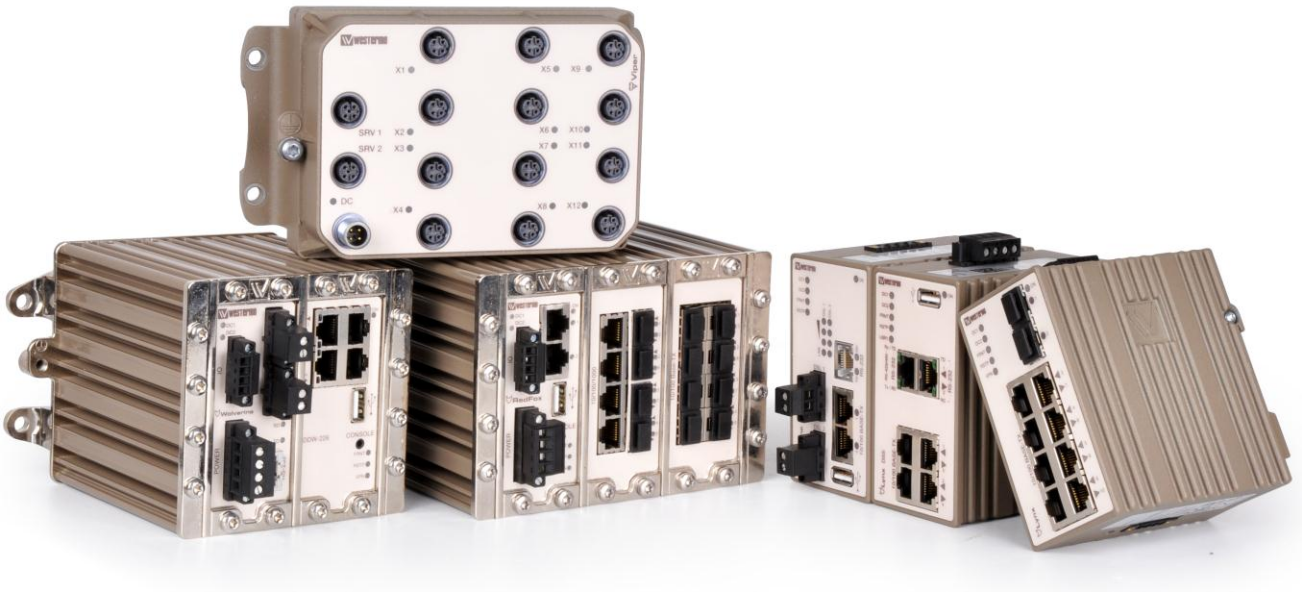
APPLICATION NOTE

Westermo WeOS Multicast Tunneling

Configure IPSec, GRE Tunneling, OSPF and Multicast Routing



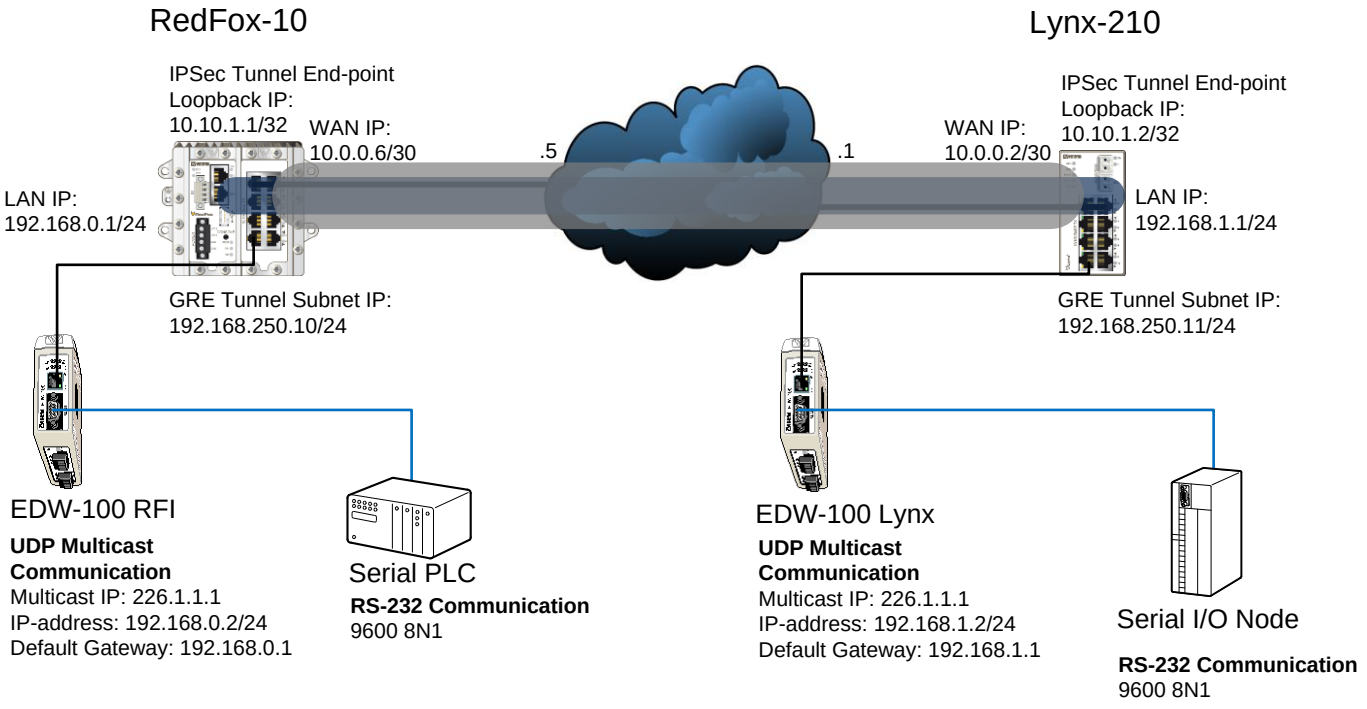
Application Note Network Layout

This Application Note shows how to pass Mulitcast traffic between two separate networks securely using VPN tunnels and Multicast routing.

Background

IPSec VPN tunnels are Layer 3 tunnels which means that separate networks on either side of the tunnel is needed. This will prohibit Multicast traffic from being sent over the tunnel.
If Multicast traffic needs to be passed between the networks a GRE tunnel can be used, however the GRE tunnel do not have any security functions.
To solve the securtiy issue the GRE tunnel can be tunneled through an IPSec tunnel which will authenticate and secure the communication.
In this way routing protocols like OSPF, that annonunces its routes using Multicast, can be ran between the routers.
Adding static Multicast routing, external Multicast traffic can also sent through the tunnels and between the networks.

All configuration in this Application Note is done using WeOS version 4.13.4 and EDW-100 version 4101-1009.



Configure the Central Site RedFox-10

Create the interfaces needed with appropriate IP-addresses.

VLANs

VID	Name	Enabled	Status	Prio	IGMP	Interface	Port(s)			
							Tagged	Untagged	Dynamic	
1	vlan1	✓	Up	–	✓	vlan1		eth 1/1, eth 1/2		✎
15	vlan15	✓	Down	–	✓	vlan15		eth 2/1		✎ 🗑
100	vlan100	✓	Down	–	✓	vlan100		eth 2/2-2/8		✎ 🗑

New VLAN

Network - Interface

Name	Enabled	Status	Address method	Address/Netmask	
vlan1+	✓	Up	Static	192.168.2.202 / 255.255.255.0	✎
vlan100	✓	Down	Static	192.168.0.1 / 255.255.255.0	✎
vlan15	✓	Down	Static	10.0.0.6 / 255.255.255.252	✎

Create the loopback interface needed for the IPSec tunnel end-point.

lo	✓	Up	Static	127.0.0.1 / 255.0.0.0 10.10.1.1 / 255.255.255.255	✎

Configure the Client Lynx-210

Create the interfaces needed with appropriate IP-addresses.

VLANs

VID	Name	Enabled	Status	Prio	IGMP	Interface	Port(s)			
							Tagged	Untagged	Dynamic	
1	vlan1	✓	Up	–	✓	vlan1		eth 1-3		✎
10	vlan10	✓	Down	–	–	vlan10		eth 7		✎ 🗑
101	vlan101	✓	Down	–	✓	vlan101		eth 4-6, 8-10		✎ 🗑

New VLAN

Network - Interface

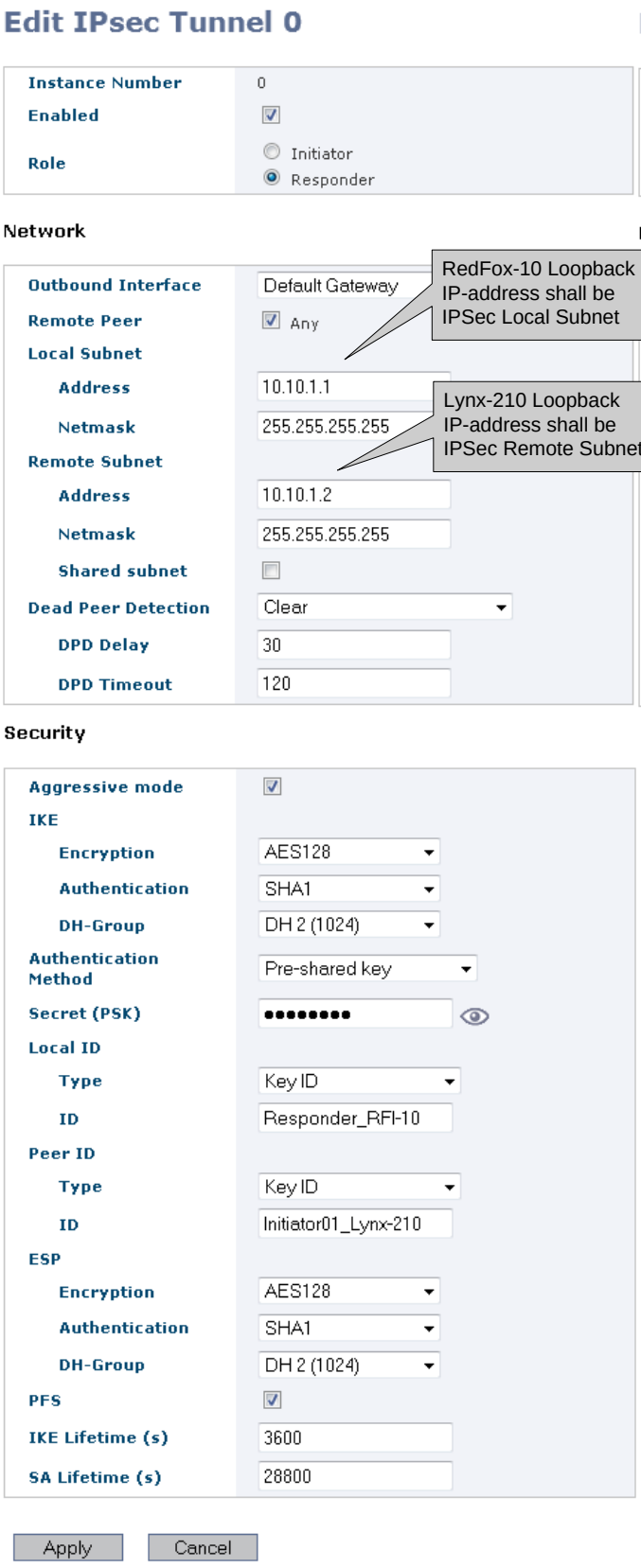
Name	Enabled	Status	Address method	Address/Netmask	
vlan1+	✓	Up	Static	192.168.2.201 / 255.255.255.0	✎
vlan10	✓	Down	Static	10.0.0.2 / 255.255.255.252	✎
vlan101	✓	Down	Static	192.168.1.1 / 255.255.255.0	✎

Create the loopback interface needed for the IPSec tunnel end-point.

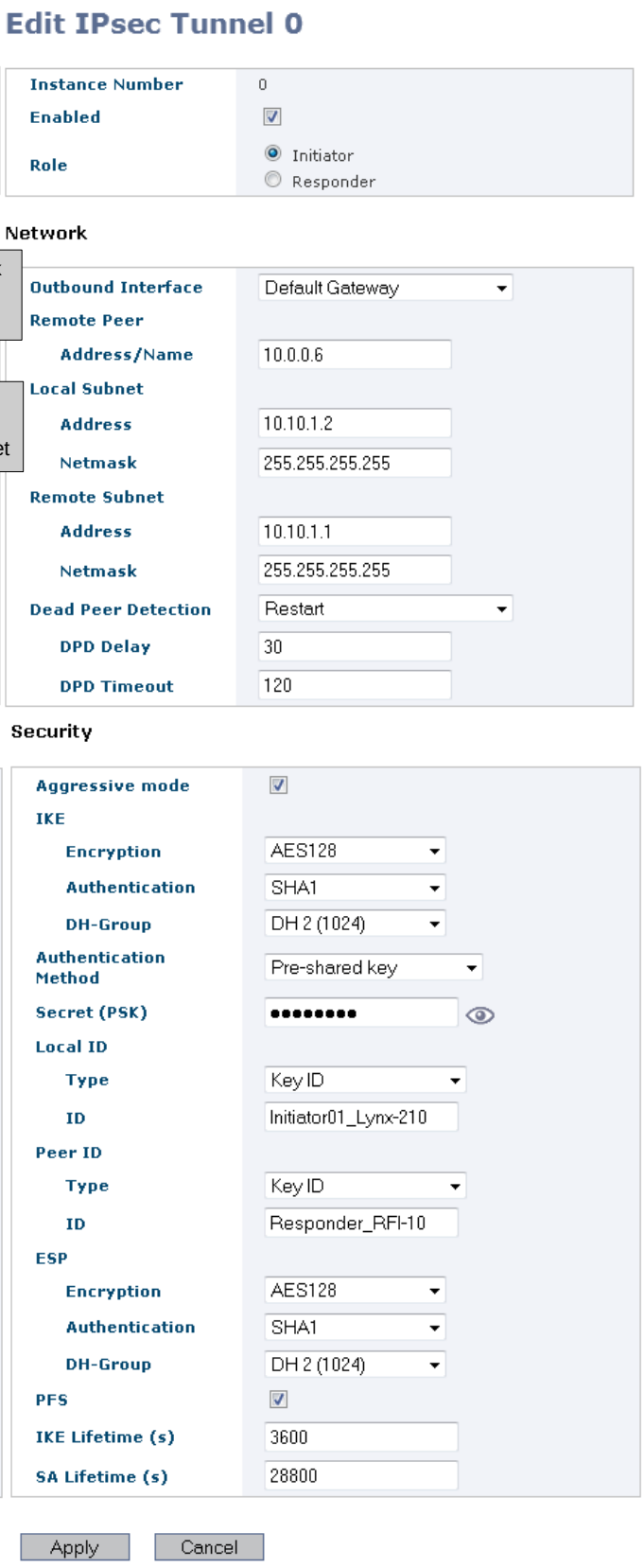
lo	✓	Up	Static	127.0.0.1 / 255.0.0.0 10.10.1.2 / 255.255.255.255	✎

Configure the IPSec Tunnel

IPSec settings RedFox-10

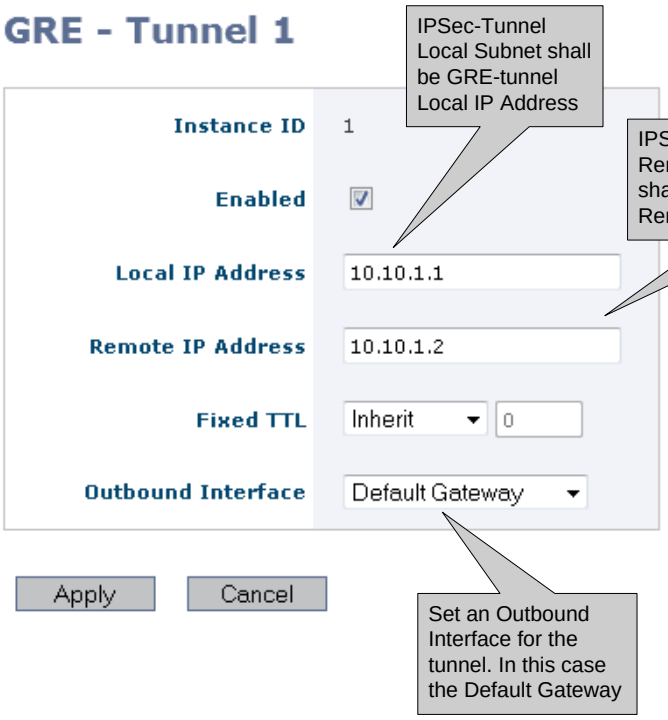


IPSec settings Lynx-210

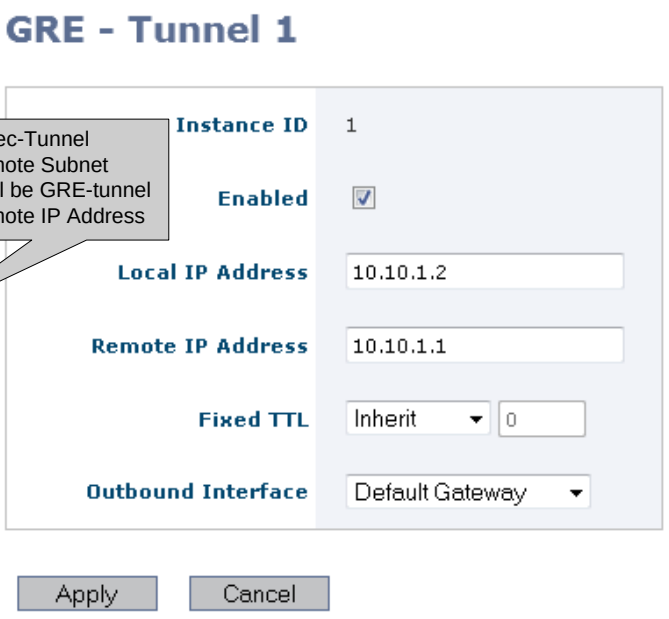


Configure the GRE Tunnel

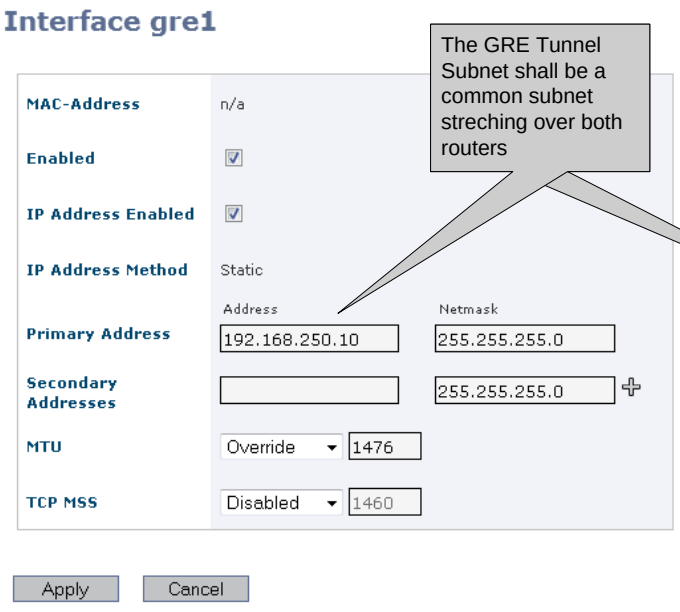
GRE-Tunnel RedFox-10



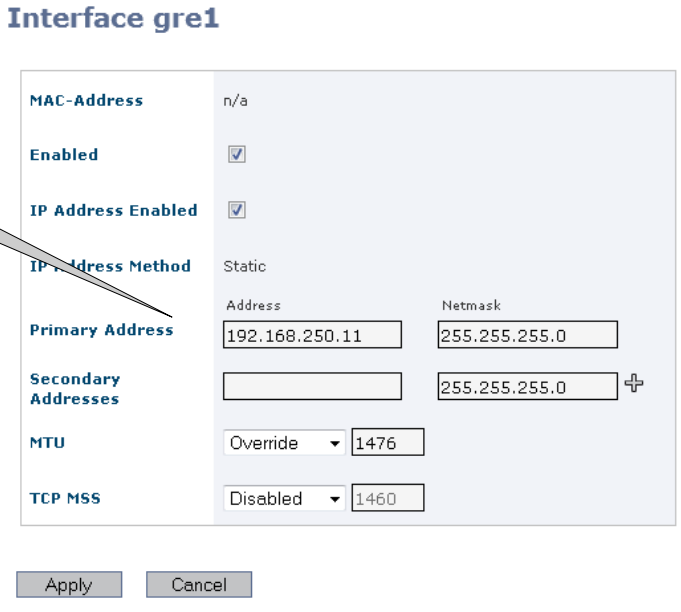
GRE-Tunnel Lynx-210



GRE-Tunnel GRE Tunnel Subnet RedFox-10

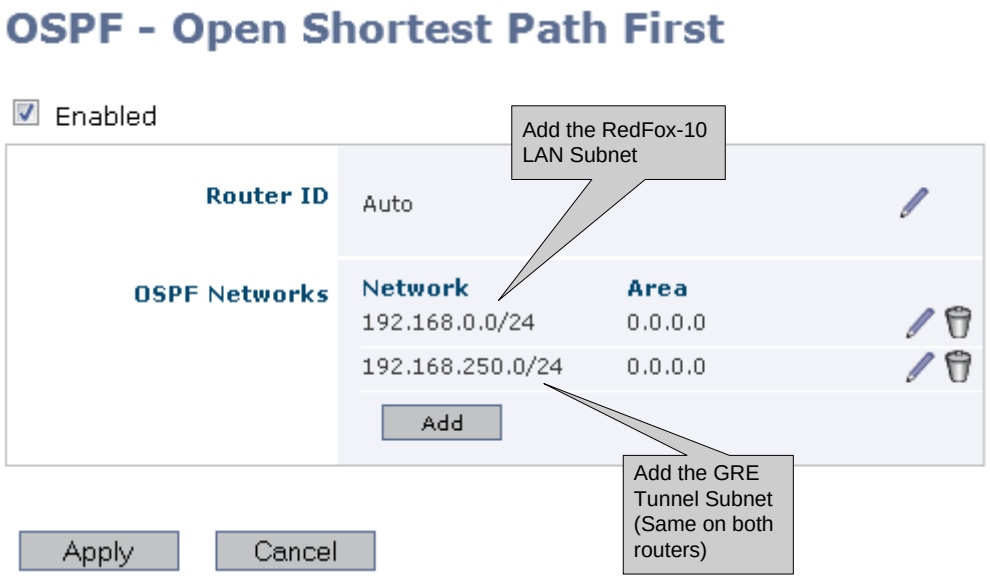


GRE-Tunnel GRE Tunnel Subnet Lynx-210

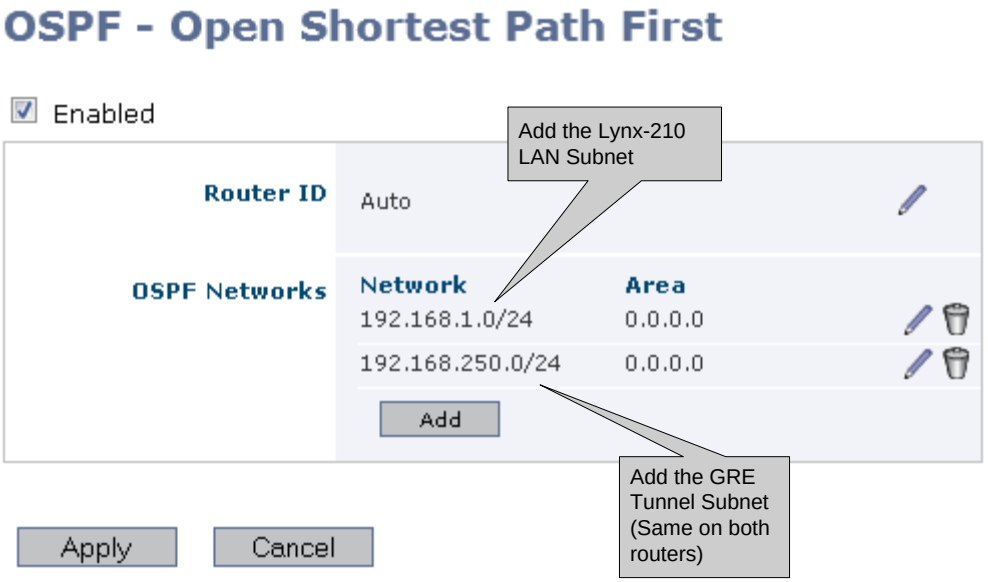


Activate OSPF Routing Protocol

Enable OSPF to announce connected networks on RedFox-10

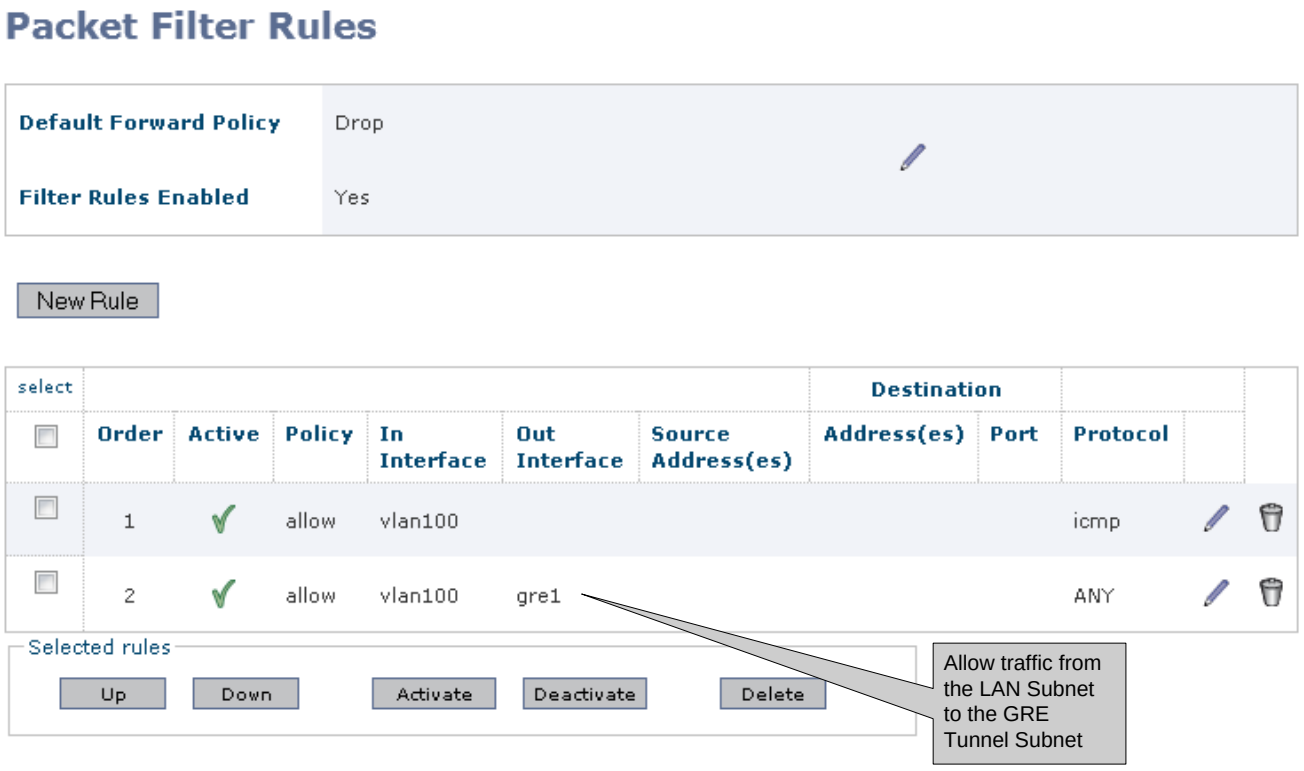


Enable OSPF to announce connected networks on Lynx-210

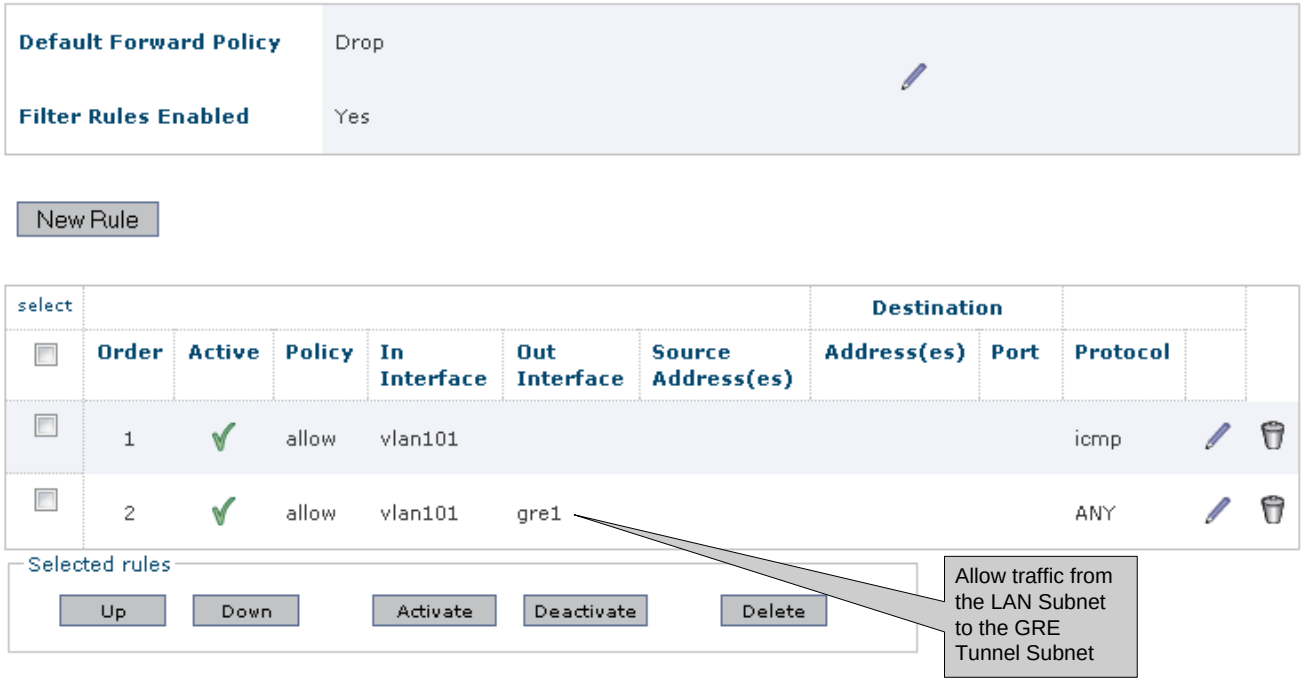


Activate the Firewall to Protect the WAN Side

RedFox-10 Firewall Rules



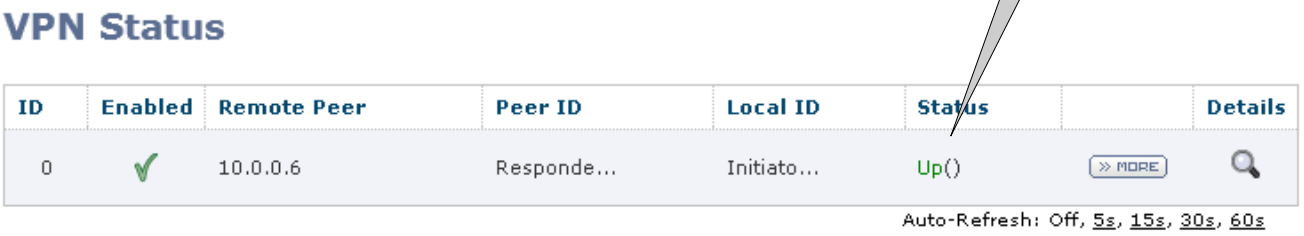
Lynx-210 Firewall Rules



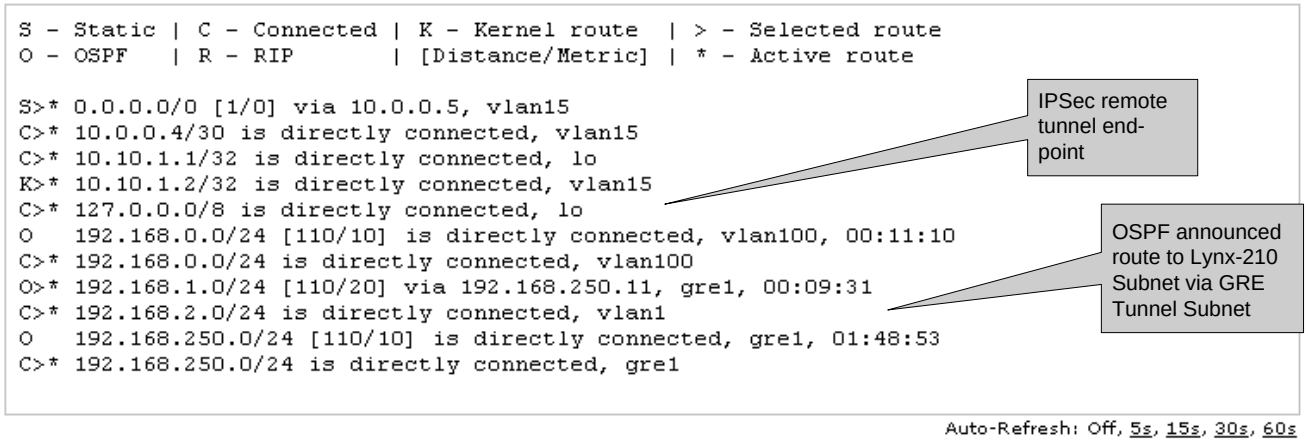
Verify Connectivity

RedFox-10 IPSec Status

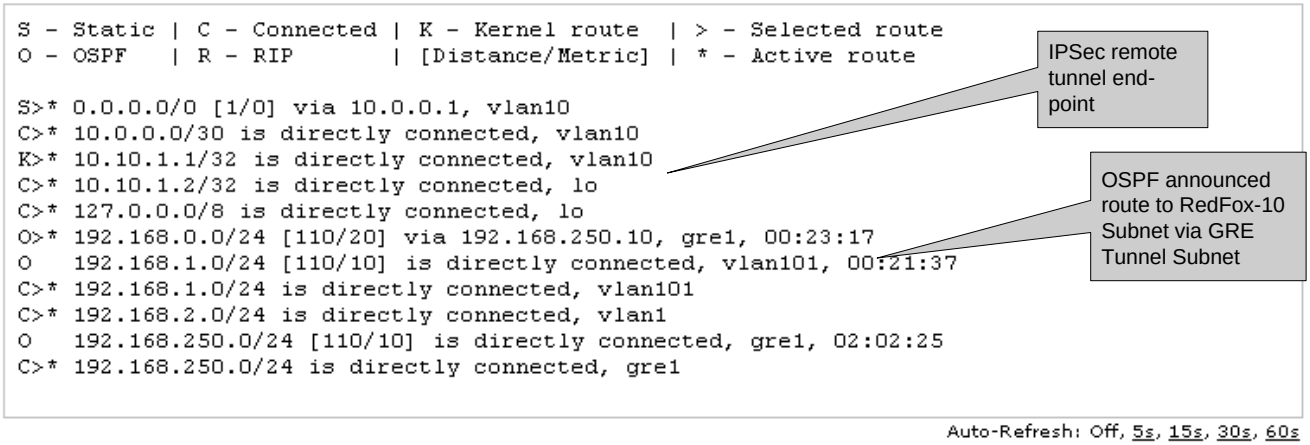
Lynx-210 IPSec Status



RedFox-10 Routing Table

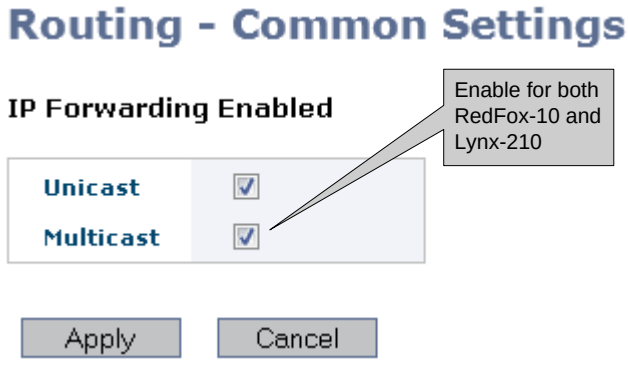


Lynx-210 Routing Table

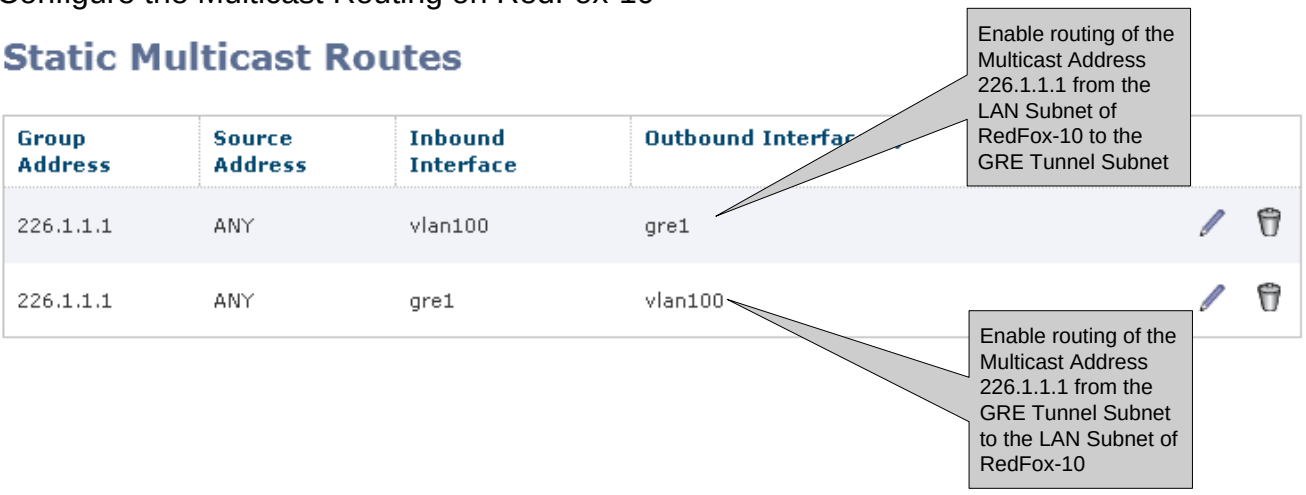


Add Static Multicast Routing in order to forward Multicast Traffic over the GRE tunnel

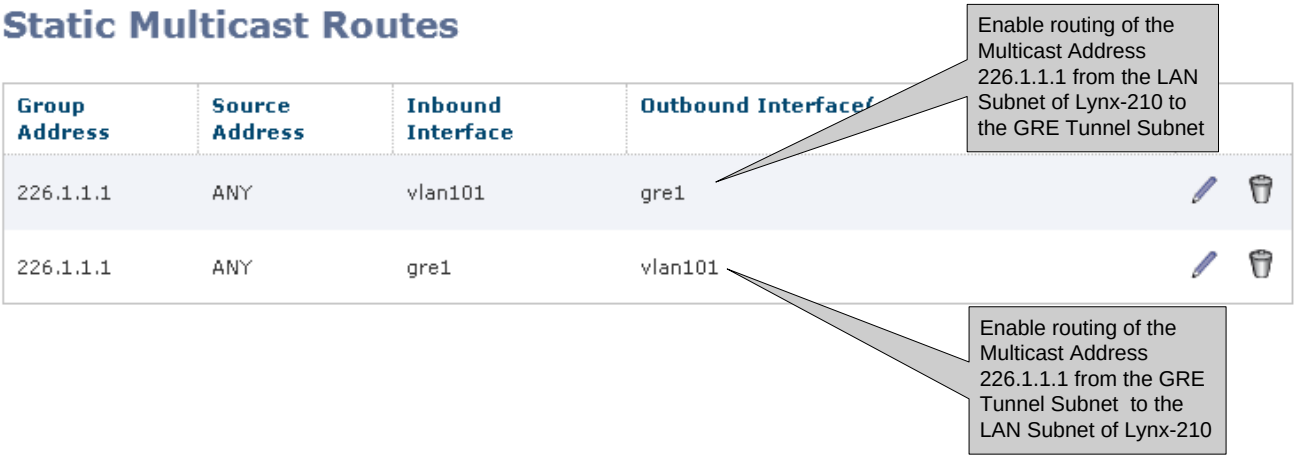
Enable Static Multicast Routing on both Routers



Configure the Multicast Routing on RedFox-10



Configure the Multicast Routing on Lynx-210



Verify Connectivity

Multicast Routing Table RedFox-10

Multicast Routes

Group Address	Source Address	Inbound Interface	Packets	Bytes	Invalid	Outbound Interface(s)
226.1.1.1	192.168.0.2	vlan100	32	930	0	gre1
226.1.1.1	192.168.1.2	gre1	32	930	0	vlan100

Auto-Refresh: Off, 5s, 15s, 30s, 60s

Multicast traffic are being routed from these addresses to and from the GRE Tunnel Subnet

Multicast Routing Table Lynx-210

Multicast Routes

Group Address	Source Address	Inbound Interface	Packets	Bytes	Invalid	Outbound Interface(s)
226.1.1.1	192.168.0.2	gre1	32	930	0	vlan101
226.1.1.1	192.168.1.2	vlan101	32	930	0	gre1

Auto-Refresh: Off, 5s, 15s, 30s, 60s

Configuration RedFox-10

```
# \\/ Westermo WeOS v4.13.4, CLI Format v1.13
# RedFox RFI-10P, art.no. 3641-3110 ser.no. 1348

aaa
        username admin hash $1$r6mXNVvD$JaDxe9xNk/MI7Ebdk7B0q.
        end

system
        hostname RedFox-10
        location CentralSite
        contact support@westermo.com
        end

fdb
        mac 01:00:5e:00:00:01 port cpu, all
        mac 01:00:5e:00:00:02 port cpu, all
        mac 01:00:5e:00:00:04 port cpu, all
        mac 01:00:5e:00:00:05 port cpu, all
        mac 01:00:5e:00:00:06 port cpu, all
        mac 01:00:5e:00:00:09 port cpu, all
        mac 01:00:5e:00:00:0a port cpu, all
        mac 01:00:5e:00:00:0d port cpu, all
        mac 01:00:5e:00:00:0e port cpu, all
        mac 01:00:5e:00:00:12 port cpu, all
        mac 01:00:5e:00:00:18 port cpu, all
        mac 01:00:5e:00:00:66 port cpu, all
        mac 01:00:5e:00:00:6b port cpu, all
        mac 01:00:5e:00:00:fb port cpu, all
        end

alarm
        action 1
                target snmp log led digout
                end
        end

port ALL
        speed-duplex auto
        end

no spanning-tree

vlan 1
        name vlan1
        untagged 1/1-1/2
        end

vlan 15
        name vlan15
        untagged 2/1
        end

vlan 100
        name vlan100
        untagged 2/2-2/8
        end

iface lo inet static
        address 10.10.1.1/32 secondary
        end

iface gre1 inet static
        mtu 1476
        no management
        address 192.168.250.10/24
        end

iface vlan1 inet static
        primary
        management ssh http https ipconfig snmp
        address 192.168.2.202/24
        end

iface vlan15 inet static
        no management
        address 10.0.0.6/30
        end

iface vlan100 inet static
        management ssh http https ipconfig snmp
        address 192.168.0.1/24
        end

ip
        route 0.0.0.0/0 10.0.0.5
        mroute group 226.1.1.1 in vlan100 out gre1
        mroute group 226.1.1.1 in gre1 out vlan100
        multicast-forwarding
        firewall
                policy input DROP
                policy forward DROP
                allow in vlan100 proto icmp
                allow in vlan100 out gre1
                enable
                end
        end

tunnel
        ipsec 0
                enable
                no initiator
                aggressive
                pfs
                ike crypto AES128 auth SHA1 dh 1024
                esp crypto AES128 auth SHA1 dh 1024
                no peer
                no outbound
                local-id key Responder_RFI-10
                remote-id key Initiator01_Lynx-210
                local-subnet 10.10.1.1/32
                remote-subnet 10.10.1.2/32
                secret westermo
                dpd-action clear
                dpd-delay 30
                dpd-timeout 120
                sa-lifetime 28800
                ike-lifetime 3600
                end
        ipsec-nat-traversal
        gre 1
                local 10.10.1.1
                remote 10.10.1.2
                end
        end

router
        ospf
                network 192.168.0.0/24 area 0.0.0.0
                network 192.168.250.0/24 area 0.0.0.0
                end
        end

snmp-server
        rocommunity public
        no rwcommunity
        trapcommunity trap
        end
```

Configuration Lynx-210

```
# \\/ Westermo WeOS v4.13.4, CLI Format v1.13
# Lynx L210, art.no. 3643-0105 ser.no. 1073

aaa
        username admin hash $1$r6mXNVvD$JaDxe9xNk/MI7Ebdk7B0q.
        end

system
        hostname Lynx-210
        location Station01
        contact support@westermo.com
        end

fdb
        mac 01:00:5e:00:00:01 port cpu, all
        mac 01:00:5e:00:00:02 port cpu, all
        mac 01:00:5e:00:00:04 port cpu, all
        mac 01:00:5e:00:00:05 port cpu, all
        mac 01:00:5e:00:00:06 port cpu, all
        mac 01:00:5e:00:00:09 port cpu, all
        mac 01:00:5e:00:00:0a port cpu, all
        mac 01:00:5e:00:00:0d port cpu, all
        mac 01:00:5e:00:00:0e port cpu, all
        mac 01:00:5e:00:00:12 port cpu, all
        mac 01:00:5e:00:00:18 port cpu, all
        mac 01:00:5e:00:00:66 port cpu, all
        mac 01:00:5e:00:00:6b port cpu, all
        mac 01:00:5e:00:00:fb port cpu, all
        end

alarm
        action 1
                target snmp log led digout
                end
        end

port ALL
        speed-duplex auto
        end

no spanning-tree

vlan 1
        name vlan1
        untagged 1-3
        end

vlan 10
        name vlan10
        untagged 7
        end

vlan 101
        name vlan101
        untagged 4-6,8-10
        end

iface lo inet static
        address 10.10.1.2/32 secondary
        end

iface gre1 inet static
        mtu 1476
        no management
        address 192.168.250.11/24
        end

iface vlan1 inet static
        primary
        management ssh http https ipconfig snmp
        address 192.168.2.201/24
        end

iface vlan10 inet static
        no management
        address 10.0.0.2/30
        end

iface vlan101 inet static
        management ssh http https ipconfig snmp
        address 192.168.1.1/24
        end

ip
        route 0.0.0.0/0 10.0.0.1
        mroute group 226.1.1.1 in vlan101 out gre1
        mroute group 226.1.1.1 in gre1 out vlan101
        multicast-forwarding
        firewall
                policy input DROP
                policy forward DROP
                allow in vlan101 proto icmp
                allow in vlan101 out gre1
                enable
                end
        end

tunnel
        ipsec 0
                enable
                initiator
                aggressive
                pfs
                ike crypto AES128 auth SHA1 dh 1024
                esp crypto AES128 auth SHA1 dh 1024
                peer 10.0.0.6
                no outbound
                local-id key Initiator01_Lynx-210
                remote-id key Responder_RFI-10
                local-subnet 10.10.1.2/32
                remote-subnet 10.10.1.1/32
                secret westermo
                dpd-action restart
                dpd-delay 30
                dpd-timeout 120
                sa-lifetime 28800
                ike-lifetime 3600
                end
        ipsec-nat-traversal
        gre 1
                local 10.10.1.2
                remote 10.10.1.1
                end
        end

router
        ospf
                network 192.168.1.0/24 area 0.0.0.0
                network 192.168.250.0/24 area 0.0.0.0
                end
        end

snmp-server
        rocommunity public
        no rwcommunity
        trapcommunity trap
        end
```

Configuration EDW-100

EDW-100 RFI

Westermo Teleindustri AB
Type: EDW-100
Art. no: 3616-0020
Firmware: 4101-1009
Build: Nov 1 2011 10:29:10

Mode
Application Mode: UDP

Advanced Settings
Function Mode: None

Network
Local IP address: 192.168.0.2:9000
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.0.1
Local Port 2: 9001
Remote IP address: 0.0.0.0:9000
Second Remote IP: 0.0.0.0
Remote IP List:
Multicast Address: 226.1.1.1

Serial
Interface: RS-232
Baudrate: 9600 bits/s
Databits: 8 bits
Parity: None
Stopbits: 1 bit
Flowcontrol: None
Telnet Option: Disabled

Packing Algoritm
End of Frame Char: 256
End of Frame Delay: 20
Max n.o Chars in Frame: 1000
Transmit EoFrame Char: Yes

Access Information
Username: edw100
Password: edw100

Modbus
Gateway mode: Server
Server port: 502
Serial mode: RTU
Ascii timeout: 1000
RTU timeout: 50
Poll delay: 50
CRC checking: Yes
Restricted access: No
Tcp request queue: Yes
Response timeout: 500
Connect timeout: 10
Inactivity timeout: 0
Broadcast timeout: 100
Fixed Slave Address: 0
Disable Broadcast: No
Exception Control: Both
Local_slaves: No

Syslog: 255
Syslog_Server: 0.0.0.0

Dipswitches
Override dipswitches: No
S1-6: Off
S1-7: Off
S1-8: Off

EDW-100 Lynx

Westermo Teleindustri AB
Type: EDW-100
Art. no: 3616-0020
Firmware: 4101-1009
Build: Nov 1 2011 10:29:10

Mode
Application Mode: UDP

Advanced Settings
Function Mode: None

Network
Local IP address: 192.168.1.2:9000
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1
Local Port 2: 9001
Remote IP address: 0.0.0.0:9000
Second Remote IP: 0.0.0.0
Remote IP List:
Multicast Address: 226.1.1.1

Serial
Interface: RS-232
Baudrate: 9600 bits/s
Databits: 8 bits
Parity: None
Stopbits: 1 bit
Flowcontrol: None
Telnet Option: Disabled

Packing Algoritm
End of Frame Char: 256
End of Frame Delay: 20
Max n.o Chars in Frame: 1000
Transmit EoFrame Char: Yes

Access Information
Username: edw100
Password: edw100

Modbus
Gateway mode: Server
Server port: 502
Serial mode: RTU
Ascii timeout: 1000
RTU timeout: 50
Poll delay: 50
CRC checking: Yes
Restricted access: No
Tcp request queue: Yes
Response timeout: 500
Connect timeout: 10
Inactivity timeout: 0
Broadcast timeout: 100
Fixed Slave Address: 0
Disable Broadcast: No
Exception Control: Both
Local_slaves: No

Syslog: 255
Syslog_Server: 0.0.0.0

Dipswitches
Override dipswitches: No
S1-6: Off
S1-7: Off
S1-8: Off

Revision history for version 1.0

Revision	Rev by	Revision note	Date
00	ML	First version	140121
01			
02			
03			
04			
05			
06			
07			

HEAD OFFICE

Sweden
Westermo
SE-640 40 Stora Sundby
Tel: +46 (0)16 42 80 00
Fax: +46 (0)16 42 80 01
info@westermo.se
www.westermo.com

Sales Units

Westermo Data Communications

China
sales.cn@westermo.com
www.cn.westermo.com

France
infos@westermo.fr
www.westermo.fr

Germany
info@westermo.de
www.westermo.de

North America
info@westermo.com
www.westermo.com

Singapore
sales@westermo.com.sg
www.westermo.com

Sweden
info.sverige@westermo.se
www.westermo.se

United Kingdom
sales@westermo.co.uk
www.westermo.co.uk

Other Offices

For complete contact information, please visit our website at www.westermo.com/contact or scan the QR code with your mobile phone.