Software 6 Release Notes

Release 6.9.5-RC2

Westermo Network Technologies AB

July 13, 2021

Contents

1 General Information

Company
Westermo Network Technologies AB

Contact Support
www.westermo.com

Release Number
6.9.5-RC2

Software Build Number
68d67a3f5494df51d530de81552e70180f581638

Date of this build
July 13, 2021

2 Release Highlights

2.1 RC0

- UI: Add ‘configure‘ command to CLI
- Network: Add protected feature per interface (interface isolation)
- VPN: Add Wireguard support
- QoS: Add support for L2 matching of traffic
- Firewall: Add L2 filtering on additional frame headers
- Regulatory: Add SINGAPORE country code

2.2 RC1

- WLAN: Bugfix FragAttacks for 802.11n devices (also see RC2 below)
- Network: Add GRE TOS and RX/TX-Keys
- Network: Bugfix DHCP-Client trigger on bridge-member
- RT610: Bugfix TX counter of wave-1 radio
- UI: Add type, enum and range to help texts
- UI: Bugfix interface status of wlan
- UI: Bugfix QoS parameter descriptions

2.3 RC2

- WLAN: Bugfix FragAttacks for 802.11ac devices
  - CVE-2020-24586 - Fragmentation cache not cleared on reconnection
  - CVE-2020-24587 - Reassembling fragments encrypted under different keys

- CVE-2020-24588 - Accepting non-SPP A-MSDU frames, which leads to payload being parsed as an L2 frame under an A-MSDU bit toggling attack
- CVE-2020-26140 - Accepting plaintext data frames in protected networks
- CVE-2020-26141 - Not verifying TKIP MIC of fragmented frames
- CVE-2020-26142 - Processing fragmented frames as full frames
- CVE-2020-26143 - Accepting fragmented plaintext frames in protected networks
- CVE-2020-26144 - Always accepting unencrypted A-MSDU frames that start with RFC1042 header with EAPOL ethertype
- CVE-2020-26145 - Accepting plaintext broadcast fragments as full frames
- CVE-2020-26146 - Reassembling encrypted fragments with non-consecutive packet numbers
- CVE-2020-26147 - Reassembling mixed encrypted/plaintext fragments

3 Limitations

- When the device is reconfigured to Mesh with SAE as encryption, the device has to be rebooted after applying the configuration
- Multi-SSID with DFS channels is not working (802.11n products only)

4 Configuration Parameter Changes

The following configuration items have been added/changed/removed:

- cfgNetEthProtected (added)
- cfgNetWlanProtected (added)
- cfgNetVlanProtected (added)
- cfgNetVlanPriority (added)
- cfgNetOpenvpnProtected (added)

- cfgNetTepProtected (added)
- cfgNetWgName (added)
- cfgNetWgEnabled (added)
- cfgNetWgMtu (added)
- cfgWlanGlblAclRejectLog (added)
- cfgQosDefaultTid (added)
- cfgQosEthertypeToL2Enabled (added)
- cfgQosEthertypeToL2Ethertype (added)
- cfgQosEthertypeToL2Tid (added)
- cfgCellSimUnlockTimeout (added)
- cfgVpnWgName (added)
- cfgVpnWgListenPort (added)
- cfgVpnWgPrivateKey (added)
- cfgVpnWgPublicKey (added)
- cfgVpnWgPEnabled (added)
- cfgVpnWgPInstance (added)
- cfgVpnWgPPeer (added)
- cfgVpnWgPEndpoint (added)
- cfgVpnWgPAllowedIps (added)
- cfgVpnWgPPsk (added)
- cfgVpnWgPPersistentKeepalive (added)
- cfgVpnTepTos (added)
- cfgVpnTepRxKeyId (added)
- cfgVpnTepTxKeyId (added)

- setCfgFileFormat (added)
- swNlmMonState (added)
- cfgFwL2IpFltrProtocol (added)
- cfgFwL2IpFltrSourcePort (added)
- cfgFwL2IpFltrDestinationPort (added)
- cfgFwL2IpFltrSourceMac (added)
- cfgFwL2IpFltrDestinationMac (added)
- cfgFwL2IpFltrEthertype (added)
- cfgFwL2IpFltrVlan (added)
- cfgFwL2IpFltrInputInterface (added)
- cfgFwL2IpFilterMode (added)
- cfgDhcpDmnOvrDomain (changed)
- swDrvCntWlanNumAssocSta (changed)
- cfgFwL2IpFltrIndex (changed)
- cfgWlanHoFilterMode (removed)
- cfgChMgrEnabled (removed)
- cfgChanCleanEnabled (removed)

5 Changed Configuration Parameter Descriptions

5.1 MIB Reference: WESTERMO-SW6-MIB

5.1.1 cfgVpnWgName

Name of the Wireguard Interface

Type	DisplayString
Range	1 - 255
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.5.1.1.2

5.1.2 cfgVpnWgListenPort

Wireguard Listen Port

Specify the port which is used by this wireguard instance.

Set this to a fixed value when expecting inbound connections. The official wireguard port is 51820.

A random port is used when set to 0.

Range	0 - 65535
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.5.1.1.3

5.1.3 cfgVpnWgPrivateKey

Wireguard Private Key

Base 64 encoded private key used by this wireguard instance. The public key in `cfgVpnWgPublicKey` is derived from this private key.

Will automatically generate a new private/public key-pair when set to `generate` or `not_yet_generated`.

May be generated on the CLI with the command `wg genkey`.

Examples:

- generate
- not_yet_generated
- 4CwLw8p8UGdv6baTN1dMxhxVq+m779vl2IjDpSFecW8=

Type	DisplayString
Range	8 - 44
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.5.1.1.4

5.1.4 cfgVpnWgPublicKey

Wireguard Public Key

Base 64 encoded public key provided by this wireguard instance. This key is derived from what is set in `cfgVpnWgPrivateKey`.

When the private key changes or is regenerated, the content of this field is updated during the apply.

Configure this public key on the remote peer(s).

Type	DisplayString
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.5.1.1.5

5.1.5 cfgVpnWgPEnabled

Wireguard Peer Disabled or Enabled

Disable or enabled this peer instance.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.5.2.1.2

5.1.6 cfgVpnWgPInstance

Wireguard Peer Instance

Specify a wireguard instance defined in `cfgVpnWireguardTable`. All peers with a matching instance are set up for the referenced instance.

Range	0 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.5.2.1.3

5.1.7 cfgVpnWgPPeer

Wireguard Peer Public Key

Specifys the remote peer by its public key. This Peer is considered disabled when set to `none`.

Example:

*Su05SN6WIje1PFlHMO8C2GmCzPp1R85ciwYAo6yvIhA=

Type	DisplayString
Range	4 - 44
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.5.2.1.4

5.1.8 cfgVpnWgPEndpoint

Wireguard Peer Endpoint

Specifies the remote end by IP and port.

Set to `0.0.0.0:0`, when the local peer accepts connections, but does not initiate by itself.

Examples:

- 192.168.1.20:51820
- 0.0.0.0:0

Type	DisplayString
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.5.2.1.5

5.1.9 cfgVpnWgPAllowedIps

Wireguard Peer Allowed IPs

The Allowed IPs refers to the addresses inside the tunnel. It has two meanings:

In TX direction it acts as routing table. Frames with a destination matching the Allowed IPs are encrypted. All other frames that are routed to the interface but don't match the Allowed IPs are dropped.

In RX direction it acts as ACL. Only frames where the source matches the Allowed IPs are accepted. Everything else is dropped.

Multiple space and/or comma separated networks in CIDR notation may be specified.

When set to `none`, no frames will be sent nor received.

Examples:

- none
- 0.0.0.0/0
- 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8

Type	DisplayString
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.5.2.1.6

5.1.10 cfgVpnWgPPsk

Wireguard Peer Private Shared Key

Base 64 encoded privately shared key. Provides an additional layer of cryptography with a symmetric key for post-quantum resistance. Has negligible impact on performance. A separate key should be used for every peer.

Set to `none` when not used.

May be generated on the CLI with the command `wg genpsk`.

Examples:

- none
- F6wPakowIilChk4FRcHrAP+/jO5jdsQ7xphXi8UzG6Y=

Type	DisplayString
Range	4 - 44
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.5.2.1.7

5.1.11 cfgVpnWgPPersistentKeepalive

Wireguard Peer Persistent Keepalive

Interval in seconds to send a keepalive message to the peer.

Only set this, when connecting through NAT or a firewall blocking inbound connections. When not set to 0, a sane value is 25.

Range	0 - 65535
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.5.2.1.8

5.1.12 cfgVpnTepTos

Outer TOS Field of the Tunnel

The outer IP header will have it's TOS field set to the value specified here.

To force the outer TOS header to an explicit value, set the field to a value between '00' and 'ff'.

The outer TOS header may inherit its TOS field from the inner IP header. To achieve this set to 'inherit'. Non-IP frames will have the value 00.

Usually, only the upper most 3 bits have a significant impact on prioritisation, thus it is recommended to preferably use the values: 00, 20, 40, 60, 80, a0, c0, e0

Examples:

- inherit
- 00
- a0
- ff

Type	DisplayString
Range	2 - 7
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.6.1.1.6

5.1.13 cfgVpnTepRxKeyId

RX Tunnel Key ID

The key allows to run multiple tunnels between peers in parallel. The RX Key specifies which value is expected in the header of frames during reception.

This is a 32 bit number which may be specified directly (a number between 0 and 4294967295) or as an IP address-like dotted quad: '123.123.0.255'.

The value configured in this field should match the `cfgVpnTepTxKeyId` on the remote side.

Set to -1 to not expect a key.

Examples:

- -1
- 0
- 4000
- 100.0.0.1

Type	DisplayString
Range	1 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.6.1.1.7

5.1.14 cfgVpnTepTxKeyId

TX Tunnel Key ID

The key allows to run multiple tunnels between peers in parallel. The TX Key specifies which value is set in the header of frames during transmission.

This is a 32 bit number which may be specified directly (a number between 0 and 4294967295) or as an IP address-like dotted quad: '123.123.0.255'.

The value configured in this field should match the `cfgVpnTepRxKeyId` on the remote side.

Set to -1 to not set a key.

Examples:

- -1
- 0
- 4000
- 100.0.0.1

Type	DisplayString
Range	1 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.6.1.1.8

5.1.15 cfgCellSimUnlockTimeout

SIM Unlock Timeout

The time in milliseconds how long the unlocking process waits until the SIM card is ready to be unlocked. Increase the timeout if older SIMs cannot be unlocked. A high timeout affects the performance of SIM rotation.

Note: Changes become effective after restarting the device.

Applies to cellular products only.

Range	300 - 30000
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.101.1.1.5

5.1.16 cfgDhcpDmnOvrDomain

Domain Override Entry Domain

Domain to match. Queries for the matched domain are sent to the server specified in `cfgDhcpHstOvrServer`. This entry is considered disabled when set to `none`.

All subdomains of a specified domain are included. Multiple servers may be specified for the same domain. These servers are querried in the order defined in `cfgDhcpDnsmasqDnsResolveOrder`.

When set to `*`, this server is queried for all domains, and the servers specified in `cfgSysNameserverTable` are ignored. Multiple servers may be specified for the same domain. These servers are querried in the order defined in `cfgDhcpDnsmasqDnsResolveOrder`.

Examples:

- none
- example.com
- mydomain.net
- *

To exclude a subdomain from another override, set the corresponding `cfgDhcpDmnOvrServer` to `#`.

Example:

- specify example.com via 192.168.1.20
- specify blocked.example.com via #
- example.com is querried via 192.168.1.20
- subdomain.example.com is querried via 192.168.1.20
- blocked.example.com is querried via `cfgSysNameserverTable`

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.13.4.1.4

5.1.17 cfgNetEthProtected

Eth Port Protection

This feature only applies to bridged interfaces.

The protected port feature allows bridged ports to be designated as protected. Traffic between protected ports is blocked. Protected ports can send traffic to unprotected ports. Unprotected ports can send traffic to any port.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.2.1.1.13

5.1.18 cfgNetOpenvpnProtected

OpenVPN Port Protection

This feature only applies to bridged interfaces.

The protected port feature allows bridged ports to be designated as protected. Traffic between protected ports is blocked. Protected ports can send traffic to unprotected ports. Unprotected ports can send traffic to any port.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.2.12.1.13

5.1.19 cfgNetTepProtected

Tunnel Endpoint Port Protection

This feature only applies to bridged interfaces.

The protected port feature allows bridged ports to be designated as protected. Traffic between protected ports is blocked. Protected ports can send traffic to unprotected ports. Unprotected ports

can send traffic to any port.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.2.15.1.13

5.1.20 cfgNetWgMtu

The MTU of the Wireguard Interface

The default value is -1, which does not change what is set by the system (usually 1420).

Range	-1 - 65504
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.2.16.1.16

5.1.21 cfgNetWgName

Name of the Wireguard Interface

Type	DisplayString
Range	1 - 255
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.1.2.16.1.2

5.1.22 cfgNetWgEnabled

Wireguard Interface Disabled or Enabled

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.2.16.1.3

5.1.23 cfgNetWlanProtected

WLAN Port Protection

This feature only applies to bridged interfaces.

The protected port feature allows bridged ports to be designated as protected. Traffic between protected ports is blocked. Protected ports can send traffic to unprotected ports. Unprotected ports can send traffic to any port.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.2.2.1.13

5.1.24 cfgNetVlanProtected

VLAN Port Protection

This feature only applies to bridged interfaces.

The protected port feature allows bridged ports to be designated as protected. Traffic between protected ports is blocked. Protected ports can send traffic to unprotected ports. Unprotected ports can send traffic to any port.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.2.3.1.13

5.1.25 cfgNetVlanPriority

The VLAN Priority (PCP) of the VLAN Interface

Sets the PCP of the 802.1Q header to the value specified.

When set to -1, will not set anything. However the PCP may be inherited from the priority of a frame received via another interface, e.g. wlan (TID), when L2 prioritisation is enabled (see `cfgQosL3PrioEnabled`).

Range	-1 - 7
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.2.3.1.18

5.1.26 cfgWlanGlblAclRejectLog

ACL reject logging

If enabled, hostapd will log stations rejected based on MAC ACL.

Applies to AP. 802.11n products only.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.9.5

5.1.27 cfgQosDefaultTid

Default TID For Frames That Do Not Match Any Other Rule

The default TID is set to to frames to be transmitted that do not match the mode to which `cfgQosL3PrioEnabled` is set and there is no matching entry in `cfgQosEthertypeToL2Table`. This means when `cfgQosL3PrioEnabled` is set to **disabled(0)**, that the frame is not a VLAN frame. And when `cfgQosL3PrioEnabled` is set to **enabled(1)**, that the frame is not an IP frame.

Applies to AP and STA. 802.11n products only.

Range	0 - 7
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.6.5

5.1.28 cfgQosEthertypeToL2Enabled

Disable Or Enable Ethertype Rule

Applies to AP and STA. 802.11n products only.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.6.6.1.2

5.1.29 cfgQosEthertypeToL2Ethertype

Ethertype To Match

Some popular Ethertypes:

- 0800: IPv4
- 0806: ARP
- 0835: RARP
- 8100: VLAN

- 86DD: IPv6
- 8847: MPLS unicast
- 8848: MPLS multicast
- 8892: Profinet
- 9100: stacked VLAN

Applies to AP and STA. 802.11n products only.

Range	4 - 4
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.6.6.1.3

5.1.30 cfgQosEthertypeToL2Tid

TID To Set For Ethertype

Applies to AP and STA. 802.11n products only.

Range	0 - 7
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.6.6.1.4

5.1.31 setCfgFileFormat

Configuration File Format

This parameter specifies which format shall be used to export the current configuration.

- **snmp(0)** A flat list of the configuration parameters in an SNMP-based format.
- **cli(1)** A hierarchical structure of the configuration parameters in the way they are used in the CLI.

Note: Because the configuration format is automatically recognised whilst importing configurations, this parameter has no influence in this case.

Applies to AP and STA.

Enumeration	snmp (0), cli (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.1.4

5.1.32 swDrvCntWlanNumAssocSta

Number of associated STA.

Applies to AP. 802.11n products only.

Type	Integer32
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.5.9.1.7

5.1.33 swNlmMonState

Status Of Monitor

This value is cached and updates at most once a second.

Enumeration	down (0), up (1), disabled (2)
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.52.1.1.2

5.2 MIB Reference: WESTERMO-SW6-FIREWALL-MIB

5.2.1 cfgFwL2IpFltrIndex

Entry Index of Table

Range	0 - 255
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.2.1.1.3.3.1.1

5.2.2 cfgFwL2IpFltrSourcePort

The Source Port On Which The Rule Matches

Set to `-1`, to not use the source port to match.

When `cfgFwL2IpFltrEthertype` is set to `0800` and `cfgFwL2IpFltrProtocol` is `6` (TCP) or `17` (UDP), this field ‘may be used to match a specific source port.

Range	-1 - 65535
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.3.3.1.10

5.2.3 cfgFwL2IpFltrDestinationPort

The Destination Port On Which The Rule Matches

Set to `-1`, to not use the destination port to match.

When `cfgFwL2IpFltrEthertype` is set to `0800` and `cfgFwL2IpFltrProtocol` is `6` (TCP) or `17` (UDP), this field 'may be used to match a specific source port.

Range	-1 - 65535
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.3.3.1.11

5.2.4 cfgFwL2IpFltrSourceMac

The Source MAC Addresses On Which The Rule Matches

This is a MAC address and a mask in the form of `xx:xx:xx:xx:xx:xx/yy:yy:yy:yy:yy:yy`.

Examples:

- `00:00:00:00:00:00/00:00:00:00:00:00` match any source
- `00:14:5a:02:04:4c/ff:ff:ff:ff:ff:ff` exact match of the source address 00:14:5a:02:04:4c
- `00:14:5a:00:00:00/ff:ff:ff:00:00:00` match any source addresses with the vendor OUI `00:14:5a`

Type	DisplayString
Range	35 - 35
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.3.3.1.12

5.2.5 cfgFwL2IpFltrDestinationMac

The Destination MAC Addresses On Which The Rule Matches

This is a MAC address and a mask in the form of `xx:xx:xx:xx:xx:xx/yy:yy:yy:yy:yy:yy`.

Examples:

- `00:00:00:00:00:00/00:00:00:00:00:00` match any destination
- `01:00:00:00:00:00/01:00:00:00:00:00` match all frames with a multicast destination (including broadcast)
- `00:14:5a:02:04:4c/ff:ff:ff:ff:ff:ff` exact match of the destination address 00:14:5a:02:04:4c
- `00:14:5a:00:00:00/ff:ff:ff:00:00:00` match any destination addresses with the vendor OUI `00:14:5a`

Type	DisplayString
Range	35 - 35
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.3.3.1.13

5.2.6 cfgFwL2IpFltrEthertype

The Ethertype On Which The Rule Matches

This is an ethertype in the form of `XXXX` where each X is a hexadecimal character [0-9A-Fa-f].

Default is `0800`, which represents IPv4.

Set to `0000`, to match any ethertype.

Examples:

- 0000: any
- 0800: IPv4
- 0806: ARP
- 8035: RARP
- 86DD: IPv6
- 8847: MPLS unicast
- 8848: MPLS multicast
- 8892: Profinet

For a full list of IANA assigned ethertypes see https://www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.xhtml

Type	DisplayString
Range	4 - 4
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.3.3.1.14

5.2.7 cfgFwL2IpFltrVlan

The VLAN On Which The Rule Matches

Set to `-1`, to not use the VLAN to match.

Match on the VLAN number in the 802.1Q header when it is present.

NOTE: Frames that ingress on an access ports are not considered part of the assigned vlan yet.

Range	-1 - 4095
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.3.3.1.15

5.2.8 cfgFwL2IpFltrInputInterface

The Ingress Interface On Which The Rule Matches

The name of the interface on which a frame ingresses.

Set to `any`, to match any interface.

Examples:

- **any**
- **wlan0**
- **eth0**

Type	DisplayString
Range	1 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.3.3.1.16

5.2.9 cfgFwL2IpFltrProtocol

IP Protocol On Which The Rule Matches

Set to `-1`, to not use the protocol to match.

When `cfgFwL2IpFltrEthertype` is set to `0800`, this field may be used to match a specific IP protocol.

Examples:

- **-1**: any protocol
- **1**: ICMP
- **2**: IGMP
- **6**: TCP
- **17**: UDP
- **50**: ESP (IPsec)
- **51**: AH (IPsec)
- **112**: VRRP / CARP

For a full list of available protocols see https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers

When `cfgFwL2IpFltrEthertype` is set to `0806` or `8035`, this field may be used to match the OP code of an ARP frame.

Examples:

- **-1**: any OP code
- **1**: request
- **2**: response
- **3**: request reverse
- **4**: response reverse

Range	-1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.3.3.1.9

5.2.10 cfgFwL2IpFilterMode

Filter Mode

The filtering bridge provides two modes of operation:

- **ip(0)**: A simplified mode to filter IP traffic. All non-IP traffic is allowed.
- **full(1)**: The full mode allows to filter on any kind of header information present.

Enumeration	ip (0), full (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.3.4