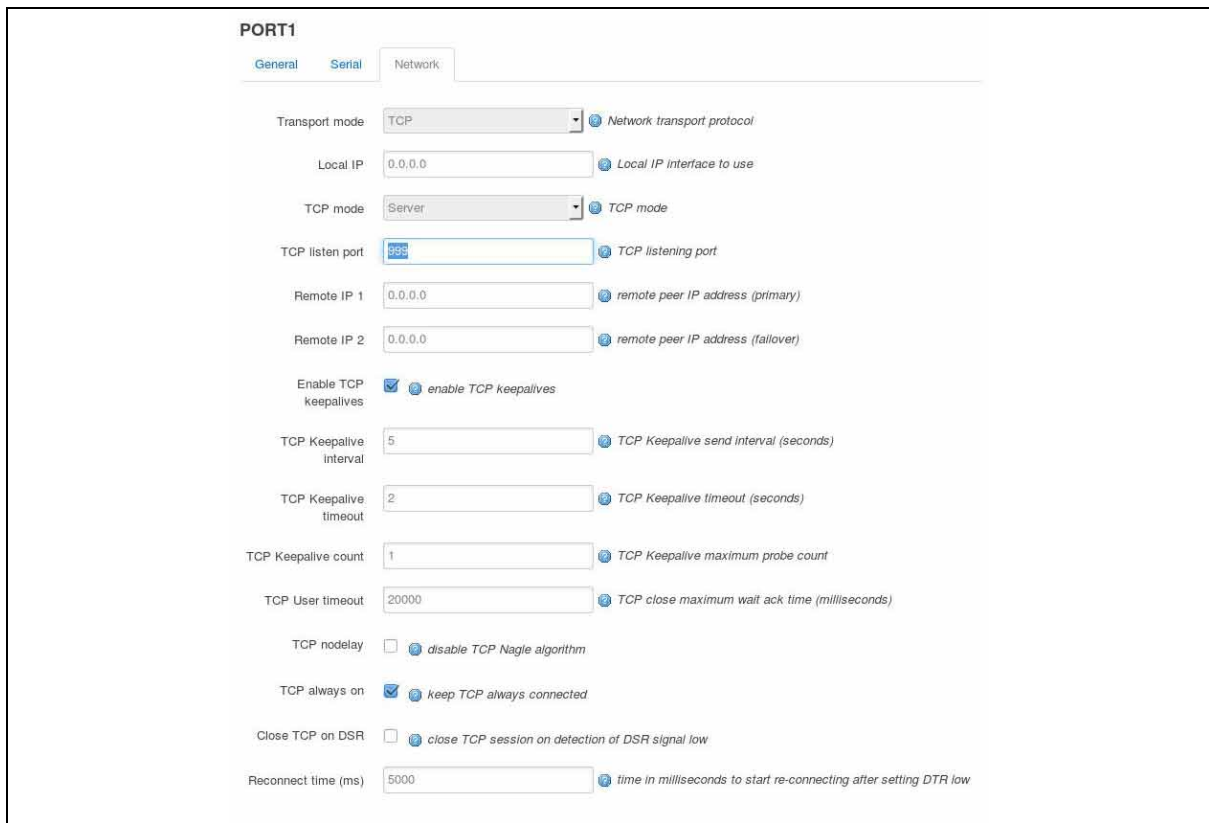
|  |   |     |        |       |         |
|--|---|-----|--------|-------|---------|
| Web: n/a<br>UCI: tserverd.@port[0].v23_is_four_wire<br>Opt: v23_is_four_wire | Defines the V23 modem LIM operation. <table border="1"> <tr> <td>0</td> <td>2-wire</td> </tr> <tr> <td>1</td> <td>4-wire</td> </tr> </table>  | 0   | 2-wire | 1     | 4-wire  |
| 0  | 2-wire  |     |        |       |         |
| 1  | 4-wire  |     |        |       |         |
| Web: n/a<br>UCI: tserverd.@port[0].v23_tx_timeout<br>Opt: v23_tx_timeout     | Defines the V23 modem receive echo suppression timeout in milliseconds. <table border="1"> <tr> <td>20</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table>                                | 20  |        | Range |         |
| 20   |   |     |        |       |         |
| Range  |   |     |        |       |         |
| Web: n/a<br>UCI: tserverd.@port[0].v23_tx_rampdown<br>Opt: v23_tx_rampdown   | Defines the time, in milliseconds, it takes the V23 transmitter to rampdown carrier from peak to zero. <table border="1"> <tr> <td>30</td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table> | 30  |        | Range |         |
| 30   |   |     |        |       |         |
| Range  |   |     |        |       |         |
| Web: n/a<br>UCI: tserverd.@port[0].v23_tx_maxfill<br>Opt: v23_tx_maxfill     | Defines the maximum transmit queue fill level in bytes. <table border="1"> <tr> <td>127</td> <td></td> </tr> <tr> <td>Range</td> <td>0 - 255</td> </tr> </table>  | 127 |        | Range | 0 - 255 |
| 127  |   |     |        |       |         |
| Range  | 0 - 255   |     |        |       |         |

**Table 191: Information table for port settings serial section**

### 46.3.2.3 Port settings: network section

In this section you can configure the network side of the terminal server.

**Note:** the displayed settings vary depending on options selected.



**Figure 259: The port settings network fields (TCP server mode)**

| Web Field/UCI/Package Option  | Description   |   |     |   |     |
|---|---|---|-----|---|-----|
| Web: Transport Mode<br>UCI: tserverd.@port[0].udpMode<br>Opt: udpMode | Selects the transport mode. <table border="1"> <tr> <td>0</td> <td>TCP</td> </tr> <tr> <td>1</td> <td>UDP</td> </tr> </table> | 0 | TCP | 1 | UDP |
| 0   | TCP   |   |     |   |     |
| 1   | UDP   |   |     |   |     |

|  |  |         |                          |       |   |
|--|--|---------|--------------------------|-------|---|
| <p>Web: Local IP<br/>UCI: tserverd.@port[0].local_ip<br/>Opt: local_ip</p>   | <p>Sets the local IP address to listen on.</p> <table border="1"> <tr> <td>0.0.0.0</td> <td>Listen on any interface.</td> </tr> <tr> <td>Range</td> <td>IPv4 address.</td> </tr> </table>  | 0.0.0.0 | Listen on any interface. | Range | IPv4 address.   |
| 0.0.0.0  | Listen on any interface.   |         |                          |       |   |
| Range  | IPv4 address.  |         |                          |       |   |
| <p>Web: TCP Mode<br/>UCI: tserverd.@port[0].server_mode<br/>Opt: server_mode</p>   | <p>Select between server and client modes of TCP. Only displayed if Transport Mode is TCP.</p> <table border="1"> <tr> <td>0</td> <td>Client Mode.</td> </tr> <tr> <td>1</td> <td>Server Mode.</td> </tr> </table>   | 0       | Client Mode.             | 1     | Server Mode.  |
| 0  | Client Mode.   |         |                          |       |   |
| 1  | Server Mode.   |         |                          |       |   |
| <p>Web: TCP Listen Port<br/>UCI: tserverd.@port[0].listen_port<br/>Opt: listen_port</p>                                  | <p>Sets the TCP listen port for server mode. Only displayed if transport mode is TCP and server mode is enabled.</p> <table border="1"> <tr> <td>999</td> <td></td> </tr> <tr> <td>Range</td> <td>1 - 65535</td> </tr> </table>  | 999     |                          | Range | 1 - 65535   |
| 999  |  |         |                          |       |   |
| Range  | 1 - 65535  |         |                          |       |   |
| <p>Web: Remote TCP Port 1<br/>UCI: tserverd.@port[0].ip_port1<br/>Opt: ip_port1</p>                                      | <p>Destination peer port IP 1 number. Only displayed if client mode is enabled.</p> <table border="1"> <tr> <td>951</td> <td></td> </tr> <tr> <td>Range</td> <td>1 - 65535</td> </tr> </table>   | 951     |                          | Range | 1 - 65535   |
| 951  |  |         |                          |       |   |
| Range  | 1 - 65535  |         |                          |       |   |
| <p>Web: Remote TCP Port 2<br/>UCI: tserverd.@port[0].ip_port2<br/>Opt: ip_port2</p>                                      | <p>Destination peer port IP 2 number for failover. Only displayed if client mode is enabled.</p> <table border="1"> <tr> <td>951</td> <td></td> </tr> <tr> <td>Range</td> <td>1 - 65535</td> </tr> </table>  | 951     |                          | Range | 1 - 65535   |
| 951  |  |         |                          |       |   |
| Range  | 1 - 65535  |         |                          |       |   |
| <p>Web: Remote IP 1<br/>UCI: tserverd.@port[0].remote_ip1<br/>Opt: remote_ip1</p>  | <p>Destination peer IP 1 address.</p> <table border="1"> <tr> <td>0.0.0.0</td> <td></td> </tr> <tr> <td>Range</td> <td>IPv4 address.</td> </tr> </table>   | 0.0.0.0 |                          | Range | IPv4 address.   |
| 0.0.0.0  |  |         |                          |       |   |
| Range  | IPv4 address.  |         |                          |       |   |
| <p>Web: Remote IP 2<br/>UCI: tserverd.@port[0].remote_ip2<br/>Opt: remote_ip2</p>  | <p>Destination peer IP 2 address for failover.</p> <table border="1"> <tr> <td>0.0.0.0</td> <td></td> </tr> <tr> <td>Range</td> <td>IPv4 address.</td> </tr> </table>  | 0.0.0.0 |                          | Range | IPv4 address.   |
| 0.0.0.0  |  |         |                          |       |   |
| Range  | IPv4 address.  |         |                          |       |   |
| <p>Web: Enable TCP Keepalives<br/>UCI:<br/>tserverd.@port[0].tcp_keepalives_enabled<br/>Opt: tcp_keepalives_enabled</p>  | <p>Enables or disables TCP keepalives. Only displayed if transport mode is TCP.</p> <table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0       | Disabled.                | 1     | Enabled.  |
| 0  | Disabled.  |         |                          |       |   |
| 1  | Enabled.   |         |                          |       |   |
| <p>Web: TCP Keepalive Interval<br/>UCI:<br/>tserverd.@port[0].tcp_keepalive_interval<br/>Opt: tcp_keepalive_interval</p> | <p>Interval in seconds between TCP keepalive probes. Only displayed if transport mode is TCP.</p> <table border="1"> <tr> <td>5</td> <td>5 seconds.</td> </tr> <tr> <td>Range</td> <td>0-65535</td> </tr> </table>   | 5       | 5 seconds.               | Range | 0-65535   |
| 5  | 5 seconds.   |         |                          |       |   |
| Range  | 0-65535  |         |                          |       |   |
| <p>Web: TCP Keepalive Timeout<br/>UCI:<br/>tserverd.@port[0].tcp_keepalive_timeout<br/>Opt: tcp_keepalive_timeout</p>    | <p>Time in seconds to wait for response to a TCP keepalive probe. Only displayed if transport mode is TCP.</p> <table border="1"> <tr> <td>2</td> <td>2 seconds.</td> </tr> <tr> <td>Range</td> <td>0-65535</td> </tr> </table>  | 2       | 2 seconds.               | Range | 0-65535   |
| 2  | 2 seconds.   |         |                          |       |   |
| Range  | 0-65535  |         |                          |       |   |
| <p>Web: TCP Keepalive Count<br/>UCI:<br/>tserverd.@port[0].tcp_keepalive_count<br/>Opt: tcp_keepalive_count</p>          | <p>Number of TCP keepalive probes to send before connection is closed. Only displayed if transport mode is TCP.</p> <table border="1"> <tr> <td>1</td> <td></td> </tr> <tr> <td>Range</td> <td>0-65535</td> </tr> </table>   | 1       |                          | Range | 0-65535   |
| 1  |  |         |                          |       |   |
| Range  | 0-65535  |         |                          |       |   |
| <p>Web: TCP User Timeout<br/>UCI:<br/>tserverd.@port[0].tcp_user_timeout<br/>Opt: tcp_user_timeout</p>                   | <p>Maximum time in milliseconds for TCP to wait for transmitted data to be 'acked' before closing connection in established state. Set to 0 to use kernel defaults. Only displayed if transport mode is TCP.</p> <table border="1"> <tr> <td>20000</td> <td>20 seconds.</td> </tr> <tr> <td>Range</td> <td>0-65535</td> </tr> </table> | 20000   | 20 seconds.              | Range | 0-65535   |
| 20000  | 20 seconds.  |         |                          |       |   |
| Range  | 0-65535  |         |                          |       |   |
| <p>Web: TCP Nodelay<br/>UCI: tserverd.@port[0].tcp_nodelay<br/>Opt: tcp_nodelay</p>                                      | <p>Sets TCP to delay behaviour. Only displayed if transport mode is TCP.</p> <table border="1"> <tr> <td>0</td> <td>Normal operation.</td> </tr> <tr> <td>1</td> <td>Disable TCP Nagle algorithm. Only displayed if transport mode is TCP.</td> </tr> </table>   | 0       | Normal operation.        | 1     | Disable TCP Nagle algorithm. Only displayed if transport mode is TCP. |
| 0  | Normal operation.  |         |                          |       |   |
| 1  | Disable TCP Nagle algorithm. Only displayed if transport mode is TCP.  |         |                          |       |   |



|  |  |      |  |       |   |
|--|--|------|--|-------|---|
| <p>Web: TCP Always on<br/>UCI: tserverd.@port[0].tcp_always_on<br/>Opt: tcp_always_on</p>              | <p>Keep TCP session always connected. Only displayed if transport mode is TCP and client mode is enabled.</p> <table border="1"> <tr> <td>0</td> <td>Disabled. TCP connection/UDP session is initiated on detecting high state on the DSR interface signal.</td> </tr> <tr> <td>1</td> <td>Enabled. If it disconnects in the established state the TCP connection/UDP session is re-initiated.</td> </tr> </table> | 0    | Disabled. TCP connection/UDP session is initiated on detecting high state on the DSR interface signal. | 1     | Enabled. If it disconnects in the established state the TCP connection/UDP session is re-initiated. |
| 0  | Disabled. TCP connection/UDP session is initiated on detecting high state on the DSR interface signal.   |      |  |       |   |
| 1  | Enabled. If it disconnects in the established state the TCP connection/UDP session is re-initiated.  |      |  |       |   |
| <p>Web: Close TCP on DSR<br/>UCI: tserverd.@port[0].close_tcp_on_dsr<br/>Opt: close_tcp_on_dsr</p>     | <p>Close TCP session on detection of DSR signal low. Only displayed if Transport Mode is TCP and client mode is enabled.</p> <table border="1"> <tr> <td>0</td> <td>Disabled. Detecting DSR down does not affect the TCP connection.</td> </tr> <tr> <td>1</td> <td>Enabled. Detecting DSR down closes the established TCP connection.</td> </tr> </table>   | 0    | Disabled. Detecting DSR down does not affect the TCP connection.                                       | 1     | Enabled. Detecting DSR down closes the established TCP connection.                                  |
| 0  | Disabled. Detecting DSR down does not affect the TCP connection.   |      |  |       |   |
| 1  | Enabled. Detecting DSR down closes the established TCP connection.   |      |  |       |   |
| <p>Web: Reconnect Time (ms)<br/>UCI: tserverd.@port[0].disc_time_ms<br/>Opt: disc_time_ms</p>          | <p>Time in milliseconds to start reconnecting after setting DTR low.</p> <table border="1"> <tr> <td>5000</td> <td>5 seconds.</td> </tr> <tr> <td>Range</td> <td>0 - 10000</td> </tr> </table>   | 5000 | 5 seconds.   | Range | 0 - 10000   |
| 5000   | 5 seconds.   |      |  |       |   |
| Range  | 0 - 10000  |      |  |       |   |
| <p>Web: UDP Keepalive Interval<br/>UCI: tserverd.@port[0].udpKaIntervalMs<br/>Opt: udpKaIntervalMs</p> | <p>Defines time in milliseconds to send UDP keepalives (empty UDP packets) when no data to send. Only displayed if transport mode is UDP.</p> <table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>Range</td> <td>0-65535</td> </tr> </table>  | 0    | Disabled.  | Range | 0-65535   |
| 0  | Disabled.  |      |  |       |   |
| Range  | 0-65535  |      |  |       |   |
| <p>Web: UDP Keepalive Count<br/>UCI: tserverd.@port[0].udpKaCount<br/>Opt: udpKaCount</p>              | <p>Defines the maximum number of remote UDP keepalives not received before UDP stream is considered broken. Only displayed if transport mode is UDP.</p> <table border="1"> <tr> <td>3</td> <td></td> </tr> <tr> <td>Range</td> <td>0-65535</td> </tr> </table>  | 3    |  | Range | 0-65535   |
| 3  |  |      |  |       |   |
| Range  | 0-65535  |      |  |       |   |
| <p>Web: local UDP Port<br/>UCI: tserverd.@port[0].udpLocalPort<br/>Opt: udpLocalPort</p>               | <p>Local UDP port used by terminal server. Only displayed if transport mode is UDP.</p> <table border="1"> <tr> <td>0</td> <td></td> </tr> <tr> <td>Range</td> <td>0-65535</td> </tr> </table>   | 0    |  | Range | 0-65535   |
| 0  |  |      |  |       |   |
| Range  | 0-65535  |      |  |       |   |
| <p>Web: remote UDP Port<br/>UCI: tserverd.@port[0].udpRemotePort<br/>Opt: udpRemotePort</p>            | <p>Remote UDP port used by terminal server. Only displayed if transport mode is UDP.</p> <table border="1"> <tr> <td>0</td> <td></td> </tr> <tr> <td>Range</td> <td>0-65535</td> </tr> </table>  | 0    |  | Range | 0-65535   |
| 0  |  |      |  |       |   |
| Range  | 0-65535  |      |  |       |   |

Table 192: Information table for port settings network section

## 46.4 Configuring terminal server using UCI

```

root@VA_router:~# uci show tserverd
tserverd.main=tserverd
tserverd.main.log_severity=0
tserverd.main.debug_rx_tx_enable=1
tserverd.main.debug_ev_enable=1
tserverd.@port[0]=port
tserverd.@port[0].devName=/dev/ttySC0
tserverd.@port[0].remote_ip1=0.0.0.0
tserverd.@port[0].remote_ip2=0.0.0.0

```

## 46.5 Configuring terminal server using package options

```

root@VA_router:~# uci export tserverd
package tserverd

config tserverd 'main'
    option log_severity '0'
    option debug_rx_tx_enable '1'
    option debug_ev_enable '1'

config port
    option devName '/dev/ttySC0'
    option remote_ip1 '0.0.0.0'
    option remote_ip2 '0.0.0.0'

```

## 46.6 Configuring terminal server DSR signal management network

On the IP network side, the terminal server can operate in one of three modes:

- TCP Client
- TCP Server
- UDP

Based on the chosen network configuration, the DSR behaviour may vary.

### 46.6.1 DSR signal behaviour in TCP client mode

#### 46.6.1.1 TCP connection management

Initial TCP connection initiation or next TCP connection initiation after disconnection is affected by configuration options `tcp_always_on` and `close_tcp_on_dsr`.

When option `tcp_always_on` is enabled terminal server keeps the TCP session always connected. If it disconnects in the established state, the TCP session is reinitiated.

If `tcp_always_on` is disabled TCP connection is initiated on detection of a high state on the DSP interface signal.

When option `close_tcp_on_dsr` is enabled terminal server detecting DSR down signal and closes the established TCP connection.

If option `close_tcp_on_dsr` is disabled then detecting DSR down does not affect the TCP connection.

#### 46.6.1.2 TCP connection initiation at startup

If you have set option `tcp_always_on1`, or DSR state is UP, the TCP connection setup is initiated immediately.

If you have set option `tcp_always_on0`, and DSR is DOWN, the terminal server waits for a DSR UP signal. When DSR UP is detected, the TCP connection is initiated.

#### **46.6.1.3 TCP connection clearing**

The TCP connection is cleared either by the network or by the terminal server application itself.

The TCP connection is cleared by the terminal server when it detects DSR interface signal DOWN and option `close_tcp_on_dsr` is 1.

#### **46.6.1.4 TCP connection re-initiation**

After TCP connection clearing, the terminal server takes action to re-setup the TCP connection after a hand off timeout.

If you have set option `tcp_always_on1`, or DSR state is UP, the TCP connection setup is initiated.

If you have set option `tcp_always_on0`, and DSR is DOWN, the terminal server waits for a DSR UP signal and then initiates a new TCP connection.

### **46.6.2 DSR signal behaviour in TCP server mode**

#### **46.6.2.1 TCP connection initiation at startup**

After a short startup delay, the terminal server starts listening for an incoming TCP connection from the remote peer.

#### **46.6.2.2 TCP connection clearing**

When in a TCP connection state, the TCP connection is cleared only by the network. Serial interface signals such as DSR do not cause TCP disconnection.

#### **46.6.2.3 TCP connection re-initiation**

When a TCP session goes down in the connected state, the terminal server immediately restarts listening for a new TCP connection from a remote peer.

### **46.6.3 DSR signal behaviour in UDP mode**

#### **46.6.3.1 UDP session setup at startup**

If you have set option `tcp_always_on1`, or DSR state is UP, the UDP session is setup immediately on startup.

If you have set option `tcp_always_on0`, and DSR is DOWN, the terminal server waits for a DSR UP signal. When DSR UP is detected, the UDP session is setup.

#### **46.6.3.2 UDP session clearing**

A UDP session is normally never cleared, but if it is closed by the network sub-system, it gets re-setup after a hand off timeout.

A DSR signal DOWN event does not clear UDP session in the connected state.

### 46.6.3.3 UDP session reset

After UDP session clearing the terminal server takes action to reset up a UDP session after a hand off timeout.

If you have set option `tcp_always_on1`, or DSR state is UP, the UDP session is setup.

If you have set option `tcp_always_on0`, and DSR is DOWN, the terminal server waits for a DSR UP signal and then it resets up the UDP session.

## 46.7 Serial mode GPIO control

On some models of Virtual Access routers it is possible to change the physical transmission mode between RS232 and RS485. This is only applicable to the second serial port on the routers: `/dev/ttySC1`.

To enable `serial_mode_gpio_control` set the option to **1**.

Use the `portmode` option in addition to `serial_mode_gpio_control` to select between RS232, RS485 full duplex, RS485 half duplex, X.21 and V.23.

### 46.7.1 Checking the current `serial_mode_gpio_control`

To check if terminal server is running, enter the following command:

```
root@VA_router:~# uci show tserverd | grep serial_mode_gpio_control
```

The output of the above command will look similar to the example below if `serial_mode_gpio_control` is enabled for the second serial port.

```
tserverd.port0.serial_mode_gpio_control=0
tserverd.port1.serial_mode_gpio_control=1
```

## 46.8 Terminal server diagnostics

The `tserverd` process has to be running otherwise diagnostics options for terminal server will not be available.

### 46.8.1 Checking the terminal server process

To check if the terminal server is running, enter:

```
root@VA_router:~# -fl tserverd
1264 root      1032 S  tserverd
```

If terminal server is running it will be shown with its process ID.

### 46.8.2 Terminal server statistics

To view Terminal Server statistics, enter:

```

root@VA_router:~# tserv show stats
TERMINAL 1, Dev: /dev/ttySC0
State:          LISTENING
Serial Bytes   Rx (0)  Tx (0)  TxErrs (0)
TCP Packets    Rx (0)  Tx (0)  TxErrs (0)    TxBlocked (0)
TCP Bytes      Rx (0)  Tx (0)
UDP Datagrams  Rx (0)  Tx (0)  TxErrs (0)
UDP Bytes      Rx (0)  Tx (0)
DSR            Up (0)  Down (0)

```

### 46.8.3 Terminal Server debug statistics

To see debug statistics about Terminal Server, enter:

```

root@VA_router:~# tserv show debug all

TERMINAL 1, Dev: /dev/ttySC0
State:          LISTENING
netRxBuf length=0 offset=0 hdrsz=0
ttyRxBuf length=0 offset=16 hdrsz=16
line_status_mask = 0x0 line_status = 0x0
RFC2217 negotiated=0
Tcp tx last error: 0

```

### 46.8.4 Terminal Server serial signals debugging

To see Terminal Server serial signals statistics, enter:

```

root@VA_router:~# tserv show serial

TERMINAL-1, Dev: /dev/ttySC1
DSR=0 DTR=1 RTS=1 CTS=0 CAR=0 CD=0 RNG=0 LE=0 RI=0 ST=0 SR=0

TERMINAL-2, Dev: /dev/ttySC0
DSR=0 DTR=1 RTS=1 CTS=0 CAR=0 CD=0 RNG=0 LE=0 RI=0 ST=0 SR=0

```

## 46.8.5 Terminal Server advanced debugging

To view Terminal Server advanced debug commands for the terminal server, enter:

```
root@VA_router:~# tserv
=== Termserv disgnostics. Command syntax: ===
tserv show stats - show statistics
tserv clear stats - clear statistics
tserv show serial - show serial interface status
tserv send serial0 <data>- send data to serial port 0
tserv start capture N, N=port number (0 to 3) - start capturing rx serial
data
tserv print capture N, N=port number (0 to 3) - print captured rx serial
data
tserv show serial txlog-hex <Port> [length], Port=port cfg index (0 to 3),
length=length to show
tserv show serial rxlog-hex <Port> [length], Port=port cfg index (0 to 3),
length=length to show
tserv show serial txlog-asc <Port> [length], Port=port cfg index (0 to 3),
length=length to show
tserv show serial rxlog-asc <Port> [length], Port=port cfg index (0 to 3),
length=length to show
tserv show debug - show debug info
tserv start useerial rxlog - start USB serial card rx log
tserv show useerial rxlog <offs> <length> - show USB serial card rx log
tserv quit - terminate termserv process
```

## 47 Configuring terminal package

Terminal package is used to automatically add entries for getty to inittab for extra incoming console/terminal connections.

### 47.1 Configuration packages used

| Package  | Sections |
|----------|----------|
| terminal | terminal |

### 47.2 Configuring terminal package using the web interface

Terminal package is not available to configure using the web interface.

| Web Field/UCI/Package Option                                      | Description  |        |           |          |   |
|---|--|--------|-----------|----------|---|
| Web: n/a<br>UCI: terminal.console.enabled<br>Opt: enabled         | Enables Terminal on the router.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>  | 0      | Disabled. | 1        | Enabled.  |
| 0   | Disabled.  |        |           |          |   |
| 1   | Enabled.   |        |           |          |   |
| Web: n/a<br>UCI: terminal.console.device<br>Opt: device           | String value point at the tty device in /dev folder.<br><table border="1"> <tr> <td>None</td> <td>Default.</td> </tr> <tr> <td>&lt;string&gt;</td> <td>Device name.( e.g. ttySC0 to use serial port 0)</td> </tr> </table> | None   | Default.  | <string> | Device name.( e.g. ttySC0 to use serial port 0) |
| None  | Default.   |        |           |          |   |
| <string>  | Device name.( e.g. ttySC0 to use serial port 0)  |        |           |          |   |
| Web: n/a<br>UCI: terminal.console.speed<br>Opt: speed             | Set the speed of serial connection.<br><table border="1"> <tr> <td>115200</td> <td>Default.</td> </tr> <tr> <td>&lt;range&gt;</td> <td>Supported port speed.</td> </tr> </table>   | 115200 | Default.  | <range>  | Supported port speed.                           |
| 115200  | Default.   |        |           |          |   |
| <range>   | Supported port speed.  |        |           |          |   |
| Web: n/a<br>UCI: terminal.console.type<br>Opt: type               | String value represents supported terminal emulation mode.<br><table border="1"> <tr> <td>vt100</td> <td>Default.</td> </tr> <tr> <td>&lt;string&gt;</td> <td>Supported terminal type.</td> </tr> </table>                 | vt100  | Default.  | <string> | Supported terminal type.                        |
| vt100   | Default.   |        |           |          |   |
| <string>  | Supported terminal type.   |        |           |          |   |
| Web: n/a<br>UCI: terminal.console.flowcontrol<br>Opt: flowcontrol | Enables hardware flow control RTS/CTS.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0      | Disabled. | 1        | Enabled.  |
| 0   | Disabled.  |        |           |          |   |
| 1   | Enabled.   |        |           |          |   |

Table 193: Information table for terminal settings

### 47.3 Configuring terminal package using UCI

```
root@VA_router:~# uci show terminal
terminal.ttySC0=terminal
terminal.ttySC0.enabled=1
terminal.ttySC0.device=ttySC0
terminal.ttySC0.speed=115200
terminal.ttySC0.type=vt100
terminal.ttySC0.flowcontrol=1
```

## 47.4 Configuring terminal using package options

```
root@VA_router:~# uci export terminal
package terminal

config terminal 'ttySC0'
    option enabled '0'
    option device 'ttySC0'
    option speed '115200'
    option type 'vt100'
    option flowcontrol '1'
```

## 47.5 Terminal diagnostics

### 47.5.1 Checking terminal entry in inittab

To check if terminal configuration is running, enter the following commands and confirm the line referring to the device name is present and looks similar to the last line below:

```
root@VA_router:~# cat /etc/inittab
::sysinit:/etc/init.d/rcS S boot
::shutdown:/etc/init.d/rcS K stop
ttyLTQ0::askfirst:getty -L 115200 ttyLTQ0 vt100
ttyLTQ1::askfirst:getty -L 115200 ttyLTQ1 vt100
ttySC0::respawn:getty -h -L 115200 ttySC0 vt100
```



## 48 Configuring GPIO on the GW2300 Series router

The Virtual Access GW2300 Series router digital IO interface has the following features:

- Two digital input ports with 2 controls for wet/dry control
- Two digital outputs driving relays

You can use digital input ports to connect to a device to monitor its status, for example an external sensor. The digital connectors are labelled as follows:

- IN1
- IN2
- OUT1
- OUT2

An event is raised in the router's syslog when the status of the digital inputs/outputs changes. You can use the router's event system to forward the events to a syslog server, SNMP, email or SMS. For information on how to configure the event system, read the chapter 'Event System'.

### 48.1 GPIO connectors

The GPIO connectors are presented as 4 x 2 pin connector comprising two inputs and two outputs. The output is a connected to a pair of relay contacts that are normally open when no power is applied.

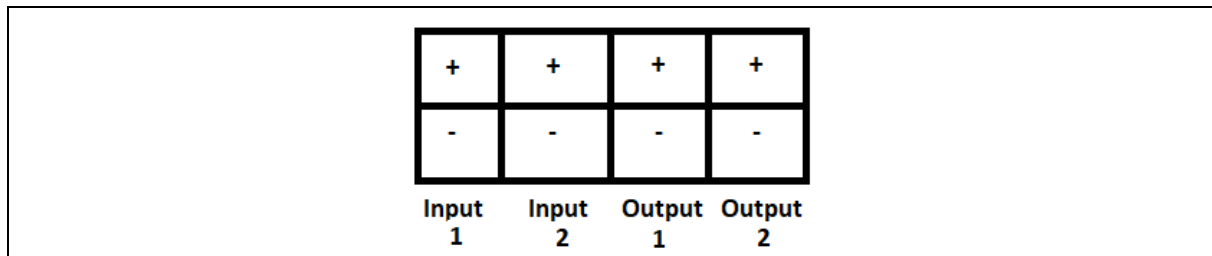


Figure 260: Pin out of GPIO connectors

### 48.2 GPIO diagnostics

#### 48.2.1 Syslog

All GPIO events can be monitored in the router's system log. The following example shows how to monitor syslog when syslog is being stored in a file called syslog.messages. For more information on syslog, read the chapter 'System Settings'.

```
root@VA_router:~# tail -f /root/syslog.messages &
```

## 49 Configuring SCADA RTU (RTUD)

This chapter describes how to configure the SCADA RTU feature on a Virtual Access router. SCADA RTU is only available on routers with a digital I/O interface.

You can edit parameters using:

- the text editor `vi` or `nano` after logging in using SSH;
- the router's web interface; or
- Virtual Access' Activator.

### 49.1 Terminology

|   |   |
|---|---|
| DI  | Digital Input                             |
| DO  | Digital Output                            |
| DNP3  | Distributed Network Protocol version 3    |
| I/O   | Input/Output                              |
| RTU   | Remote Terminal Unit                      |
| SCADA   | Supervisory Control and Data Acquisition  |
| Where a configuration parameter has the value of 1 or 0 | <b>1</b> = Enabled<br><b>0</b> = Disabled |
| Where a configuration parameter has the value NULL      | This means blank. Specify as " "          |

### 49.2 SCADA RTU overview

The GW2027, GW2028 and GW2300 routers have an integrated digital IO block consisting of three digital inputs (DI) and 1 digital output (DO). The digital inputs are presented on the terminal block as a series of input contact terminals. The digital output is presented on the terminal block as a relay output contact.

The SCADA RTU feature is implemented on the router by the RTUD daemon application. It allows the remote SCADA master to monitor and control the digital IOs of the Virtual Access router that acts as the RTU slave using several supported SCADA communication protocols:

- IEC 60870-5-104 (IEC104)
- DNP3 over TCP
- Modbus TCP

### 49.3 Configuration package used

| Package | Sections |
|---------|----------|
| rtud    | main     |

## 49.4 Configuring SCADA RTUD using the web interface

To configure SCADA RTUD using the web interface, in the top menu browse to **Services -> SCADA RTUD**. The SCADA RTU page appears.

There are five sections in the SCADA RTU page:

| Section   | Description  |
|-----------|--|
| General   | Enables the SCADA RTU and selects the RTU protocol |
| IEC104    | Configuration of IEC104 protocol options           |
| DNP3      | Configuration of DNP3 protocol options             |
| ModbusTCP | Configuration of ModbusTCP protocol options        |
| Advanced  | Advanced debug configuration options               |

### 49.4.1 Configure general options

The screenshot shows the SCADA RTU configuration web interface. At the top, there is a navigation menu with 'Status', 'System', 'Services', 'Network', and 'Logout'. Below the menu, the page title is 'SCADA RTU' with the subtitle 'Configuration of SCADA RTU'. The main section is 'Main Settings' with tabs for 'General', 'IEC104', 'DNP3', 'ModbusTCP', and 'Advanced'. The 'General' tab is active. The settings include:
 

- Enable:** A checked checkbox with a tooltip 'Enable SCADA RTU outstation emulation'.
- RTU Protocol:** A dropdown menu set to 'ModbusTCP' with a tooltip 'Sets the RTU communication protocol'.
- Local IP:** A text input field containing '0.0.0.0' with a tooltip 'Local IP interface address RTU binds to'.
- Synchronize time:** An unchecked checkbox with a tooltip 'Enables RTU time synchronization to SCADA Master time'.
- Short Pulse:** A text input field containing '50' with a tooltip 'Short pulse duration (milliseconds)'.
- Long Pulse:** A text input field containing '1000' with a tooltip 'Long pulse duration (milliseconds)'.

 At the bottom right, there are three buttons: 'Save & Apply', 'Save', and 'Reset'.

Figure 261: The SCADA RTU general options page

| Web Field/UCI/Package Option                                  | Description   |         |                 |       |                              |      |   |
|---|---|---------|-----------------|-------|------------------------------|------|---|
| Web: Enabled<br>UCI: .rtud.main.enabled<br>Opt: enabled       | Enables or disables SCADA RTU application.<br><table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table>  | 1       | Enabled.        | 0     | Disabled.                    |      |   |
| 1   | Enabled.  |         |                 |       |                              |      |   |
| 0   | Disabled.   |         |                 |       |                              |      |   |
| Web: RTU Protocol<br>UCI: rtud.main.protocol<br>Opt: protocol | Sets the RTU communication protocol.<br><table border="1"> <tr> <td>iec104</td> <td>IEC 60870-5-104</td> </tr> <tr> <td>mbtcp</td> <td>Modbus TCP</td> </tr> <tr> <td>dnp3</td> <td>Distributed Network Protocol V3 (over TCP).</td> </tr> </table> | iec104  | IEC 60870-5-104 | mbtcp | Modbus TCP                   | dnp3 | Distributed Network Protocol V3 (over TCP). |
| iec104  | IEC 60870-5-104   |         |                 |       |                              |      |   |
| mbtcp   | Modbus TCP  |         |                 |       |                              |      |   |
| dnp3  | Distributed Network Protocol V3 (over TCP).   |         |                 |       |                              |      |   |
| Web: Local IP<br>UCI: rtud.main.local_ip<br>Opt: local_ip     | Defines the local IP interface address the RTU binds to.<br><table border="1"> <tr> <td>0.0.0.0</td> <td></td> </tr> <tr> <td>Range</td> <td>A valid IPv4 or IPv6 address</td> </tr> </table>   | 0.0.0.0 |                 | Range | A valid IPv4 or IPv6 address |      |   |
| 0.0.0.0   |   |         |                 |       |                              |      |   |
| Range   | A valid IPv4 or IPv6 address  |         |                 |       |                              |      |   |

|   |   |      |          |       |           |
|---|---|------|----------|-------|-----------|
| Web: Synchronize Time<br>UCI: rtud.main.sync_time<br>Opt: sync_time | Enables RTU time synchronisation to master time. If enabled, the router will set its clock as the corresponding commands from the master station in each communication protocol. <table border="1"> <tr><td>1</td><td>Enabled.</td></tr> <tr><td>0</td><td>Disabled.</td></tr> </table> | 1    | Enabled. | 0     | Disabled. |
| 1   | Enabled.  |      |          |       |           |
| 0   | Disabled.   |      |          |       |           |
| Web: Short Pulse<br>UCI: rtud.main.short_pulse<br>Opt: short_pulse  | Short pulse duration in milliseconds, currently used in IEC104 protocol in processing digital output setting command, if the master specifies its use. <table border="1"> <tr><td>50</td><td></td></tr> <tr><td>Range</td><td>10-1000</td></tr> </table>                                | 50   |          | Range | 10-1000   |
| 50  |   |      |          |       |           |
| Range   | 10-1000   |      |          |       |           |
| Web: Long Pulse<br>UCI: rtud.main.long_pulse<br>Opt: long_pulse     | Long pulse duration in milliseconds, currently used in IEC104 protocol in processing digital output setting command, if the master specifies its use. <table border="1"> <tr><td>1000</td><td></td></tr> <tr><td>Range</td><td>10-1000</td></tr> </table>                               | 1000 |          | Range | 10-1000   |
| 1000  |   |      |          |       |           |
| Range   | 10-1000   |      |          |       |           |

Table 194: Information table for RTUD general options

### 49.4.2 Configure advanced options

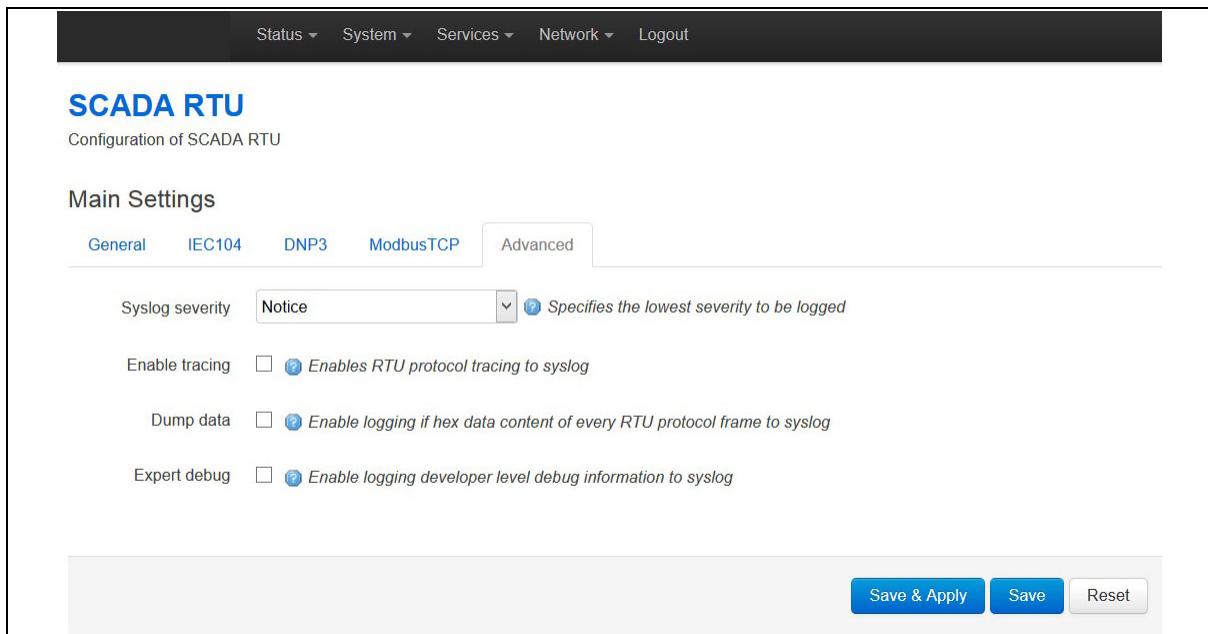


Figure 262: The SCADA RTU advanced setting page

| Web Field/UCI/Package Option                               | Description  |           |          |       |           |          |   |       |   |         |   |        |   |      |   |       |   |
|--|--|-----------|----------|-------|-----------|----------|---|-------|---|---------|---|--------|---|------|---|-------|---|
| Web: Log level<br>UCI: rtud.main.loglevel<br>Opt: loglevel | Determines the syslog level. Events up to this priority will be logged. <table border="1"> <tr><td>Emergency</td><td>0</td></tr> <tr><td>Alert</td><td>1</td></tr> <tr><td>Critical</td><td>2</td></tr> <tr><td>Error</td><td>3</td></tr> <tr><td>Warning</td><td>4</td></tr> <tr><td>Notice</td><td>5</td></tr> <tr><td>Info</td><td>6</td></tr> <tr><td>Debug</td><td>7</td></tr> </table> | Emergency | 0        | Alert | 1         | Critical | 2 | Error | 3 | Warning | 4 | Notice | 5 | Info | 6 | Debug | 7 |
| Emergency  | 0  |           |          |       |           |          |   |       |   |         |   |        |   |      |   |       |   |
| Alert  | 1  |           |          |       |           |          |   |       |   |         |   |        |   |      |   |       |   |
| Critical   | 2  |           |          |       |           |          |   |       |   |         |   |        |   |      |   |       |   |
| Error  | 3  |           |          |       |           |          |   |       |   |         |   |        |   |      |   |       |   |
| Warning  | 4  |           |          |       |           |          |   |       |   |         |   |        |   |      |   |       |   |
| Notice   | 5  |           |          |       |           |          |   |       |   |         |   |        |   |      |   |       |   |
| Info   | 6  |           |          |       |           |          |   |       |   |         |   |        |   |      |   |       |   |
| Debug  | 7  |           |          |       |           |          |   |       |   |         |   |        |   |      |   |       |   |
| Web: Trace<br>UCI: rtud.main.trace_on<br>Opt: trace_on     | Enables protocol tracing to syslog. <table border="1"> <tr><td>1</td><td>Enabled.</td></tr> <tr><td>0</td><td>Disabled.</td></tr> </table>   | 1         | Enabled. | 0     | Disabled. |          |   |       |   |         |   |        |   |      |   |       |   |
| 1  | Enabled.   |           |          |       |           |          |   |       |   |         |   |        |   |      |   |       |   |
| 0  | Disabled.  |           |          |       |           |          |   |       |   |         |   |        |   |      |   |       |   |

|   |   |   |          |   |           |
|---|---|---|----------|---|-----------|
| Web: Dump data<br>UCI: rtud.main.dump_data<br>Opt: dump_data          | Enables logging the context of protocol frames in ASCII hex format to syslog.<br><table border="1"> <tr> <td>1</td> <td>Enabled.</td> </tr> <tr> <td>0</td> <td>Disabled.</td> </tr> </table> | 1 | Enabled. | 0 | Disabled. |
| 1   | Enabled.  |   |          |   |           |
| 0   | Disabled.   |   |          |   |           |
| Web: Expert debug<br>UCI: rtud.main.expert_debug<br>Opt: expert_debug | Enables highest level of debug logging. For Virtual Access engineering use only.  |   |          |   |           |

**Table 195: Information table for advanced options**

### 49.4.3 Configuring IEC104 options

The screenshot shows the 'Main Settings' page for IEC104. It has tabs for 'General', 'IEC104', 'DNP3', 'ModbusTCP', and 'Advanced'. The 'IEC104' tab is active. A 'Delete' button is in the top right. The settings are as follows:

- IEC104 Listening TCP Port: 2404 (Local TCP port IEC104 RTU listens on)
- IEC104 K: 12 (IEC104 Maximum number of outstanding I frames)
- IEC104 T2: 10000 (IEC104 Timeout for sending S frames in case of no data (milliseconds))
- IEC104 ASDU Common Address: 6 (ASDU address of the IEC104 RTU)
- IEC104 COT Source Octet: 1 (Most significant octet in the cause of transmission field)
- IEC104 DI Type ID: SPI (single point) (Specifies IEC104 type ID to use when sending Digital Inputs)
- Digital Input 0 IOA: 1 (IEC104 Information Object Address of INPUT 0)
- Digital Input 1 IOA: 2 (IEC104 Information Object Address of INPUT 1)

**Figure 263: The SCADA RTU IEC104 settings page**

| Web Field/UCI/Package Option   | Description  |       |         |       |  |
|--|--|-------|---------|-------|--|
| Web: IEC104 Listening TCP Port<br>UCI: rtud.main.iec104_listen_tcpport<br>Opt: iec104_listen_tcpport   | Local TCP port IEC104 RTC listens on.<br><table border="1"> <tr> <td>Range</td> <td>1-65535</td> </tr> <tr> <td>2404</td> <td></td> </tr> </table>   | Range | 1-65535 | 2404  |  |
| Range  | 1-65535  |       |         |       |  |
| 2404   |  |       |         |       |  |
| Web: IEC104 K<br>UCI: rtud.main.iec104_k<br>Opt: iec104_k  | IEC parameter K. Maximum number of outstanding frames.<br><table border="1"> <tr> <td>Range</td> <td>1-3267</td> </tr> <tr> <td>12</td> <td></td> </tr> </table>   | Range | 1-3267  | 12    |  |
| Range  | 1-3267   |       |         |       |  |
| 12   |  |       |         |       |  |
| Web: IEC104 T2<br>UCI: rtud.main.iec104_t2<br>Opt: iec104_t2   | IEC 104 parameter T2. Timeout for sending, in milliseconds, S frames in case of no data.<br><table border="1"> <tr> <td>Range</td> <td>1-6000</td> </tr> <tr> <td>10000</td> <td></td> </tr> </table>                    | Range | 1-6000  | 10000 |  |
| Range  | 1-6000   |       |         |       |  |
| 10000  |  |       |         |       |  |
| Web: IEC104 ASDU Common Address<br>UCI: rtud.main.iec104_asdu_addr<br>Opt: iec104_asdu_addr            | IEC 104 parameter CA (also known as CASDU). ASDU common address of the RTU.<br><table border="1"> <tr> <td>Range</td> <td>1-65535</td> </tr> <tr> <td>0</td> <td></td> </tr> </table>                                    | Range | 1-65535 | 0     |  |
| Range  | 1-65535  |       |         |       |  |
| 0  |  |       |         |       |  |
| Web: IEC104 COT Source Octet<br>UCI: rtud.main.iec104_cot_source_octet<br>Opt: iec104_cot_source_octet | IEC104 parameter COT value. The value of the most significant octet in the 'cause of transmission' header field.<br><table border="1"> <tr> <td>Range</td> <td>0-255</td> </tr> <tr> <td>1</td> <td></td> </tr> </table> | Range | 0-255   | 1     |  |
| Range  | 0-255  |       |         |       |  |
| 1  |  |       |         |       |  |

| Web: IEC104 DI Type ID<br>UCI: rtud.main.iec104_type_id<br>Opt: iec104_type_id          | Defines the IEC104 Type ID for digital inputs                |                        |
|---|--|------------------------|
|   | Option   | Description            |
|   | SPI (single point)   | Single point           |
|   | DPI (double point)   | Double point           |
|   | SPI (single point with time)                                 | Single point with time |
|   | DPI (double point with time)                                 | Double point with time |
| Web: Digital Input 0 IOA<br>UCI: rtud.main.dg_input0_ioaddr<br>Opt: dg_input0_ioaddr    | IEC104 Information Object Address (IOA) of Digital Input 0.  |                        |
|   | Range  | 1-1677712              |
| Web: Digital Input 1 IOA<br>UCI: rtud.main.dg_input1_ioaddr<br>Opt: dg_input1_ioaddr    | IEC104 Information Object Address (IOA) of Digital Input 1.  |                        |
|   | Range  | 1-1677712              |
| Web: Digital Output 0 IOA<br>UCI: rtud.main.dg_output0_ioaddr<br>Opt: dg_output0_ioaddr | IEC104 Information Object Address (IOA) of Digital Output 0. |                        |
|   | Range  | 1-1677712              |

Table 196: Information table for IEC104 options

### 49.4.4 Configure DNP3 options

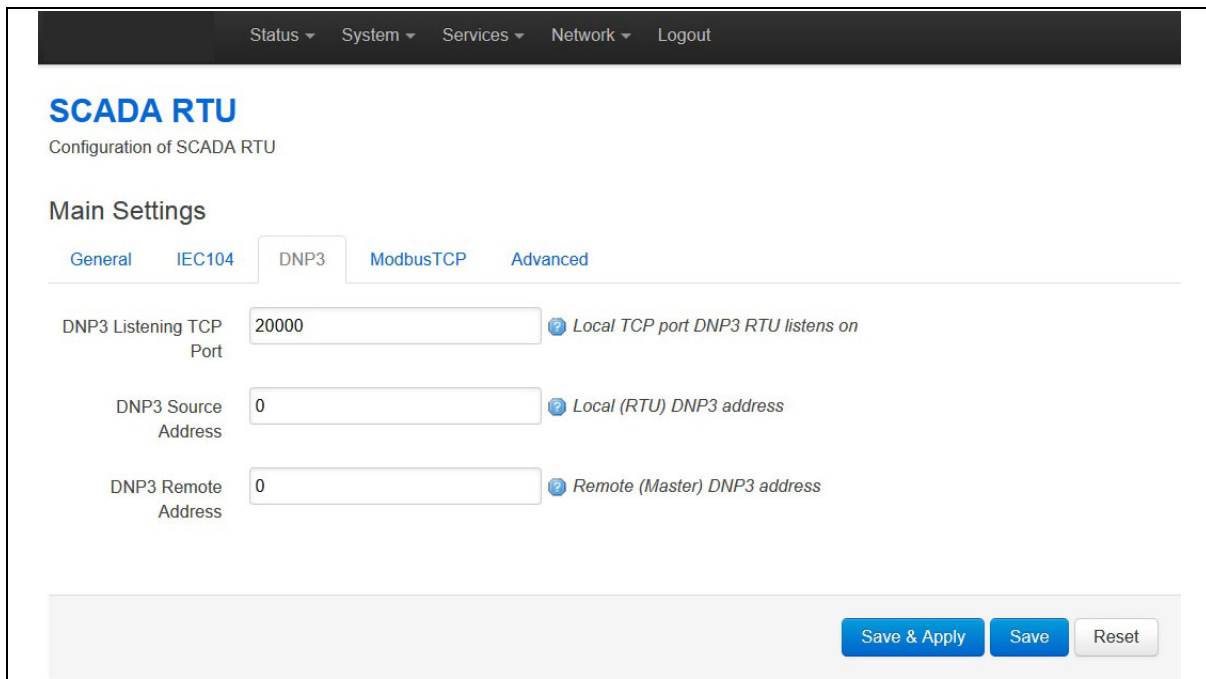


Figure 264: The SCADA RTU DNP3 settings page

| Web Field/UCI/Package Option   | Description   |       |         |      |  |
|--|---|-------|---------|------|--|
| Web: DNP3 Listening TCP Port<br>UCI: rtud.main.dnp3_listen_tcpport<br>Opt: dnp3_listen_tcpport | Sets the local TCP port the DNP3 RTU listens on.<br><table border="1"> <tr> <td>Range</td> <td>1-65535</td> </tr> <tr> <td>2000</td> <td></td> </tr> </table> | Range | 1-65535 | 2000 |  |
| Range  | 1-65535   |       |         |      |  |
| 2000   |   |       |         |      |  |
| Web: DNP3 Source Address<br>UCI: rtud.main.dnp3_dl_srcaddr<br>Opt: dnp3_dl_srcaddr             | Sets the local (RTU) DNP3 address.<br><table border="1"> <tr> <td>Range</td> <td>0-65535</td> </tr> <tr> <td>0</td> <td></td> </tr> </table>                  | Range | 0-65535 | 0    |  |
| Range  | 0-65535   |       |         |      |  |
| 0  |   |       |         |      |  |
| Web: DNP3 Remote Address<br>UCI: rtud.main.dnp3_dl_dstadr<br>Opt: dnp3_dl_dstadr               | Sets the remote (Master) DNP3 address.<br><table border="1"> <tr> <td>Range</td> <td>0-255</td> </tr> <tr> <td>1</td> <td></td> </tr> </table>                | Range | 0-255   | 1    |  |
| Range  | 0-255   |       |         |      |  |
| 1  |   |       |         |      |  |

Table 197: Information table for DNP3 options

## 49.4.5 Configure Modbus options

Status ▾ System ▾ Services ▾ Network ▾ Logout

## SCADA RTU

Configuration of SCADA RTU

### Main Settings

General IEC104 DNP3 **ModbusTCP** Advanced

ModbusTCP Slave Address:  ⓘ Modbus TCP slave address (decimal 1..247)

Modbus TCP Listening Port:  ⓘ Local TCP port Modbus RTU listens on

Modbus Discreet Inputs Start Address:  ⓘ Modbus Digital Inputs Start Address

Modbus Coils Start Address:  ⓘ Modbus Digital Outputs (Coils) Start Address

Save & Apply Save Reset

Figure 265: The SCADA RTU modbus settings page

| Web Field/UCI/Package Option  | Description   |       |         |     |  |
|---|---|-------|---------|-----|--|
| Web: Modbus TCP Slave Address<br>UCI: rtud.main.mbtcp_devaddr<br>Opt: mbtcp_devaddr                         | Sets the Modbus slave address.<br><table border="1"> <tr> <td>Range</td> <td>1-247</td> </tr> <tr> <td>0</td> <td></td> </tr> </table>  | Range | 1-247   | 0   |  |
| Range   | 1-247   |       |         |     |  |
| 0   |   |       |         |     |  |
| Web: Modbus TCP Listening Port<br>UCI: rtud.main.mbtcp_listen_tcpport<br>Opt: mbtcp_listen_tcpport          | Sets the local TCP port Modbus RTU listens on.<br><table border="1"> <tr> <td>Range</td> <td>1-65535</td> </tr> <tr> <td>502</td> <td></td> </tr> </table>  | Range | 1-65535 | 502 |  |
| Range   | 1-65535   |       |         |     |  |
| 502   |   |       |         |     |  |
| Web: Modbus Discreet Inputs Start Address<br>UCI: rtud.main.mbtcp_di_start_addr<br>Opt: mbtcp_di_start_addr | Sets the Modbus Discreet Inputs start address. This is the address of the first digital input in the modbus data model.<br><b>Note:</b> address of inputs and outputs are allowed to overlap, that is, may be the same.<br><table border="1"> <tr> <td>Range</td> <td>0-65535</td> </tr> <tr> <td>0</td> <td></td> </tr> </table> | Range | 0-65535 | 0   |  |
| Range   | 0-65535   |       |         |     |  |
| 0   |   |       |         |     |  |
| Web: Modbus Coils Start Address<br>UCI: rtud.main.mbtcp_co_start_addr<br>Opt: mbtcp_co_start_addr           | Sets the Modbus Coils Start address. This is the address of the first digital output in the modbus data model.<br><b>Note:</b> address of inputs and outputs are allowed to overlap, that is, may be the same.<br><table border="1"> <tr> <td>Range</td> <td>0-65535</td> </tr> <tr> <td>0</td> <td></td> </tr> </table>          | Range | 0-65535 | 0   |  |
| Range   | 0-65535   |       |         |     |  |
| 0   |   |       |         |     |  |

Table 198: Information table for modbus options

## 49.5 Controlling the RTUD application manually using the web interface

When you have enabled RTUD, the application starts automatically. If necessary, you can control the application manually.

Browse to the top menu and select **System -> Startup**.

| Status | System     | Services | Network | Logout       |
|--------|------------|----------|---------|--------------|
| 50     | ripd       | Enabled  | Start   | Restart Stop |
| 50     | rtud       | Enabled  | Start   | Restart Stop |
| 50     | slad       | Enabled  | Start   | Restart Stop |
| 50     | snmpd      | Enabled  | Start   | Restart Stop |
| 50     | strongswan | Enabled  | Start   | Restart Stop |
| 50     | telnet     | Enabled  | Start   | Restart Stop |
| 50     | tservd     | Enabled  | Start   | Restart Stop |
| 50     | uhttpd     | Enabled  | Start   | Restart Stop |
| 50     | vald       | Enabled  | Start   | Restart Stop |
| 50     | vnstat     | Enabled  | Start   | Restart Stop |

Figure 266: The startup page

Find the RTUD entry and click either **Enabled/Disabled**, **Start**, **Restart**, or **Stop**, depending on which option you require.

To check if the application is running, select **Status -> Processes**. The Processes page appears.



| Status ▾ System ▾ Services ▾ Network ▾ Logout |      |   |    |      |  |         |  |           |  |      |
|---|------|---|----|------|--|---------|--|-----------|--|------|
| 2557  | root | /usr/sbin/crond -c /etc/crontabs -l 5   | 0% | 3%   |  | Hang Up |  | Terminate |  | Kill |
| 2666  | root | /usr/sbin/dropbear -P /var/run/dropbear.1.pid -p 22 -b /etc/banner  | 0% | 2%   |  | Hang Up |  | Terminate |  | Kill |
| 2900  | root | /usr/sbin/rtud  | 0% | 2%   |  | Hang Up |  | Terminate |  | Kill |
| 2955  | root | /usr/sbin/snmpd -Lsd0-6 -p /var/run/snmpd.pid -m -c /var/conf/snmpd.conf  | 0% | 7%   |  | Hang Up |  | Terminate |  | Kill |
| 3003  | root | /usr/lib/ipsec/starter  | 0% | 2%   |  | Hang Up |  | Terminate |  | Kill |
| 3005  | root | /usr/lib/ipsec/charon --use-syslog  | 0% | 51%  |  | Hang Up |  | Terminate |  | Kill |
| 3147  | root | /usr/sbin/uhttpd_mon  | 0% | 2%   |  | Hang Up |  | Terminate |  | Kill |
| 3587  | root | [worker/0.0]  | 0% | 0%   |  | Hang Up |  | Terminate |  | Kill |
| 3841  | root | 0% /usr/sbin/uhttpd -f -h /www -r VirtualAccess -c /etc/http.conf -x /cgi-bin -t 60 -T 30 -R -p 0.0.0.0.80 -C /etc/uhttpd.crt -K /etc/uhttpd.key -s 0.0.0.0.443 -l /cgi-bin/luci -L /usr/lib/uhttpd.lua | 8% | 5076 |  | Hang Up |  | Terminate |  | Kill |
| 3842  | root | 0% sh -c top -bn1   | 3% | 1780 |  | Hang Up |  | Terminate |  | Kill |
| 3843  | root | 31% top -bn1  | 3% | 1780 |  | Hang Up |  | Terminate |  | Kill |

Figure 267: The status process page

## 49.6 Viewing RTUD statistics using the web interface

To view the SCADA RTU point list, session status and counters, from the top menu select **Status -> SCADA RTU**.

| Status ▾ System ▾ Services ▾ Network ▾ Logout |           |                 |                |
|---|-----------|-----------------|----------------|
| <b>SCADA RTU Points</b>                       |           |                 |                |
| IO Name                                       | IO Type   | IO Address      | IO Value       |
| dg_input0                                     | Input     | IOA1            | 0              |
| dg_input1                                     | Input     | IOA2            | 0              |
| dg_output0                                    | Output    | IOA3            | 0              |
| <b>SCADA RTU Statistics</b>                   |           |                 |                |
| Protocol                                      | State     | Link Rx/Tx/Errs | App Rx/Tx/Errs |
| IEC104  | LISTENING | 0 / 0 / 0       | 0 / 0 / 0      |

Figure 268: The SCADA RTU points screen

## 49.7 Configuring RTUD using command line

The RTUD configuration is stored in `/etc/config/rtud`

You must restart the RTUD application for your option changes to take effect.

The default content of the RTUD configuration file is shown below.

## 49.7.1 RTUD using UCI

```
root@VA_router:~# uci show rtud
rtud.main=rtud
rtud.main.enable=1
# set to 1 to enable RTUD daemon
rtud.main.protocol=iec104
rtud.main.local_ip=0.0.0.0
rtud.main.sync_time=0
rtud.main.short_pulse=50
rtud.main.long_pulse=1000
rtud.main.loglevel=5
rtud.main.trace_on=0
rtud.main.dump_data=0
rtud.main.expert_debug=0

rtud.main.iec104_listen_tcpport=2404
rtud.main.iec104_k=12
rtud.main.iec104_t2=10000
rtud.main.iec104_asdu_addr=0
rtud.main.iec104_cot_source_octet=1

rtud.main.dg_input0_ioaddr=1
rtud.main.dg_input1_ioaddr=2
rtud.main.dg_output0_ioaddr=3

rtud.main.dnp3_listen_tcpport=20000
rtud.main.dnp3_dl_srcaddr=0
rtud.main.dnp3_dl_dstaddr=0

rtud.main.mbtcp_devaddr=0
rtud.main.mbtcp_listen_port=502
rtud.main.mbtcp_di_start_addr=0
rtud.main.mbtcp_co_start_addr=0
```

## 49.7.2 RTUD using package options

```
root@VA_router:~# uci export rtud
package rtud
config rtud main
    # set to 1 to enable RTUD daemon
    option enable 0
    option protocol 'iec104'
    option local_ip '0.0.0.0'
    option sync_time 0
    option short_pulse 50
    option long_pulse 1000
    option loglevel 5
    option trace_on 0
    option dump_data 0
    option expert_debug 0

    option iec104_listen_tcpport 2404
    option iec104_k 12
    option iec104_t2 10000
    option iec104_asdu_addr 0
    option iec104_cot_source_octet 1

    option dg_input0_ioaddr 1
    option dg_input1_ioaddr 2
    option dg_output0_ioaddr 3

    option dnp3_listen_tcpport 20000
    option dnp3_dl_srcaddr 0
    option dnp3_dl_dstaddr 0

    option mbtcp_devaddr 0
    option mbtcp_listen_port 502
    option mbtcp_di_start_addr 0
    option mbtcp_co_start_addr 0
```

## 49.7.3 Controlling the RTUD application manually using UCI

When you have enabled RTUD, the application starts automatically. If necessary, you can control the application manually using the router's command line.

### 49.7.3.1 Starting the application

```
/etc/init.d/rtud start
```

### 49.7.3.2 Restarting the application

```
/etc/init.d/rtud restart
```

### 49.7.3.3 Stopping the application

```
/etc/init.d/rtud stop
```

### 49.7.3.4 Checking the application is running

```
ps | grep rtud
```

This command returns the process ID if the application is running or nothing if the application is not running.

## 49.8 RTUD diagnostics

To view RTUD diagnostic options, enter:

```
root@VA_router:~# rtu
=== RTU daemon diagnostics. Command syntax: ===

rtu set loglevel <level> (0 to 7)
rtu show config - show config
rtu show stats - show stats
rtu clear stats - clear stats
rtu show points - show RTU IO points
rtu show dnp3 - show DNP3 stats
rtu show modbus - show Modbus stats
rtu set point <IO name> <value> set output IO point value
```

## 50 SCADA IEC104 gateway

### 50.1 Overview

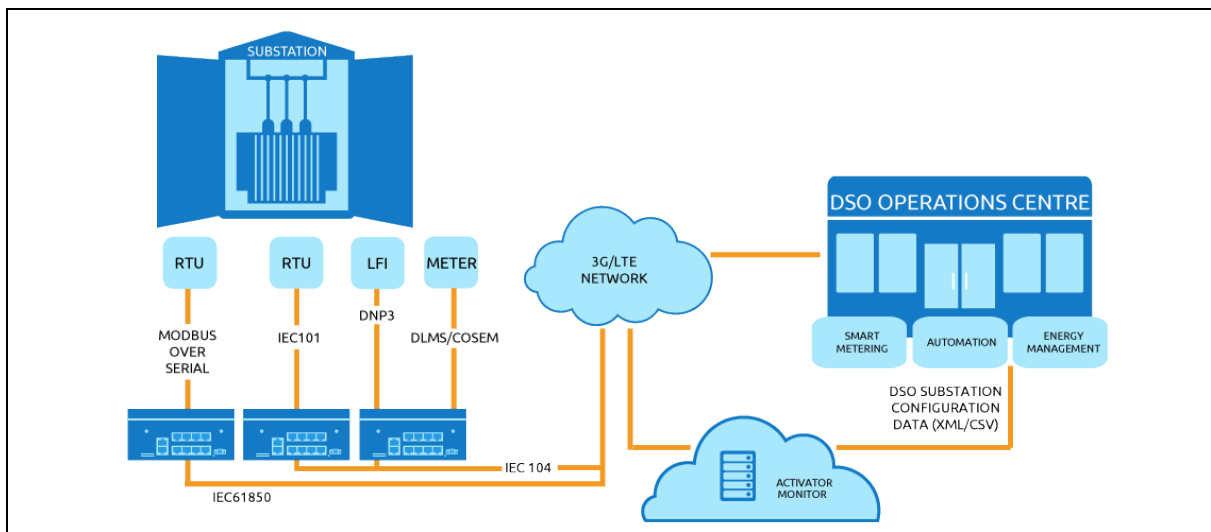
Supervisory control and data acquisition (SCADA) systems are used by industrial organisations and companies to control and monitor physical processes, examples of which are electricity transmission, gas and oil transportation in pipelines, water distribution and traffic lights control. Alarm handling is usually an important part of most SCADA implementations.

SCADA systems usually consist of:

- Supervisory computers
- Remote terminal units (RTUs)
- Programmable logic controllers (PLCs)

The IEC104 gateway feature on the router is used for SCADA protocol conversion where the SCADA master is running IEC104 protocol:

- IEC104 to IEC101 conversion (balanced and unbalanced)
- IEC104 to DNP3
- IEC104 to MODBUS (serial and TCP)
- IEC61850 to IEC101 unbalanced conversion



**Figure 269: Example network for IEC104 to RTU protocol conversion**

Configuration for the above conversions is done in two parts:

- IEC104 gateway (iecd package), and
- Terminal server (tservd package).

The IEC104 gateway handles the protocol processing while the terminal server handles low level serial communication.

**Note:** the terminal server is not required for IEC104 to Modbus TCP.

## 50.2 Configuration packages used

| Package | Sections          |
|---------|-------------------|
| iecd    | main, port, point |
| tservd  | main, port        |

## 50.3 IEC104 gateway configuration using the web interface

In the top menu, select **Services -> IEC104 Gateway**. The IEC104 gateway page appears.

**Figure 270: The IEC104 gateway configuration page**

There are four sections in the IEC104 Gateway page:

| Section       | Description   |
|---------------|---|
| Main Settings | Enables the IEC104 gateway.   |
| Port Settings | Sets the IEC104 SCADA master communication settings and the protocol methods used by the RTUs: <ul style="list-style-type: none"> <li>• IEC101 unbalanced or balanced</li> <li>• DNP3</li> <li>• Modbus over serial</li> <li>• Modbus over TCP</li> </ul>   |
| IEC101 Links  | Defines the IEC101 slave links used in IEC101 conversion. Each link is defined by a config iec101link section block.<br>There is a maximum of 32 links supported.<br>In IEC101 unbalanced mode all of these links can be used. In IEC101 balanced mode only one outstation per serial port is assumed since these will be point to point links. |
| Points        | Configures the data point mappings.<br><b>Note:</b> there are no data point mappings in IEC104 to IEC101 conversion.  |

### 50.3.1 Main settings



Figure 271: The IEC104 gateway main settings configuration page

| Web Field/UCI/Package Option | Description             |
|------------------------------|-------------------------|
| Web: Enable                  | Enables IEC104 gateway. |
| UCI: iecd.main.enable        | 0 Disabled.             |
| Opt: enable                  | 1 Enabled.              |

Table 199: Information table for IEC104 gateway main settings configuration

### 50.3.2 Port settings

The port configuration will depend on the desired protocol conversion. There are 5 sections.

| Section  | Description   |
|----------|---|
| General  | Enables an IEC104 port and selects the RTU protocol method.                                 |
| IEC104   | Defines the IEC104 gateway configuration for communication with the SCADA Master.           |
| IEC101   | Defines the IEC104 to IEC101 conversion parameters.   |
| DNP3     | Defines the IEC104 to DNP3 conversion parameters.   |
| Modbus   | Defines the IEC104 to MODBUS conversion parameters (Modbus over serial or Modbus over TCP). |
| Advanced | Defines logging and TCP keepalive options for all conversion methods.                       |

In the Port Settings section, enter a text name that will be used for the iecd port section, for example, Port1. Select **Add**. The IECD port configuration options appear.

#### 50.3.2.1 Port settings: general

In this section you can configure general port settings. Check **Enable** to enable the port and select the appropriate RTU protocol from the Slave Protocol and Master Protocol drop-down menus.

Port Settings Delete

**PORT1**

General IEC104 IEC101 DNP3 Modbus Advanced

Enable  [Enables IEC104 Gateway port](#)

Slave Protocol  [Sets protocol method used by SCADA master to connect to this router \(acting as a slave\)](#)

Master Protocol  [Sets protocol method used by this router \(acting as a master\) to connect to outstations](#)

**Figure 272: The IEC104 gateway port general configuration page**

| Web Field/UCI/Package Option   | Description   |        |           |        |          |          |          |        |        |
|--|---|--------|-----------|--------|----------|----------|----------|--------|--------|
| Web: Enable<br>UCI: iecd.<port>.enable<br>Opt: enable                            | Enables an IEC104 port.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0      | Disabled. | 1      | Enabled. |          |          |        |        |
| 0  | Disabled.   |        |           |        |          |          |          |        |        |
| 1  | Enabled.  |        |           |        |          |          |          |        |        |
| Web: Slave Protocol<br>UCI: iecd.<port>.slave_protocol<br>Opt: slave_protocol    | Defines the protocol method used by the SCADA master to connect to this router (acting as slave).<br><table border="1"> <tr> <td>iec104</td> <td>IEC104</td> </tr> <tr> <td>modbus</td> <td>MODBUS</td> </tr> <tr> <td>iec61850</td> <td>IEC61850</td> </tr> </table>                                     | iec104 | IEC104    | modbus | MODBUS   | iec61850 | IEC61850 |        |        |
| iec104   | IEC104  |        |           |        |          |          |          |        |        |
| modbus   | MODBUS  |        |           |        |          |          |          |        |        |
| iec61850   | IEC61850  |        |           |        |          |          |          |        |        |
| Web: Master Protocol<br>UCI: iecd.<port>.master_protocol<br>Opt: master_protocol | Defines the protocol method used by this router (acting as a master) to connect to the outstations.<br><table border="1"> <tr> <td>iec101</td> <td>IC101</td> </tr> <tr> <td>iec104</td> <td>IEC104</td> </tr> <tr> <td>dnp3</td> <td>DNP3</td> </tr> <tr> <td>modbus</td> <td>MODBUS</td> </tr> </table> | iec101 | IC101     | iec104 | IEC104   | dnp3     | DNP3     | modbus | MODBUS |
| iec101   | IC101   |        |           |        |          |          |          |        |        |
| iec104   | IEC104  |        |           |        |          |          |          |        |        |
| dnp3   | DNP3  |        |           |        |          |          |          |        |        |
| modbus   | MODBUS  |        |           |        |          |          |          |        |        |
| Web: n/a<br>UCI: iecd.<port>.pointmap_file<br>Opt: pointmap_file                 | Defines the path to the points map file, for example:<br>/root/iecd/iecd_points1.csv  |        |           |        |          |          |          |        |        |

**Table 200: Information table for IEC104 gateway port general configuration**



### 50.3.2.2 Port settings: IEC104

In this section you can configure IEC104 settings.

**PORT1**

General IEC104 IEC101 DNP3 Modbus Advanced

**IEC104 Track RTU DL**   0=Keep IEC104 Always Up; 1=IEC104 UP only while RTU data link up

IEC104 IOA Offset  Value to add to each Information Object Address of each configured point

IEC104 Local IP  Local IP address this IEC104 peer binds to

IEC104 Listening TCP Port  Local TCP port this IEC104 peer listens on

IEC61850 Local IP  Local IP address this IEC61850 peer binds to

IEC61850 Listening TCP Port  Local TCP port this IEC61850 peer listens on

IEC104 K  Maximum number of outstanding I frames

IEC104 W  Receiver acknowledges sender frames after at most W frames (Recommended 2/3 of K)

IEC104 T2  Timeout for sending S frames in case of no data (milliseconds)

Enable IEC104 time synchronization   Enables synchronization of router time to IEC104 master time

Transfer comms status in NT bit   Enables transfer of RTU comms status in IEC104 Not Topical bit with each data point

IEC104 CASDU  Common ASDU address

Send EOI   Enables sending of IEC104 End Of Initialization message to Master

Enable IEC 62351-5 secure mode   Enables IEC 62351-5 security

**Figure 273: The IEC104 gateway port IEC104 configuration page**

| Web Field/UCI/Package Option   | Description  |         |   |       |   |
|--|--|---------|---|-------|---|
| Web: IEC104 Track RTU DL<br>UCI: iecd.<port>.iec104_track_rtu_dl<br>Opt: iec104_track_rtu_dl         | Defines whether the IEC104 link follows the state of the RTU data link. <table border="1" style="width: 100%;"> <tr> <td style="width: 50px; text-align: center;">0</td> <td>Always listens and accepts connection from the IEC104 master. This means IEC104 is always up independently of the RTU protocol.</td> </tr> <tr> <td style="width: 50px; text-align: center;">1</td> <td>IEC104 is up only while RTU data link is up. The IEC104 socket is closed and IEC104 will only start listening when RTU data link is up.</td> </tr> </table> | 0       | Always listens and accepts connection from the IEC104 master. This means IEC104 is always up independently of the RTU protocol. | 1     | IEC104 is up only while RTU data link is up. The IEC104 socket is closed and IEC104 will only start listening when RTU data link is up. |
| 0  | Always listens and accepts connection from the IEC104 master. This means IEC104 is always up independently of the RTU protocol.  |         |   |       |   |
| 1  | IEC104 is up only while RTU data link is up. The IEC104 socket is closed and IEC104 will only start listening when RTU data link is up.  |         |   |       |   |
| Web: IEC104 IOA Offset<br>UCI: iecd.<port>.ioa_offset<br>Opt: ioa_offset                             | Defines the value to add to each Information Object Address of each configured point. <table border="1" style="width: 100%;"> <tr> <td style="width: 50px; text-align: center;">0</td> <td></td> </tr> <tr> <td style="width: 50px; text-align: center;">Range</td> <td></td> </tr> </table>   | 0       |   | Range |   |
| 0  |  |         |   |       |   |
| Range  |  |         |   |       |   |
| Web: IEC104 Local IP<br>UCI: iecd.<port>.iec104_local_ip<br>Opt: iec104_local_ip                     | Defines the local IP address this IEC104 peer binds to. <table border="1" style="width: 100%;"> <tr> <td style="width: 50px; text-align: center;">0.0.0.0</td> <td>Bind to outgoing port.</td> </tr> <tr> <td style="width: 50px; text-align: center;">Range</td> <td></td> </tr> </table>   | 0.0.0.0 | Bind to outgoing port.  | Range |   |
| 0.0.0.0  | Bind to outgoing port.   |         |   |       |   |
| Range  |  |         |   |       |   |
| Web: IEC104 Listening TCP Port<br>UCI: iecd.<port>.iec104_local_tcpport<br>Opt: iec104_local_tcpport | Defines the local TCP port this IEC104 peer listens on. <table border="1" style="width: 100%;"> <tr> <td style="width: 50px; text-align: center;">2404</td> <td></td> </tr> <tr> <td style="width: 50px; text-align: center;">Range</td> <td>1 - 65535</td> </tr> </table>   | 2404    |   | Range | 1 - 65535   |
| 2404   |  |         |   |       |   |
| Range  | 1 - 65535  |         |   |       |   |
| Web: IEC61850 Local IP<br>UCI: iecd.<port>.iec61850_local_ip<br>Opt: iec61850_local_ip               | Defines the local IP address this IEC61850 peer binds to. <table border="1" style="width: 100%;"> <tr> <td style="width: 50px; text-align: center;">0.0.0.0</td> <td>Bind to outgoing port.</td> </tr> <tr> <td style="width: 50px; text-align: center;">Range</td> <td></td> </tr> </table>   | 0.0.0.0 | Bind to outgoing port.  | Range |   |
| 0.0.0.0  | Bind to outgoing port.   |         |   |       |   |
| Range  |  |         |   |       |   |

|   |  |
|---|--|
| Web: IEC61850 Listening TCP Port<br>UCI: iecd.<port>.iec61850_local_tcpport<br>Opt: iec61850_local_tcpport        | Defines the local TCP port this IEC61850 peer listens on.<br>102<br>Range 1 - 65535  |
| Web: IEC104 K<br>UCI: iecd.<port>.iec104_k<br>Opt: iec104_k   | Defines the maximum number of outstanding I frames.<br>12<br>Range   |
| Web: IEC104 W<br>UCI: iecd.<port>.iec104_w<br>Opt: iec104_w   | Defines the number of frames after which the receiver will acknowledge. It is recommended that this value is 2/3 the value of IEC104 K.<br>9<br>Range  |
| Web: IEC104 T2<br>UCI: iecd.<port>.iec104_t2<br>Opt: iec104_t2  | Defines the timeout in milliseconds for sending S frames in case of no data.<br>10000 milliseconds<br>Range  |
| Web: Enable IEC104 time synchronization<br>UCI: iecd.<port>.iec104_sync_time<br>Opt: iec104_sync_time             | Enables synchronisation of router time to IEC104 master time.<br>1 Enable synchronisation.<br>0 Disable synchronisation.   |
| Web: Transfer comms status in NT bit<br>UCI:<br>iecd.<port>.iec104_comms_status_nt<br>Opt: iec104_comms_status_nt | Enables transfer of RTU comms status in IEC104 Not Topical bit with each data point.<br>0<br>1   |
| Web: IEC104 CASDU<br>UCI: iecd.<port>.iec104_casdu<br>Opt: iec104_casdu   | Defines IEC104 common ASDU address.<br>1<br>Range  |
| Web: Send EOI<br>UCI: iecd.<port>.iec104_send_eoi<br>Opt: iec104_send_eoi   | Enables sending of IEC104 End Of Initialisation message to the master.<br>0<br>1   |
| Web: Enable IEC 62351-5 secure mode<br>UCI: iecd.<port>.iec104_secure_on<br>Opt: iec104_secure_on                 | Enables IEC 62351-5 security.<br>0<br>1  |
| Web: n/a<br>UCI: iecd.<port>.iec104_rtu_dl_start_dt<br>Opt: iec104_rtu_dl_start_dt                                | Defines the start operation of the RTU data link.<br>0 The RTU data link is always started and established at startup and kept up.<br>1 The RTU data link layer is started and established when IEC104 is up <b>and</b> the START DT message from the IEC104 master is received. When the RTU data link comes up: send START DT CONF to the IEC104 master. |
| Web: n/a<br>UCI: iecd.<port>.iec104_gi_resp_time<br>Opt: iec104_gi_resp_time                                      | Defines the time in milliseconds between sending successive general interrogation response messages.<br>200 milliseconds<br>Range 50 - 1000  |
| Web: n/a<br>UCI: iecd.<port>.iec104_txq_size<br>Opt: iec104_txq_size  | Defines the maximum size of transmit ASDU queue in the application layer (number of frames).<br>128<br>Range 2 - 256   |
| Web: n/a<br>UCI: iecd.<port>.iec104_cmd_delay_time<br>Opt: iec104_cmd_delay_time                                  | Defines the maximum allowable received command age in milliseconds. If set to 0, control commands time verification is disabled.<br>5000 Milliseconds.<br>Range 1000 - 60000   |

|  |  |   |         |   |          |
|--|--|---|---------|---|----------|
| Web: n/a<br>UCI: iecd.<port>.iec104_fsm_debug_on<br>Opt: iec104_fsm_debug_on | Enables the log for IEC104 state transitions and events.<br><table border="1"> <tr><td>0</td><td>Enable.</td></tr> <tr><td>1</td><td>Disable.</td></tr> </table> | 0 | Enable. | 1 | Disable. |
| 0  | Enable.  |   |         |   |          |
| 1  | Disable.   |   |         |   |          |
| Web: n/a<br>UCI: iecd.<port>.iec104_dump_data<br>Opt: iec104_dump_data       | Enables RX/TX Hex dump.<br><table border="1"> <tr><td>0</td><td>Enable.</td></tr> <tr><td>1</td><td>Disable.</td></tr> </table>                                  | 0 | Enable. | 1 | Disable. |
| 0  | Enable.  |   |         |   |          |
| 1  | Disable.   |   |         |   |          |
| Web: n/a<br>UCI: iecd.<port>.iec104_trace_on<br>Opt: iec104_trace_on         | Enables protocol tracing.<br><table border="1"> <tr><td>0</td><td>Enable.</td></tr> <tr><td>1</td><td>Disable.</td></tr> </table>                                | 0 | Enable. | 1 | Disable. |
| 0  | Enable.  |   |         |   |          |
| 1  | Disable.   |   |         |   |          |

**Table 201: Information table for IEC104 gateway port IEC104 configuration**

### 50.3.2.3 Port settings: IEC101

The IEC104 to IEC101 conversion feature on the router allows converting commands in the control direction, and the responses and process data in the monitor direction, between the SCADA master running the IEC104 protocol and the remote RTUs running IEC101 protocol over a serial interface.

IEC104 to IEC101 conversion can be configured for two modes:

| IEC 101 Mode | Description   |
|--------------|---|
| Unbalanced   | In IEC101 unbalanced mode, the router supports communication of up to 32 IEC101 slaves connected onto the same serial interface.  |
| Balanced     | IEC101 balanced mode is used in point-to-point configuration. That is, the router is communicating to a single IEC101 outstation on the serial interface. Each peer, either the controlling station (Master) or controlled station (RTU) can initiate communication in balanced mode. |

Port Settings Delete

**PORT1**

General IEC104 IEC101 DNP3 Modbus Advanced

---

IEC101 Station Target IP:  Remote IP address of IEC101 station to connects to

IEC101 Station Target TCP Port:  Remote TCP port of IEC101 station to connect to

IEC101 Link Mode:  Specifies IEC101 link communication mode

IEC101 Station COT Tx Length:  Cause Of Transmission length (1 or 2 bytes)

IEC101 Station COT Source Octet:  Most significant octet in the cause of transmission field

IEC101 Station ASDU Addr Length:  Length of Common Address of ASDU (1 or 2 bytes)

IEC101 Station Info Object Addr Length:  Length of the information object address (1, 2 or 3 bytes)

IEC101 Station poll time:  RTU polling interval if line idle (milliseconds)

IEC101 Station Link Addr Length:  Length of the link address field (0, 1 or 2 bytes)

**Figure 274: The IEC104 gateway port IEC101 configuration page**

| Web Field/UCI/Package Option  | Description  |
|---|--|
| Web: IEC101 Station Target IP<br>UCI: iecd.<port>.iec101_target_ip<br>Opt: iec101_target_ip                           | Defines the remote IP address of the IEC101 station to connect to.<br>127.0.0.1<br>Range                   |
| Web: IEC101 Station Target TCP Port<br>UCI: iecd.<port>.iec101_target_tcpport<br>Opt: iec101_target_tcpport           | Defines the remote TCP port of the IEC101 station to connect to.<br>999<br>Range                           |
| Web: IEC101 Link Mode<br>UCI: iecd.<port>.iec101_mode<br>Opt: iec101_mode   | Defines the IEC101link communication mode.<br>unbalanced<br>balanced                                       |
| Web: IEC101 Station COT Tx Length<br>UCI: iecd.<port>.iec101_cot_tx_length<br>Opt: iec101_cot_tx_length               | Defines the Cause of Transmission length (1 or 2 bytes).<br>2 bytes<br>Range                               |
| Web: IEC101 Station COT Source Length<br>UCI: iecd.<port>.iec101_cot_source_octet<br>Opt: iec101_cot_source_octet     | Defines the most significant octet in the Cause of Transmission field.<br>0<br>Range                       |
| Web: IEC101 Station ASDU Addr Length<br>UCI: iecd.<port>.iec101_asdu_addrln<br>Opt: iec101_asdu_addrln                | Defines the length of Common Address of ASDU (1 or 2 bytes).<br>2 bytes<br>Range                           |
| Web: IEC101 Station Info Object Addr Length<br>UCI: iecd.<port>.iec101_info_obj_addrln<br>Opt: iec101_info_obj_addrln | Defines the length of the Information Object Address (1, 2 or 3 bytes).<br>2 bytes<br>Range                |
| Web: IEC101 Station Poll Time<br>UCI: iecd.<port>.iec101_data_polling_time<br>Opt: iec101_data_polling_time           | Defines the RTU polling interval in milliseconds if the line is idle.<br>10000 milliseconds<br>Range       |
| Web: IEC101 Link Addr Length<br>UCI: iecd.<port>.iec101_link_addrln<br>Opt: iec101_link_addrln                        | Defines the length of the link address field (0, 1 or 2 bytes).<br>1 bytes<br>Range                        |
| Web: n/a<br>UCI: iecd.<port>.iec101_ack_delay<br>Opt: iec101_ack_delay  | Defines the time to wait in milliseconds for an IEC101 ACK.<br>0 seconds<br>Range                          |
| Web: n/a<br>UCI: iecd.<port>.iec101_frame_rsp_time<br>Opt: iec101_frame_rsp_time                                      | Defines the maximum number of milliseconds before resending an IEC101 frame.<br>2000 milliseconds<br>Range |
| Web: n/a<br>UCI: iecd.<port>.iec101_max_tx_retry<br>Opt: iec101_max_tx_retry  | Defines the maximum number of times to retry sending an IEC101 frame.<br>3<br>Range                        |
| Web: n/a<br>UCI: iecd.<port>.iec101_txq_size<br>Opt: iec101_txq_size  | Defines the size of transmit ASDU queue (number of frames) in the IEC101 link layer.<br>128<br>Range       |

|  |  |   |  |   |   |
|--|--|---|--|---|---|
| Web: n/a<br>UCI: iecd.<port>.iec101_send_spont_delay_acq<br>Opt: iec101_send_spont_delay_acq | Defines whether to send DELAY ACQUISITION SPONTANEOUS message as part of 'Acquisition of Transmission Delay' procedure.<br><b>Note:</b> this option is used in the scenario where an IEC104 Master is talking to an IEC101 RTU. <table border="1"> <tr> <td>0</td> <td>Do not send DELAY ACQUISITION SPONTANEOUS message.</td> </tr> <tr> <td>1</td> <td>Send DELAY ACQUISITION SPONTANEOUS message.</td> </tr> </table> | 0 | Do not send DELAY ACQUISITION SPONTANEOUS message. | 1 | Send DELAY ACQUISITION SPONTANEOUS message. |
| 0  | Do not send DELAY ACQUISITION SPONTANEOUS message.   |   |  |   |   |
| 1  | Send DELAY ACQUISITION SPONTANEOUS message.  |   |  |   |   |
| Web: n/a<br>UCI: iecd.<port>.iec101_fsm_debug_on<br>Opt: iec101_fsm_debug_on                 | Enables logging IEC104 state transitions and events. <table border="1"> <tr> <td>0</td> <td></td> </tr> <tr> <td>1</td> <td></td> </tr> </table>   | 0 |  | 1 |   |
| 0  |  |   |  |   |   |
| 1  |  |   |  |   |   |
| Web: n/a<br>UCI: iecd.<port>.iec101_dump_data<br>Opt: iec101_dump_data                       | Enables RX/TX Hex dump. <table border="1"> <tr> <td>0</td> <td></td> </tr> <tr> <td>1</td> <td></td> </tr> </table>  | 0 |  | 1 |   |
| 0  |  |   |  |   |   |
| 1  |  |   |  |   |   |
| Web: n/a<br>UCI: iecd.<port>.iec101_trace_on<br>Opt: iec101_trace_on                         | Enables IEC101 protocol tracing. <table border="1"> <tr> <td>0</td> <td></td> </tr> <tr> <td>1</td> <td></td> </tr> </table>   | 0 |  | 1 |   |
| 0  |  |   |  |   |   |
| 1  |  |   |  |   |   |

**Table 202: Information table for IEC104 gateway port IEC101 configuration**

### 50.3.2.4 Port settings: DNP3

The IEC104 to DNP3 conversion feature on the router allows converting commands in the control direction, and the responses and process data in the monitor direction, between the SCADA master running the IEC104 protocol and the remote RTU running DNP3 over serial protocol.

Port Settings Delete

**PORT1**

General IEC104 IEC101 **DNP3** Modbus Advanced

---

DNP3 Station Target IP:  Remote IP address of DNP3 station to connects to

DNP3 Station Target TCP Port:  Remote TCP port of DNP3 station to connect to

DNP3 Master Station Address:  Local (Master) DNP3 address

DNP3 Outstation Address:  Remote (Outstation) DNP3 address

Enable DNP3 Data Link Confirms:  Enables DNP3 Data Link Level User Data Confirmations

DNP3 Data Link Keep Alive:  DNP3 Data Link Keep Alive interval in milliseconds (0=disable)

DNP3 Frame Response Time:  Maximum time allowed to receive frame acknowledge from DNP3 outstation (milliseconds)

DNP3 Maximum Frame Retry:  Maximum number of times to retry confirmed frame delivery to DNP3 outstation

DNP3 Outstation Poll Time:  DNP3 Outstation Poll Time in milliseconds

Enable DNP3 Unsolicited Responses:  Enables DNP3 Application Level Unsolicited Responses

Enable DNP3 Time Synchronization:  Enables DNP3 Time Synchronization

**Figure 275: The IEC104 gateway port DNP3 configuration page**

| Web Field/UCI/Package Option   | Description  |       |              |       |           |
|--|--|-------|--------------|-------|-----------|
| Web: DNP3 Station Target IP<br>UCI: iecd.<port>.dnp3_target_ip<br>Opt: dnp3_target_ip                          | Defines the remote IP address of the DNP3 station to connect to.   |       |              |       |           |
| Web: DNP3 Station Target TCP Port<br>UCI: iecd.<port>.dnp3_target_tcpport<br>Opt: dnp3_target_tcpport          | Defines the remote TCP port of the DNP3 station to connect to.<br><table border="1"> <tr><td>999</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>  | 999   |              | Range |           |
| 999  |  |       |              |       |           |
| Range  |  |       |              |       |           |
| Web: DNP3 Master Station Address<br>UCI: iecd.<port>.dnp3_dl_srcaddr<br>Opt: dnp3_dl_srcaddr                   | Defines the local (Master) DNP3 address.<br><table border="1"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>  | 0     |              | Range |           |
| 0  |  |       |              |       |           |
| Range  |  |       |              |       |           |
| Web: DNP3 Outstation Address<br>UCI: iecd.<port>.dnp3_dl_dstaddr<br>Opt: dnp3_dl_dstaddr                       | Defines the remote (Outstation) DNP3 address.<br><table border="1"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>   | 0     |              | Range |           |
| 0  |  |       |              |       |           |
| Range  |  |       |              |       |           |
| Web: Enable DNP3 Data Link Confirms<br>UCI: iecd.<port>.dnp3_dl_cfrm_user_data<br>Opt: dnp3_dl_cfrm_user_data  | Enables DNP3 data link layer user data confirmations.<br><table border="1"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>   | 0     |              | Range |           |
| 0  |  |       |              |       |           |
| Range  |  |       |              |       |           |
| Web: DNP3 Data Link Keep Alive<br>UCI: iecd.<port>.dnp3_dl_keep_alive_int<br>Opt: dnp3_dl_keep_alive_int       | Defines the DNP3 data link keepalive interval in milliseconds (0 to disable).<br><table border="1"> <tr><td>15000</td><td>Milliseconds</td></tr> <tr><td>Range</td><td></td></tr> </table>   | 15000 | Milliseconds | Range |           |
| 15000  | Milliseconds   |       |              |       |           |
| Range  |  |       |              |       |           |
| Web: DNP3 Frame Response Time<br>UCI: iecd.<port>.dnp3_dl_frame_rsp_time<br>Opt: dnp3_dl_frame_rsp_time        | Defines the maximum amount of time in milliseconds to receive a frame acknowledgement from the DNP3 outstation.<br><table border="1"> <tr><td>1000</td><td>Milliseconds</td></tr> <tr><td>Range</td><td></td></tr> </table>              | 1000  | Milliseconds | Range |           |
| 1000   | Milliseconds   |       |              |       |           |
| Range  |  |       |              |       |           |
| Web: DNP3 Maximum Frame Retry<br>UCI: iecd.<port>.dnp3_dl_max_tx_retry<br>Opt: dnp3_dl_max_tx_retry            | Defines the maximum number of times to retry confirmed frame delivery to the DNP3 outstation.<br><table border="1"> <tr><td>3</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>   | 3     |              | Range |           |
| 3  |  |       |              |       |           |
| Range  |  |       |              |       |           |
| Web: DNP3 Outstation Poll Time<br>UCI: iecd.<port>.dnp3_app_poll_time<br>Opt: dnp3_app_poll_time               | Defines the DNP3 outstation poll time in milliseconds.<br><table border="1"> <tr><td>30000</td><td>Milliseconds</td></tr> <tr><td>Range</td><td></td></tr> </table>  | 30000 | Milliseconds | Range |           |
| 30000  | Milliseconds   |       |              |       |           |
| Range  |  |       |              |       |           |
| Web: Enable DNP3 Unsolicited Responses<br>UCI: iecd.<port>.dnp3_app_unsol_enable<br>Opt: dnp3_app_unsol_enable | Enables DNP3 application level unsolicited responses.<br><table border="1"> <tr><td>1</td><td>Enabled.</td></tr> <tr><td>0</td><td>Disabled.</td></tr> </table>  | 1     | Enabled.     | 0     | Disabled. |
| 1  | Enabled.   |       |              |       |           |
| 0  | Disabled.  |       |              |       |           |
| Web: Enable DNP3 Time Synchronization<br>UCI: iecd.<port>.dnp3_app_sync_time<br>Opt: dnp3_app_sync_time        | Enables DNP3 time synchronisation.<br><table border="1"> <tr><td>1</td><td>Enabled.</td></tr> <tr><td>0</td><td>Disabled.</td></tr> </table>   | 1     | Enabled.     | 0     | Disabled. |
| 1  | Enabled.   |       |              |       |           |
| 0  | Disabled.  |       |              |       |           |
| Web: n/a<br>UCI: iecd.<port>.dnp3_dl_utxq_size<br>Opt: dnp3_dl_utxq_size                                       | Defines the size of DNP3 data link transmit unconfirmed service frame queue (number of frames).<br><table border="1"> <tr><td>128</td><td></td></tr> <tr><td>Range</td><td>2 - 256</td></tr> </table>                                    | 128   |              | Range | 2 - 256   |
| 128  |  |       |              |       |           |
| Range  | 2 - 256  |       |              |       |           |
| Web: n/a<br>UCI: iecd.<port>.dnp3_dl_ctxq_size<br>Opt: dnp3_dl_ctxq_size                                       | Defines the size of DNP3 data link transmit confirmed service frame queue (number of frames).<br><table border="1"> <tr><td>128</td><td></td></tr> <tr><td>Range</td><td>2 - 256</td></tr> </table>                                      | 128   |              | Range | 2 - 256   |
| 128  |  |       |              |       |           |
| Range  | 2 - 256  |       |              |       |           |
| Web: n/a<br>UCI: iecd.<port>.dnp3_app_read_attr<br>Opt: dnp3_app_read_attr                                     | Enables reading DNP3 device attributes at the start of the session. This feature is useful for debugging and is not recommended for production.<br><table border="1"> <tr><td>0</td><td></td></tr> <tr><td>1</td><td></td></tr> </table> | 0     |              | 1     |           |
| 0  |  |       |              |       |           |
| 1  |  |       |              |       |           |

|  |  |
|--|--|
| Web: n/a<br>UCI: iecd.<port>.dnp3_app_firstpoll_delay<br>Opt: dnp3_app_firstpoll_delay       | Defines initial timeout from start-up in milliseconds before performing the first DNP3 integrity poll.<br>5000 milliseconds<br>Range 5000 – 65535  |
| Web: n/a<br>UCI: iecd.<port>.dnp3_app_evpoll_time<br>Opt: dnp3_app_evpoll_time               | Defines DNP3 outstation event polling interval in milliseconds.<br>3000 milliseconds<br>Range 1000 – 65535   |
| Web: n/a<br>UCI: iecd.<port>.dnp3_app_frag_rx_time<br>Opt: dnp3_app_frag_rx_time             | Defines DNP3 application level fragment response timeout.<br>10000 Milliseconds<br>Range 1000 – 65535  |
| Web: n/a<br>UCI: iecd.<port>.dnp3_app_txq_size<br>Opt:                                       | Defines DNP3 application level transmit queue size (number of frames).<br>64<br>Range 2 – 256  |
| Web: n/a<br>UCI: iecd.<port>.dnp3_app_output_mode<br>Opt: dnp3_app_output_mode               | Defines a decimal code that controls how the router sends a DNP3 binary output command to a DNP3 RTU. The most commonly used model is Select/Operate.<br><b>Note:</b> this command is used where the router is acting as a DNP3 master.<br>0 Use WRITE command.<br>1 Use Select/Operate message sequence.<br>2 Use Direct Operate message. |
| Web: n/a<br>UCI: iecd.<port>.dnp3_app_evpoll_mode<br>Opt: dnp3_app_evpoll_mode               | Defines DNP3 outstation event polling interval in milliseconds.<br>3000 milliseconds<br>Range 1000 – 65535   |
| Web: n/a<br>UCI: iecd.<port>.dnp3_fsm_debug_on<br>Opt: dnp3_fsm_debug_on                     | Enables DNP3 link and application level state machine transition and event logging into syslog.<br>1 Enabled.<br>0 Disabled.   |
| Web: n/a<br>UCI: iecd.<port>.dnp3_object_parser_debug_on<br>Opt: dnp3_object_parser_debug_on | Enables or disables logging low level debug information when parsing DNP3 objects in the received DNP3 slave messages<br>1 Enabled.<br>0 Disabled.   |
| Web: n/a<br>UCI: iecd.<port>.dnp3_dump_data<br>Opt: dnp3_dump_data                           | Enables RX/TX Hex dump.<br>1 Enabled.<br>0 Disabled.   |
| Web: n/a<br>UCI: iecd.<port>.dnp3_trace_on<br>Opt: dnp3_trace_on                             | Enables DNP3 protocol tracing.<br>1 Enabled.<br>0 Disabled.  |

Table 203: Information table for IEC104 gateway port DNP3 configuration

### 50.3.2.5 Port settings: Modbus

The IEC104 to Modbus conversion feature on the router allows converting commands in the control direction and the responses and process data in the monitor direction between the SCADA Master running the IEC104 protocol and the remote RTUs running Modbus protocol.

The router software supports two variations of the Modbus protocol:

- Modbus over serial: the Modbus devices are connected to the serial interface of the router.
- Modbus TCP: the Modbus devices are located on the IP network reachable from the router.

In the Modbus over serial variation, currently the router supports Modbus 'RTU mode' frame format of the Modbus specification only.

Port Settings Delete

**PORT1**

General IEC104 IEC101 DNP3 **Modbus** Advanced

Modbus protocol Modbus Serial ⓘ Sets protocol variation used by RTU that connects to this router

Modbus local IP 0.0.0.0 ⓘ Local IP interface to use in modbus mode

Modbus local port 888 ⓘ Local port to use in modbus mode

Modbus remote IP 127.0.0.1 ⓘ Remote IP address to use in modbus mode

Modbus remote port 999 ⓘ Remote port to use in modbus mode

Modbus polling time 3000 ⓘ Modbus slave polling interval in milliseconds

Modbus frame response time 1000 ⓘ Maximum time allowed to receive a response frame from a Modbus slave (milliseconds)

**Figure 276: The IEC104 gateway port modbus configuration page**

| Web Field/UCI/Package Option  | Description  |  |                    |       |               |                    |               |            |                 |            |
|---|--|--|--------------------|-------|---------------|--------------------|---------------|------------|-----------------|------------|
| Web: Modbus Protocol<br>UCI: iecd.<port>.modbus_protocol<br>Opt: modbus_protocol              | Defines the protocol variation used by RTU that connects to this router. <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Option</th> <th>Description</th> <th>UCI</th> </tr> </thead> <tbody> <tr> <td>Modbus Serial</td> <td>Modbus over serial</td> <td>modbus_serial</td> </tr> <tr> <td>Modbus TCP</td> <td>Modbus over TCP</td> <td>modbus_tcp</td> </tr> </tbody> </table> | Option   | Description        | UCI   | Modbus Serial | Modbus over serial | modbus_serial | Modbus TCP | Modbus over TCP | modbus_tcp |
| Option  | Description  | UCI  |                    |       |               |                    |               |            |                 |            |
| Modbus Serial   | Modbus over serial   | modbus_serial  |                    |       |               |                    |               |            |                 |            |
| Modbus TCP  | Modbus over TCP  | modbus_tcp   |                    |       |               |                    |               |            |                 |            |
| Web: Modbus local IP<br>UCI: iecd.<port>.modbus_local_ip<br>Opt: modbus_local_ip              | Defines the local IP to use in Modbus mode. <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td style="width: 50%;"><span style="border: 1px solid gray; padding: 2px;">0.0.0.0</span></td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </tbody> </table>  | <span style="border: 1px solid gray; padding: 2px;">0.0.0.0</span>   |                    | Range |               |                    |               |            |                 |            |
| <span style="border: 1px solid gray; padding: 2px;">0.0.0.0</span>                            |  |  |                    |       |               |                    |               |            |                 |            |
| Range   |  |  |                    |       |               |                    |               |            |                 |            |
| Web: Modbus local port<br>UCI: iecd.<port>.modbus_local_port<br>Opt: modbus_local_port        | Defines the local port to use in Modbus mode. <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td style="width: 50%;"><span style="border: 1px solid gray; padding: 2px;">888</span></td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </tbody> </table>  | <span style="border: 1px solid gray; padding: 2px;">888</span>       |                    | Range |               |                    |               |            |                 |            |
| <span style="border: 1px solid gray; padding: 2px;">888</span>                                |  |  |                    |       |               |                    |               |            |                 |            |
| Range   |  |  |                    |       |               |                    |               |            |                 |            |
| Web: Modbus remote IP<br>UCI: iecd.<port>.modbus_remote_ip<br>Opt: modbus_remote_ip           | Defines the remote IP address. <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td style="width: 50%;"><span style="border: 1px solid gray; padding: 2px;">127.0.0.1</span></td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </tbody> </table>   | <span style="border: 1px solid gray; padding: 2px;">127.0.0.1</span> |                    | Range |               |                    |               |            |                 |            |
| <span style="border: 1px solid gray; padding: 2px;">127.0.0.1</span>                          |  |  |                    |       |               |                    |               |            |                 |            |
| Range   |  |  |                    |       |               |                    |               |            |                 |            |
| Web: Modbus remote port<br>UCI: iecd.<port>.modbus_remote_port<br>Opt: modbus_remote_port     | Defines the remote port. <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td style="width: 50%;"><span style="border: 1px solid gray; padding: 2px;">999</span></td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </tbody> </table>   | <span style="border: 1px solid gray; padding: 2px;">999</span>       |                    | Range |               |                    |               |            |                 |            |
| <span style="border: 1px solid gray; padding: 2px;">999</span>                                |  |  |                    |       |               |                    |               |            |                 |            |
| Range   |  |  |                    |       |               |                    |               |            |                 |            |
| Web: Modbus polling time<br>UCI: iecd.<port>.modbus_polling_time<br>Opt: modbus_polling_time  | Defines the slave polling interval in milliseconds. <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td style="width: 50%;"><span style="border: 1px solid gray; padding: 2px;">3000</span></td> <td>3000 milliseconds</td> </tr> <tr> <td>Range</td> <td></td> </tr> </tbody> </table>  | <span style="border: 1px solid gray; padding: 2px;">3000</span>      | 3000 milliseconds  | Range |               |                    |               |            |                 |            |
| <span style="border: 1px solid gray; padding: 2px;">3000</span>                               | 3000 milliseconds  |  |                    |       |               |                    |               |            |                 |            |
| Range   |  |  |                    |       |               |                    |               |            |                 |            |
| Web: Modbus frame response time<br>UCI: iecd.<port>.modbus_resp_time<br>Opt: modbus_resp_time | Defines in milliseconds the maximum time allowed to receive a response frame from a Modbus slave. <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td style="width: 50%;"><span style="border: 1px solid gray; padding: 2px;">1000</span></td> <td>1000 milliseconds.</td> </tr> <tr> <td>Range</td> <td></td> </tr> </tbody> </table>   | <span style="border: 1px solid gray; padding: 2px;">1000</span>      | 1000 milliseconds. | Range |               |                    |               |            |                 |            |
| <span style="border: 1px solid gray; padding: 2px;">1000</span>                               | 1000 milliseconds.   |  |                    |       |               |                    |               |            |                 |            |
| Range   |  |  |                    |       |               |                    |               |            |                 |            |
| Web: n/a<br>UCI: iecd.<port>.modbus_dump_data<br>Opt: modbus_dump_data                        | Enables RX/TX Hex dump. <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td style="width: 50%;"><input type="checkbox"/></td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </tbody> </table>  | <input type="checkbox"/>   |                    | Range |               |                    |               |            |                 |            |
| <input type="checkbox"/>  |  |  |                    |       |               |                    |               |            |                 |            |
| Range   |  |  |                    |       |               |                    |               |            |                 |            |
| Web: n/a<br>UCI: iecd.<port>.modbus_trace_on<br>Opt: modbus_trace_on                          | Enables Modbus protocol tracing. <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td style="width: 50%;"><input type="checkbox"/></td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </tbody> </table>   | <input type="checkbox"/>   |                    | Range |               |                    |               |            |                 |            |
| <input type="checkbox"/>  |  |  |                    |       |               |                    |               |            |                 |            |
| Range   |  |  |                    |       |               |                    |               |            |                 |            |

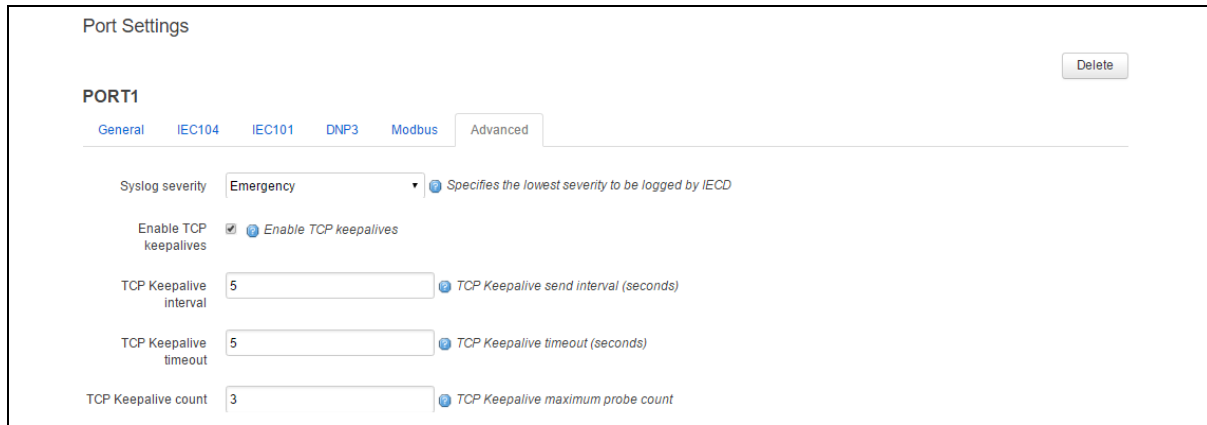


|                                      |   |
|--------------------------------------|---|
| Web: n/a                             | Enables Modbus state machine debugging. |
| UCI: iecd.<port>.modbus_fsm_debug_on |   |
| Opt: modbus_fsm_debug_on             |   |
|                                      | Range                                   |

**Table 204: Information table for IEC104 gateway port modbus configuration**

### 50.3.2.6 Port settings: advanced

In this section you can configure the advanced port settings.



**Figure 277: The IEC104 gateway port advanced configuration page**

| Web Field/UCI/Package Option  | Description   |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |
|---|---|-------|---------------|-------|----------|---|----------|---|-------|---|---------|---|--------|---|---------------|---|-------|
| Web: Syslog severity<br>UCI: iecd.<port>.loglevel<br>Opt: loglevel                                    | Defines the lowest severity used for logging events by iecd.<br><table border="1"> <tr><td>0</td><td>Emergency</td></tr> <tr><td>1</td><td>Alert</td></tr> <tr><td>2</td><td>Critical</td></tr> <tr><td>3</td><td>Error</td></tr> <tr><td>4</td><td>Warning</td></tr> <tr><td>5</td><td>Notice</td></tr> <tr><td>6</td><td>Informational</td></tr> <tr><td>7</td><td>Debug</td></tr> </table> | 0     | Emergency     | 1     | Alert    | 2 | Critical | 3 | Error | 4 | Warning | 5 | Notice | 6 | Informational | 7 | Debug |
| 0   | Emergency   |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 1   | Alert   |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 2   | Critical  |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 3   | Error   |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 4   | Warning   |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 5   | Notice  |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 6   | Informational   |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 7   | Debug   |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |
| Web: Enable TCP keepalives<br>UCI: iecd.<port>.tcp_keepalive_enabled<br>Opt: tcp_keepalive_enabled    | Defines whether to enable TCP keepalive.<br><table border="1"> <tr><td>1</td><td>Disabled.</td></tr> <tr><td>0</td><td>Enabled.</td></tr> </table>  | 1     | Disabled.     | 0     | Enabled. |   |          |   |       |   |         |   |        |   |               |   |       |
| 1   | Disabled.   |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 0   | Enabled.  |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |
| Web: TCP Keepalive interval<br>UCI: iecd.<port>.tcp_keepalive_interval<br>Opt: tcp_keepalive_interval | Defines the TCP keepalive interval in seconds.<br><table border="1"> <tr><td>5</td><td>Seconds.</td></tr> <tr><td>Range</td><td></td></tr> </table>   | 5     | Seconds.      | Range |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 5   | Seconds.  |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |
| Range   |   |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |
| Web: TCP Keepalive timeout<br>UCI: iecd.<port>.tcp_keepalive_timeout<br>Opt: tcp_keepalive_timeout    | Defines the TCP keepalive timeout in seconds.<br><table border="1"> <tr><td>5</td><td>Seconds.</td></tr> <tr><td>Range</td><td></td></tr> </table>  | 5     | Seconds.      | Range |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 5   | Seconds.  |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |
| Range   |   |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |
| Web: TCP Keepalive count<br>UCI: iecd.<port>.tcp_keepalive_count<br>Opt: tcp_keepalive_count          | Defines the number of unanswered keepalives before terminating the TCP session.<br><table border="1"> <tr><td>3</td><td>Seconds.</td></tr> <tr><td>Range</td><td></td></tr> </table>  | 3     | Seconds.      | Range |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 3   | Seconds.  |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |
| Range   |   |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |
| Web: n/a<br>UCI: iecd.<port>.tcp_user_timeout<br>Opt: tcp_user_timeout                                | Defines the maximum time in milliseconds to wait for a TCP ACK after data transmission before closing the connection in TCP established state.<br>Set to <b>0</b> to use kernel defaults (about 15-20 minutes).<br><table border="1"> <tr><td>20000</td><td>milliseconds.</td></tr> <tr><td>Range</td><td></td></tr> </table>   | 20000 | milliseconds. | Range |          |   |          |   |       |   |         |   |        |   |               |   |       |
| 20000   | milliseconds.   |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |
| Range   |   |       |               |       |          |   |          |   |       |   |         |   |        |   |               |   |       |

**Table 205: Information table for IEC104 gateway port advanced configuration**

### 50.3.3 IEC101 links

The following section defines the IEC101 slave links used in IEC101 conversion. Each link is defined by a config `iecd.iec101link` section block. There is a maximum of 32 links supported.

In IEC101 unbalanced mode all of these links can be used. However, as IEC101 balanced mode is used in a point to point scenario, it is assumed there will be only one outstation per serial port. Only the first link configured for that port will be used. Each peer, either the controlling station (Master) or the controlled station (RTU) can initiate communication in balanced mode.

| Port number        | IEC101 Link Address                | IEC101 Link ASDU Addr              |
|--------------------|------------------------------------|------------------------------------|
| (1..4) Serial port | Link address of the IEC101 station | ASDU address of the IEC101 station |
| 1                  | 0                                  | 0                                  |

Buttons: Add, Delete

**Table 206: IEC101 slave links configuration page**

| Web Field/UCI/Package Option  | Description   |
|---|---|
| Web: Port Number<br>UCI: <code>iecd.iec101link[x].portno</code><br>Opt: <code>portno</code>                   | Defines the serial port number to which this point belongs.<br>Range: 1 - 4 |
| Web: IEC101 Link Address<br>UCI: <code>iecd.iec101link[x].address</code><br>Opt: <code>address</code>         | Defines the IEC101 station link address.<br>Range: 0                        |
| Web: IEC101 Link ASDU Station<br>UCI: <code>iecd. iec101link[x].asduaddr</code><br>Opt: <code>asduaddr</code> | Defines the IEC101 station common ASDU address.<br>Range: 0                 |

**Table 207: Information table for IEC104 gateway port IEC101 configuration**

### 50.3.4 Points

IEC104 point mappings are used for DNP3 and Modbus conversion only.

The point mappings comprise the information necessary to perform conversion between each data variable (point) on the remote RTU and the corresponding variable in the IEC104 domain.

Modbus TCP requires a device route file (`/root/iecd/devroute.csv`) to map the point configuration to an IP address. For more information, read the Modbus route file section below.

There is a maximum of 1200 point mappings supported per serial port.

Points Delete

|                                  |                                |   |
|----------------------------------|--------------------------------|---|
| Port number                      | <input type="text" value="1"/> | <a href="#">?</a> (1..4) Serial port                                    |
| IEC101 Type ID                   | <input type="text" value="1"/> | <a href="#">?</a> IEC101 Data Type ID                                   |
| IEC104 Type ID                   | <input type="text" value="1"/> | <a href="#">?</a> IEC104 Data Type ID                                   |
| IEC101 IOA                       | <input type="text" value="1"/> | <a href="#">?</a> IEC101 Information Object Address                     |
| IEC104 IOA                       | <input type="text" value="1"/> | <a href="#">?</a> IEC104 Information Object Address                     |
| Device Addr                      | <input type="text" value="1"/> | <a href="#">?</a> Modbus slave address                                  |
| DNP3 options                     | <input type="text" value="0"/> | <a href="#">?</a> DNP3 options bitmap                                   |
| Group                            | <input type="text" value="0"/> | <a href="#">?</a> DNP3 group id or Modbus data type                     |
| Index                            | <input type="text" value="0"/> | <a href="#">?</a> DNP3 Point index or Modbus data index                 |
| Index2                           | <input type="text" value="0"/> | <a href="#">?</a> DNP3 Point secondary index                            |
| Modbus options                   | <input type="text" value="0"/> | <a href="#">?</a> Modbus options bitmap                                 |
| Modbus bitmap mask               | <input type="text" value="0"/> | <a href="#">?</a> Modbus bitmap mask                                    |
| Modbus CtrlMode index            | <input type="text" value="0"/> | <a href="#">?</a> Modbus Control Mode register index                    |
| Modbus CtrlMode value            | <input type="text" value="0"/> | <a href="#">?</a> Modbus Control Mode register value                    |
| Local Digital Output GPIO number | <input type="text" value="0"/> | <a href="#">?</a> Local Digital Output GPIO number                      |
| IEC61850 DO                      | <input type="text"/>           | <a href="#">?</a> IEC61850 Data Object reference, Maximum 32 characters |

Figure 278: The IEC104 gateway point mapping configuration page

| Web Field/UCI/Package Option  | Description   |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
|---|---|-------|---------------------------|---|---------------------------|---|--------------------|---|---|----|-------------------------------------|----|---|----|--|----|---|----|---|----|--|----|--|----|--|----|--|----|---|----|--|----|---|----|---|
| Web: Port Number<br>UCI: iecd.point[x].portno<br>Opt: portno                    | Defines the port number to which this point belongs (1 to 4). This corresponds to the serial port number.<br><table border="1" data-bbox="719 286 1369 360"> <tr> <td data-bbox="719 286 836 318">Range</td> <td data-bbox="836 286 1369 318">1 - 4</td> </tr> </table>   | Range | 1 - 4                     |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| Range   | 1 - 4   |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| Web: IEC101 Type ID<br>UCI: iecd.point[x].iec101_type_id<br>Opt: iec101_type_id | Defines the IEC104 type ID (data type). All types are defined in IEC-60870-5-104<br><table border="1" data-bbox="719 421 1369 1225"> <tr> <td data-bbox="719 421 836 452">1</td> <td data-bbox="836 421 1369 452">Single point information.</td> </tr> <tr> <td data-bbox="719 452 836 483">2</td> <td data-bbox="836 452 1369 483">Double point information.</td> </tr> <tr> <td data-bbox="719 483 836 515">7</td> <td data-bbox="836 483 1369 515">Bitstring 32 bits.</td> </tr> <tr> <td data-bbox="719 515 836 546">9</td> <td data-bbox="836 515 1369 546">Measured normalised value short signed.</td> </tr> <tr> <td data-bbox="719 546 836 577">11</td> <td data-bbox="836 546 1369 577">Measured scaled value short signed.</td> </tr> <tr> <td data-bbox="719 577 836 609">13</td> <td data-bbox="836 577 1369 609">IEEE STD 754 = Short floating point number.</td> </tr> <tr> <td data-bbox="719 609 836 640">14</td> <td data-bbox="836 609 1369 640">IEEE STD 754 = Short floating point number with time tag CP24Time2a.</td> </tr> <tr> <td data-bbox="719 640 836 672">15</td> <td data-bbox="836 640 1369 672">Integrated totals, 32 bit signed integer.</td> </tr> <tr> <td data-bbox="719 672 836 703">20</td> <td data-bbox="836 672 1369 703">Packed single point information with status change detection.</td> </tr> <tr> <td data-bbox="719 703 836 734">21</td> <td data-bbox="836 703 1369 734">Measured normalised value short signed without quality descriptor.</td> </tr> <tr> <td data-bbox="719 734 836 766">30</td> <td data-bbox="836 734 1369 766">Single point information with time tag CP56Time2a.</td> </tr> <tr> <td data-bbox="719 766 836 797">31</td> <td data-bbox="836 766 1369 797">Double point information with time tag CP56Time2a.</td> </tr> <tr> <td data-bbox="719 797 836 828">33</td> <td data-bbox="836 797 1369 828">Bitstring of 32 bits with time tag CP56Time2a.</td> </tr> <tr> <td data-bbox="719 828 836 860">34</td> <td data-bbox="836 828 1369 860">Measured normalised value short signed time tag CP56Time2a.</td> </tr> <tr> <td data-bbox="719 860 836 891">35</td> <td data-bbox="836 860 1369 891">Measured value, scaled value with time tag CP56Time2a.</td> </tr> <tr> <td data-bbox="719 891 836 922">36</td> <td data-bbox="836 891 1369 922">Measured value, short floating point number with time tag CP56Time2a.</td> </tr> <tr> <td data-bbox="719 922 836 954">37</td> <td data-bbox="836 922 1369 954">Integrated totals with time tag CP56Time2a.</td> </tr> </table> | 1     | Single point information. | 2 | Double point information. | 7 | Bitstring 32 bits. | 9 | Measured normalised value short signed. | 11 | Measured scaled value short signed. | 13 | IEEE STD 754 = Short floating point number. | 14 | IEEE STD 754 = Short floating point number with time tag CP24Time2a. | 15 | Integrated totals, 32 bit signed integer. | 20 | Packed single point information with status change detection. | 21 | Measured normalised value short signed without quality descriptor. | 30 | Single point information with time tag CP56Time2a. | 31 | Double point information with time tag CP56Time2a. | 33 | Bitstring of 32 bits with time tag CP56Time2a. | 34 | Measured normalised value short signed time tag CP56Time2a. | 35 | Measured value, scaled value with time tag CP56Time2a. | 36 | Measured value, short floating point number with time tag CP56Time2a. | 37 | Integrated totals with time tag CP56Time2a. |
| 1   | Single point information.   |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 2   | Double point information.   |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 7   | Bitstring 32 bits.  |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 9   | Measured normalised value short signed.   |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 11  | Measured scaled value short signed.   |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 13  | IEEE STD 754 = Short floating point number.   |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 14  | IEEE STD 754 = Short floating point number with time tag CP24Time2a.  |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 15  | Integrated totals, 32 bit signed integer.   |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 20  | Packed single point information with status change detection.   |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 21  | Measured normalised value short signed without quality descriptor.  |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 30  | Single point information with time tag CP56Time2a.  |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 31  | Double point information with time tag CP56Time2a.  |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 33  | Bitstring of 32 bits with time tag CP56Time2a.  |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 34  | Measured normalised value short signed time tag CP56Time2a.   |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 35  | Measured value, scaled value with time tag CP56Time2a.  |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 36  | Measured value, short floating point number with time tag CP56Time2a.   |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 37  | Integrated totals with time tag CP56Time2a.   |       |                           |   |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |

|  |   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
|--|---|---|---------------------------|-------|---------------------------|---|--------------------|---|---|----|-------------------------------------|----|---|----|--|----|---|----|---|----|--|----|--|----|--|----|--|----|---|----|--|----|---|----|---|
| <p>Web: IEC104 Type ID<br/>UCI: iecd.point[x].iec104_type_id<br/>Opt: iec104_type_id</p> | <p>Defines the IEC104 type ID (data type). All types are defined in IEC-60870-5-104</p> <table border="1" data-bbox="719 253 1350 1111"> <tr><td>1</td><td>Single point information.</td></tr> <tr><td>2</td><td>Double point information.</td></tr> <tr><td>7</td><td>Bitstring 32 bits.</td></tr> <tr><td>9</td><td>Measured normalised value short signed.</td></tr> <tr><td>11</td><td>Measured scaled value short signed.</td></tr> <tr><td>13</td><td>IEEE STD 754 = Short floating point number.</td></tr> <tr><td>14</td><td>IEEE STD 754 = Short floating point number with time tag CP24Time2a.</td></tr> <tr><td>15</td><td>Integrated totals, 32 bit signed integer.</td></tr> <tr><td>20</td><td>Packed single point information with status change detection.</td></tr> <tr><td>21</td><td>Measured normalised value short signed without quality descriptor.</td></tr> <tr><td>30</td><td>Single point information with time tag CP56Time2a.</td></tr> <tr><td>31</td><td>Double point information with time tag CP56Time2a.</td></tr> <tr><td>33</td><td>Bitstring of 32 bits with time tag CP56Time2a.</td></tr> <tr><td>34</td><td>Measured normalised value short signed time tag CP56Time2a.</td></tr> <tr><td>35</td><td>Measured value, scaled value with time tag CP56Time2a.</td></tr> <tr><td>36</td><td>Measured value, short floating point number with time tag CP56Time2a.</td></tr> <tr><td>37</td><td>Integrated totals with time tag CP56Time2a.</td></tr> </table> | 1 | Single point information. | 2     | Double point information. | 7 | Bitstring 32 bits. | 9 | Measured normalised value short signed. | 11 | Measured scaled value short signed. | 13 | IEEE STD 754 = Short floating point number. | 14 | IEEE STD 754 = Short floating point number with time tag CP24Time2a. | 15 | Integrated totals, 32 bit signed integer. | 20 | Packed single point information with status change detection. | 21 | Measured normalised value short signed without quality descriptor. | 30 | Single point information with time tag CP56Time2a. | 31 | Double point information with time tag CP56Time2a. | 33 | Bitstring of 32 bits with time tag CP56Time2a. | 34 | Measured normalised value short signed time tag CP56Time2a. | 35 | Measured value, scaled value with time tag CP56Time2a. | 36 | Measured value, short floating point number with time tag CP56Time2a. | 37 | Integrated totals with time tag CP56Time2a. |
| 1  | Single point information.   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 2  | Double point information.   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 7  | Bitstring 32 bits.  |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 9  | Measured normalised value short signed.   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 11   | Measured scaled value short signed.   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 13   | IEEE STD 754 = Short floating point number.   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 14   | IEEE STD 754 = Short floating point number with time tag CP24Time2a.  |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 15   | Integrated totals, 32 bit signed integer.   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 20   | Packed single point information with status change detection.   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 21   | Measured normalised value short signed without quality descriptor.  |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 30   | Single point information with time tag CP56Time2a.  |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 31   | Double point information with time tag CP56Time2a.  |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 33   | Bitstring of 32 bits with time tag CP56Time2a.  |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 34   | Measured normalised value short signed time tag CP56Time2a.   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 35   | Measured value, scaled value with time tag CP56Time2a.  |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 36   | Measured value, short floating point number with time tag CP56Time2a.   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 37   | Integrated totals with time tag CP56Time2a.   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| <p>Web: IEC101 IOA<br/>UCI: iecd.point[x].iec101_ioa<br/>Opt: iec101_ioa</p>             | <p>Defines IEC104 information object address. This is how remote an IEC104 SCADA master knows one point from another.</p> <table border="1" data-bbox="719 1200 1350 1267"> <tr><td>1</td><td></td></tr> <tr><td>Range</td><td>1 - 116777215</td></tr> </table>   | 1 |                           | Range | 1 - 116777215             |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 1  |   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| Range  | 1 - 116777215   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| <p>Web: IEC104 IOA<br/>UCI: iecd.point[x].iec104_ioa<br/>Opt: iec104_ioa</p>             | <p>Defines IEC104 information object address. This is how a remote IEC104 SCADA master knows one point from another.</p> <table border="1" data-bbox="719 1335 1350 1402"> <tr><td>1</td><td></td></tr> <tr><td>Range</td><td>1 - 116777215</td></tr> </table>  | 1 |                           | Range | 1 - 116777215             |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 1  |   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| Range  | 1 - 116777215   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| <p>Web: IEC101 IOA<br/>UCI: iecd.point[x].iec101_ioa<br/>Opt: iec101_ioa</p>             | <p>Defines IEC101 information object address.</p> <table border="1" data-bbox="719 1435 1350 1514"> <tr><td></td><td></td></tr> <tr><td>Range</td><td>1 - 116777215</td></tr> </table>  |   |                           | Range | 1 - 116777215             |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
|  |   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| Range  | 1 - 116777215   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| <p>Web: Device Addr<br/>UCI: iecd.point[x].devaddr<br/>Opt: devaddr</p>                  | <p>Defines the Modbus device address of the RTU (Modbus slave address). Used for identifying the point mapping to IP address in the device route file for Modbus TCP.<br/>This is not used in DNP3 mode.</p> <table border="1" data-bbox="719 1626 1350 1704"> <tr><td>1</td><td></td></tr> <tr><td>Range</td><td></td></tr> </table>   | 1 |                           | Range |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 1  |   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| Range  |   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| <p>Web: DNP3 Options<br/>UCI: iecd.point[x].dnp3options<br/>Opt: dnp3options</p>         | <p>For DNP3. Defines the DNP3 options bitmap.</p> <table border="1" data-bbox="719 1738 1350 1809"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td>0 - 255</td></tr> </table>   | 0 |                           | Range | 0 - 255                   |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| 0  |   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |
| Range  | 0 - 255   |   |                           |       |                           |   |                    |   |   |    |                                     |    |   |    |  |    |   |    |   |    |  |    |  |    |  |    |  |    |   |    |  |    |   |    |   |

|   |   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
|---|---|---|---------------------------------------|-------|---|---|-----------------|---|-----------------|---|-------------------|---|-------|
| Web: Group<br>UCI: iecd.point[x].group<br>Opt: group  | For DNP3. Defines the DNP3 group number to which this data point maps to.<br><table border="1"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td>0 - 255</td></tr> </table><br>For Modbus. Defines the Modbus data type.<br><table border="1"> <tr><td>0</td><td>Discreet input.</td></tr> <tr><td>1</td><td>Input register.</td></tr> <tr><td>2</td><td>Holding register.</td></tr> <tr><td>3</td><td>Coil.</td></tr> </table> | 0 |                                       | Range | 0 - 255   | 0 | Discreet input. | 1 | Input register. | 2 | Holding register. | 3 | Coil. |
| 0   |   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| Range   | 0 - 255   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| 0   | Discreet input.   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| 1   | Input register.   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| 2   | Holding register.   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| 3   | Coil.   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| Web: Index<br>UCI: iecd.point[x].index<br>Opt: index  | For DNP3. Defines the DNP3 point index.<br>For Modbus. Defines the Modbus data index (point number).<br><table border="1"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td>0 - 65535</td></tr> </table>  | 0 |                                       | Range | 0 - 65535   |   |                 |   |                 |   |                   |   |       |
| 0   |   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| Range   | 0 - 65535   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| Web: Index2<br>UCI: iecd.point[x].index2<br>Opt: index2   | For DNP3. Defines the DNP3 secondary point index.<br>For Modbus. Defines the Modbus data index (point number).<br><table border="1"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td>0 - 65535</td></tr> </table>  | 0 |                                       | Range | 0 - 65535   |   |                 |   |                 |   |                   |   |       |
| 0   |   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| Range   | 0 - 65535   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| Web: Modbus options<br>UCI: iecd.point[x].mb_options<br>Opt: mb_options                                       | For Modbus. Defines the Modbus options bitmap.<br><table border="1"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td>0 - 65535</td></tr> </table>  | 0 |                                       | Range | 0 - 65535   |   |                 |   |                 |   |                   |   |       |
| 0   |   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| Range   | 0 - 65535   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| Web: Modbus bitmap mask<br>UCI: iecd.point[x].bitmap_mask<br>Opt: bitmap_mask                                 | For Modbus. Defines the Modbus bitmap mask.<br><table border="1"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td>0 - 65535</td></tr> </table>   | 0 |                                       | Range | 0 - 65535   |   |                 |   |                 |   |                   |   |       |
| 0   |   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| Range   | 0 - 65535   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| Web: Modbus CtrlMode index<br>UCI: iecd.point[x].ctrlmode_index<br>Opt: ctrlmode_index                        | For Modbus. Defines the Modbus control mode register index.<br><table border="1"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td>0 - 65535</td></tr> </table>   | 0 |                                       | Range | 0 - 65535   |   |                 |   |                 |   |                   |   |       |
| 0   |   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| Range   | 0 - 65535   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| Web: Modbus CtrlMode value<br>UCI: iecd.point[x].ctrlmode_val<br>Opt: ctrlmode_val                            | For Modbus. Defines the Modbus control mode register value.<br><table border="1"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td>0 - 65535</td></tr> </table>   | 0 |                                       | Range | 0 - 65535   |   |                 |   |                 |   |                   |   |       |
| 0   |   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| Range   | 0 - 65535   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| Web: Local Digital Output GPIO number<br>UCI: iecd.point[x].local_gpio_output_nr<br>Opt: local_gpio_output_nr | Defines the local digital output GPIO number.<br><table border="1"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td>0 - 65535</td></tr> </table>   | 0 |                                       | Range | 0 - 65535   |   |                 |   |                 |   |                   |   |       |
| 0   |   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| Range   | 0 - 65535   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| Web: IEC61850 DO<br>UCI: iecd.point[x].iec61850_do<br>Opt: iec61850_do  | Defines the IEC61850 Data Object reference. (Maximum 32 characters).<br><table border="1"> <tr><td>0</td><td></td></tr> <tr><td>Range</td><td>0 - 32 characters</td></tr> </table>  | 0 |                                       | Range | 0 - 32 characters   |   |                 |   |                 |   |                   |   |       |
| 0   |   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| Range   | 0 - 32 characters   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| Web: n/a<br>UCI: iecd.point[x].dword<br>Opt: dword  | Defines the DWORD type. Relevant for Modbus data types IR (input registers) and HR (holding registers).<br><table border="1"> <tr><td>0</td><td>Data point is treated as 16 bit wide.</td></tr> <tr><td>1</td><td>Data point is treated as 32 bit wide. Two consecutive 16 bit registers are read from the Modbus device.</td></tr> </table>  | 0 | Data point is treated as 16 bit wide. | 1     | Data point is treated as 32 bit wide. Two consecutive 16 bit registers are read from the Modbus device. |   |                 |   |                 |   |                   |   |       |
| 0   | Data point is treated as 16 bit wide.   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |
| 1   | Data point is treated as 32 bit wide. Two consecutive 16 bit registers are read from the Modbus device.   |   |                                       |       |   |   |                 |   |                 |   |                   |   |       |

**Table 208: Information table for IEC104 gateway point mapping configuration**

### 50.3.4.1 MODBUS device route file

If the configured MODBUS protocol variation is Modbus TCP, then the device route file at `/root/iecd/devroute.csv` is used to map the device address (`iecd.point[x].devaddr`) from the point mapping to the remote IP address of the Modbus TCP slave device.

The `devroute.csv` file entries will have the following format:

```
<Modbus device addr>, <IP address>
```

For example, for the point mapping file, enter:

```
config point
    option portno 1
    option iec104_type_id 30
    option iec104_ioa 64213
    option devaddr 1
    option group 0
    option index 2
```

For the devroute.csv entry, enter:

```
1,192.168.0.106
```

## 50.4 IEC104 gateway configuration using command line

The IEC104 gateway uses the `iecd` package `/etc/config/iecd`.

You can configure multiple port, `iec101link` and `points` sections.

By default, IEC104 gateway port instances are named `port`. It is identified by `@port` followed by the port position in the package as a number. For example, for the first port in the package using UCI:

```
iecd.@port[0]=port
iecd.@port[0].enable=1
```

Or using package options:

```
config port
    option enable '1'
```

By default, all IEC104 gateway IEC101 link instances are named `iec101link`, the instance is identified by `@iec101link` followed by the link position in the package as a number.

For example, for the first IEC101 link in the package using UCI:

```
iecd.@iec101link[0]=iec101link
iecd.@iec101link[0].portno=1
```

Or using package options:

```
config iec101link
    option portno '1'
```

By default, all IEC104 gateway point instances are named `point`, it is identified by `@point` followed by the point position in the package as a number. For example, for the first point in the package using UCI:

```
iecd.@point[0]=point
iecd.@point[0].portno=1
```

Or using package options:

```
config point
    option portno '1'
```

## 50.4.1 IEC104 to IEC101 conversion (balanced or unbalanced)

The following example shows IEC104 to IEC101 unbalanced conversion with one IEC101 link.

To configure IEC104 to IEC101 balanced conversion set option `iecd101_mode` to **balanced**.

### 50.4.1.1 IEC104 to IEC101 using uci

```
root@VA_router:~# uci show iecd
iecd.main=iecd
iecd.main.enable=1
iecd.port1=port
iecd.port1.enable=1
iecd.port1.loglevel=5
iecd.port1.tcp_keepalive_enabled=1
iecd.port1.tcp_keepalive_interval=5
iecd.port1.tcp_keepalive_timeout=5
iecd.port1.tcp_keepalive_count=3
iecd.port1.tcp_user_timeout=20000
iecd.port1.master_protocol=iec101
iecd.port1.slave_protocol=iec104
iecd.port1.ioa_offset=0
iecd.port1.pointmap_file=/root/iecd/iecd_points1.csv
iecd.port1.iec104_local_ip=0.0.0.0
iecd.port1.iec104_local_tcpport=2404
iecd.port1.iec104_k=12
iecd.port1.iec104_w=9
iecd.port1.iec104_t2=10000
iecd.port1.iec104_gi_resp_time=200
iecd.port1.iec104_txq_size=128
iecd.port1.iec104_sync_time=1
iecd.port1.iec104_time_tagged_cmds=0
```



```
iecd.port1.iec104_cmd_delay_time=5000
iecd.port1.iec104_fsm_debug_on=0
iecd.port1.iec104_dump_data=0
iecd.port1.iec104_trace_on=0

#IEC101 conversion options
iecd.port1.iec101_target_ip=127.0.0.1
iecd.port1.iec101_target_tcpport=999
iecd.port1.iec101_mode=unbalanced      #balanced or unbalanced
iecd.port1.iec101_cot_tx_length=1
iecd.port1.iec101_cot_source_octet=0
iecd.port1.iec101_asdu_addrln=1
iecd.port1.iec101_info_obj_addrln=2
iecd.port1.iec101_data_polling_time=500
iecd.port1.iec101_ack_delay=0
iecd.port1.iec101_link_addrln=1
iecd.port1.iec101_frame_rsp_time=2000
iecd.port1.iec101_max_tx_retry=3
iecd.port1.iec101_txq_size=128
iecd.port1.iec101_send_spont_delay_acq=1
iecd.port1.iec101_fsm_debug_on=0
iecd.port1.iec101_dump_data=0
iecd.port1.iec101_trace_on=0

# The following section defines IEC101 slave links used in IEC101
unbalanced mode on each link is defined by a config block 'config
iecd101link'

# To add more links repeat the section block for each added link.
# Maximum 32 links are supported
iecd.@iecd101link[0]=iecd101link
iecd.@iecd101link[0].portno=1
iecd.@iecd101link[0].address=6
iecd.@iecd101link[0].asduaddr=6

#No data point mappings for IEC104 to IEC101 conversion
```

### 50.4.1.2 IEC104 to IEC101 using package options

```
root@VA_router:~# uci export iecd
package iecd

config iecd 'main'
    option enable '1'

config port 'port1'
    option enable '1'
    option loglevel '5'
    option tcp_keepalive_enabled '1'
    option tcp_keepalive_interval '5'
    option tcp_keepalive_timeout '5'
    option tcp_keepalive_count '3'
    option tcp_user_timeout '20000'
    option master_protocol 'iec101'
    option slave_protocol 'iec104'
    option ioa_offset '0'
    option pointmap_file '/root/iecd/iecd_points1.csv'
    option iec104_local_ip '0.0.0.0'
    option iec104_local_tcpport '2404'
    option iec104_k '12'
    option iec104_w '9'
    option iec104_t2 '10000'
    option iec104_gi_resp_time '200'
    option iec104_txq_size '128'
    option iec104_sync_time '1'
    option iec104_time_tagged_cmds '0'
    option iec104_cmd_delay_time '5000'
    option iec104_fsm_debug_on '0'
    option iec104_dump_data '0'
    option iec104_trace_on '0'

    #IEC101 conversion options
    option iec101_target_ip '127.0.0.1'
    option iec101_target_tcpport '999'
    option iec101_mode 'unbalanced'           #balanced or unbalanced
```

```
option iec101_cot_tx_length '1'
option iec101_cot_source_octet '0'
option iec101_asdu_addrln '1'
option iec101_info_obj_addrln '2'
option iec101_data_polling_time '500'
option iec101_ack_delay '0'
option iec101_link_addrln '1'
option iec101_frame_rsp_time '2000'
option iec101_max_tx_retry '3'
option iec101_txq_size '128'
option iec101_send_spont_delay_acq '1'
option iec101_fsm_debug_on '0'
option iec101_dump_data '0'
option iec101_trace_on '0'

# The following section defines IEC101 slave links used in IEC101
unbalanced mode on
# Each link is defined by a config block 'config iec101link'
# To add more links repeat the section block for each added link. To remove
links, simply remove the link block from the configuration
# Maximum 32 links are supported
#
# Definition of options within the section block:
# portno - port number to which this point belongs (1 to 4)
# address - IEC101 slave link address
# asduaddr IEC101 slave common ASDU address

config iec101link
    option portno 1
    option address 6
    option asduaddr 6

#No data point mappings for IEC104 to IEC101 conversion
```

## 50.4.2 IEC104 to DNP3 conversion

The following example shows definition of two conversion points. The config point section should be repeated for each point to be defined.

### 50.4.2.1 IEC104 to DNP3 conversion using uci

```
root@VA_router:~# uci show iecd
iecd.main=iecd
iecd.main.enable=1
iecd.port1=port
iecd.port1.enable=1
iecd.port1.loglevel=5
iecd.port1.tcp_keepalive_enabled=1
iecd.port1.tcp_keepalive_interval=5
iecd.port1.tcp_keepalive_timeout=5
iecd.port1.tcp_keepalive_count=3
iecd.port1.tcp_user_timeout=20000
iecd.port1.master_protocol=dnp3
iecd.port1.slave_protocol=iec104
iecd.port1.ioa_offset=0
iecd.port1.pointmap_file=/root/iecd/iecd_points1.csv
iecd.port1.iec104_local_ip=0.0.0.0
iecd.port1.iec104_local_tcpport=2404
iecd.port1.iec104_k=12
iecd.port1.iec104_w=9
iecd.port1.iec104_t2=10000
iecd.port1.iec104_gi_resp_time=200
iecd.port1.iec104_txq_size=128
iecd.port1.iec104_sync_time=1
iecd.port1.iec104_time_tagged_cmds=0
iecd.port1.iec104_cmd_delay_time=5000
iecd.port1.iec104_fsm_debug_on=0
iecd.port1.iec104_dump_data=0
iecd.port1.iec104_trace_on=0
iecd.port1.iec101_cot_source_octet=0

#DNP3 conversion options
iecd.port1.dnp3_target_ip=127.0.0.1
```

```
iecd.port1.dnp3_target_tcpport=999
iecd.port1.dnp3_dl_srcaddr=3
iecd.port1.dnp3_dl_dstaddr=4
iecd.port1.dnp3_dl_cfrm_user_data=0
iecd.port1.dnp3_dl_keep_alive_int=15000
iecd.port1.dnp3_dl_frame_rsp_time=1500
iecd.port1.dnp3_dl_max_tx_retry=3
iecd.port1.dnp3_dl_utxq_size=128
iecd.port1.dnp3_dl_ctxq_size=128
iecd.port1.dnp3_app_read_attr=0
iecd.port1.dnp3_app_unsol_enable=0
iecd.port1.dnp3_app_poll_time=30000
iecd.port1.dnp3_app_firstpoll_delay=5000
iecd.port1.dnp3_app_evpoll_time=3000
iecd.port1.dnp3_app_frag_rx_time=10000
iecd.port1.dnp3_app_sync_time=1
iecd.port1.dnp3_app_txq_size=64
iecd.port1.dnp3_app_output_mode=0
iecd.port1.dnp3_app_evpoll_mode=0
iecd.port1.dnp3_fsm_debug_on=0
iecd.port1.dnp3_object_parser_debug_on=0
iecd.port1.dnp3_dump_data=0
iecd.port1.dnp3_trace_on=0

#DNP3 data point mappings
iecd.@point[0]=point
iecd.@point[0].portno=1
iecd.@point[0].iec104_type_id=1
iecd.@point[0].iec104_ioa=1
iecd.@point[0].devaddr=1
iecd.@point[0].group=1
iecd.@point[0].index=0
iecd.@point[1]=point
iecd.@point[1].portno=1
iecd.@point[1].iec104_type_id=1
iecd.@point[1].iec104_ioa=2
iecd.@point[1].devaddr=1
```

```
iecd.@point[1].group=1
iecd.@point[1].index=39
```

### 50.4.2.2 IEC104 to DNP3 conversion using package options

```
root@VA_router:~# uci export iecd
package iecd

config iecd 'main'
    option enable '1'

config port 'port1'
    option enable '1'
    option loglevel '5'
    option tcp_keepalive_enabled '1'
    option tcp_keepalive_interval '5'
    option tcp_keepalive_timeout '5'
    option tcp_keepalive_count '3'
    option tcp_user_timeout '20000'
    option master_protocol 'dnp3'
    option slave_protocol 'iec104'
    option ioa_offset '0'
    option pointmap_file '/root/iecd/iecd_points1.csv'
    option iec104_local_ip '0.0.0.0'
    option iec104_local_tcpport '2404'
    option iec104_k '12'
    option iec104_w '9'
    option iec104_t2 '10000'
    option iec104_gi_resp_time '200'
    option iec104_txq_size '128'
    option iec104_sync_time '1'
    option iec104_time_tagged_cmds '0'
    option iec104_cmd_delay_time '5000'
    option iec104_fsm_debug_on '0'
    option iec104_dump_data '0'
    option iec104_trace_on '0'
    option iec101_cot_source_octet '0'
```

```
#DNP3 conversion options
option dnp3_target_ip '127.0.0.1'
option dnp3_target_tcpport '999'
option dnp3_dl_srcaddr '3'
option dnp3_dl_dstaddr '4'
option dnp3_dl_cfrm_user_data '0'
option dnp3_dl_keep_alive_int '15000'
option dnp3_dl_frame_rsp_time '1500'
option dnp3_dl_max_tx_retry '3'
option dnp3_dl_utxq_size '128'
option dnp3_dl_ctxq_size '128'
option dnp3_app_read_attr '0'
option dnp3_app_unsol_enable '0'
option dnp3_app_poll_time '30000'
option dnp3_app_firstpoll_delay '5000'
option dnp3_app_evpoll_time '3000'
option dnp3_app_frag_rx_time '10000'
option dnp3_app_sync_time '1'
option dnp3_app_txq_size '64'
option dnp3_app_output_mode '0'
option dnp3_app_evpoll_mode '0'
option dnp3_fsm_debug_on '0'
option dnp3_object_parser_debug_on '0'
option dnp3_dump_data '0'
option dnp3_trace_on '0'
```

```
config point
```

```
option portno '1'
option iec104_type_id '1'
option iec104_ioa '1'
option devaddr '1'
option group '1'
option index '0'
```

```
config point
```

```
option portno '1'
option iec104_type_id '1'
```

```
option iec104_ioa '2'
option devaddr '1'
option group '1'
option index '39'
```

### 50.4.3 IEC104 to Modbus conversion

The following example shows IEC104 to Modbus over serial.

To configure Modbus TCP, set `option modbus_protocol` to **modbus\_tcp**.

When configuring Modbus TCP, the device route file at `/root/iecd/devroute.csv` must be configured to map the device address `option devaddr` from the point mapping to the remote IP address of the Modbus TCP slave device.

The `devroute.csv` file entries will have the following format:

```
<Modbus device addr>, <IP address>
```

For example, for the point mapping file:

```
config point
    option portno 1
    option iec104_type_id 30
    option iec104_ioa 64213
    option devaddr 1
    option group 0
    option index 2
```

For the `devroute.csv` entry:

```
1,192.168.0.106
```

#### 50.4.3.1 IEC104 to Modbus using uci

```
root@VA_router:~# uci show iecd
iecd.main=iecd
iecd.main.enable=1
iecd.port1=port
iecd.port1.enable=1
iecd.port1.loglevel=5
iecd.port1.tcp_keepalive_enabled=1
iecd.port1.tcp_keepalive_interval=5
iecd.port1.tcp_keepalive_timeout=5
iecd.port1.tcp_keepalive_count=3
iecd.port1.tcp_user_timeout=20000
```



```
iecd.port1.master_protocol=modbus
iecd.port1.slave_protocol=iecd104
iecd.port1.ioa_offset=0
iecd.port1.pointmap_file=/root/iecd/iecd_points1.csv
iecd.port1.iecd104_local_ip=0.0.0.0
iecd.port1.iecd104_local_tcpport=2404
iecd.port1.iecd104_k=12
iecd.port1.iecd104_w=9
iecd.port1.iecd104_t2=10000
iecd.port1.iecd104_gi_resp_time=200
iecd.port1.iecd104_txq_size=128
iecd.port1.iecd104_sync_time=1
iecd.port1.iecd104_time_tagged_cmds=0
iecd.port1.iecd104_cmd_delay_time=5000
iecd.port1.iecd104_fsm_debug_on=0
iecd.port1.iecd104_dump_data=0
iecd.port1.iecd104_trace_on=0
iecd.port1.iecd101_cot_source_octet=0

#Modbus conversion options
iecd.port1.modbus_protocol=modbus_serial
iecd.port1.modbus_local_ip=0.0.0.0
iecd.port1.modbus_local_port=888
iecd.port1.modbus_remote_ip=127.0.0.1
iecd.port1.modbus_remote_port=999
iecd.port1.modbus_polling_time=3000
iecd.port1.modbus_resp_time=1000
iecd.port1.modbus_dump_data=0
iecd.port1.modbus_trace_on=0
iecd.port1.modbus_fsm_debug_on=0

#Modbus data point mappings
iecd.@point[0]=point
iecd.@point[0].portno=1
iecd.@point[0].iecd104_type_id=36
iecd.@point[0].iecd104_ioa=6620161
iecd.@point[0].iecd101_ioa=0
```

```
iecd.@point[0].devaddr=11
iecd.@point[0].group=1
iecd.@point[0].index=18459
iecd.@point[0].dword=1
iecd.@point[1]=point
iecd.@point[1].portno=1
iecd.@point[1].iec104_type_id=36
iecd.@point[1].iec104_ioa=6620162
iecd.@point[1].iec101_ioa=0
iecd.@point[1].devaddr=11
iecd.@point[1].group=1
iecd.@point[1].index=18461
iecd.@point[1].dword=1
```

### 50.4.3.2 IEC104 to Modbus using package options

```
root@VA_router:~# uci export iecd
package iecd

config iecd 'main'
    option enable '1'

config port 'port1'
    option enable '1'
    option loglevel '5'
    option tcp_keepalive_enabled '1'
    option tcp_keepalive_interval '5'
    option tcp_keepalive_timeout '5'
    option tcp_keepalive_count '3'
    option tcp_user_timeout '20000'
    option master_protocol 'modbus'
    option slave_protocol 'iec104'
    option ioa_offset '0'
    option pointmap_file '/root/iecd/iecd_points1.csv'
    option iec104_local_ip '0.0.0.0'
    option iec104_local_tcpport '2404'
    option iec104_k '12'
    option iec104_w '9'
```

```
option iec104_t2 '10000'  
option iec104_gi_resp_time '200'  
option iec104_txq_size '128'  
option iec104_sync_time '1'  
option iec104_time_tagged_cmds '0'  
option iec104_cmd_delay_time '5000'  
option iec104_fsm_debug_on '0'  
option iec104_dump_data '0'  
option iec104_trace_on '0'  
option iec101_cot_source_octet '0'  
  
#Modbus conversion options  
option modbus_protocol 'modbus_serial'  
option modbus_local_ip '0.0.0.0'  
option modbus_local_port '888'  
option modbus_remote_ip '127.0.0.1'  
option modbus_remote_port '999'  
option modbus_polling_time '3000'  
option modbus_resp_time '1000'  
option modbus_dump_data '0'  
option modbus_trace_on '0'  
option modbus_fsm_debug_on '0'
```

config point

```
option portno '1'  
option iec104_type_id '36'  
option iec104_ioa '6620161'  
option iec101_ioa '0'  
option devaddr '11'  
option group '1'  
option index '18459'  
option dword '1'
```

config point

```
option portno '1'  
option iec104_type_id '36'  
option iec104_ioa '6620162'
```

```
option iec101_ioa '0'
option devaddr '11'
option group '1'
option index '18461'
option dword '1'
```

## 50.5 Configuring the terminal server

The terminal server is used to control the data from the serial port over the IP network.

The terminal server configuration can be found at **Services -> Terminal Server**. The Terminal Server Configuration page appears. You must configure two main sections: Main Settings and Port Settings.

The terminal server for IEC104 to each of the RTU protocol conversions differ only slightly. This section shows the command line options for configuring the terminal server for IEC104 conversion.

For more detailed information on configuring the terminal server using the web GUI and option values, read the chapter, 'Configuring terminal server'.

### 50.5.1 Configuring the terminal server for IEC104 to IEC101

#### 50.5.1.1 Configuring IEC104 to IEC101 using uci

```
root@VA_router:~# uci show tserverd
tserverd.main=tserverd
tserverd.main.enable=1
tserverd.main.debug_ev_enable=0
tserverd.main.log_severity=5
tserverd.main.debug_rx_tx_enable=0
tserverd.port1=port
tserverd.port1.enable=1
tserverd.port1.devName=/dev/ttySC0
tserverd.port1.ip_port1=0
tserverd.port1.ip_port2=0
tserverd.port1.remote_ip1=0.0.0.0
tserverd.port1.remote_ip2=0.0.0.0
tserverd.port1.tcp_always_on=1
tserverd.port1.close_tcp_on_dsr=0
tserverd.port1.tty_always_open=1
tserverd.port1.fwd_timeout=0
tserverd.port1.fwd_timer_mode=idle
```

```
tserverd.port1.fwd_buffer_size=1
tserverd.port1.sfwd_buffer_size=0
tserverd.port1.sfwd_timeout=0
tserverd.port1.sfwd_timer_mode=idle
tserverd.port1.speed=9600
tserverd.port1.wsize=8
tserverd.port1.parity=1
tserverd.port1.stops=1
tserverd.port1.fc_mode=0
tserverd.port1.disc_time_ms=5000
tserverd.port1.server_mode=1
tserverd.port1.proxy_mode=0
tserverd.port1.local_ip=0.0.0.0
tserverd.port1.listen_port=999
tserverd.port1.udpMode=0
tserverd.port1.udpLocalPort=0
tserverd.port1.udpRemotePort=0
tserverd.port1.udpKaIntervalMs=0
tserverd.port1.udpKaCount=3
tserverd.port1.serial_mode_gpio_control=1
tserverd.port1.tcp_nodelay=1
tserverd.port1.portmode=rs232
```

### 50.5.1.2 Configuring IEC104 to IEC101 using package options

```
root@VA_router:~# uci export tserverd
package tserverd

config tserverd main
    # set to 1 to enable terminal server
    option enable 1

    # enables detailed debug logging (state transitions, data transfer etc)
    option debug_ev_enable 0

    # sets syslog level (0 to 7), default is 6
    option log_severity 5
```

```
option debug_rx_tx_enable 0

config port 'port1'
# enables this port
option enable 1

# serial device name
option devName '/dev/ttySC0'

# destination peer port IP number (two number for failover)
option ip_port1 0
option ip_port2 0

# destination peer ip address (two addresses for failover)
option remote_ip1 '0.0.0.0'
option remote_ip2 '0.0.0.0'

# keep TCP session always connected
option tcp_always_on 1

# close TCP session on detection of DSR signal low
option close_tcp_on_dsr 0

# keep serial port always open (if option not present, default is 0)
option tty_always_open 1

# Forwarding timeout in milliseconds (serial to network)
option fwd_timeout 0

# Forwarding timer mode (serial to network), 'idle'=timer re-started on
each received data,
# 'aging'=timer started on first rx
option fwd_timer_mode 'idle'

# Forwarding buffer size (serial to network)
option fwd_buffer_size 1
```

```
# Forwarding buffer size (network to serial), 0=use maximum possible
network rx buffer size
option sfwd_buffer_size 0

# Forwarding timeout in milliseconds (network to serial), 0=forward to
serial immediately
option sfwd_timeout 0

# Forwarding timer mode (network to serial), 'idle'=timer re-started on
each received data,
# 'aging'=timer started on first rx
option sfwd_timer_mode 'idle'

# serial device speed in baud
option speed 9600

# serial device word size (5,6,7,8)
option wsize 8

# serial device parity (0=none, 1=even, 2=odd)
option parity 1

# serial device number of stop bits (1 or 2)
option stops 1

# serial flow control mode (0=none, 1=RTS CTS, 2=XONXOFF)
option fc_mode 0

# time in milliseconds to start re-connecting after setting DTR low
option disc_time_ms 5000

# TCP server mode
option server_mode 1

# Proxy mode (off by default)
option proxy_mode 0
```

```
# Local IP address to listen on (0.0.0.0=listen on any interface)
option local_ip '0.0.0.0'

# TCP listen port for server mode
option listen_port 999

# UDP mode
option udpMode 0

# UDP local port UDP mode
option udpLocalPort 0

# UDP port for UDP mode
option udpRemotePort 0

# If set to non zero, send empty UDP packets every this many
milliseconds to remote peer
option udpKaIntervalMs 0

# Max number of consecutive remote UDP keepalive missed (not received)
before UDP
# session considered broken
option udpKaCount 3

option serial_mode_gpio_control 1
option tcp_nodelay 1

# rs232 - RS-232 mode, rs485hdx - rs485 2 wire half duplex mode in
which transmitter drives
# RTS. rs485fdx - RS485 4 wire full duplex mode. 'v23' - using V.23
leased line card driver.
# x21 - use USB serial card in sync mode
option portmode 'rs232'
```



## 50.5.2 Configuring the terminal server for IEC104 to DNP3

The terminal server configuration for IEC104 to DNP3 is the same as for IEC104 to IEC101 except for serial device parity which is set to **none**.

Parity setting using uci:

```
tserverd.port1.parity=1
```

Parity setting using package options:

```
option parity 0
```

## 50.5.3 Configuring the terminal server for IEC104 to Modbus over serial

The terminal server is only used for IEC104 to Modbus over serial. It is not used for Modbus over TCP.

The options necessary for IEC104 to Modbus configuration are listed below. These options are for the first serial port only.

### 50.5.3.1 IEC104 to Modbus over serial using uci

```
root@VA_router:~# uci show tserverd
tserverd.main=tserverd
tserverd.main.enable=1
tserverd.main.debug_ev_enable=0
tserverd.main.log_severity=5
tserverd.main.debug_rx_tx_enable=0
tserverd.port1=port
tserverd.port1.enable=1
tserverd.port1.devName=/dev/ttySC0
tserverd.port1.ip_port1=999
tserverd.port1.ip_port2=999
tserverd.port1.remote_ip1=127.0.0.1
tserverd.port1.remote_ip2=127.0.0.1
tserverd.port1.tcp_always_on=1
tserverd.port1.close_tcp_on_dsr=0
tserverd.port1.tty_always_open=1
tserverd.port1.fwd_timeout=10
tserverd.port1.fwd_timer_mode=idle
tserverd.port1.fwd_buffer_size=300
tserverd.port1.sfdw_buffer_size=0
tserverd.port1.sfdw_timeout=0
```

```
tserverd.port1.sfwd_timer_mode=idle
tserverd.port1.speed=19200
tserverd.port1.wsize=8
tserverd.port1.parity=1
tserverd.port1.stops=1
tserverd.port1.fc_mode=0
tserverd.port1.disc_time_ms=5000
tserverd.port1.server_mode=1
tserverd.port1.proxy_mode=0
tserverd.port1.local_ip=0.0.0.0
tserverd.port1.listen_port=999
tserverd.port1.udpMode=1
tserverd.port1.udpLocalPort=999
tserverd.port1.udpRemotePort=888
tserverd.port1.udpKaIntervalMs=0
tserverd.port1.udpKaCount=3
tserverd.port1.serial_mode_gpio_control=1
tserverd.port1.portmode=rs232
```

### 50.5.3.2 IEC104 to Modbus over serial using package options

```
root@VA_router:~# uci export tserverd
package tserverd

config tserverd main
    # set to 1 to enable terminal server
    option enable 1

    # enables detailed debug logging (state transitions, data transfer etc)
    option debug_ev_enable 0

    # sets syslog level (0 to 7), default is 6
    option log_severity 5

    option debug_rx_tx_enable 0

config port 'port1'
    # enables this port
```

```
option enable 1

# serial device name
option devName '/dev/ttySC0'

# destination peer port IP number (two number for failover)
option ip_port1 999
option ip_port2 999

# destination peer ip address (two addresses for failover)
option remote_ip1 '127.0.0.1'
option remote_ip2 '127.0.0.1'

# keep TCP session always connected
option tcp_always_on 1

# close TCP session on detection of DSR signal low
option close_tcp_on_dsr 0

# keep serial port always open (if option not present, default is 0)
option tty_always_open 1

# Forwarding timeout in milliseconds (serial to network)
option fwd_timeout 10

# Forwarding timer mode (serial to network), 'idle'=timer re-started on
each received data,
# 'aging'=timer started on first rx
option fwd_timer_mode 'idle'

# Forwarding buffer size (serial to network)
option fwd_buffer_size 300

# Forwarding buffer size (network to serial), 0=use maximum possible
network rx buffer size
option sfwd_buffer_size 0
```

```
# Forwarding timeout in milliseconds (network to serial), 0=forward to
serial immediately
option sfwd_timeout 0

# Forwarding timer mode (network to serial), 'idle'=timer re-started on
each received data,
# 'aging'=timer started on first rx
option sfwd_timer_mode 'idle'

# serial device speed in baud
option speed 19200

# serial device word size (5,6,7,8)
option wsize 8

# serial device parity (0=none, 1=even, 2=odd)
option parity 1

# serial device number of stop bits (1 or 2)
option stops 1

# serial flow control mode (0=none, 1=RTS CTS, 2=XONXOFF)
option fc_mode 0

# time in milliseconds to start re-connecting after setting DTR low
option disc_time_ms 5000

# TCP server mode
option server_mode 1

# Proxy mode (off by default)
option proxy_mode 0

# Local IP address to listen on (0.0.0.0=listen on any interface)
option local_ip '0.0.0.0'

# TCP listen port for server mode
```

```
option listen_port 999

# UDP mode
option udpMode 1

# UDP local port UDP mode
option udpLocalPort 999

# UDP port for UDP mode
option udpRemotePort 888

# If set to non zero, send empty UDP packets every this many
milliseconds to remote peer
option udpKaIntervalMs 0

# Max number of consecutive remote UDP keepalive missed (not received)
before UDP
# session considered broken
option udpKaCount 3

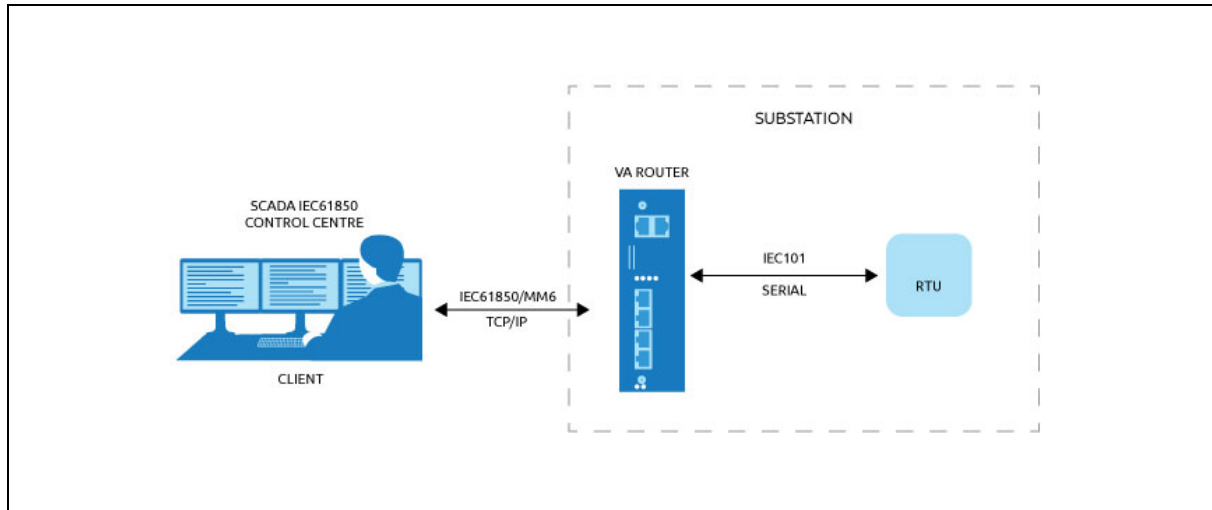
option serial_mode_gpio_control 1

# rs232 - RS-232 mode, rs485hdx - rs485 2 wire half duplex mode in
which transmitter drives
# RTS. rs485fdx - RS485 4 wire full duplex mode. 'v23' - using V.23
leased line card driver.
# x21 - use USB serial card in sync mode
option portmode 'rs232'
```

## 50.6 Configuring IEC61850 to IEC101 conversion

The IEC61850 to IEC101-unbalanced conversion feature of the router allows converting commands in the control direction and the responses and process data in the monitor direction between the SCADA master running the IEC61850 protocol and the remote RTUs running IEC101 protocol in unbalanced mode over serial interface.

In IEC101 unbalanced mode, the router supports communication of up to 32 IEC101 slaves connected onto the same serial interface.



**Figure 279: Example of IEC61850 to IEC101 conversion scenario**

The IEC104 gateway and terminal server are used for IEC61850 to IEC101 conversion, as in the other protocol conversions however the IEC61850 options are currently not available via the web interface. The following section details command line configuration.

| Web Field/UCI/Package Option   | Description  |         |       |           |              |
|--|--|---------|-------|-----------|--------------|
| <b>iecd port config section</b>  |  |         |       |           |              |
| Web: n/a<br>UCI: iecd.<port>.slave_protocol<br>Opt: slave_protocol                   | Defines what protocol the SCADA control centre is using to connect to this gateway. <table border="1"> <tr> <td>iecd104</td> <td>IC104</td> </tr> <tr> <td>iecd61850</td> <td>IEC61850</td> </tr> </table>   | iecd104 | IC104 | iecd61850 | IEC61850     |
| iecd104  | IC104  |         |       |           |              |
| iecd61850  | IEC61850   |         |       |           |              |
| Web: n/a<br>UCI: iecd.<port>.iecd61850_local_ip<br>Opt: iecd61850_local_ip           | Defines the local IP address this IEC61850 peer binds to.  |         |       |           |              |
| Web: n/a<br>UCI: iecd.<port>.iecd61850_local_tcpport<br>Opt: iecd61850_local_tcpport | Defines the local TCP port this IEC104 peer listens on. <table border="1"> <tr> <td>2404</td> <td></td> </tr> <tr> <td>Range</td> <td>1 - 65535</td> </tr> </table>  | 2404    |       | Range     | 1 - 65535    |
| 2404   |  |         |       |           |              |
| Range  | 1 - 65535  |         |       |           |              |
| <b>iecd point config section</b>   |  |         |       |           |              |
| Web: n/a<br>UCI: iecd.point[x].iecd61850_id<br>Opt: iecd61850_id                     | Defines the IEC61850 logical device name. For example:<br><pre>option iecd61850 ld 'SENSORS'</pre> <table border="1"> <tr> <td></td> <td></td> </tr> <tr> <td>Range</td> <td>0 - 32 chars</td> </tr> </table>  |         |       | Range     | 0 - 32 chars |
|  |  |         |       |           |              |
| Range  | 0 - 32 chars   |         |       |           |              |
| Web: n/a<br>UCI: iecd.point[x].iecd61850_in<br>Opt: iecd61850_in                     | Defines the IEC61850 logical node name. For example:<br><pre>option iecd61850 ln 'LLN0'</pre> <table border="1"> <tr> <td></td> <td></td> </tr> <tr> <td>Range</td> <td>0 - 32 chars</td> </tr> </table>   |         |       | Range     | 0 - 32 chars |
|  |  |         |       |           |              |
| Range  | 0 - 32 chars   |         |       |           |              |
| Web: n/a<br>UCI: iecd.point[x].iecd61850_do<br>Opt: iecd61850_do                     | Defines the IEC61850 data object name. For example:<br><pre>option iecd61850 do 'SPS01'</pre> <table border="1"> <tr> <td></td> <td></td> </tr> <tr> <td>Range</td> <td>0 - 32 chars</td> </tr> </table>   |         |       | Range     | 0 - 32 chars |
|  |  |         |       |           |              |
| Range  | 0 - 32 chars   |         |       |           |              |
| Web: n/a<br>UCI: iecd.point[x] iec101_type_id<br>Opt: iec101_type_id                 | Defines the IEC104 type ID (data type). For example:<br>1 - Single Point Information<br>2 - Double Point Information<br>All types are defined in IEC-60870-5-101. <table border="1"> <tr> <td></td> <td></td> </tr> <tr> <td>Range</td> <td></td> </tr> </table> |         |       | Range     |              |
|  |  |         |       |           |              |
| Range  |  |         |       |           |              |

|                              |  |                          |
|------------------------------|--|--------------------------|
| Web: IEC101 IOA              | Defines IEC101 information object address. |                          |
| UCI: iecd.point[x].ieci01_ia | 1  | Single Point Information |
| Opt: ieci01_ia               | Range                                      | 1 - 16777215             |

Table 209: Information table for IEC61850 specific configuration

### 50.6.1 Relation of IEC101 data types to IEC61850 data types

Supported data type combinations are listed below:

| option iec101_type_id<br>(IEC101 explanation)        | option iec61850_do<br>(IEC61850 explanation) | IEC101 point R/W | IEC61850 point R/W |
|--|--|------------------|--------------------|
| '1'<br>SPI (Single Point Information)                | 'SPS'<br>Single-point status                 | read only        | read only          |
| '1'<br>SPI (Single Point Information)                | 'SPC'<br>Controllable single-point           | read-write       | read-write         |
| '1'<br>SPI (Single Point Information)                | 'SPG'<br>Single point setting                | --               | write only         |
| '3'<br>DPI (Double Point Information)                | 'DPS'<br>Double-point status                 | read only        | read only          |
| '3'<br>DPI (Double Point Information)                | 'DPC'<br>Controllable double-point           | read-write       | read-write         |
| '11'<br>Measured value, scaled value<br>short signed | 'INS'<br>Integer status                      | read only        | read only          |
| '11'<br>Measured value, scaled value<br>short signed | 'STV'<br>Status value                        | read only        | read only          |
| '11'<br>Measured value, scaled value<br>short signed | 'ENS'<br>Enumerated Status                   | read only        | read only          |
| '11'<br>Measured value, scaled value<br>short signed | 'ENC'<br>Controllable enumerated status      | read-write       | read-write         |
| '11'<br>Measured value, scaled value<br>short signed | 'ENG'<br>Enumerated status setting           | --               | write only         |
| '11'<br>Measured value, scaled value<br>short signed | 'INC'<br>Controllable integer status         | read-write       | read-write         |
| '11'<br>Measured value, scaled value<br>short signed | 'CMD'<br>Command                             | --               | write only         |
| '11'<br>Measured value, scaled value<br>short signed | 'ING'<br>Integer status setting              | --               | write only         |

|  |  |            |            |
|--|--|------------|------------|
| '11'<br>Measured value, scaled value<br>short signed   | 'MV'<br>Measured Value                 | read only  | read only  |
| '13'<br>Measured value, short floating<br>point number | 'MV'<br>Measured Value                 | read only  | read only  |
| '13'<br>Measured value, short floating<br>point number | 'APC'<br>Controllable analog set point | read-write | read-write |
| '13'<br>Measured value, short floating<br>point number | 'SPV'<br>Set point value               | --         | write only |
| '13'<br>Measured value, short floating<br>point number | 'ASG'<br>Analog setting                | --         | write only |

Table 210: IEC101 data types to IEC61850 data types

## 50.6.2 IEC61850 to IEC101 conversion using the command line

For IEC61850 to IEC101 conversion, you must configure two configuration packages:

- **iecd** for the IEC104 gateway; **/etc/config/iecd**
- **tserverd** for the terminal server; **/etc/config/tserverd**

The IECD point mappings comprise the information necessary to perform conversion between each data variable (point) on the remote IEC101 RTU and the corresponding variable in the IEC61850 domain.

In the IEC61850 domain, the data points are identified by unique textual names in the general form.

```
LogicalDevice/LogicalNode/DataObject, e.g. 'SENSORS/LLN0/SPSS01'
```

In the IEC101 domain, the data points are identified by type ID and information object address (IOA). For example:

```
Type ID 1 (Single Point Information), IOA 3
```

Each point is defined at the end of the **/etc/config/iecd** configuration file by a **config point** section block. A sample definition of two points is given below. The example configuration shows the points of IEC61850 domain belonging to logical device 'SENSORS' (option `iec61850_id`), logical node 'LLN0' (option `iec61850_ln`) with data objects (option `iec61850_do`) 'SPS01' and 'SPS02' (single point status) mapping to IEC101 data points of type id 1 (M\_SP\_NA\_1 – Single Point Information) and having IEC101 Information Object Addresses (option `iec101_ioa`) 5 and 6

To add more points repeat the section block for each added point.

To remove points, simply remove the section block.

**Note:** maximum 1200 points supported per serial port.



### 50.6.2.1 IEC61850 to IEC101 conversion using uci

```
root@VA_router:~# uci show iecd
iecd.main=iecd
iecd.main.enable=1
iecd.port1=port
iecd.port1.enable=1
iecd.port1.loglevel=5
iecd.port1.tcp_keepalive_enabled=1
iecd.port1.tcp_keepalive_interval=5
iecd.port1.tcp_keepalive_timeout=5
iecd.port1.tcp_keepalive_count=3
iecd.port1.tcp_user_timeout=20000
iecd.port1.master_protocol=iec101
iecd.port1.slave_protocol=iec61850
iecd.port1.ioa_offset=0
iecd.port1.pointmap_file=/root/iecd/iecd_points1.csv
iecd.port1.iec104_local_ip=0.0.0.0
iecd.port1.iec104_local_tcpport=2404
iecd.port1.iec104_k=12
iecd.port1.iec104_w=9
iecd.port1.iec104_t2=10000
iecd.port1.iec104_gi_resp_time=200
iecd.port1.iec104_txq_size=128
iecd.port1.iec104_sync_time=1
iecd.port1.iec104_time_tagged_cmds=0
iecd.port1.iec104_cmd_delay_time=5000
iecd.port1.iec104_fsm_debug_on=0
iecd.port1.iec104_dump_data=0
iecd.port1.iec104_trace_on=0
iecd.port1.iec61850_local_ip=0.0.0.0
iecd.port1.iec61850_local_tcpport=104
iecd.port1.iec101_target_ip=127.0.0.1
iecd.port1.iec101_target_tcpport=999
iecd.port1.iec101_mode=unbalanced
iecd.port1.iec101_cot_tx_length=1
iecd.port1.iec101_cot_source_octet=0
iecd.port1.iec101_asdu_addrln=1
```

```
iecd.port1.iec101_info_obj_addrln=2
iecd.port1.iec101_data_polling_time=500
iecd.port1.iec101_ack_delay=0
iecd.port1.iec101_link_addrln=1
iecd.port1.iec101_frame_rsp_time=2000
iecd.port1.iec101_max_tx_retry=3
iecd.port1.iec101_txq_size=128
iecd.port1.iec101_send_spont_delay_acq=1
iecd.port1.iec101_fsm_debug_on=0
iecd.port1.iec101_dump_data=0
iecd.port1.iec101_trace_on=0
iecd.@iec101link[0]=iec101link
iecd.@iec101link[0].portno=1
iecd.@iec101link[0].address=6
iecd.@iec101link[0].asduaddr=6
iecd.@point[0]=point
iecd.@point[0].portno=1
iecd.@point[0].iec61850_ld=SENSORS
iecd.@point[0].iec61850_ln=LLN0
iecd.@point[0].iec61850_do=SPSS01
iecd.@point[0].iec104_type_id=1
iecd.@point[0].iec104_ioa=5
iecd.@point[0].iec101_type_id=1
iecd.@point[0].iec101_ioa=5
iecd.@point[0].devaddr=1
iecd.@point[0].group=1
iecd.@point[0].index=0
iecd.@point[0].dword=0
iecd.@point[1]=point
iecd.@point[1].portno=1
iecd.@point[1].iec61850_ld=SENSORS
iecd.@point[1].iec61850_ln=LLN0
iecd.@point[1].iec61850_do=SPSS02
iecd.@point[1].iec104_type_id=1
iecd.@point[1].iec104_ioa=6
iecd.@point[1].iec101_type_id=1
iecd.@point[1].iec101_ioa=6
```

```
iecd.@point[1].devaddr=1
iecd.@point[1].group=1
iecd.@point[1].index=0
iecd.@point[1].dword=0
```

### 50.6.2.2 IEC61850 to IEC101 conversion using package options

```
root@VA_router:~# uci export iecd
package iecd

config iecd 'main'
    option enable '1'

config port 'port1'
    option enable '1'
    option loglevel '5'
    option tcp_keepalive_enabled '1'
    option tcp_keepalive_interval '5'
    option tcp_keepalive_timeout '5'
    option tcp_keepalive_count '3'
    option tcp_user_timeout '20000'
    option master_protocol 'iec101'
    option slave_protocol 'iec61850'
    option ioa_offset '0'
    option pointmap_file '/root/iecd/iecd_points1.csv'

# IEC104 related settings
option iec104_local_ip '0.0.0.0'
option iec104_local_tcpport '2404'
option iec104_k '12'
option iec104_w '9'
option iec104_t2 '10000'
option iec104_gi_resp_time '200'
option iec104_txq_size '128'
option iec104_sync_time '1'
option iec104_time_tagged_cmds '0'
option iec104_cmd_delay_time '5000'
option iec104_fsm_debug_on '0'
```

```
option iec104_dump_data '0'
option iec104_trace_on '0'

# IEC61850 related settings
option iec61850_local_ip '0.0.0.0'
option iec61850_local_tcpport '104'

option iec101_target_ip '127.0.0.1'
option iec101_target_tcpport '999'
option iec101_mode 'unbalanced'
option iec101_cot_tx_length '1'
option iec101_cot_source_octet '0'
option iec101_asdu_addrln '1'
option iec101_info_obj_addrln '2'
option iec101_data_polling_time '500'
option iec101_ack_delay '0'
option iec101_link_addrln '1'
option iec101_frame_rsp_time '2000'
option iec101_max_tx_retry '3'
option iec101_txq_size '128'
option iec101_send_spont_delay_acq '1'
option iec101_fsm_debug_on '0'
option iec101_dump_data '0'
option iec101_trace_on '0'

# The following section defines IEC101 slave links used in IEC101
unbalanced mode on
# Each link is defined by a config block 'config iec101link'
# To add more links repeat the section block for each added link. To remove
links, simply remove the link block from the configuration
# Maximum 32 links are supported
#
# Definition of options within the section block:
# portno - port number to which this point belongs (1 to 4)
# address - IEC101 slave link address
# asduaddr IEC101 slave common ASDU address
```

```
config iec101link
    option portno 1
    option address 6
    option asduaddr 6

config point
    option portno '1'
    option iec61850_ld 'SENSORS'
    option iec61850_ln 'LLN0'
    option iec61850_do 'SPSS01'
    option iec104_type_id '1'
    option iec104_ioa '5'
    option iec101_type_id 1
    option iec101_ioa '5'
    option devaddr '1'
    option group '1'
    option index '0'
    option dword '0'

config point
    option portno '1'
    option iec61850_ld 'SENSORS'
    option iec61850_ln 'LLN0'
    option iec61850_do 'SPSS02'
    option iec104_type_id '1'
    option iec104_ioa '6'
    option iec101_type_id 1
    option iec101_ioa '6'
    option devaddr '1'
    option group '1'
    option index '0'
    option dword '0'
```

## 50.7 Diagnostics

### 50.7.1 Starting and stopping services

The `iecd` and `tserve` background services are started automatically at router power up.

You can manually stop, start or restart these services as follows:

#### **iecd**

```
/etc/init.d/iecd stop - stops IECD service
/etc/init.d/iecd start - starts IECD service
/etc/init.d/iecd restart - stops and starts IECD service
```

#### **tserve**

```
/etc/init.d/tserve stop - stops TSERVD service
/etc/init.d/ tserve start - starts TSERVD service
/etc/init.d/ tserve restart - stops and starts TSERVD service
```

### 50.7.2 Events

The diagnosing and protocol tracing on the router the following features are available:

- Viewing syslog events (error messages)
- Running and viewing protocol traces (using syslog)
- Viewing statistic counters and debug information using diagnostic commands

To see the appropriate debug information, you must enable different debug options.

The following table summarizes various options for tracing and diagnostics of the IEC104 to IEC101/DNP3/Modbus conversion:

| Diagnostic feature        | IEC104   | IEC101   | DNP3   | MODBUS   |
|---------------------------|--|--|--|--|
| Protocol Tracing          | option log_severity '7'<br>option iec104_trace_on '1'<br>/etc/init.d/iecd restart<br>logread -f          | option log_severity '7'<br>option iec101_trace_on '1'<br>/etc/init.d/iecd restart<br>logread -f          | option log_severity '7'<br>option dnp3_trace_on '1'<br>/etc/init.d/iecd restart<br>logread -f          | option log_severity '7'<br>option modbus_trace_on '1'<br>/etc/init.d/iecd restart<br>logread -f          |
| Viewing Rx / Tx Hex dump  | option log_severity '7'<br>option iec104_dump_data '1'<br><br>/etc/init.d/iecd restart<br><br>logread -f | option log_severity '7'<br>option iec101_dump_data '1'<br><br>/etc/init.d/iecd restart<br><br>logread -f | option log_severity '7'<br>option dnp3_dump_data '1'<br><br>/etc/init.d/iecd restart<br><br>logread -f | option log_severity '7'<br>option modbus_dump_data '1'<br><br>/etc/init.d/iecd restart<br><br>logread -f |
| Viewing Statistics        | iec show stats   | iec show stats   | iec show stats   | iec show stats   |
| Clearing Statistics       | iec clear stats  | iec clear stats  | iec clear stats  | iec clear stats  |
| Viewing debug information | N/a  | N/a  | N/a  | iec show modbus debug  |
| View point loaded points  | iec show points  | iec show points  | iec show points  | iec show points  |

Table 211: SCADA applications debug options table

### 50.7.3 Viewing statistics

To view IEC104 gateway statistics, enter:

```

root@VA_router:~/iecd# iec show stats
Modbus stats:
=====
Modbus DL Frames Rx 20 Tx 3845 TxErrs 0
Modbus DL CRCErrs 0 Bad Addr 0 LengthErrs 0 UnknownPeer 0 SessionClose 0
Modbus App PDU Rx 20 PDU Tx 3845 PDU Rx Errors 0 PDU Rx Exception 0
Modbus App PDU Rx Timeout 3825 Unknown DevAddr 0 Rx Unexpected FC 0
Modbus App PDU TxQ Overrun 0

IEC104 stats:
=====
IEC104 DL state: CLOSED
IEC104 DL uptime: 0 hrs 0 mins 0 secs

```

```
IEC104 DL PktsRx 15 PktsTx 21 TxQ Overrun 0
IEC104 App ASDU Rx 6 ASDU Tx 12 Bad ASDU 0
```

## 50.7.4 Viewing point mappings

To view IEC104 gateway point mappings, enter:

```
root@VA_router:~/iecd# iec show points
==== IEC104 point map: ====
IEC 104 Types Legend:
-----
SPI: Single point information (1 bit)
DPI: Double point information (2 bit)
MVA: Measured normalized value (16 bit signed)
MVAFP: Measured value, floating point number (32 bit signed)
SVA: Measured scaled value (16 bit signed)
BSTR32: Bitstring of 32 bits
IT: Integrated Total (Counter 32 bit)
CP24: with 3 octet time tag CP24Time2a
CP56: with 7 octet time tag CP56Time2a
NQD: Without quality descriptor
-----
(#1) IOA=64213, Val=0x00000000, IEC104TypeId=30 (SPI-CP56) DevAddr 1 Modbus pt 1, Type 0 (Discreet Input (1bit))
(#2) IOA=64214, Val=0x00000000, IEC104TypeId=30 (SPI-CP56) DevAddr 1 Modbus pt 2, Type 0 (Discreet Input (1bit))
(#3) IOA=64215, Val=0x00000000, IEC104TypeId=30 (SPI-CP56) DevAddr 1 Modbus pt 9, Type 0 (Discreet Input (1bit))
(#4) IOA=64216, Val=0x00000000, IEC104TypeId=30 (SPI-CP56) DevAddr 1 Modbus pt 10, Type 0 (Discreet Input (1bit))
(#5) IOA=64217, Val=0x00000000, IEC104TypeId=34 (MVA-CP56) DevAddr 1 Modbus pt 2, Type 1 (Input Register (16 bit))
(#6) IOA=64218, Val=0x00000000, IEC104TypeId=34 (MVA-CP56) DevAddr 1 Modbus pt 7, Type 1 (Input Register (16 bit))
(#7) IOA=64219, Val=0x00000000, IEC104TypeId=34 (MVA-CP56) DevAddr 1 Modbus pt 1, Type 2 (Holding Register (16 bit))
```



## 51 DNP3 outstation application

Virtual Access routers have a feature that allows the router to operate as a DNP3 outstation application. A DNP3 SCADA master can poll the router and obtain the following information:

- Router uptime in seconds.
- The serial number of the router.
- The status of up to two router interfaces.

### 51.1 Configuration packages used

| Package | Sections |
|---------|----------|
| dnposd  | dnposd   |

### 51.2 Configuring using the web interface

To configure the DNP3 outstation, from the top menu select **Services -> DNP3 Outstation**.

Check the **Enable** box and fill in your unique parameters.

The router listens for inbound UDP connections from the SCADA master on the specified port.

The web automatically names the dnposd config section 'main'.

**DNP3 Outstation**  
Configuration of the DNP3 Outstation Daemon

Settings

Enable

Local DNP Address

Master DNP Address

Master IP Address

Local Port  ⓘ Local udp port to listen to incoming DNP requests

Monitor Interface1  ⓘ Name of first interface to monitor and report status

Monitor Interface2  ⓘ Name of second interface to monitor and report status

**Figure 280: DNP3 outstation settings**

| Web Field/UCI/Package Option   | Description  |       |           |       |          |
|--|--|-------|-----------|-------|----------|
| Web: Enable<br>UCI: dnpsd.main.enabled<br>Opt: enabled                           | Enables the DNP3 outstation application on the router.<br><table border="1"> <tr> <td>0</td> <td>Disabled.</td> </tr> <tr> <td>1</td> <td>Enabled.</td> </tr> </table>   | 0     | Disabled. | 1     | Enabled. |
| 0  | Disabled.  |       |           |       |          |
| 1  | Enabled.   |       |           |       |          |
| Web: Local DNP Address<br>UCI: dnpsd.main.local_address<br>Opt: local_address    | Defines the DNP3 address of the router.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>0-65535</td> </tr> </table>  | Blank |           | Range | 0-65535  |
| Blank  |  |       |           |       |          |
| Range  | 0-65535  |       |           |       |          |
| Web: Master DNP Address<br>UCI: dnpsd.main.master_address<br>Opt: master_address | Defines the DNP3 address of the SCADA master.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>0-65535</td> </tr> </table>  | Blank |           | Range | 0-65535  |
| Blank  |  |       |           |       |          |
| Range  | 0-65535  |       |           |       |          |
| Web: Master IP Address<br>UCI: dnpsd.main.master_host<br>Opt: master_host        | Defines the IP address of the SCADA master. Only requests from this host will be processed.  |       |           |       |          |
| Web: Local Port<br>UCI: dnpsd.main.local_port<br>Opt: local_port                 | Defines the UDP port for the router to listen on for incoming DNP3 messages from the SCADA master.<br><table border="1"> <tr> <td>20000</td> <td></td> </tr> <tr> <td>Range</td> <td>0-65535</td> </tr> </table>   | 20000 |           | Range | 0-65535  |
| 20000  |  |       |           |       |          |
| Range  | 0-65535  |       |           |       |          |
| Web: Monitor Interface1<br>UCI: dnpsd.main.monitor_if1<br>Opt: monitor_if1       | Defines the first interface to monitor for status.<br><b>Note:</b> the interface names need to exactly match to the physical names. You can view the physical name by using the <code>ifconfig</code> command via command line.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>0-65535</td> </tr> </table>  | Blank |           | Range | 0-65535  |
| Blank  |  |       |           |       |          |
| Range  | 0-65535  |       |           |       |          |
| Web: Monitor Interface2<br>UCI: dnpsd.main.monitor_if2<br>Opt: monitor_if2       | Defines the second interface to monitor for status.<br><b>Note:</b> the interface names need to exactly match to the physical names. You can view the physical name by using the <code>ifconfig</code> command via command line.<br><table border="1"> <tr> <td>Blank</td> <td></td> </tr> <tr> <td>Range</td> <td>0-65535</td> </tr> </table> | Blank |           | Range | 0-65535  |
| Blank  |  |       |           |       |          |
| Range  | 0-65535  |       |           |       |          |

Table 212: Information table for DNP3 outstation settings

## 51.3 Configuring DNP3 outstation using command line

DNP3 outstation is configured under the `dnpsd` package `/etc/config/dnp3osd`

### 51.3.1 DNP3 outstation using UCI

```
root@VA_router:~# uci show dnpsd
dnpsd.main=dnpsd
dnpsd.main.local_port=20000
dnpsd.main.enabled=yes
dnpsd.main.local_address=1
dnpsd.main.master_address=2
dnpsd.main.master_host=10.1.10.21
dnpsd.main.monitor_if1=wwan0
```

```
dnposd.main.monitor_if2=pppoa-DSL
```

Modify these commands by running a `uci set <parameter>` command followed by `uci commit`.

### 51.3.2 DNP3 outstation using package options

```
root@VA_router:~# uci export dnposd
package dnposd

config dnposd 'main'
    option local_port '20000'
    option enabled 'yes'
    option local_address '1'
    option master_address '2'
    option master_host '10.1.10.21'
    option monitor_if1 'wwan0'
    option monitor_if2 'pppoa-DSL'
```

## 51.4 DNP3 outstation diagnostics

### 51.4.1 Restarting dnposd

To restart dnposd service, enter:

```
root@VA_router:~# /etc/init.d/dnposd restart
```

### 51.4.2 Tracing DNP3 packets

By default, the DNP3 outstation listens on UDP port 20000. To trace UDP packets on port 20000, enter:

```
root@VA_router:~# tcpdump -i any -n udp -p port 20000 &
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535
bytes
```

To stop tracing enter `fg` to bring tracing task to foreground, and then `<CTRL-C>` to stop the trace.

```
root@VA_router:~# fg
tcpdump -i any -n udp -p port 20000
^C
33 packets captured
33 packets received by filter
0 packets dropped by kernel
```

## 52 Serial interface

### 52.1 Overview

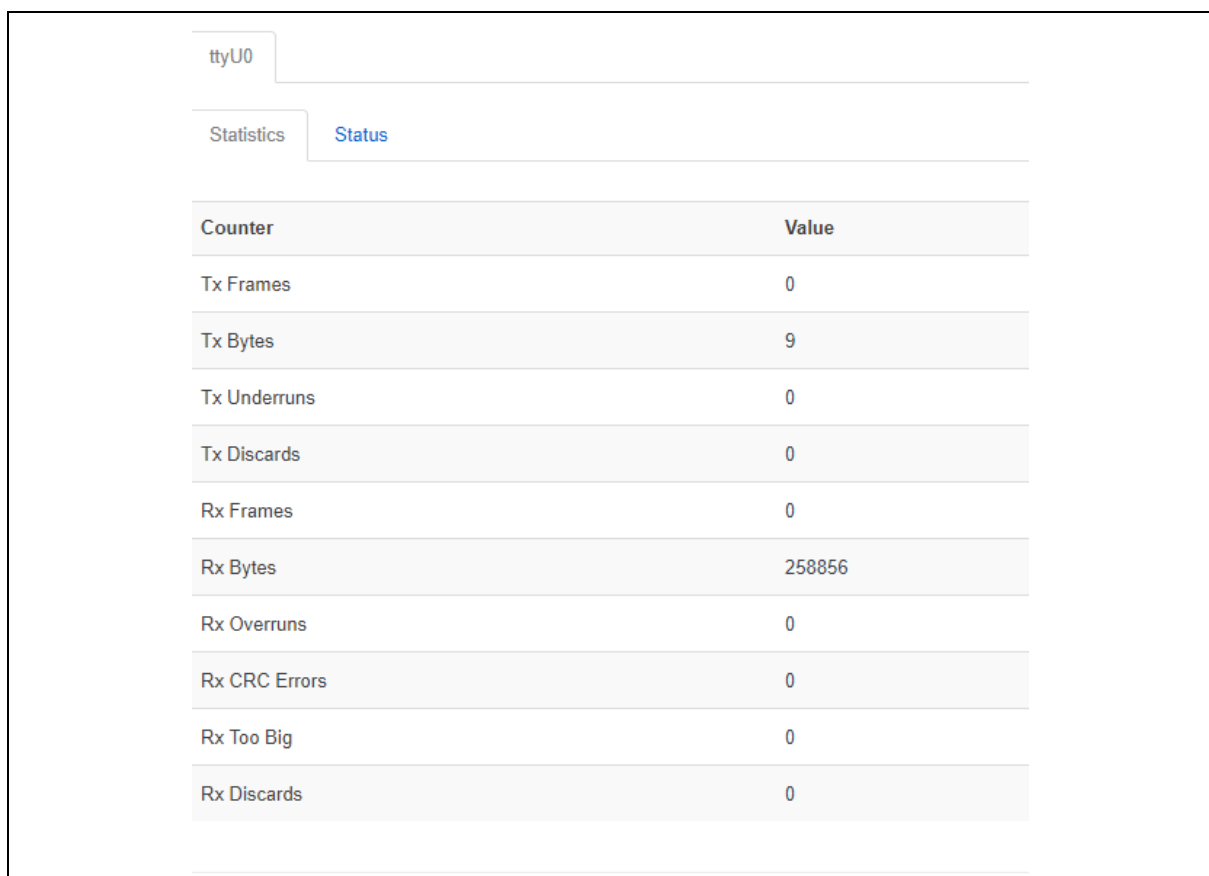
Many different applications and device drivers use the serial interface. You configure the serial interface using the relevant application; for example Terminal Server, therefore there is no standalone serial configuration page.

You can monitor the various serial interfaces using either the command line or the web interface.

### 52.2 Monitoring serial interfaces using the web interface

In the top menu, select **Status -> Serial Interfaces**. Depending on the number of serial interfaces present on the device, a number of tabs will appear giving access to information about each interface. The information presented will also depend on the actual type of the serial interface.

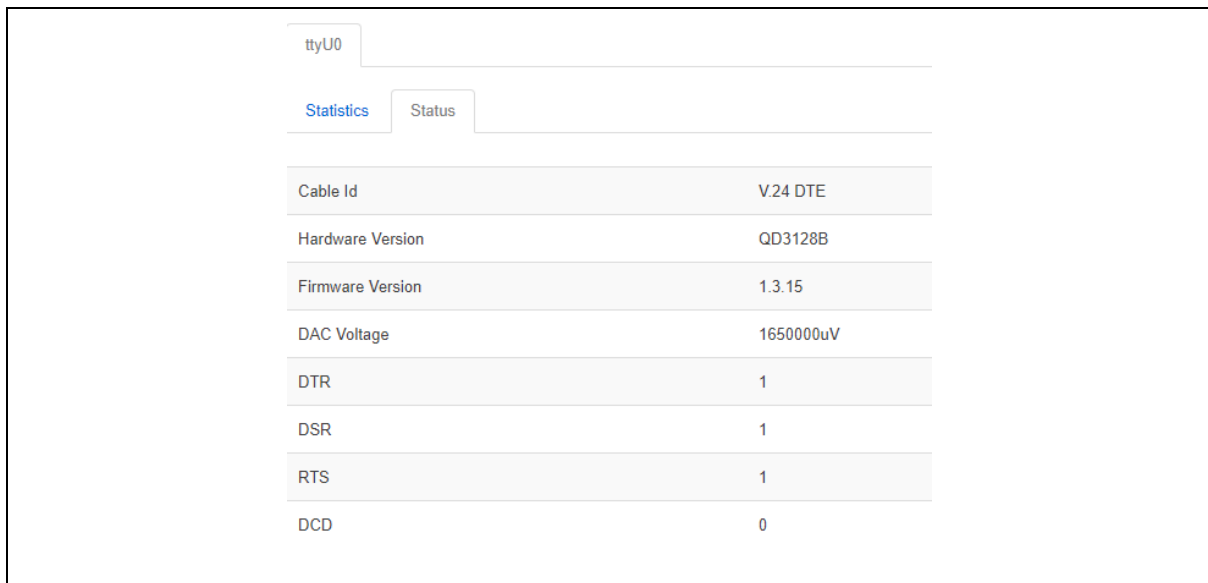
#### 52.2.1 Serial statistics



| Counter       | Value  |
|---------------|--------|
| Tx Frames     | 0      |
| Tx Bytes      | 9      |
| Tx Underruns  | 0      |
| Tx Discards   | 0      |
| Rx Frames     | 0      |
| Rx Bytes      | 258856 |
| Rx Overruns   | 0      |
| Rx CRC Errors | 0      |
| Rx Too Big    | 0      |
| Rx Discards   | 0      |

Figure 281: The serial statistics page for serial-0

## 52.2.2 Serial status



| ttyU0            |           |
|------------------|-----------|
| Statistics       |           |
| Status           |           |
| Cable Id         | V.24 DTE  |
| Hardware Version | QD3128B   |
| Firmware Version | 1.3.15    |
| DAC Voltage      | 1650000uV |
| DTR              | 1         |
| DSR              | 1         |
| RTS              | 1         |
| DCD              | 0         |

Figure 282: The serial status page for serial-0

## 52.3 Monitoring serial interfaces using command line

### 52.3.1 Serial statistics using command line

To view serial statistics, enter:

```
root@VirtualAccess:~# serial_stats
ttyU0 statistics
Tx Frames          0
Tx Bytes           9
Tx Underruns       0
Tx Discards        0
Rx Frames          0
Rx Bytes          258856
Rx Overruns        0
Rx CRC Errors      0
Rx Too Big         0
Rx Discards        0
```

### 52.3.2 Serial status using command line

To view serial statistics, enter:

```
root@VirtualAccess:~# serial_status
ttyU0 status
Cable Id          V.24 DTE
Hardware Version  QD3128B
Firmware Version  1.3.15
DAC Voltage       1650000uV
DTR               1
DSR               1
RTS               1
DCD               0
```

### 52.3.3 Resetting serial statistics

To reset serial statistics, enter:

```
root@VirtualAccess:~# serial_stats_reset ttyU0
Serial interface statistics reset
```

You can reset statistics for all or individual serial interfaces.