



INSTALLATION AND OPERATION MANUAL

CNGE3FE8MS[POE][HO]

Environmentally Hardened Managed Ethernet Switch
3 SFP + 8 Electrical Ports with Optional 30 or 60 Watt PoE

**This guide serves the following
ComNet Model Numbers:**

CNGE3FE8MS
CNGE3FE8MSPOE
CNGE3FE8MSPOEHO

The ComNet CNGE3FE8MS[POE][HO] has three 100/1000Base-FX SFP ports and eight 10/100Base-TX ports. Two of the SFP ports support 2.5 Gbps SFPs for high speed communication in bandwidth intensive applications. All SFP ports utilize ComNet SFP modules for fiber and connector type and distance. The IEEE802.3-compliant unit offers multiple Ethernet redundancy protocols (MSTP/RSTP/STP/ERPS (G.8032)) which protect your applications from network interruptions or temporary malfunctions by redirecting transmission within the network. The switch provides advanced IP-based management that can limit the maximum bandwidth for each connected IP device, allowing the user to adjust usage. Two models are available which supply Power over Ethernet (PoE). The CNGE3FE8MSPOE model provides eight electrical ports supporting up to thirty watts of power. On the CNGE3FE8MSPOEHO model, four of the eight PoE ports can support up to sixty watts of PoE power. All PoE ports are IEEE802.3at compliant.

Contents

| | |
|--|-----------|
| Regulatory Compliance Statement | 6 |
| Warranty | 6 |
| Disclaimer | 6 |
| Safety Information | 7 |
| Hardware Installation | 8 |
| Installing the Switch on DIN-Rail | 8 |
| Wall Mounting Installation | 10 |
| Hardware Overview | 11 |
| Power Supply | 12 |
| Front Panel LEDs | 12 |
| POEHO 60 W PoE Model | 12 |
| WEB Management | 13 |
| Login | 13 |
| Configuration | 17 |
| Green Ethernet | 24 |
| Thermal Protection | 26 |
| DHCP | 29 |
| DHCP Pool Configuration | 32 |
| Security | 37 |
| Network | 55 |
| Screen | 58 |
| Aggregation | 85 |
| Loop Protection | 87 |
| Spanning Tree | 88 |
| IPMC Profile | 95 |
| MVR | 98 |
| IPMC | 100 |
| LLDP | 108 |
| PoE | 110 |
| EPS | 112 |
| Ethernet Protection Switch Configuration | 113 |

| | |
|---|------------|
| Ethernet Ring Protection Switch Configuration | 130 |
| MAC Table | 133 |
| VLAN Translation | 134 |
| VLANs | 136 |
| Private VLANs | 139 |
| VCL | 141 |
| Protocol-based VLAN | 142 |
| Voice VLAN | 146 |
| Mirroring & Remote Mirroring Configuration | 167 |
| UPnP | 170 |
| GVRP | 171 |
| Monitor Menu | 173 |
| System | 173 |
| CUP Load | 174 |
| Input Power Status | 175 |
| System IP Status | 176 |
| System Log | 178 |
| Port State | 181 |
| Green Ethernet | 182 |
| Thermal Protection | 183 |
| Ports | 183 |
| QoS Statistics | 184 |
| DHCP | 188 |
| Security | 194 |
| AAA | 202 |
| Aggregation Status | 208 |
| LACP | 209 |
| Loop Protection | 211 |
| MVR | 216 |
| IPMC | 219 |
| LLDP | 225 |
| PoE | 230 |
| MAC Table | 231 |
| VLANs | 232 |

| | |
|---|------------|
| Diagnostics Menu | 235 |
| Ping | 235 |
| Ping6 | 236 |
| PHYtest | 237 |
| Maintenance Menu | 238 |
| Restart Device | 238 |
| Factory Defaults | 238 |
| Software | 239 |
| Configuration | 241 |
| Using Switch CLI | 244 |
| About CLI Management | 244 |
| CLI Management by RS-232 Serial Console | 244 |
| CLI Management by Telnet | 247 |
| Commander Groups | 248 |
| Quick Start | 249 |
| Log In and Reset Configuration to Factory Default | 249 |
| Set Device Hostname and Admin User Password | 250 |
| Set VLAN 1 IP Address | 250 |
| Display and Save Configuration to Flash | 252 |
| ICLI Basics | 254 |
| Command Structure and Syntax | 255 |
| Syntax | 255 |
| Ethernet Interface Naming | 258 |
| Using the Keyboard | 260 |
| Basic Line Editing | 260 |
| Command History | 261 |
| Context-Sensitive Help | 263 |
| Using Context-Sensitive Help | 263 |
| Long Lines and Pagination | 265 |
| Other Special Keys | 266 |
| Filtering Output | 266 |
| Understanding Modes and Sub-Modes | 267 |
| Using 'do' While in a Sub-Mode | 270 |
| Changing Between ICLI Modes | 271 |

| | |
|--|------------|
| Understanding Privilege Levels | 272 |
| Configuring Privilege Level Passwords | 273 |
| Understanding Terminal Parameters | 274 |
| Changing Terminal Parameters | 275 |
| Using Banners | 277 |
| Configuring Banners | 277 |
| Configuring the System | 279 |
| Configuration Example | 279 |
| Resetting or Removing Configuration with "no" | 281 |
| Using "no" Forms | 281 |
| Managing Users | 282 |
| Adding, Modifying, and Deletion Users | 282 |
| Using Show Commands | 283 |
| Listing All Show Commands | 284 |
| Show running-config | 287 |
| Default vs. Non-default vs. All Defaults | 287 |
| Show running-config [all-defaults] | 289 |
| Show running-config feature feature_name [all-defaults] | 289 |
| Show running-config interface list [all-defaults] | 290 |
| Working with Configuration Files | 291 |
| Reverting to Default Configuration | 292 |
| Working with Configuration Files | 293 |
| Using Reload Commands | 295 |
| Working with Software Images | 296 |
| Appendix A | 297 |
| Ethernet Ring Protection Switching Example Configuration | 297 |
| Configuring ERPS from the Web GUI | 298 |
| Ethernet Ring Protection Switching Configuration | 305 |
| Configuring ERPS from the ICLI | 310 |

Regulatory Compliance Statement

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

Warranty

ComNet warrants that all ComNet products are free from defects in material and workmanship for a specified warranty period from the invoice date for the life of the installation. ComNet will repair or replace products found by ComNet to be defective within this warranty period, with shipment expenses apportioned by ComNet and the distributor. This warranty does not cover product modifications or repairs done by persons other than ComNet-approved personnel, and this warranty does not apply to ComNet products that are misused, abused, improperly installed, or damaged by accidents.

Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

Disclaimer

Information in this publication is intended to be accurate. ComNet shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ComNet reserves the right to revise the contents of this publication without notice.

Safety Information

- » Only ComNet service personnel can service the equipment. Please contact ComNet Technical Support.
- » The equipment should be installed in locations with controlled access, or other means of security, and controlled by persons of authority. When operating at temperatures above 51° C, the equipment surfaces will be hot to the touch. Installation in restricted access location is required for this case.
- » For POE models requiring a power supply not labeled LPS, the unit should be installed in a restricted access location using a 60950-1, 2nd Edition + Am. 1 + Am. 2 Certified power supply rated for the ambient temperature in which it is installed. Total derated power rating should be greater than the sum of the attached loads plus 15 W for the switch.
- » Use CDRH compliant SFP modules when using fiber connectivity with this device.
- » When used in Australia or New Zealand, the product is certified for intra building applications only, and should not be directly connected to network cables with outside plant routing.

Hardware Installation

Installing the Switch on DIN-Rail

Each switch has a Din-Rail kit on the rear panel. The DIN-Rail kit affixes the switch to the DIN-Rail.



It is easy to install the switch on the Din-Rail:

Mount Series on DIN-Rail

Step 1: Tilt the switch and mount the metal spring to DIN-Rail.



Step 2: Push the switch toward the DIN-Rail until you hear the spring snap into place



Wall Mounting Installation

Each switch has another installation method for users to fix the switch. A wall mount panel can be found in the package. The following steps show how to mount the switch on the wall:

Mounting the switch on a wall

Note: For drywall applications where no studs are available, use drywall anchors rated for 50 lbs or more.

In order to prevent switches from being damaged, use appropriate hardware (not supplied) for securing the unit to the wall.

#6 screws with at least 1/2-inch penetration into wood surface recommended.

Step 1: Remove DIN-Rail kit if it is installed.

Step 2: Remove the two screws at the top of the unit's back panel. Remove only one pair of back panel screws at time (these hold the back panel in place on the unit).

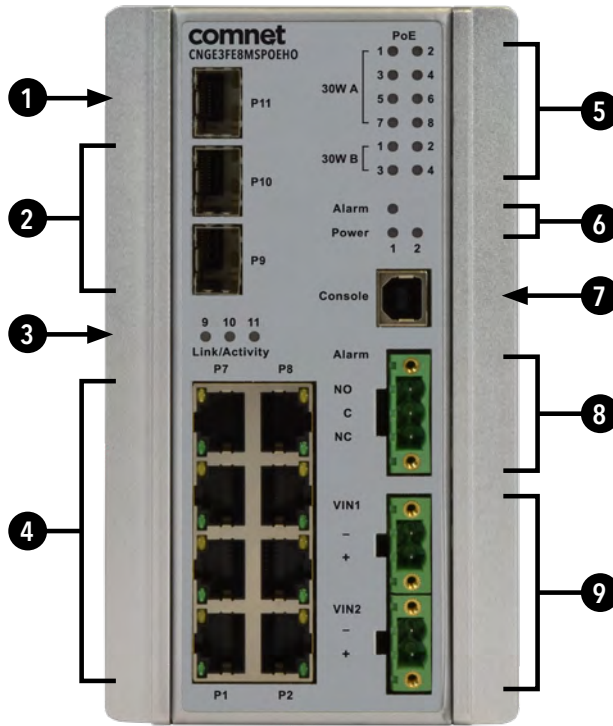
Step 3: Use the same two screws plus one of the included screws to attach the wall mount panel to the top set of screw holes as shown in the diagram below.



Step 4: Repeat Steps 2 and 3 to mount the second wall mount panel on the bottom of the unit's back panel.

ATTENTION: Do not remove the top and bottom panel screws at the same time, or the back panel will detach from the unit. Install the wall mount panels one at a time. When operating at temperatures above 51°C, the equipment surfaces will be hot to the touch. Installation in restricted access location is required for this case.

Hardware Overview



CNGE3FE8MS[POE][HO]

| Call-out | Description |
|----------|---|
| 1 | 1 × 100/1000Base-FX SFP Port |
| 2 | 2 × 100/1000/2500Base-FX SFP Ports |
| 3 | Link/Activity LED Indicators for SFP Ports |
| 4 | 8 × 10/100Base-TX RJ45 Ports |
| 5 | PoE LED Indicators (PoE models only) |
| 6 | Alarm and Power LED Indicators |
| 7 | USB Console Port |
| 8 | Fault Relay 3-Pin Terminal Block Connector |
| 9 | Redundant Power 2-Pin Terminal Block Connectors |

Power Supply

For CNGE3FE8MS Models, Power Supply must be 12 to 57 VDC @ 10 W max.

For CNGE3FE8MSPOE Model, Power Supply must be 44 to 57 VDC @ 250W max.

For CNGE3FE8MSPOEHO Model, Power Supply must be 44 to 57 VDC @ 370W max.

IMPORTANT SAFEGUARDS:

A) Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (T_{ma}) specified by the manufacturer.

B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Front Panel LEDs

| LED | Color | Status | Description |
|----------------------------------|-------|----------|--|
| Alarm | Red | On | Alarm Fault Status has been triggered |
| Power 1 Alarm | Green | On | Power Input on VIN1 terminal block Input |
| | Red | On | Power lost to VIN1 terminal block |
| Power 2 Alarm | Green | On | Power Input on VIN1 terminal block Input |
| | Red | On | Power lost to VIN2 terminal block |
| PoE (Power over Ethernet) | | | |
| 30W A | Green | On | MODE A PoE is being supplied on indicated RJ-45 port |
| 30W B | Green | On | MODE B PoE is being supplied on indicated RJ-45 port |
| 100 Mbps Ethernet ports | | | |
| Link | Green | On | Port in Full Duplex mode |
| Activity | Amber | Blinking | Data transmitted |
| Gigabit SFP ports | | | |
| Link/Activity | Amber | Blinking | Data transmitted |

POEHO 60 W PoE Model

Port 1 to 4 support both mode A and mode B PoE which is 60 W in total. When a greater than 30 W PoE supported device is connected to ports 1 to 4, both 30 W A and B Indicator LEDs will be turned on to indicate the high-power application device is connected.

WEB Management

Login

Open a web browser and navigate to the switch using http:// and the IP address of the switch.

The default IP address is 192.168.10.1

This is the main login page. Default user name is "admin" with maximum length 32 Default password is "admin" with maximum length 32.

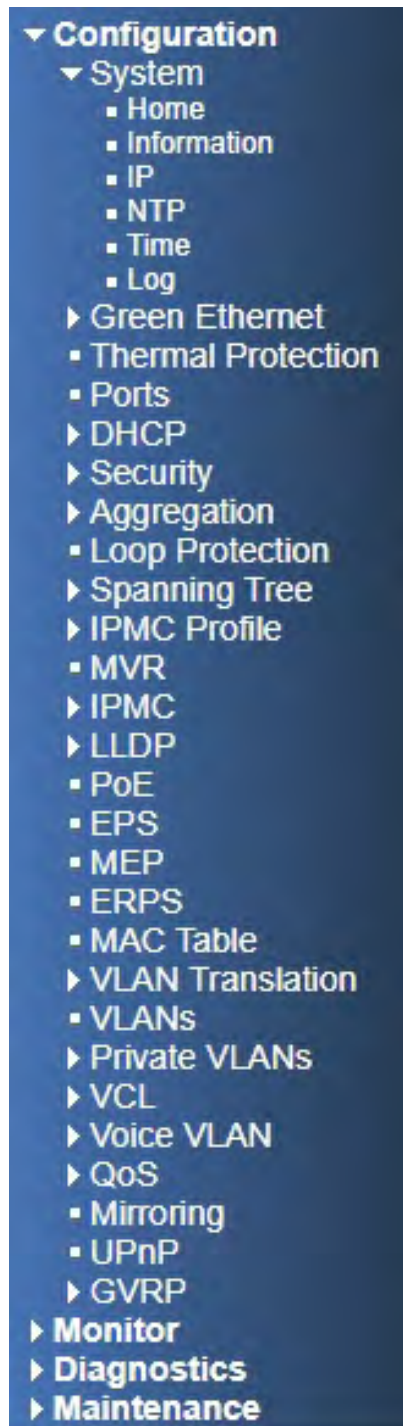


Warning - Any changes made to the settings will apply only to the current running configuration of the switch and will be lost in the event of a power cycle.

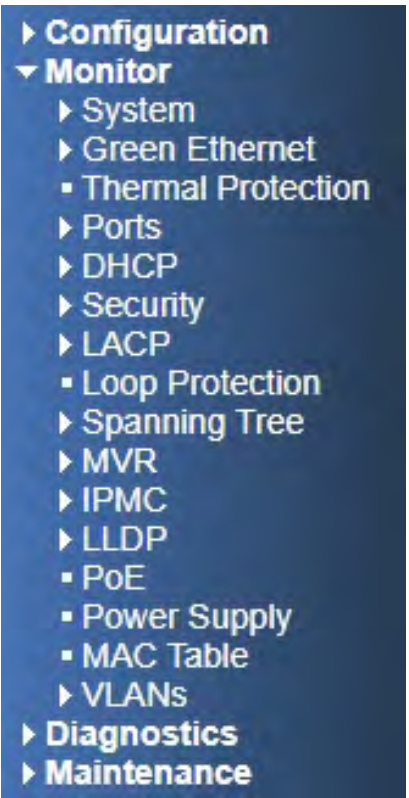
To save any changes made to persistent memory please go to "Maintenance ; Configuration ; Save startup-config" to write the changes to the switches startup configuration.

Menu Trees

The following tree views show the available menus within the switch web GUI. It offers the user quick access to all the configuration settings within the switch.



Configuration Menu



Monitor Menu



Diagnostics Menu



Maintenance Menu

Configuration

System Information

The switch system information is provided here.

System Information Configuration

| | |
|-----------------|--|
| System Contact | |
| System Name | |
| System Location | |

| Object | Description |
|-----------------|--|
| System Contact | The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126. |
| System Name | An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255. |
| System Location | The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126. |
| Apply | Click to apply changes without saving. * |
| Reset | Click to revert to previous values. |

Save to startup-config is under Maintenance Menu tree.

System IP

Configure IP basic settings, control IP interfaces and IP routes. The maximum number of interfaces supported is 8 and the maximum number of routes is 32.

IP Configuration

| | |
|--------------|--------------------------|
| Mode | Host ▾ |
| DNS Server 0 | No DNS server ▾ |
| DNS Server 1 | No DNS server ▾ |
| DNS Server 2 | No DNS server ▾ |
| DNS Server 3 | No DNS server ▾ |
| DNS Proxy | <input type="checkbox"/> |

IP Interfaces

| Delete | VLAN | DHCPv4 | | | IPv4 | | DHCPv6 | | | IPv6 | |
|--------------------------|------|--------------------------|----------|---------------|--------------|-------------|--------------------------|--------------------------|---------------|---------|-------------|
| | | Enable | Fallback | Current Lease | Address | Mask Length | Enable | Rapid Commit | Current Lease | Address | Mask Length |
| <input type="checkbox"/> | 1 | <input type="checkbox"/> | 0 | | 192.168.10.1 | 24 | <input type="checkbox"/> | <input type="checkbox"/> | | | |

Add Interface

IP Routes

| Delete | Network | Mask Length | Gateway | Next Hop VLAN |
|--------------------------|---------|-------------|----------------|---------------|
| <input type="checkbox"/> | 0.0.0.0 | 0 | 192.168.10.254 | 0 |

Add Route

Apply Reset

| Object | Description |
|----------------------------|--|
| IP Configuration | |
| Mode | Configure whether the IP stack should act as a Host or a Router. In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces. |
| DNS Server | This setting controls the DNS name resolution done by the switch. The following modes are supported: <ul style="list-style-type: none"> • From any DHCP interfaces The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used. • No DNS server No DNS server will be used. • Configured Explicitly provide the IP address of the DNS Server in dotted decimal notation. • From this DHCP interface Specify from which DHCP-enabled interface a provided DNS server should be preferred. |
| DNS Proxy | When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network. |
| IP Interfaces | |
| Delete | Select this option to delete an existing IP interface. |
| VLAN | The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface. |
| IPv4 DHCP Enabled | Enable the DHCP client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCP protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup. |
| IPv4 DHCP Fallback Timeout | The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds. |
| IPv4 DHCP Current Lease | For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server. |

| Object | Description |
|-------------------------------|--|
| IPv4 Address | The IPv4 address of the interface in dotted decimal notation. If DHCP is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired. |
| IPv4 Mask | The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for an IPv4 address.If DHCP is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired. |
| DHCPv6 Enable | Enable the DHCPv6 client by checking this box. If this option is enabled, the system will configure the IPv6 address of the interface using the DHCPv6 protocol. |
| DHCPv6 Rapid Commit | Enable the DHCPv6 Rapid-Commit option by checking this box. If this option is enabled, the DHCPv6 client terminates the waiting process as soon as a Reply message with a Rapid Commit option is received. This option is only manageable when DHCPv6 client is enabled. |
| DHCPv6 Current Lease | For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server. |
| IPv6 Address | The IPv6 address of the interface. An IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, ::192.1.2.34. The field may be left blank if IPv6 operation on the interface is not desired. |
| IPv6 Mask | The IPv6 network mask, in number of bits (prefix length). Valid values are between 1 and 128 bits for an IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired. |
| Default Gateway | |
| Address | The IP address of the gateway valid format is dotted decimal notation. |
| IP Routes | |
| Delete | Select this option to delete an existing IP route. |
| Network | The destination IP network or host address of this route. Valid format is notation or a valid IPv6 notation. A default route can use the value 0.0.0.0or IPv6 :: notation. |
| Mask Length | The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything). |
| Gateway | The IP address of the IP gateway. Valid format is notation or a valid IPv6 notation. Gateway and Network must be of the same type. |
| Next Hop VLAN (Only for IPv6) | The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway. If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway. |
| Add Interface | Click to add a new IP Interface. A maximum of 8 interfaces is supported. |
| Add Route | Click to add a new IP route. A maximum of 32 routes is supported. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

System NTP

NTP Configuration

| | |
|----------|------------|
| Mode | Disabled ▼ |
| Server 1 | |
| Server 2 | |
| Server 3 | |
| Server 4 | |
| Server 5 | |

Apply Reset

Configure NTP on this page.

| Object | Description |
|----------|--|
| Mode | Indicates the NTP mode operation. Possible modes are: Enabled: Enable NTP client mode operation. Disabled: Disable NTP client mode operation. |
| Server # | Provide the IPv4 or IPv6 address of a NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

System Time

Time Zone Configuration

| Time Zone Configuration | |
|-------------------------|-----------------------|
| Time Zone | None ▼ |
| Acronym | (0 - 16 characters) |

Daylight Saving Time Configuration

| Daylight Saving Time Mode | |
|---------------------------|------------|
| Daylight Saving Time | Disabled ▼ |

| Start Time settings | |
|---------------------|----------------------|
| Month | Jan ▼ |
| Date | 1 ▼ |
| Year | 2014 ▼ |
| Hours | 0 ▼ |
| Minutes | 0 ▼ |
| End Time settings | |
| Month | Jan ▼ |
| Date | 1 ▼ |
| Year | 2097 ▼ |
| Hours | 0 ▼ |
| Minutes | 0 ▼ |
| Offset settings | |
| Offset | 1 (1 - 1440) Minutes |

This page allows you to configure the Time Zone.

| Object | Description |
|--------|-------------|
|--------|-------------|

Time Zone Configuration

Time Zone Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down

Acronym User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range : Up to 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default : Disabled)

Recurring Configurations

Start time settings

Week Select the starting week number.

Day Select the starting day.

Month Select the starting month.

Hours Select the starting hour.

Minutes Select the starting minute

Object Description**End time settings**

Week Select the ending week number.

Day Select the ending day.

Month Select the ending month.

Hours Select the ending hour.

Minutes Select the ending minute

Offset settings

Offset Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

Non Recurring Configurations**Start time settings**

Month Select the starting month.

Date Select the starting date.

Year Select the starting year.

Hours Select the starting hour.

Minutes Select the starting minute

End time settings

Month Select the ending month.

Date Select the ending date.

Year Select the ending year.

Hours Select the ending hour.

Minutes Select the ending minute

Offset settings

Offset Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

System Log

System Log Configuration

| | |
|----------------|-----------------|
| Server Mode | Disabled ▼ |
| Server Address | |
| Syslog Level | Informational ▼ |

Configure System Log on this page.

| Object | Description |
|----------------|---|
| Server Mode | Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are: Enabled: Enable server mode operation. Disabled: Disable server mode operation. |
| Server Address | Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a host name. |
| Syslog Level | Indicates what kind of messages will sent to the syslog server. Possible modes are: Error: Send the specific messages which severity code is less or equal than Error(3). Warning: Send the specific messages which severity code is less or equal than Warning(4). Notice: Send the specific messages which severity code is less or equal than Notice(5). Informational: Send the specific messages which severity code is less or equal than Informational(6). |
| Apply | Click to apply changes. |
| Revert | Click to revert to previous values. |

Green Ethernet

LED

LED Power Reduction Configuration

LED Intensity Timers

| Delete | Start Time | End Time | Intensity |
|--------------------------|------------|----------|-----------|
| <input type="checkbox"/> | 00:00 ▾ | 00:00 ▾ | 80 ▾ % |

Add Time

Maintenance

| On time at link change | On at errors |
|------------------------|--------------------------|
| 10 Sec. | <input type="checkbox"/> |

Apply Reset

| Object | Description |
|----------------|---|
| LEDs Intensity | The LEDs power consumption can be reduced by lowering the LEDs intensity. LEDs intensity could for example be lowered during night time, or they could be turn completely off. It is possible to configure 24 different hours of the day, at where the LEDs intensity should be set. |
| Start Time | The time at which the LEDs intensity shall be set to the corresponding intensity. |
| End Time | The time at which the LEDs intensity shall be set to a new intensity. If no intensity is specified for the next hour, the intensity is set to default intensity. |
| Intensity | The LEDs intensity (100% = Full power, 0% = LED off). |
| Maintenance | <p>On time at link change</p> <p>When a network administrator does maintenance of the switch (e.g. adding or moving users) he might want to have full LED intensity during the maintenance period . Therefore it is possible to specify that the LEDs shall use full intensity a specific period of time. Maintenance Time is the number of seconds that the LEDs will have full intensity after either a port has changed link state, or the LED pushbutton has been pushed. Valid range is from 0 to 65535 seconds.</p> <p>On at errors</p> <p>In the case where maximum power saving is enabled by turning the LEDs completely off, it might be convenient to indicate to the network administrator that an error has been recorded in the system log. By checking the "On at errors" the LEDs will be turned on at 100% in the case that errors are logged in the system log.</p> |

Port Power Savings

Port Power Savings Configuration

Optimize EEE for Latency ▾

Port Configuration

| Port | ActiPHY | PerfectReach | EEE | EEE Urgent Queues | | | | | | | | |
|------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | |
| * | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

This page allows the user to configure the port power saving features.

| Object | Description |
|---|--|
| Port Power Savings Configuration | |
| Optimize EEE for | The switch can be set to optimize EEE for either best power saving or least traffic latency. |
| Port Configuration | |
| Port | The switch port number of the logical port. |
| ActiPHY | Link down power savings enabled. ActiPHY works by lowering the power for a port when there is no link. The port is power up for short moment in order to determine if cable is inserted. |
| PerfectReach | Cable length power savings enabled. PerfectReach works by determining the cable length and lowering the power for ports with short cables. |
| EEE | Controls whether EEE is enabled for this switch port. For maximizing power savings, the circuit isn't started at once transmit data is ready for a port, but is instead queued until a burst of data is ready to be transmitted. This will give some traffic latency. If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time. |
| EEE Urgent Queues | Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted. |

Thermal Protection

Thermal Protection Configuration

Temperature settings for groups

| Group | Temperature | |
|-------|-------------|----|
| 0 | 255 | °C |
| 1 | 255 | °C |
| 2 | 255 | °C |
| 3 | 255 | °C |

Port groups

| Port | Group |
|------|------------|
| * | <> ▼ |
| 1 | Disabled ▼ |
| 2 | Disabled ▼ |
| 3 | Disabled ▼ |
| 4 | Disabled ▼ |
| 5 | Disabled ▼ |
| 6 | Disabled ▼ |
| 7 | Disabled ▼ |
| 8 | Disabled ▼ |
| 9 | Disabled ▼ |
| 10 | Disabled ▼ |
| 11 | Disabled ▼ |

Apply Reset

This page allows the user to inspect and configure the current setting for controlling thermal protection. Thermal protection is used to protect the chip from getting overheated.

When the temperature exceeds the configured thermal protection temperature, ports will be turned off in order to decrease the power consumption. It is possible to arrange the ports with different groups. Each group can be given a temperature at which the corresponding ports shall be turned off.

| Object | Description |
|-------------|---|
| Temperature | The temperature at which the ports with the corresponding group will be turned off. Temperatures between 0 and 255 C are supported. |
| Group | The group the port belongs to. 4 groups are supported. |

Ports

This page displays current port configurations. Ports can also be configured here.

Port Configuration

| Port | Description | Link | Speed | | Adv Duplex | | | Adv speed | | | Flow Control | | | Maximum Frame Size | Excessive Collision Mode | Frame Length Check | |
|------|-------------|-------|---------|------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | | | Current | Configured | Fdx | Hdx | 10M | 100M | 1G | Enable | Curr Rx | Curr Tx | Enable | | | | Curr Rx |
| 1 | | 1Gfdx | Auto | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2 | | Down | Auto | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3 | | Down | Auto | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 4 | | Down | Auto | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 5 | | Down | Auto | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 6 | | Down | Auto | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 7 | | Down | Auto | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 8 | | Down | Auto | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 9 | | Down | Auto | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 10 | | Down | Auto | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 11 | | Down | Auto | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Apply Reset

| Object | Description |
|--------------------------|--|
| Port | This is the logical port number for this row. |
| Description | The description of the port. It is an ASCII string no longer than 256 characters. |
| Link | The current link state is displayed graphically. Green indicates the link is up and red that it is down. |
| Current Link Speed | Provides the current link speed of the port. |
| Configured Link Speed | <p>Selects any available link speed for the given switch port. Only speeds supported by the specific ports are shown. Possible speeds are:</p> <ul style="list-style-type: none"> Disabled - Disables the switch port operation. Auto - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner. 10Mbps HDX - Forces the cu port in 10Mbps half duplex mode. 10Mbps FDX - Forces the cu port in 10Mbps full duplex mode. 100Mbps HDX - Forces the cu port in 100Mbps half duplex mode. 100Mbps FDX - Forces the cu port in 100Mbps full duplex mode. 1Gbps FDX - Forces the port in 1Gbps full duplex. 2.5Gbps FDX - Forces the port in 2.5Gbps full duplex mode. |
| Advertise Duplex | When duplex is set as auto i.e auto negotiation, the port will only advertise the specified duplex as either Fdx or Hdx to the link partner. By default port will advertise all the supported duplexes if the Duplex is Auto. |
| Advertise Speed | When Speed is set as auto i.e auto negotiation, the port will only advertise the specified speeds (10M 100M 1G) to the link partner. By default port will advertise all the supported speeds if speed is set as Auto. |
| Flow Control | <p>When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner.</p> <p>When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation.</p> <p>Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.</p> |
| Maximum Frame Size | Enter the maximum frame size allowed for the switch port, including FCS. |
| Excessive Collision Mode | <p>Configure port transmit collision behavior.</p> <ul style="list-style-type: none"> Discard: Discard frame after 16 collisions (default). Restart: Restart back off algorithm after 16 collisions. |

| Object | Description |
|--------------------|--|
| Frame Check Length | <p>Configures whether frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If "frame length check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actually payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch.</p> <p>Note: No drop counters count frames dropped due to frame length mismatch.</p> |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

DHCP

DHCP Server

Mode

This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN.

DHCP Server Mode Configuration

Global Mode

Mode

VLAN Mode

| Object | Description |
|--------------------|---|
| Global Mode | |
| Mode | Configure the operation mode per system. Possible modes are: Enabled: Enable DHCP server per system. Disabled: Disable DHCP server per system. |
| VLAN Mode | |
| VLAN Range | Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. BUT, if the VLAN range contains only 1 VLAN ID, then you can just input it into either one of the first and second VLAN ID or both. On the other hand, if you want to disable existed VLAN range, then you can follow the steps. 1. press "Add VLAN Range" to add a new VLAN range. 2. input the VLAN range that you want to disable. 3. choose Mode to be Disabled. 4. press "Save" to apply the change. Then, you will see the disabled VLAN range is removed from the DHCP Server mode configuration page. |
| Mode | Indicate the operation mode per VLAN. Possible modes are: Enabled: Enable DHCP server per VLAN. Disabled: Disable DHCP server pre VLAN. |
| Add VLAN Range | Click to apply to add a new VLAN range. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

Excluded IP

This page configures excluded IP addresses. DHCP server will not allocate these excluded IP addresses to DHCP client.

DHCP Server Excluded IP Configuration

Excluded IP Address

Delete **IP Range**

Add IP Range

Apply Reset

| | |
|--------------|---|
| IP Range | Define the IP range to be excluded IP addresses. The first excluded IP must be smaller than or equal to the second excluded IP. BUT, if the IP range contains only 1 excluded IP, then you can just input it to either one of the first and second excluded IP or both. |
| Add IP Range | Click to add a new IP range. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

Pool

This page manages DHCP pools. According to the DHCP pool, DHCP server will allocate IP address and deliver configuration parameters to DHCP client.

DHCP Server Pool Configuration

Pool Setting

| Delete | Name | Type | IP | Subnet Mask | Lease Time |
|--------|------|------|----|-------------|------------|
|--------|------|------|----|-------------|------------|

| Object | Description |
|--------------|---|
| Pool Setting | Add or delete pools. Adding a pool and giving a name is to create a new pool with "default" configuration. If you want to configure all settings including type, IP subnet mask and lease time, you can click the pool name to go into the configuration page. |
| Name | Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page. |
| Type | Display which type of the pool is. Network: the pool defines a pool of IP addresses to service more than one DHCP client. Host: the pool services for a specific DHCP client identified by client identifier or hardware address. If "-" is displayed, it means not defined. |
| IP | Display network number of the DHCP address pool. If "-" is displayed, it means not defined. |
| Subnet Mask | Display subnet mask of the DHCP address pool. If "-" is displayed, it means not defined. |
| Lease Time | Display lease time of the pool. |
| Add New Pool | Click to add a new DHCP pool. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

DHCP Pool Configuration

DHCP Pool Configuration Help

DHCP Pool Configuration

This page configures all settings of a DHCP pool.

DHCP Pool Configuration

Pool

Name | DHCP_Pool_A ▼

Setting

| | | |
|-------------------------------|-------------|----------------|
| Pool Name | DHCP_Pool_A | |
| Type | None ▼ | |
| IP | | |
| Subnet Mask | | |
| Lease Time | 1 | days (0-365) |
| | 0 | hours (0-23) |
| | 0 | minutes (0-59) |
| Domain Name | | |
| Broadcast Address | | |
| Default Router | 0.0.0.0 | |
| | 0.0.0.0 | |
| | 0.0.0.0 | |
| | 0.0.0.0 | |
| DNS Server | 0.0.0.0 | |
| | 0.0.0.0 | |
| | 0.0.0.0 | |
| | 0.0.0.0 | |
| NTP Server | 0.0.0.0 | |
| | 0.0.0.0 | |
| | 0.0.0.0 | |
| | 0.0.0.0 | |
| NetBIOS Node Type | None ▼ | |
| NetBIOS Scope | | |
| NetBIOS Name Server | 0.0.0.0 | |
| | 0.0.0.0 | |
| | 0.0.0.0 | |
| | 0.0.0.0 | |
| NIS Domain Name | | |
| NIS Server | 0.0.0.0 | |
| | 0.0.0.0 | |
| | 0.0.0.0 | |
| | 0.0.0.0 | |
| Client Identifier | None ▼ | |
| Hardware Address | | |
| Client Name | | |
| Vendor 1 Class Identifier | | |
| Vendor 1 Specific Information | | |
| Vendor 2 Class Identifier | | |
| Vendor 2 Specific Information | | |
| Vendor 3 Class Identifier | | |
| Vendor 3 Specific Information | | |
| Vendor 4 Class Identifier | | |
| Vendor 4 Specific Information | | |

Apply | Reset

| Object | Description |
|---------------------|---|
| Pool | |
| Name | Select a pool by pool name. |
| Setting | |
| Name | Display the selected pool name. |
| Type | Specify which type of the pool is. Network: the pool defines a pool of IP addresses to service more than one DHCP client. Host: the pool services for a specific DHCP client identified by client identifier or hardware address. |
| IP | Specify network number of the DHCP address pool. |
| Subnet Mask | DHCP option 1. Specify subnet mask of the DHCP address pool. |
| Lease Time | DHCP option 51, 58 and 59. Specify lease time that allows the client to request a lease time for the IP address. If all are 0's, then it means the lease time is infinite. |
| Domain Name | DHCP option 15. Specify domain name that client should use when resolving hostname via DNS. |
| Broadcast Address | DHCP option 28. Specify the broadcast address in use on the client's subnet. |
| Default Router | DHCP option 3. Specify a list of IP addresses for routers on the client's subnet. |
| DNS Server | DHCP option 6. Specify a list of Domain Name System name servers available to the client. |
| NTP Server | DHCP option 42. Specify a list of IP addresses indicating NTP servers available to the client. |
| NetBIOS Node Type | DHCP option 46. Specify NetBIOS node type option to allow Netbios over TCP/IP clients which are configurable to be configured as described in RFC 1001/1002. |
| NetBIOS Scope | DHCP option 47. Specify the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002. |
| NetBIOS Name Server | DHCP option 44. Specify a list of NBNS name servers listed in order of preference. |
| NIS Domain Name | DHCP option 40. Specify the name of the client's NIS domain. |
| NIS Server | DHCP option 41. Specify a list of IP addresses indicating NIS servers available to the client. |
| Client Identifier | DHCP option 61. Specify client's unique identifier to be used when the pool is the type of host. |
| Hardware Address | Specify client's hardware(MAC) address to be used when the pool is the type of host. |
| Client Name | DHCP option 12. Specify the name of client to be used when the pool is the type of host. |

| Object | Description |
|-------------------------------|---|
| Vendor i Class Identifier | DHCP option 60. Specify to be used by DHCP client to optionally identify the vendor type and configuration of a DHCP client. DHCP server will deliver the corresponding option 43 specific information to the client that sends option 60 vendor class identifier. |
| Vendor i Specific Information | DHCP option 43. Specify vendor specific information according to option 60 vendor class identifier. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

DHCP Snooping

Configure DHCP Snooping on this page.

DHCP Snooping Configuration

| | |
|---------------|------------|
| Snooping Mode | Disabled ▼ |
|---------------|------------|

Port Mode Configuration

| Port | Mode |
|------|-----------|
| * | <> ▼ |
| 1 | Trusted ▼ |
| 2 | Trusted ▼ |
| 3 | Trusted ▼ |
| 4 | Trusted ▼ |
| 5 | Trusted ▼ |
| 6 | Trusted ▼ |
| 7 | Trusted ▼ |
| 8 | Trusted ▼ |
| 9 | Trusted ▼ |
| 10 | Trusted ▼ |
| 11 | Trusted ▼ |

| | |
|-------|-------|
| Apply | Reset |
|-------|-------|

| Object | Description |
|-------------------------|--|
| Snooping Mode | Indicates the DHCP snooping mode operation. Possible modes are: Enabled: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP requests messages will be forwarded to trusted ports and only allow reply packets from trusted ports. Disabled: Disable DHCP snooping mode operation. |
| Port Mode Configuration | Indicates the DHCP snooping port mode. Possible port modes are: Trusted: Configures the port as trusted source of the DHCP messages. Untrusted: Configures the port as untrusted source of the DHCP messages. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

DHCP Relay

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such condition, please make sure the switch configuration of VLAN interface IP address and PVID (Port VLAN ID) correctly.

DHCP Relay Configuration

| | |
|--------------------------|------------|
| Relay Mode | Disabled ▼ |
| Relay Server | 0.0.0.0 |
| Relay Information Mode | Disabled ▼ |
| Relay Information Policy | Keep ▼ |

Apply Reset

| Object | Description |
|--------------------------|---|
| Relay Mode | Indicates the DHCP relay mode operation. Possible modes are: Enabled: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations. Disabled: Disable DHCP relay mode operation. |
| Relay Server | Indicates the DHCP relay server IP address. |
| Relay Information Mode | Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID (in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receives form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address. Possible modes are: Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled. Disabled: Disable DHCP relay information mode operation. |
| Relay Information Policy | Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are: Keep: Keep the original relay information when a DHCP message that already contains it is received. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

Security

Switch Security

Users

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.

Add User

| User Settings | |
|------------------|--------------------------|
| User Name | <input type="text"/> |
| Password | <input type="password"/> |
| Password (again) | <input type="password"/> |
| Privilege Level | 0 ▾ |

| Object | Description |
|-----------------|--|
| User Name | A string identifying the user name that this entry should belong to. The allowed string length is 1 to 31. The valid user name allows letters, numbers and underscores. |
| Password | The password of the user. The allowed string length is 0 to 31. Any printable characters including space are accepted. |
| Privilege Level | The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most group privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account. |
| Add New User | Click to add a new user. |
| Cancel | Click to undo any changes made locally and return to the Users. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Delete User | Click to delete the currently selected user. |

Privilege Levels

This page provides an overview of the privilege levels.

Privilege Level Configuration

| Group Name | Privilege Levels | | | |
|-----------------------|-------------------------|----------------------------------|-----------------------------|------------------------------|
| | Configuration Read only | Configuration/Execute Read/write | Status/Statistics Read only | Status/Statistics Read/write |
| Aggregation | 5 | 10 | 5 | 10 |
| Debug | 15 | 15 | 15 | 15 |
| DHCP | 5 | 10 | 5 | 10 |
| DHCPv6_Client | 5 | 10 | 5 | 10 |
| Diagnostics | 5 | 10 | 5 | 10 |
| EEE | 5 | 10 | 5 | 10 |
| EPS | 5 | 10 | 5 | 10 |
| ERFIS | 5 | 10 | 5 | 10 |
| ETH_LINK_OAM | 5 | 10 | 5 | 10 |
| FVC | 5 | 10 | 5 | 10 |
| Green_Ethernet | 5 | 10 | 5 | 10 |
| IP | 5 | 10 | 5 | 10 |
| IPMC_Snooping | 5 | 10 | 5 | 10 |
| JSON_RPC | 5 | 10 | 5 | 10 |
| JSON_RPC_Notification | 5 | 10 | 5 | 10 |
| LACP | 5 | 10 | 5 | 10 |
| LLDP | 5 | 10 | 5 | 10 |
| Loop_Protect | 5 | 10 | 5 | 10 |
| MAC_Table | 5 | 10 | 5 | 10 |
| Maintenance | 15 | 15 | 15 | 15 |
| MFP | 5 | 10 | 5 | 10 |
| MVR | 5 | 10 | 5 | 10 |
| NTP | 5 | 10 | 5 | 10 |
| POE | 5 | 10 | 5 | 10 |
| Ports | 5 | 10 | 1 | 10 |
| Private_VLANs | 5 | 10 | 5 | 10 |
| PTP | 5 | 10 | 5 | 10 |
| QoS | 5 | 10 | 5 | 10 |
| RMirror | 5 | 10 | 5 | 10 |
| Security | 5 | 10 | 5 | 10 |
| sFlow | 5 | 10 | 5 | 10 |
| Spanning_Tree | 5 | 10 | 5 | 10 |
| System | 5 | 10 | 1 | 10 |
| UID.D | 5 | 10 | 5 | 10 |
| UPnP | 5 | 10 | 5 | 10 |
| VCI | 5 | 10 | 5 | 10 |
| VLAN_Translation | 5 | 10 | 5 | 10 |
| VLANs | 5 | 10 | 5 | 10 |
| Voice_VLAN | 5 | 10 | 5 | 10 |
| XXRP | 5 | 10 | 5 | 10 |

Apply Reset

Group Name The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:
 System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.
 Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.
 IP: Everything except 'ping'.
 Port: Everything except 'VeriPHY'.
 Diagnostics: 'ping' and 'VeriPHY'.
 Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.
 Debug: Only present in CLI.

Privilege Levels Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

Apply Click to apply changes.

Reset Click to revert to previous values.

Authentication Method

This page allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.

Authentication Method Configuration

| Client | Methods | | |
|---------|---------|------|------|
| console | local ▼ | no ▼ | no ▼ |
| telnet | local ▼ | no ▼ | no ▼ |
| ssh | local ▼ | no ▼ | no ▼ |
| http | local ▼ | no ▼ | no ▼ |

Command Authorization Method Configuration

| Client | Method | Cmd Lvl | Cfg Cmd |
|---------|--------|---------|--------------------------|
| console | no ▼ | 0 | <input type="checkbox"/> |
| telnet | no ▼ | 0 | <input type="checkbox"/> |
| ssh | no ▼ | 0 | <input type="checkbox"/> |

Accounting Method Configuration

| Client | Method | Cmd Lvl | Exec |
|---------|--------|---------|--------------------------|
| console | no ▼ | | <input type="checkbox"/> |
| telnet | no ▼ | | <input type="checkbox"/> |
| ssh | no ▼ | | <input type="checkbox"/> |

| Object | Description |
|---------|---|
| Client | The management client for which the configuration below applies. |
| Methods | <p>Method can be set to one of the following values:</p> <ul style="list-style-type: none"> no: Authentication is disabled and login is not possible. local: Use the local user database on the switch for authentication. radius: Use remote RADIUS server(s) for authentication. tacacs+: Use remote TACACS+ server(s) for authentication. <p>Methods that involve remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.</p> |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

SSH

Configure SSH on this page.

SSH Configuration

| | |
|------|-----------|
| Mode | Enabled ▼ |
|------|-----------|

| | |
|-------|-------|
| Apply | Reset |
|-------|-------|

| Object | Description |
|--------|---|
| Mode | Indicates the SSH mode operation. Possible modes are: Enabled: Enable SSH mode operation. Disabled: Disable SSH mode operation. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

HTTPS

Configure HTTPS on this page.

HTTPS Configuration

| | |
|----------------------|---|
| Mode | Disabled ▼ |
| Automatic Redirect | Disabled ▼ |
| Certificate Maintain | None ▼ |
| Certificate Status | Switch secure HTTP certificate is presented |

Apply Reset

| Object | Description |
|-----------------------|--|
| Mode | Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are: Enabled: Enable HTTPS mode operation. Disabled: Disable HTTPS mode operation. |
| Automatic Redirect | Indicates the HTTPS redirect mode operation. It only significant if HTTPS mode "Enabled" is selected. Automatically redirects web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled. Possible modes are: Enabled: Enable HTTPS redirect mode operation. Disabled: Disable HTTPS redirect mode operation. |
| Certificate Maintain | This field only can be configured when HTTPS is disabled. It is used to maintain the certification. Possible actions are: None: None action for certification. Delete: To delete certification. Upload: To upload certification, there are two kind of upload method can be selected: Web Browser or URL. Generate: To generate certification. |
| Certificate Algorithm | HTTPS can generate two types of certification. Possible types are: RSA: RSA certification. DSA: DSA certification. |
| PassPhrase | The pattern is used for encrypting the certification. |
| Certificate Upload | Possible modes are: Web Browser: To Upload certification via Web browser. URL: To Upload certification via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is <protocol>://[<username>[:<password>]@]<host>[:<port>]/<path>/<file_name>. For example, tftp://10.10.10.10/new_image_path/new_image.dat, http://username:password@10.10.10.10:80/new_image_path/new_image.dat. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score (_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed. |
| Certificate Status | Possible status is: Switch secure HTTP certificate is presented: The certification is stored in HTTPS' database. Switch secure HTTP certificate is not presented: No certification is stored in HTTPS' database. Switch secure HTTP certificate is generating ...: The certification is generating. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

Access Management

Configure access management table on this page. The maximum number of entries is 16. If the application's type matches any one of the access management entries, it will allow access to the switch.

Access Management Configuration

Mode

Delete VLAN ID Start IP Address End IP Address HTTP/HTTPS SNMP TELNET/SSH

| Object | Description |
|------------------|--|
| Mode | Indicates the access management mode operation. Possible modes are: Enabled: Enable access management mode operation. Disabled: Disable access management mode operation. |
| Delete | Check to delete the entry. It will be deleted during the next save. |
| VLAN ID | Indicates the VLAN ID for the access management entry. |
| Start IP address | Indicates the start IP address for the access management entry. |
| End IP address | Indicates the end IP address for the access management entry. |
| HTTP/HTTPS | Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry. |
| SNMP | Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry. |
| TELNET/SSH | Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Add New Entry | Click to add a new access management entry. |

SNMP

System

Configure SNMP on this page.

SNMP System Configuration

| | |
|-----------------|-------------------|
| Mode | Enabled ▼ |
| Version | SNMP v2c ▼ |
| Read Community | public |
| Write Community | private |
| Engine ID | 800007e5017f00001 |

| Object | Description |
|-----------------|--|
| Mode | Indicates the SNMP mode operation. Possible modes are: Enabled: Enable SNMP mode operation. Disabled: Disable SNMP mode operation. |
| Version | Indicates the SNMP supported version. Possible versions are: SNMP v1: Set SNMP supported version 1. SNMP v2c: Set SNMP supported version 2c. SNMP v3: Set SNMP supported version 3. |
| Read Community | Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet. |
| Write Community | Indicates the community writes access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet. |
| Engine ID | Indicates the SNMPv3 engine ID. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

SNMP Trap

Configure SNMP trap on this page.

Trap Configuration

Global Settings

Mode

Trap Destination Configurations

| Delete | Name | Enable | Version | Destination Address | Destination Port |
|---|------|--------|---------|---------------------|------------------|
| <input type="button" value="Add New Entry"/> | | | | | |
| <input type="button" value="Apply"/> <input type="button" value="Reset"/> | | | | | |

| Object | Description |
|--|--|
| Global Settings | |
| Mode | Indicates the trap mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation. |
| Trap Destination Configurations | |
| Name | Indicates the trap Configuration's name. Indicates the trap destination's name. |
| Enable | Indicates the trap destination mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation. |
| Version | Indicates the SNMP trap supported version. Possible versions are: SNMPv1: Set SNMP trap supported version 1. SNMPv2c: Set SNMP trap supported version 2c. SNMPv3: Set SNMP trap supported version 3. |
| Destination Address | Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). And it also allows a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash. Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.168.10.1'. |
| Destination port | Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535. |

Click on "Add New Entry".

The SNMP Trap Configuration page includes the following fields:

SNMP Trap Configuration

| | |
|-------------------------------|------------|
| Trap Config Name | |
| Trap Mode | Disabled ▼ |
| Trap Version | SNMP v2c ▼ |
| Trap Community | Public |
| Trap Destination Address | |
| Trap Destination Port | 162 |
| Trap Inform Mode | Disabled ▼ |
| Trap Inform Timeout (seconds) | 3 |
| Trap Inform Retry Times | 5 |
| Trap Probe Security Engine ID | Enabled ▼ |
| Trap Security Engine ID | |
| Trap Security Name | None ▼ |

SNMP Trap Event

| | |
|----------------|---|
| System | <input type="checkbox"/> * <input type="checkbox"/> Warm Start <input type="checkbox"/> Cold Start |
| Interface | Link up <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches |
| | * Link down <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches |
| | LLDP <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches |
| Authentication | <input type="checkbox"/> * <input type="checkbox"/> SNMP Authentication Fail |
| Switch | <input type="checkbox"/> * <input type="checkbox"/> STP <input type="checkbox"/> RMON |
| Power Supply | <input type="checkbox"/> * <input type="checkbox"/> PSFAIL |

Apply Reset

| Object | Description |
|----------------------------|---|
| Trap Mode | Indicates the SNMP trap mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation. |
| Trap Version | Indicates the SNMP trap supported version. Possible versions are: SNMP v1: Set SNMP trap supported version 1. SNMP v2c: Set SNMP trap supported version 2c. SNMP v3: Set SNMP trap supported version 3. |
| Trap Community | Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126. |
| Trap Destination Address | Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). And it also allows a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash |
| Trap Link-up and Link-down | Indicates the SNMP trap link-up and link-down mode operation. Possible modes are: Enabled: Enable SNMP trap link-up and link-down mode operation. Disabled: Disable SNMP trap link-up and link-down mode operation. |
| Trap Destination Port | Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535. |

| Object | Description |
|-------------------------------|--|
| Trap Inform Timeout (seconds) | Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147. |
| Trap Inform Retry Times | Indicates the SNMP trap informs retry times. The allowed range is 0 to 255. |
| Trap Probe Security Engine ID | Indicates the SNMP trap probe security engine ID mode of operation. Possible values are: Enabled: Enable SNMP trap probe security engine ID mode of operation. Disabled: Disable SNMP trap probe security engine ID mode of operation. |
| Trap Security Engine ID | Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. |
| Trap Security Name | Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled. |
| SNMP Trap Event | <p>System</p> <p>Enable/disable that the Interface group's traps. Possible traps are: Warm Start: Enable/disable Warm Start trap. Cold Start: Enable/disable Cold Start trap.</p> <p>Interface</p> <p>Indicates that the Interface group's traps. Possible traps are: Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible modes are: Link Up: Enable/disable Link up trap. Link Down: Enable/disable Link down trap. LLDP: Enable/disable LLDP trap.</p> <p>Authentication</p> <p>Indicates that the authentication group's traps. Possible traps are: SNMP Authentication Fail : Enable/disable SNMP trap authentication failure trap.</p> <p>Switch</p> <p>Indicates that the Switch group's traps. Possible traps are: STP: Enable/disable STP trap. RMON: Enable/disable RMON trap.</p> <p>Power Supply</p> <p>Indicates that one of the power supply inputs has failed. Possible traps are: PSFAIL: Enable/disable power supply fail trap.</p> |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

SNMP Communities

Configure SNMPv3 community table on this page. The entry index key is Community.

SNMPv3 Community Configuration

| Delete | Community | Source IP | Source Mask |
|--------------------------|-----------|-----------|-------------|
| <input type="checkbox"/> | public | 0.0.0.0 | 0.0.0.0 |
| <input type="checkbox"/> | private | 0.0.0.0 | 0.0.0.0 |

| Object | Description |
|---------------|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| Community | Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string. |
| Source IP | Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask. |
| Source Mask | Indicates the SNMP access source address mask. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Add New Entry | Click to add a new community. |

SNMP Users

Configure SNMPv3 user table on this page. The entry index keys are Engine ID and User Name.

SNMPv3 User Configuration

| Delete | Engine ID | User Name | Security Level | Authentication Protocol | Authentication Password | Privacy Protocol | Privacy Password |
|--------------------------|--------------------|--------------|----------------|-------------------------|-------------------------|------------------|------------------|
| <input type="checkbox"/> | 800007e5017f000001 | default_user | NoAuth, NoPriv | None | None | None | None |

| Object | Description |
|-------------------------|--|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| Engine ID | An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user. |
| User name | A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. |
| Security Level | Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: No authentication and no privacy. Auth, NoPriv: Authentication and no privacy. Auth, Priv: Authentication and privacy. The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly. |
| Authentication Protocol | Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are: None: No authentication protocol. MD5: An optional flag to indicate that this user uses MD5 authentication protocol. SHA: An optional flag to indicate that this user uses SHA authentication protocol. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly. |
| Authentication Password | A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126. |
| Privacy Protocol | Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are: None: No privacy protocol. DES: An optional flag to indicate that this user uses DES authentication protocol. AES: An optional flag to indicate that this user uses AES authentication protocol. |
| Privacy Password | A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Add New Entry | Click to add new user configurations. |

SNMP Groups

Configure SNMPv3 group table on this page. The entry index keys are Security Model and Security Name.

SNMPv3 Group Configuration

| Delete | Security Model | Security Name | Group Name |
|--------------------------|----------------|---------------|------------------|
| <input type="checkbox"/> | v1 | public | default_ro_group |
| <input type="checkbox"/> | v1 | private | default_rw_group |
| <input type="checkbox"/> | v2c | public | default_ro_group |
| <input type="checkbox"/> | v2c | private | default_rw_group |
| <input type="checkbox"/> | usm | default_user | default_rw_group |

| Object | Description |
|----------------|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| Security Model | Indicates the security model that this entry should belong to. Possible security models are: v1: Reserved for SNMPv1. v2c: Reserved for SNMPv2c. usm: User-based Security Model (USM). |
| Security Name | A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. |
| Group Name | A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Add New Entry | Click to add a new group. |

SNMP Views

Configure SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.

SNMPv3 View Configuration

| Delete | View Name | View Type | OID Subtree |
|--------------------------|--------------|------------|-------------|
| <input type="checkbox"/> | default_view | included ▼ | .1 |

| Object | Description |
|---------------|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| View Name | A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. |
| View Type | Indicates the view type that this entry should belong to. Possible view types are: included: An optional flag to indicate that this view subtree should be included. excluded: An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and its OID subtree should overstep the 'excluded' view entry. |
| OID Subtree | The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*). |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Add New Entry | Click to add new viewer configurations. |

SNMP Access

Configure SNMPv3 access table on this page. The entry index keys are Group Name, Security Model and Security Level.

SNMPv3 Access Configuration

| Delete | Group Name | Security Model | Security Level | Read View Name | Write View Name |
|--------------------------|------------------|----------------|----------------|----------------|-----------------|
| <input type="checkbox"/> | default_ro_group | any | NoAuth, NoPriv | default_view ▼ | None ▼ |
| <input type="checkbox"/> | default_rw_group | any | NoAuth, NoPriv | default_view ▼ | default_view ▼ |

| Object | Description |
|-----------------|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| Group Name | A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. |
| Security Model | Indicates the security model that this entry should belong to. Possible security models are: any: Any security model accepted (v1 v2c usm). v1: Reserved for SNMPv1. v2c: Reserved for SNMPv2c. usm: User-based Security Model (USM). |
| Security Level | Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: No authentication and no privacy. Auth, NoPriv: Authentication and no privacy. Auth, Priv: Authentication and privacy. |
| Read View Name | The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. |
| Write View Name | The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Add New Entry | Click to add new access configurations. |

RMON

Statistics

Configure RMON Statistics table on this page. The entry index key is ID.

RMON Statistics Configuration

| Delete | ID | Data Source |
|--------|----------------------|--|
| Delete | <input type="text"/> | .1.3.6.1.2.1.2.2.1.1. <input type="text" value="0"/> |

| Object | Description |
|---------------|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| ID | Indicates the index of the entry. The range is from 1 to 65535. |
| Data Source | Indicates the port ID which wants to be monitored. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Add New Entry | Click to add new RMON statistic configurations. |

History

Configure RMON History table on this page. The entry index key is ID.

RMON History Configuration

| Delete | ID | Data Source | Interval | Buckets | Buckets Granted |
|--------|----------------------|--|-----------------------------------|---------------------------------|-----------------|
| Delete | <input type="text"/> | .1.3.6.1.2.1.2.2.1.1. <input type="text" value="0"/> | <input type="text" value="1800"/> | <input type="text" value="50"/> | |

| Object | Description |
|-----------------|--|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| ID | Indicates the index of the entry. The range is from 1 to 65535. |
| Data Source | Indicates the port ID which wants to be monitored. |
| Interval | Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds. |
| Buckets | Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50. |
| Buckets Granted | The number of data shall be saved in the RMON. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Add New Entry | Click to add a new history configurations. |

Alarm

Configure RMON Alarm table on this page. The entry index key is ID.

RMON Alarm Configuration

| Delete | ID | Interval | Variable | Sample Type | Value | Startup Alarm | Rising Threshold | Rising Index | Falling Threshold | Falling Index |
|--------|----|----------|---------------------|-------------|-------|---------------|------------------|--------------|-------------------|---------------|
| Delete | | 30 | .1.3.6.1.2.1.2.2.1. | 0.0 | Delta | 0 | RisingOrFalling | 0 | 0 | 0 |

| Object | Description |
|-------------------|--|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| ID | Indicates the index of the entry. The range is from 1 to 65 |
| Interval | Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2 ³¹ -1. |
| Variable | Indicates the particular variable to be sampled, the possible variables are: InOctets: The total number of octets received on the interface, including framing characters. InUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol. InNUcastPkts: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. InDiscards: The number of inbound packets that are discarded even the packets are normal. InErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. InUnknownProtos: the number of the inbound packets that were discarded because of the unknown or un-support protocol. OutOctets: The number of octets transmitted out of the interface , including framing characters. OutUcastPkts: The number of uni-cast packets that request to transmit. OutNUcastPkts: The number of broad-cast and multi-cast packets that request to transmit. OutDiscards: The number of outbound packets that are discarded event the packets are normal. OutErrors: The number of outbound packets that could not be transmitted because of errors. OutQLen: The length of the output packet queue (in packets). |
| Sample Type | The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: Absolute: Get the sample directly. Delta: Calculate the difference between samples (default). |
| Value | The value of the statistic during the last sampling period. |
| Startup Alarm | The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: RisingTrigger alarm when the first value is larger than the rising threshold. FallingTrigger alarm when the first value is less than the falling threshold. RisingOrFallingTrigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default). |
| Rising Threshold | Rising threshold value (-2147483648-2147483647). |
| Rising Index | Rising event index (1-65535). |
| Falling Threshold | Falling threshold value (-2147483648-2147483647) |
| Falling Index | Falling event index (1-65535). |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Add New Entry | Click to add new RMON alarm configurations. |

Event

Configure RMON Event table on this page. The entry index key is ID.

RMON Event Configuration

| Delete | ID | Desc | Type | Community | Event Last Time |
|--------|----|------|--------|-----------|-----------------|
| Delete | | | none ▼ | public | 0 |

| Object | Description |
|-----------------|--|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| ID | Indicates the index of the entry. The range is from 1 to 65535. |
| Desc | Indicates this event, the string length is from 0 to 127, default is a null string. |
| Type | Indicates the notification of the event, the possible types are: none: No SNMP log is created, no SNMP trap is sent. log: Create SNMP log entry when the event is triggered. snmptrap: Send SNMP trap when the event is triggered. logandtrap: Create SNMP log entry and sent SNMP trap when the event is triggered. |
| Community | Specify the community when trap is sent, the string length is from 0 to 127, default is "public". |
| Event Last Time | Indicates the value of sysUpTime at the time this event entry last generated an event. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Add New Entry | Click to add new RMON event configurations. |

Network

Limit Control

This page allows you to configure the Port Security Limit Control system and port settings.

Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below.

The Limit Control module utilizes a lower-layer module, Port Security module, which manages MAC addresses learnt on the port.

The Limit Control configuration consists of two sections, a system- and a port-wide.

Port Security Limit Control Configuration

System Configuration

| | |
|---------------|--------------------------|
| Mode | Disabled ▼ |
| Aging Enabled | <input type="checkbox"/> |
| Aging Period | 3600 seconds |

Port Configuration

| Port | Mode | Limit | Action | State | Re-open |
|------|------------|-------|--------|----------|---------|
| * | <> ▼ | 4 | <> ▼ | | |
| 1 | Disabled ▼ | 4 | None ▼ | Disabled | Reopen |
| 2 | Disabled ▼ | 4 | None ▼ | Disabled | Reopen |
| 3 | Disabled ▼ | 4 | None ▼ | Disabled | Reopen |
| 4 | Disabled ▼ | 4 | None ▼ | Disabled | Reopen |
| 5 | Disabled ▼ | 4 | None ▼ | Disabled | Reopen |
| 6 | Disabled ▼ | 4 | None ▼ | Disabled | Reopen |
| 7 | Disabled ▼ | 4 | None ▼ | Disabled | Reopen |
| 8 | Disabled ▼ | 4 | None ▼ | Disabled | Reopen |
| 9 | Disabled ▼ | 4 | None ▼ | Disabled | Reopen |
| 10 | Disabled ▼ | 4 | None ▼ | Disabled | Reopen |
| 11 | Disabled ▼ | 4 | None ▼ | Disabled | Reopen |

Apply Reset

| Object | Description |
|-----------------------------|--|
| System Configuration | |
| Mode | Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled. |
| Aging Enabled | If checked, secured MAC addresses are subject to aging as discussed under Aging Period . |
| Aging Period | If Aging Enabled is checked, then the aging period is controlled with this input. If other Amodules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality. The Aging Period can be set to a number between 10 and 10,000,000 seconds. To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch. |

| Object | Description |
|---------------------------|--|
| Port Configuration | |
| Port | The port number to which the configuration below applies. |
| Mode | Controls whether Limit Control is enabled on this port. Both this and the Global Mode. must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port. |
| Limit | The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses. |
| Action | If Limit is reached, the switch can take one of the following actions: None: Do not allow more than Limit MAC addresses on the port, but take no further action. is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded. Shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port: 1) Boot the switch, 2) Disable and re-enable Limit Control on the port or the switch, 3) Click the Reopen button. Trap & Shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken. |
| State | This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values: Disabled: Limit Control is either globally disabled or disabled on the port. Ready: The limit is not yet reached. This can be shown for all actions. Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap. Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown. |
| Re-open Button | If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shutdown in the Action section. Note that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Refresh | Click to refresh the page. |

Screen

NAS

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Configuration»Security»AAA" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

The NAS configuration consists of two sections, a system- and a port-wide.

Network Access Server Configuration

System Configuration

| | | |
|--------------------------------|--------------------------|---------|
| Mode | Disabled | ▼ |
| Reauthentication Enabled | <input type="checkbox"/> | |
| Reauthentication Period | 3600 | seconds |
| EAPOL Timeout | 30 | seconds |
| Aging Period | 300 | seconds |
| Hold Time | 10 | seconds |
| RADIUS-Assigned QoS Enabled | <input type="checkbox"/> | |
| RADIUS-Assigned VLAN Enabled | <input type="checkbox"/> | |
| Guest VLAN Enabled | <input type="checkbox"/> | |
| Guest VLAN ID | 1 | |
| Max. Reauth. Count | 2 | |
| Allow Guest VLAN if EAPOL Seen | <input type="checkbox"/> | |

Port Configuration

| Port | Admin State | RADIUS-Assigned QoS Enabled | RADIUS-Assigned VLAN Enabled | Guest VLAN Enabled | Port State | Restart | |
|------|--------------------|-----------------------------|------------------------------|--------------------------|-------------------|----------------|--------------|
| * <> | ▼ | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | | |
| 1 | Force Authorized ▼ | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate | Reinitialize |
| 2 | Force Authorized ▼ | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate | Reinitialize |
| 3 | Force Authorized ▼ | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate | Reinitialize |
| 4 | Force Authorized ▼ | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate | Reinitialize |
| 5 | Force Authorized ▼ | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate | Reinitialize |
| 6 | Force Authorized ▼ | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate | Reinitialize |
| 7 | Force Authorized ▼ | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate | Reinitialize |
| 8 | Force Authorized ▼ | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate | Reinitialize |
| 9 | Force Authorized ▼ | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate | Reinitialize |
| 10 | Force Authorized ▼ | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate | Reinitialize |
| 11 | Force Authorized ▼ | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate | Reinitialize |

Apply Reset

| Object | Description |
|--------|-------------|
|--------|-------------|

System Configuration

| | |
|--------------------------|--|
| Mode | Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames. |
| Reauthentication Enabled | If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below). |
| Reauthentication Period | Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds. |
| EAPOL Timeout | Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports. |

| Object | Description |
|------------------------------|---|
| Aging Period | <p>This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:</p> <ul style="list-style-type: none"> • Single 802.1X • Multi 802.1X • MAC-Based Auth. <p>When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.</p> <p>If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.</p> <p>For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.</p> |
| Hold Time | <p>This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:</p> <ul style="list-style-type: none"> • Single 802.1X • Multi 802.1X • MAC-Based Auth. <p>If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration»Security»AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.</p> <p>In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.</p> <p>The Hold Time can be set to a number between 10 and 1000000 seconds.</p> |
| RADIUS-Assigned QoS Enabled | <p>RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description).</p> <p>The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.</p> |
| RADIUS-Assigned VLAN Enabled | <p>RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description).</p> <p>The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.</p> |

| Object | Description |
|--------------------------------|--|
| Guest VLAN Enabled | <p>A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.</p> |
| Guest VLAN ID | <p>This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4095].</p> |
| Max. Reauth. Count | <p>The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].</p> |
| Allow Guest VLAN if EAPOL Seen | <p>The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.</p> |
| Port Configuration | |
| Port | <p>The port number for which the configuration below applies.</p> |

| Object | Description |
|-------------|---|
| Admin State | <p>If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:</p> <p>Force Authorized In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.</p> <p>Force Unauthorized In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.</p> <p>Port-based 802.1X In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.</p> <p>When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.</p> <p>Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.</p> <p>Single 802.1X In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant.</p> <p>Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.</p> <p>Multi 802.1X Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.</p> <p>In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.</p> <p>The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.</p> <p>MAC-based Auth. Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.</p> <p>When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.</p> <p>The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.</p> |

| Object | Description |
|------------------------------|---|
| RADIUS-Assigned QoS Enabled | <p>When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).</p> <p>This option is only available for single-client modes, i.e.</p> <ul style="list-style-type: none"> • Port-based 802.1X • Single 802.1X <p>RADIUS attributes used in identifying a QoS Class: The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet. Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:</p> <ul style="list-style-type: none"> • All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7]. |
| RADIUS-Assigned VLAN Enabled | <p>When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).</p> <p>This option is only available for single-client modes, i.e.</p> <ul style="list-style-type: none"> • Port-based 802.1X • Single 802.1X <p>For trouble-shooting VLAN assignments, use the "Monitor»VLANs»VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.</p> <p>RADIUS attributes used in identifying a VLAN ID: RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:</p> <ul style="list-style-type: none"> • The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet. • The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag): <ul style="list-style-type: none"> - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6). - Value of Tunnel-Type must be set to "VLAN" (ordinal 13). - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095]. |

| Object | Description |
|--------------------|--|
| Guest VLAN Enabled | <p>When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes, i.e.:</p> <ul style="list-style-type: none"> • Port-based 802.1X • Single 802.1X • Multi 802.1X <p>For trouble-shooting VLAN assignments, use the "Monitor»VLANs»VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.</p> <p>Guest VLAN Operation:</p> <p>When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.</p> <p>Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.</p> <p>While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.</p> |
| Port State | <p>The current state of the port. It can undertake one of the following values:</p> <p>Globally Disabled: NAS is globally disabled.</p> <p>Link Down: NAS is globally enabled, but there is no link on the port.</p> <p>Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.</p> <p>Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.</p> <p>X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.</p> |
| Restart | <p>Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect.</p> <p>Reauthenticate: Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.</p> <p>The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.</p> <p>Reinitialize: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress</p> |
| Refresh | Click to refresh the page. |
| Reset | Click to revert to previous values. |
| Apply | Click to apply changes. |

ACL

Ports

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

ACL Ports Configuration

| Port | Policy ID | Action | Rate Limiter ID | EVC Policer | EVC Policer ID | Port Redirect | Mirror | Logging | Shutdown | State | Counter |
|------|-----------|--------|-----------------|-------------|----------------|------------------------------|----------|----------|----------|---------|---------|
| 0 | 0 | <> | <> | <> | 1 | Disabled Port 1 Port 2 | <> | <> | <> | <> | 0 |
| 1 | 0 | Permit | Disabled | Disabled | 1 | Disabled Port 1 Port 2 | Disabled | Disabled | Disabled | Enabled | 72218 |
| 2 | 0 | Permit | Disabled | Disabled | 1 | Disabled Port 1 Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 3 | 0 | Permit | Disabled | Disabled | 1 | Disabled Port 1 Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 4 | 0 | Permit | Disabled | Disabled | 1 | Disabled Port 1 Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 5 | 0 | Permit | Disabled | Disabled | 1 | Disabled Port 1 Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 6 | 0 | Permit | Disabled | Disabled | 1 | Disabled Port 1 Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 7 | 0 | Permit | Disabled | Disabled | 1 | Disabled Port 1 Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 8 | 0 | Permit | Disabled | Disabled | 1 | Disabled Port 1 Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 9 | 0 | Permit | Disabled | Disabled | 1 | Disabled Port 1 Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 10 | 0 | Permit | Disabled | Disabled | 1 | Disabled Port 1 Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 11 | 0 | Permit | Disabled | Disabled | 1 | Disabled Port 1 Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |

Apply Reset

| Object | Description |
|-----------------|--|
| Port | The logical port for the settings contained in the same row. |
| Policy ID | Select the policy to apply to this port. The allowed values are 0 through 255. The default value is 0. |
| Action | Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit". |
| Rate Limiter ID | Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled". |
| EVC Policer | Select whether EVC policer is enabled or disabled. The default value is "Disabled". Note that ACL rate limiter and EVC policer can not both be enabled. |
| EVC Policer ID | Select which EVC policer ID to apply on this port. The allowed values are Disabled or the values 1 through 256. |
| Port Redirect | Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled". |
| Mirror | Specify the mirror operation of this port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is "Disabled". |
| Logging | Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC. The allowed values are: Enabled: Frames received on the port are stored in the System Log. Disabled: Frames received on the port are not logged. The default value is "Disabled". Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited. |

| Object | Description |
|----------|---|
| Shutdown | Specify the port shut down operation of this port. The allowed values are: Enabled: If a frame is received on the port, the port will be disabled. Disabled: Port shut down is disabled. The default value is "Disabled". Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags). |
| State | Specify the port state of this port. The allowed values are: Enabled: To reopen ports by changing the volatile port configuration of the ACL user module. Disabled: To close ports by changing the volatile port configuration of the ACL user module. The default value is "Enabled". |
| Counter | Counts the number of frames that match this ACE. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Refresh | Click to refresh the page. |
| Clear | Click to clear the counters. |

Rate Limiters

Configure the rate limiter for the ACL of the switch.

ACL Rate Limiter Configuration

| Rate Limiter ID | Rate | Unit |
|-----------------|------|-------|
| * | 1 | <> ▼ |
| 1 | 1 | pps ▼ |
| 2 | 1 | pps ▼ |
| 3 | 1 | pps ▼ |
| 4 | 1 | pps ▼ |
| 5 | 1 | pps ▼ |
| 6 | 1 | pps ▼ |
| 7 | 1 | pps ▼ |
| 8 | 1 | pps ▼ |
| 9 | 1 | pps ▼ |
| 10 | 1 | pps ▼ |
| 11 | 1 | pps ▼ |
| 12 | 1 | pps ▼ |
| 13 | 1 | pps ▼ |
| 14 | 1 | pps ▼ |
| 15 | 1 | pps ▼ |
| 16 | 1 | pps ▼ |

| Object | Description |
|-----------------|---|
| Rate Limiter ID | The rate limiter ID for the settings contained in the same row. |
| Rate | The rate range is located 0-3276700 in pps. Or 0, 100, 200, 300, ..., 1000000 in kbps. |
| Unit | Specify the rate unit. The allowed values are: pps: packets per second. kbps: Kbits per second. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

Access Control List

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch.

Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.

Access Control List Configuration

Auto-refresh

Refresh

Clear

Remove All

| ACE | Ingress Port | Policy / Bitmask | Frame Type | Action | Rate Limiter | Port Redirect | Mirror | Counter | |
|-----|--------------|------------------|------------|--------|--------------|---------------|--------|---------|--|
| + | | | | | | | | | |

| Object | Description |
|----------------------|--|
| Ingress Port | Indicates the ingress port of the ACE. Possible values are: All: The ACE will match all ingress port. Port: The ACE will match a specific ingress port. |
| Policy / Bitmask | Indicates the policy number and bitmask of the ACE. |
| Frame Type | Indicates the frame type of the ACE. Possible values are: Any: The ACE will match any frame type. EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ARP: The ACE will match ARP/RARP frames. IPv4: The ACE will match all IPv4 frames. IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol. IPv4/UDP: The ACE will match IPv4 frames with UDP protocol. IPv4/TCP: The ACE will match IPv4 frames with TCP protocol. IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. IPv6: The ACE will match all IPv6 standard frames. |
| Action | Indicates the forwarding action of the ACE. Permit: Frames matching the ACE may be forwarded and learned. Deny: Frames matching the ACE are dropped. Filter: Frames matching the ACE are filtered. |
| Rate Limiter | Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled. |
| Port Redirect | Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled. |
| Mirror | Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is "Disabled". |
| Counter | The counter indicates the number of times the ACE was hit by a frame. |
| Modification Buttons | You can modify each ACE (Access Control Entry) in the table using the following buttons: "+": Inserts a new ACE before the current row. "e": Edits the ACE row. "up": Moves the ACE up the list. "down": Moves the ACE down the list. "X": Deletes the ACE. "+": The lowest plus sign adds a new entry at the bottom of the ACE listings. |
| Auto_Refresh | Click to force the page to refresh automatically every 3 seconds. |
| Remove All | Click to remove all ACEs. |
| Refresh | Click to refresh the page. |

| Object | Description |
|--------|------------------------------|
| Clear | Click to clear the counters. |

ACE Configuration

| | |
|---------------|---|
| Ingress Port | All Port 1 Port 2 Port 3 Port 4 |
| Policy Filter | Any |
| Frame Type | Any |

| | |
|--------------|----------|
| Action | Permit |
| Rate Limiter | Disabled |
| EVC Policer | Disabled |
| Mirror | Disabled |
| Logging | Disabled |
| Shutdown | Disabled |
| Counter | 0 |

VLAN Parameters

| | |
|----------------|-----|
| 802.1Q Tagged | Any |
| VLAN ID Filter | Any |
| Tag Priority | Any |

Apply Reset Cancel

| Object | Description |
|----------------|---|
| Ingress Port | Select the ingress port for which this ACE applies. All: The ACE applies to all port. Port n: The ACE applies to this port number, where n is the number of the switch port. |
| Policy Filter | Specify the policy number filter for this ACE. Any: No policy filter is specified. (policy filter status is "don't-care".) Specific: If you want to filter a specific policy with this ACE, choose this value. Two field for entering a policy value and bitmask appears. |
| Policy Value | When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 255. |
| Policy Bitmask | When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0xff. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [policy_value & policy_bitmask]. For example, if the policy value is 3 and the policy bitmask is 0x10(bit 0 is "don't-care" bit), then policy 2 and 3 are applied to this rule. |
| Frame Type | Select the frame type for this ACE. These frame types are mutually exclusive. Any: Any frame can match this ACE. Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal). ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with Ethernet type. IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with Ethernet type. IPv6: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type. |
| Action | Specify the action to take with a frame that hits this ACE. Permit: The frame that hits this ACE is granted permission for the ACE operation. Deny: The frame that hits this ACE is dropped. Filter: Frames matching the ACE are filtered. |
| Rate Limiter | Specify the rate limiter in number of base units. The allowed range is 1 to 16. Disabled indicates that the rate limiter operation is disabled. |
| EVC Policer | Select whether EVC policer is enabled or disabled. The default value is "Disabled". Note that the ACL rate limiter and EVC policer can not both be enabled. |

| Object | Description |
|----------------|---|
| EVC Policer ID | Select which EVC policer ID to apply on this ACE. The allowed values are Disabled or the values 1 through 256. |
| Port Redirect | Frames that hit the ACE are redirected to the port number specified here. The rate limiter will affect these ports. The allowed range is the same as the switch port number range. Disabled indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when action is permitted. |
| Mirror | Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is "Disabled". |
| Logging | Specify the logging operation of the ACE. Notice that the logging message doesn't include the 4 bytes CRC information. The allowed values are: Enabled: Frames matching the ACE are stored in the System Log. Disabled: Frames matching the ACE are not logged. Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited. |
| Shutdown | Specify the port shut down operation of the ACE. The allowed values are: Enabled: If a frame matches the ACE, the ingress port will be disabled. Disabled: Port shut down is disabled for the ACE. Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags). |
| Counter | The counter indicates the number of times the ACE was hit by a frame. |

MAC Parameters

| | |
|-------------|--|
| SMAC Filter | (Only displayed when the frame type is Ethernet Type or ARP.) Specify the source MAC filter for this ACE. Any: No SMAC filter is specified. (SMAC filter status is "don't-care"). Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears. |
| SMAC Value | When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value. |
| DMAC Filter | Specify the destination MAC filter for this ACE. Any: No DMAC filter is specified. (DMAC filter status is "don't-care"). MC: Frame must be multicast. BC: Frame must be broadcast. UC: Frame must be unicast. Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears. |
| DMAC Value | When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value. |

VLAN Parameters

| | |
|---------------|--|
| 802.1Q Tagged | Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are: Any: Any value is allowed ("don't-care"). Enabled: Tagged frame only. Disabled: Untagged frame only. The default value is "Any". |
|---------------|--|

| Object | Description |
|-----------------------|--|
| VLAN ID Filter | Specify the VLAN ID filter for this ACE. Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".) Specific: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears. |
| VLAN ID | When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value. |
| Tag Priority | Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7 or range 0-1, 2-3, 4-5, 6-7, 0-3 and 4-7. The value Any means that no tag priority is specified (tag priority is "don't-care".) |
| ARP Parameters | |
| ARP/RARP | Specify the available ARP/RARP opcode (OP) flag for this ACE. Any: No ARP/RARP OP flag is specified. (OP is "don't-care".) ARP: Frame must have ARP opcode set to ARP. RARP: Frame must have RARP opcode set to RARP. Other: Frame has unknown ARP/RARP Opcode flag. |
| Request/Reply | Specify the available Request/Reply opcode (OP) flag for this ACE. Any: No Request/Reply OP flag is specified. (OP is "don't-care".) Request: Frame must have ARP Request or RARP Request OP flag set. Reply: Frame must have ARP Reply or RARP Reply OP flag. |
| Sender IP Filter | Specify the sender IP filter for this ACE. Any: No sender IP filter is specified. (Sender IP filter is "don't-care".) Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears. Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear. |
| Sender IP Address | When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation. |
| Sender IP Mask | When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation. |
| Target IP Filter | Specify the target IP filter for this specific ACE. Any: No target IP filter is specified. (Target IP filter is "don't-care".) Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears. Network: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear. |
| Target IP Address | When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation. |
| Target IP Mask | When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation. |
| ARP Sender MAC Match | Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. 0: ARP frames where SHA is not equal to the SMAC address. 1: ARP frames where SHA is equal to the SMAC address. Any: Any value is allowed ("don't-care"). |
| RARP Target MAC Match | Specify whether frames can hit the action according to their target hardware address field (THA) settings. 0: RARP frames where THA is not equal to the target MAC address. 1: RARP frames where THA is equal to the target MAC address. Any: Any value is allowed ("don't-care"). |

| Object | Description |
|----------------------|---|
| IP/Ethernet Length | Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings. 0: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04). 1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04). Any: Any value is allowed ("don't-care"). |
| IP | Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings. 0: ARP/RARP frames where the HLD is not equal to Ethernet (1). 1: ARP/RARP frames where the HLD is equal to Ethernet (1). Any: Any value is allowed ("don't-care"). |
| Ethernet | Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings. 0: ARP/RARP frames where the PRO is not equal to IP (0x800). 1: ARP/RARP frames where the PRO is equal to IP (0x800). Any: Any value is allowed ("don't-care"). |
| IP Parameters | |
| IP Protocol Filter | Specify the IP protocol filter for this ACE. Any: No IP protocol filter is specified ("don't-care"). Specific: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears. ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file. UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file. TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file. |
| IP Protocol Value | When "Specific" is selected for the IP protocol value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value. |
| IP TTL | Specify the Time-to-Live settings for this ACE. zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry. non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry. Any: Any value is allowed ("don't-care"). |
| IP Fragment | Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame. No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry. Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry. Any: Any value is allowed ("don't-care"). |
| IP Option | Specify the options flag setting for this ACE. No: IPv4 frames where the options flag is set must not be able to match this entry. Yes: IPv4 frames where the options flag is set must be able to match this entry. Any: Any value is allowed ("don't-care"). |
| SIP Filter | Specify the source IP filter for this ACE. Any: No source IP filter is specified. (Source IP filter is "don't-care"). Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears. Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear. |

| Object | Description |
|-------------|--|
| SIP Address | When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation. |
| SIP Mask | When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation. |
| DIP Filter | Specify the destination IP filter for this ACE. Any: No destination IP filter is specified. (Destination IP filter is "don't-care".) Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears. Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear. |
| DIP Address | When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation. |
| DIP Mask | When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation. |

IPv6 Parameters

| | |
|--------------------|--|
| Next Header Filter | Specify the IPv6 next header filter for this ACE. Any: No IPv6 next header filter is specified ("don't-care"). Specific: If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears. ICMP: Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file. UDP: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file. TCP: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file. |
| Next Header Value | When "Specific" is selected for the IPv6 next header value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IPv6 protocol value. |
| SIP Filter | Specify the source IPv6 filter for this ACE. Any: No source IPv6 filter is specified. (Source IPv6 filter is "don't-care".) Specific: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear. |
| SIP address | When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address. |
| SIP BitMask | When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [sipv6_address & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFF0 (bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule. |
| Hop Limit | Specify the hop limit settings for this ACE. zero: IPv6 frames with a hop limit field greater than zero must not be able to match this entry. non-zero: IPv6 frames with a hop limit field greater than zero must be able to match this entry. Any: Any value is allowed ("don't-care"). |

ICMP Parameters

| | |
|------------------|---|
| ICMP Type Filter | Specify the ICMP filter for this ACE. Any: No ICMP filter is specified (ICMP filter status is "don't-care"). Specific: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears. |
| ICMP Type Value | When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP value. |

| Object | Description |
|----------------------------|---|
| ICMP Code Filter | Specify the ICMP code filter for this ACE. Any: No ICMP code filter is specified (ICMP code filter status is "don't-care"). Specific: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears. |
| ICMP Code Value | When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value. |
| TCP/UDP Parameters | |
| TCP/UDP Source Filter | Specify the TCP/UDP source filter for this ACE. Any: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care"). Specific: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears. Range: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears. |
| TCP/UDP Source No. | When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value. |
| TCP/UDP Source Range | When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value. |
| TCP/UDP Destination Filter | Specify the TCP/UDP destination filter for this ACE. Any: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care"). Specific: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears. Range: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears. |
| TCP/UDP Destination Number | When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value. |
| TCP/UDP Destination Range | When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value. |
| TCP FIN | Specify the TCP "No more data from sender" (FIN) value for this ACE. 0: TCP frames where the FIN field is set must not be able to match this entry. 1: TCP frames where the FIN field is set must be able to match this entry. Any: Any value is allowed ("don't-care"). |
| TCP SYN | Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE. 0: TCP frames where the SYN field is set must not be able to match this entry. 1: TCP frames where the SYN field is set must be able to match this entry. Any: Any value is allowed ("don't-care"). |
| TCP RST | Specify the TCP "Reset the connection" (RST) value for this ACE. 0: TCP frames where the RST field is set must not be able to match this entry. 1: TCP frames where the RST field is set must be able to match this entry. Any: Any value is allowed ("don't-care"). |
| TCP PSH | Specify the TCP "Push Function" (PSH) value for this ACE. 0: TCP frames where the PSH field is set must not be able to match this entry. 1: TCP frames where the PSH field is set must be able to match this entry. Any: Any value is allowed ("don't-care"). |
| TCP ACK | Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE. 0: TCP frames where the ACK field is set must not be able to match this entry. 1: TCP frames where the ACK field is set must be able to match this entry. Any: Any value is allowed ("don't-care"). |

| Object | Description |
|---------|--|
| TCP URG | Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE. 0: TCP frames where the URG field is set must not be able to match this entry. 1: TCP frames where the URG field is set must be able to match this entry. Any: Any value is allowed ("don't-care"). |

Ethernet Type Parameters

| | |
|---------------------|--|
| EtherType Filter | Specify the Ethernet type filter for this ACE. Any: No EtherType filter is specified (EtherType filter status is "don't-care"). Specific: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering an EtherType value appears. |
| Ethernet Type Value | When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Cancel | Return to the page. |

IP Source Guard

Configuration

This page provides IP Source Guard related configurations.

IP Source Guard Configuration

Mode

Port Mode Configuration

| Port | Mode | Max Dynamic Clients |
|------|------------|---------------------|
| * | <> ▼ | <> ▼ |
| 1 | Disabled ▼ | Unlimited ▼ |
| 2 | Disabled ▼ | Unlimited ▼ |
| 3 | Disabled ▼ | Unlimited ▼ |
| 4 | Disabled ▼ | Unlimited ▼ |
| 5 | Disabled ▼ | Unlimited ▼ |
| 6 | Disabled ▼ | Unlimited ▼ |
| 7 | Disabled ▼ | Unlimited ▼ |
| 8 | Disabled ▼ | Unlimited ▼ |
| 9 | Disabled ▼ | Unlimited ▼ |
| 10 | Disabled ▼ | Unlimited ▼ |
| 11 | Disabled ▼ | Unlimited ▼ |

| Object | Description |
|---------------------------------------|--|
| Mode of IP Source Guard Configuration | Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled. |
| Port Mode Configuration | Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port. |
| Max Dynamic Clients | Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Translate dynamic to static | Click to translate all dynamic entries to static entries. |

Static Table

Static IP Source Guard Table

| Delete | Port | VLAN ID | IP Address | MAC address |
|--------|------|---------|------------|-------------|
| Delete | 1 ▼ | | | |

| Object | Description |
|---------------|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| Port | The logical port for the settings. |
| VLAN ID | The vlan id for the settings. |
| IP Address | Allowed Source IP address. |
| MAC address | Allowed Source MAC address. |
| Add New Entry | Click to add a new entry to the Static IP Source Guard table. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally. |

ARP Inspection

Port Configuration

This page provides ARP Inspection related configuration.

ARP Inspection Configuration

Mode

Port Mode Configuration

| Port | Mode | Check VLAN | Log Type |
|------|---|---|-------------------------------------|
| * | <> <input type="text" value="v"/> | <> <input type="text" value="v"/> | <> <input type="text" value="v"/> |
| 1 | Disabled <input type="text" value="v"/> | Disabled <input type="text" value="v"/> | None <input type="text" value="v"/> |
| 2 | Disabled <input type="text" value="v"/> | Disabled <input type="text" value="v"/> | None <input type="text" value="v"/> |
| 3 | Disabled <input type="text" value="v"/> | Disabled <input type="text" value="v"/> | None <input type="text" value="v"/> |
| 4 | Disabled <input type="text" value="v"/> | Disabled <input type="text" value="v"/> | None <input type="text" value="v"/> |
| 5 | Disabled <input type="text" value="v"/> | Disabled <input type="text" value="v"/> | None <input type="text" value="v"/> |
| 6 | Disabled <input type="text" value="v"/> | Disabled <input type="text" value="v"/> | None <input type="text" value="v"/> |
| 7 | Disabled <input type="text" value="v"/> | Disabled <input type="text" value="v"/> | None <input type="text" value="v"/> |
| 8 | Disabled <input type="text" value="v"/> | Disabled <input type="text" value="v"/> | None <input type="text" value="v"/> |
| 9 | Disabled <input type="text" value="v"/> | Disabled <input type="text" value="v"/> | None <input type="text" value="v"/> |
| 10 | Disabled <input type="text" value="v"/> | Disabled <input type="text" value="v"/> | None <input type="text" value="v"/> |
| 11 | Disabled <input type="text" value="v"/> | Disabled <input type="text" value="v"/> | None <input type="text" value="v"/> |

| Object | Description |
|--------------------------------------|--|
| Mode of ARP Inspection Configuration | Enable the Global ARP Inspection or disable the Global ARP Inspection. |
| Port Mode Configuration | Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are: Enabled: Enable ARP Inspection operation. Disabled: Disable ARP Inspection operation. If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are: Enabled: Enable check VLAN operation. Disabled: Disable check VLAN operation. Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types are: None: Log nothing. Deny: Log denied entries. Permit: Log permitted entries. ALL: Log all entries. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Translate dynamic to static | Click to translate all dynamic entries to static entries. |

VLAN Configuration

Each page shows up to 9999 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next VLAN Table match. The ">>" button will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the warning, message is shown in the displayed table. Use the "<<" button to start over.

VLAN Mode Configuration

Start from VLAN with entries per page.

| Delete | VLAN ID | Log Type |
|--------|----------------------|----------|
| Delete | <input type="text"/> | None ▾ |

Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting.

Possible types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries

Apply Click to apply changes.

Reset Click to revert to previous values.

Add New Entry Click to add new VLAN to the ARP inspection VLAN table.

Static Table

Static ARP Inspection Table

| Delete | Port | VLAN ID | MAC Address | IP Address |
|--------|------|---------|-------------|------------|
| Delete | 1 ▼ | | | |

Add New Entry

Apply Reset

| Object | Description |
|---------------|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| Port | The logical port for the settings |
| VLAN ID | The vlan id for the settings. |
| MAC Address | Allowed Source MAC address in ARP request packets. |
| IP Address | Allowed Source IP address in ARP request packets. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Add New Entry | Click to add a new entry to the Static ARP inspection table. |

Dynamic Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learning from DHCP Snooping

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The ">>" button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "<<" button to start over.

Dynamic ARP Inspection Table Auto-refresh Refresh << >>

Start from , VLAN , MAC address and IP address with entries per page.

| Port | VLAN ID | MAC Address | IP Address | Translate to static |
|-----------------|---------|-------------|------------|---------------------|
| No more entries | | | | |

| Object | Description |
|---------------------|---|
| Port | Switch Port Number for which the entries are displayed. |
| VLAN ID | VLAN-ID in which the ARP traffic is permitted. |
| MAC Address | User MAC address of the entry. |
| IP Address | User IP address of the entry. |
| Translate to static | Select the checkbox to translate the entry to static entry. |
| Auto_refresh | Click to refresh the page automatically every 3 seconds. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Refresh | Click to refresh the table starting from input fields. |
| << | Click to update the table starting from the first entr in the Dynamic ARP Inspection Table. |
| >> | Click to update the table starting with the entry after the last entry currently displayed. |

AAA

RADIUS

This page allows you to configure the RADIUS servers.

RADIUS Server Configuration

Global Configuration

| | | |
|------------------|---|---------|
| Timeout | 5 | seconds |
| Retransmit | 3 | times |
| Deadtime | 0 | minutes |
| Key | | |
| NAS-IP-Address | | |
| NAS-IPv6-Address | | |
| NAS-Identifier | | |

Server Configuration

| Delete | Hostname | Auth Port | Acct Port | Timeout | Retransmit | Key |
|--------|----------|-----------|-----------|---------|------------|-----|
| Delete | | 1812 | 1813 | | | |

| Object | Description |
|---------------------------------|---|
| Global Configuration | |
| Timeout | Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request. |
| Retransmit | Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead. |
| Deadtime | Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. |
| Key | The secret key - up to 63 characters long - shared between the RADIUS server and the switch. |
| NAS-IP-Address (Attribute 4) | The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used. |
| NAS-IPv6-Address (Attribute 95) | The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used. |
| NAS-Identifier (Attribute 32) | The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet. |
| Server Configuration | |
| Delete | To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save. |
| Hostname | The IP address or hostname of the RADIUS server. |
| Auth Port | The UDP port to use on the RADIUS server for authentication. |
| Acct Port | The UDP port to use on the RADIUS server for accounting. |

| Object | Description |
|----------------|---|
| Timeout | This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value. |
| Retransmit | This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value. |
| Key | This optional setting overrides the global key. Leaving it blank will use the global key. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Delete | Click to undo the addition of the new server. |
| Add New Server | Click to add a new RADIUS server, up to 5 servers supported. |

TACACS+

This page allows you to configure the TACACS+ servers.

TACACS+ Server Configuration

Global Configuration

| | | |
|----------|---|---------|
| Timeout | 5 | seconds |
| Deadtime | 0 | minutes |
| Key | | |

Server Configuration

| Delete | Hostname | Port | Timeout | Key |
|--------------------------|----------|------|---------|-----|
| <input type="checkbox"/> | | 49 | | |

| Object | Description |
|-----------------------------|---|
| Global Configuration | |
| Timeout | Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead. |
| Deadtime | Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. |
| Key | The secret key - up to 63 characters long - shared between the TACACS+ server and the switch. |
| Server Configuration | |
| Delete | To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save. |
| Hostname | The IP address or hostname of the TACACS+ server. |
| Port | The TCP port to use on the TACACS+ server for authentication. |
| Timeout | This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value. |
| Key | This optional setting overrides the global key. Leaving it blank will use the global key. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Delete | Click to undo the addition of the new server. |
| Add New Server | Click to add a new TACACS+ server, up to 5 servers supported. |

Aggregation

Static

This page is used to configure the Aggregation hash mode and the aggregation group.

Aggregation Mode Configuration

| Hash Code Contributors | |
|-------------------------|-------------------------------------|
| Source MAC Address | <input checked="" type="checkbox"/> |
| Destination MAC Address | <input type="checkbox"/> |
| IP Address | <input checked="" type="checkbox"/> |
| TCP/UDP Port Number | <input checked="" type="checkbox"/> |

Aggregation Group Configuration

| Group ID | Port Members | | | | | | | | | | |
|----------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| Normal | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> |
| 1 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 2 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 3 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 4 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 5 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

| Object | Description |
|--|---|
| Hash Code Contributors | |
| Source MAC Address | The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled. |
| Destination MAC Address | The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled. |
| IP Address | The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled. |
| TCP/UDP Port Number | The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled. |
| Aggregation Group Configuration | |
| Group ID | Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port. |
| Port Members | Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group. |

Apply Click to apply changes.

Reset Click to revert to previous values.

LACP

This page allows the user to inspect the current LACP port configurations and possibly change them as well.

LACP Port Configuration

| Port | LACP Enabled | Key | Role | Timeout | Prio |
|------|--------------------------|--------|----------|---------|-------|
| * | <input type="checkbox"/> | <> ▾ | <> ▾ | <> ▾ | 32768 |
| 1 | <input type="checkbox"/> | Auto ▾ | Active ▾ | Fast ▾ | 32768 |
| 2 | <input type="checkbox"/> | Auto ▾ | Active ▾ | Fast ▾ | 32768 |
| 3 | <input type="checkbox"/> | Auto ▾ | Active ▾ | Fast ▾ | 32768 |
| 4 | <input type="checkbox"/> | Auto ▾ | Active ▾ | Fast ▾ | 32768 |
| 5 | <input type="checkbox"/> | Auto ▾ | Active ▾ | Fast ▾ | 32768 |
| 6 | <input type="checkbox"/> | Auto ▾ | Active ▾ | Fast ▾ | 32768 |
| 7 | <input type="checkbox"/> | Auto ▾ | Active ▾ | Fast ▾ | 32768 |
| 8 | <input type="checkbox"/> | Auto ▾ | Active ▾ | Fast ▾ | 32768 |
| 9 | <input type="checkbox"/> | Auto ▾ | Active ▾ | Fast ▾ | 32768 |
| 10 | <input type="checkbox"/> | Auto ▾ | Active ▾ | Fast ▾ | 32768 |
| 11 | <input type="checkbox"/> | Auto ▾ | Active ▾ | Fast ▾ | 32768 |

Apply Reset

| Object | Description |
|--------------|--|
| Port | The switch port number. |
| LACP Enabled | Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner. |
| Key | The Key value incurred by the port, range 1-65535 . The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot. |
| Role | The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to). |
| Timeout | The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet. |
| Prio | The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

Loop Protection

Please note that Loop Protection cannot be used in conjunction with ERPS or STP/RSTP/MSTP on the same switch.

This page allows the user to inspect the current Loop Protection configurations and possibly change them as well.

Loop Protection Configuration

General Settings

Global Configuration

| | | |
|------------------------|-----------|---------|
| Enable Loop Protection | Disable ▼ | |
| Transmission Time | 5 | seconds |
| Shutdown Time | 180 | seconds |

Port Configuration

| Port | Enable | Action | Tx Mode |
|------|-------------------------------------|-----------------|----------|
| * | <input checked="" type="checkbox"/> | <> ▼ | <> ▼ |
| 1 | <input checked="" type="checkbox"/> | Shutdown Port ▼ | Enable ▼ |
| 2 | <input checked="" type="checkbox"/> | Shutdown Port ▼ | Enable ▼ |
| 3 | <input checked="" type="checkbox"/> | Shutdown Port ▼ | Enable ▼ |
| 4 | <input checked="" type="checkbox"/> | Shutdown Port ▼ | Enable ▼ |
| 5 | <input checked="" type="checkbox"/> | Shutdown Port ▼ | Enable ▼ |
| 6 | <input checked="" type="checkbox"/> | Shutdown Port ▼ | Enable ▼ |
| 7 | <input checked="" type="checkbox"/> | Shutdown Port ▼ | Enable ▼ |
| 8 | <input checked="" type="checkbox"/> | Shutdown Port ▼ | Enable ▼ |
| 9 | <input checked="" type="checkbox"/> | Shutdown Port ▼ | Enable ▼ |
| 10 | <input checked="" type="checkbox"/> | Shutdown Port ▼ | Enable ▼ |
| 11 | <input checked="" type="checkbox"/> | Shutdown Port ▼ | Enable ▼ |

| Object | Description |
|---------------------------|--|
| General Settings | |
| Enable Loop Protection | Controls whether loop protections is enabled (as a whole). |
| Transmission Time | The interval between each loop protection PDU sent on each port, valid values are 1 to 10 seconds. |
| Shutdown Time | The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart). |
| Port Configuration | |
| Port | The switch port number of the port. |
| Enable | Controls whether loop protection is enabled on this switch port. |
| Action | Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log or Log Only. |
| Tx Mode | Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's. |
| Apply | Click to apply changes. |

Reset

Click to revert to previous values.

Spanning Tree

Please note that Spanning Tree cannot be used in conjunction with ERPS or Loop Protection on the same switch.

Bridge Settings

This page allows you to configure STP system settings. The settings are used by all STP Bridge Instances in the switch.

STP Bridge Configuration

| Basic Settings | |
|---------------------|---------|
| Protocol Version | RSTP ▼ |
| Bridge Priority | 32768 ▼ |
| Forward Delay | 15 |
| Max Age | 20 |
| Maximum Hop Count | 20 |
| Transmit Hold Count | 6 |

| Advanced Settings | |
|-----------------------------|--------------------------|
| Edge Port BPDU Filtering | <input type="checkbox"/> |
| Edge Port BPDU Guard | <input type="checkbox"/> |
| Port Error Recovery | <input type="checkbox"/> |
| Port Error Recovery Timeout | <input type="text"/> |

Apply Reset

| Object | Description |
|-----------------------|---|
| Basic Settings | |
| Protocol Version | The MSTP / RSTP / STP protocol version setting. Valid values are STP, RSTP and MSTP. |
| Bridge Priority | Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge |
| Forward Delay | The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds. |
| Max Age | The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds |
| Maximum Hop Count | This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops. |
| Transmit Hold Count | The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second. |

| Object | Description |
|-----------------------------|---|
| Advanced Settings | |
| Edge Port BPDU Filtering | Control whether a port explicitly configured as Edge will transmit and receive BPDUs. |
| Edge Port BPDU Guard | Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology. |
| Port Error Recovery | Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot. |
| Port Error Recovery Timeout | The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours). |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

MSTI Mapping

This page allows the user to inspect the current STP MSTI bridge instance priority configurations and possibly change them as well.

MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

| Configuration Identification | |
|------------------------------|-------------------|
| Configuration Name | 00-22-3b-02-05-34 |
| Configuration Revision | 0 |

| MSTI Mapping | |
|--------------|--------------|
| MSTI | VLANs Mapped |
| MSTI1 | |
| MSTI2 | |
| MSTI3 | |
| MSTI4 | |
| MSTI5 | |
| MSTI6 | |
| MSTI7 | |

Apply Reset

| Object | Description |
|-------------------------------------|--|
| Configuration Identification | |
| Configuration Name | The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters. |
| Configuration Revision | The revision of the MSTI configuration named above. This must be an integer between 0 and 65535. |
| MSTI Mapping | |
| MSTI | The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. |
| VLANs Mapped | The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Example: 2,5,20-40. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

MSTI Priorities

This page allows the user to inspect the current STP MSTI bridge instance priority configurations and possibly change them as well.

MSTI Configuration

MSTI Priority Configuration

| MSTI | Priority |
|-------|----------|
| * | <> ▼ |
| CIST | 32768 ▼ |
| MSTI1 | 32768 ▼ |
| MSTI2 | 32768 ▼ |
| MSTI3 | 32768 ▼ |
| MSTI4 | 32768 ▼ |
| MSTI5 | 32768 ▼ |
| MSTI6 | 32768 ▼ |
| MSTI7 | 32768 ▼ |

| Object | Description |
|------------|---|
| MSTI | The bridge instance. The CIST is the default instance, which is always active. |
| Priorities | Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

CIST Ports

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well.

This page contains settings for physical and aggregated ports.

STP CIST Port Configuration

CIST Aggregated Port Configuration

| Port | STP Enabled | Path Cost | Priority | Admin Edge | Auto Edge | Restricted Role | TCN | BPDU Guard | Point-to-point |
|------|-------------------------------------|-----------|----------|------------|-------------------------------------|--------------------------|--------------------------|--------------------------|----------------|
| - | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Forced True |

CIST Normal Port Configuration

| Port | STP Enabled | Path Cost | Priority | Admin Edge | Auto Edge | Restricted Role | TCN | BPDU Guard | Point-to-point |
|------|-------------------------------------|-----------|----------|------------|-------------------------------------|--------------------------|--------------------------|--------------------------|----------------|
| * | <input checked="" type="checkbox"/> | <> | <> | <> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <> |
| 1 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 2 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 3 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 4 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 5 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 6 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 7 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 8 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 9 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 10 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 11 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |

Apply Reset

| Object | Description |
|-----------------------|--|
| Port | The switch port number of the logical STP port. |
| STP Enabled | Controls whether STP is enabled on this switch port. |
| Path Cost | Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000. |
| Priority | Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). |
| operEdge (state flag) | Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status. |
| AdminEdge | Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized). |
| AutoEdge | Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not. |
| Restricted Role | If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard. |

| Object | Description |
|----------------|---|
| Restricted TCN | If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently. |
| BPDU Guard | If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well. |
| Point-to-Point | Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

MSTI Ports

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well.

An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports.

MSTI Port Configuration



The screenshot shows a web interface for MSTI Port Configuration. At the top, there is a blue button labeled "Select MSTI". Below it is a dropdown menu currently showing "MST1" with a downward arrow. To the right of the dropdown is a button labeled "Get".

Click "Get" to retrieve settings for a specific MSTI, the page displayed as follow.

MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

| Port | Path Cost | Priority |
|------|-----------|----------|
| - | Auto ▼ | 128 ▼ |

MSTI Normal Ports Configuration

| Port | Path Cost | Priority |
|------|-----------|----------|
| * | <> ▼ | <> ▼ |
| 1 | Auto ▼ | 128 ▼ |
| 2 | Auto ▼ | 128 ▼ |
| 3 | Auto ▼ | 128 ▼ |
| 4 | Auto ▼ | 128 ▼ |
| 5 | Auto ▼ | 128 ▼ |
| 6 | Auto ▼ | 128 ▼ |
| 7 | Auto ▼ | 128 ▼ |
| 8 | Auto ▼ | 128 ▼ |
| 9 | Auto ▼ | 128 ▼ |
| 10 | Auto ▼ | 128 ▼ |
| 11 | Auto ▼ | 128 ▼ |

| Object | Description |
|-----------|--|
| Port | The switch port number of the corresponding STP CIST (and MSTI) port. |
| Path Cost | Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000. |
| Priority | Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Get | Click to retrieve settings for a specific MSTI. |

IPMC Profile

Profile Table

This page provides IPMC Profile related configurations.

The IPMC profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each.

IPMC Profile Configurations

Global Profile Mode Disabled ▾

IPMC Profile Table Setting

| Delete | Profile Name | Profile Description | Rule |
|--------|--------------|---------------------|---|
| Delete | | |   |

Add New IPMC Profile

Apply Reset

| Object | Description |
|----------------------|--|
| Global Profile Mode | Enable/Disable the Global IPMC Profile. System starts to do filtering based on profile settings only when the global profile mode is enabled. |
| Delete | Check to delete the entry. The designated entry will be deleted during the next save. |
| Profile Name | The name used for indexing the profile table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present. |
| Profile Description | Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile. No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence. |
| Rule | When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons: "Eye": List the rules associated with the designated profile. "e": Adjust the rules associated with the designated profile. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Add New IPMC Profile | Click to add a new profile. Specify the name and configure the new entry, then click "Apply". |

IPMC Profile Rule Settings

This page provides the filtering rule settings for a specific IPMC profile. It displays the configured rule entries in precedence order. First rule entry has highest priority in lookup, while the last rule entry has lowest priority in lookup.

IPMC Profile [Test] Rule Settings (In Precedence Order)

| Profile Name & Index | Entry Name | Address Range | Action | Log | |
|----------------------|------------|---------------|----------|-----------|--|
| Test | 1 | - ▾ | ~ Deny ▾ | Disable ▾ | |

Add Last Rule

Commit

Reset

| Object | Description |
|-------------------------|--|
| Profile Name | The name of the designated profile to be associated. This field is not editable. |
| Entry Name | The name used in specifying the address range used for this rule. Only the existing profile address entries will be chosen in the selected box. This field is not allowed to be selected as none ("-") while the Rule Settings Table is committed. |
| Address Range | The corresponding address range of the selected profile entry. This field is not editable and will be adjusted automatically according to the selected profile entry. |
| Action | Indicates the learning action upon receiving the Join/Report frame that has the group address matches the address range of the rule. Permit: Group address matches the range specified in the rule will be learned. Deny: Group address matches the range specified in the rule will be dropped. |
| Log | Indicates the logging preference upon receiving the Join/Report frame that has the group address matches the address range of the rule. Enable: Corresponding information of the group address, that matches the range specified in the rule, will be logged. Disable: Corresponding information of the group address, that matches the range specified in the rule, will not be logged. |
| Rule Management Buttons | You can manage rules and the corresponding precedence order by using the following buttons: Insert: Insert a new rule before the current entry of rule. Delete: Delete the current entry of rule. Up: Moves the current entry of rule up in the list. Down: Moves the current entry of rule down in the list. |
| Add Last Rule | Click to add a new rule in the end of the specific profile's rule list. Specify the address entry and configure the new entry. Click "Commit" |
| Commit | Click to commit rule changes for the designated profile. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

Address Entry

This page provides address range settings used in IPMC profile.

The address entry is used to specify the address range that will be associated with IPMC Profile. It is allowed to create at maximum 128 address entries in the system.

IPMC Profile Address Configuration Refresh |<< >>

Navigate Address Entry Setting in IPMC Profile by entries per page.

| Delete | Entry Name | Start Address | End Address |
|--------|------------|---------------|-------------|
| Delete | | | |

| Object | Description |
|-------------------------------|--|
| Delete | Check to delete the entry. The designated entry will be deleted during the next save. |
| Entry Name | The name used for indexing the address entry table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present. |
| Start Address | The starting IPv4/IPv6 Multicast Group Address that will be used as an address range. |
| End Address | The ending IPv4/IPv6 Multicast Group Address that will be used as an address range. |
| Add New Address (Range) Entry | Click to add new address range. Specify the name and configure the addresses, then click "Apply". |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Refresh | Click to refresh the table starting from input fields. |
| << | Click to update the table starting from the first entry in the IPMC Profile Address Configuration. |
| >> | Click to update the table starting with the entry after the last entry currently displayed. |

MVR

This page provides MVR related configurations.

The MVR feature enables multicast traffic forwarding on the Multicast VLANs.

In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

It is allowed to create at maximum 4 MVR VLANs with corresponding channel profile for each Multicast VLAN. The channel profile is defined by the IPMC Profile which provides the filtering conditions.

MVR Configurations

MVR Mode: Disabled

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

| Delete | MVR VID | MVR Name | IGMP Address | Mode | Tagging | Priority | LLQI | Interface Channel Profile |
|--------|-------------------------|----------|--------------|---------|---------|----------|------|---------------------------|
| Delete | | | 0.0.0.0 | Dynamic | Tagged | 0 | 5 | |
| Port | 1 2 3 4 5 6 7 8 9 10 11 | | | | | | | |
| Role | | | | | | | | |

Add New MVR VLAN

Immediate Leave Setting

| Port | Immediate Leave |
|------|-----------------|
| 1 | Disabled |
| 2 | Disabled |
| 3 | Disabled |
| 4 | Disabled |
| 5 | Disabled |
| 6 | Disabled |
| 7 | Disabled |
| 8 | Disabled |
| 9 | Disabled |
| 10 | Disabled |
| 11 | Disabled |

Apply Reset

| Object | Description |
|----------|---|
| MVR Mode | Enable/Disable the Global MVR. The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full. |
| Delete | Check to delete the entry. The designated entry will be deleted during the next save. |
| MVR VID | Specify the Multicast VLAN ID. Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports. |
| MVR Name | MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 16. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries. |

| Object | Description |
|---------------------------|--|
| IGMP Address | Define the IPv4 address as source address used in IP header for IGMP control frames. The default IGMP address is not set (0.0.0.0). When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1. |
| Mode | Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode. |
| Tagging | Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged. |
| Priority | Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0. |
| LLQI | Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a second. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second. |
| Interface Channel Profile | When the MVR VLAN is created, select the IPMC Profile as the channel filtering condition for the specific MVR VLAN. Summary about the Interface Channel Profiling (of the MVR VLAN) will be shown by clicking the view button. Profile selected for designated interface channel is not allowed to have overlapped permit group address. |
| Profile Management Button | You can inspect the rules of the designated profile by using the following button: : List the rules associated with the designated profile. |
| Port | The logical port for the settings. |
| Port Role | Configure an MVR port of the designated MVR VLAN as one of the following roles. Inactive: The designated port does not participate MVR operations. Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. Receiver: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages. Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports. Select the port role by clicking the Role symbol to switch the setting. I indicates Inactive; S indicates Source; R indicates Receiver The default Role is Inactive. |
| Immediate Leave | Enable the fast leave on the port. |
| Add New MVR VLAN | Click to add a new MVR VLAN. Specify the VID and configure the new entry, then click "Apply". |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

IPMC

IGMP Snooping

Basic Configuration

This page provides IGMP Snooping related configuration.

IGMP Snooping Configuration

| Global Configuration | |
|--------------------------------------|-------------------------------------|
| Snooping Enabled | <input type="checkbox"/> |
| Unregistered IPMCv4 Flooding Enabled | <input checked="" type="checkbox"/> |
| IGMP SSM Range | 232.0.0.0 / 8 |
| Leave Proxy Enabled | <input type="checkbox"/> |
| Proxy Enabled | <input type="checkbox"/> |

Port Related Configuration

| Port | Router Port | Fast Leave | Throttling |
|------|--------------------------|--------------------------|-------------|
| * | <input type="checkbox"/> | <input type="checkbox"/> | <> ▼ |
| 1 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited ▼ |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited ▼ |
| 3 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited ▼ |
| 4 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited ▼ |
| 5 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited ▼ |
| 6 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited ▼ |
| 7 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited ▼ |
| 8 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited ▼ |
| 9 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited ▼ |
| 10 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited ▼ |
| 11 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited ▼ |

| Object | Description |
|--------------------------------------|--|
| Snooping Enabled | Enable the Global IGMP Snooping. |
| Unregistered IPMCv4 Flooding Enabled | Enable unregistered IPMCv4 traffic flooding. The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting. |
| IGMP SSM Range | SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. |
| Leave Proxy Enabled | Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side. |
| Proxy Enabled | Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side. |
| Router Port | Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port. |
| Fast Leave | Enable the fast leave on the port. |
| Throttling | Enable to limit the number of multicast groups to which a switch port can belong. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

VLAN Configuration

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the “entries per page” input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN ID Table.

The “VLAN” input fields allow the user to select the starting point in the VLAN Table.

IGMP Snooping VLAN Configuration Refresh | << >>

Start from VLAN with entries per page.












| Delete | VLAN ID | Snooping Enabled | Querier Election | Querier Address | Compatibility | PRI | RV | QI (sec) | QRI (0.1 sec) | LLQI (0.1 sec) | URI (sec) |
|--------|---------|--------------------------|-------------------------------------|-----------------|---------------|-----|----|----------|---------------|----------------|-----------|
| Delete | | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0.0.0.0 | IGMP-Auto | 0 | 2 | 125 | 100 | 10 | 1 |

| Object | Description |
|-----------------------|--|
| Delete | Check to delete the entry. The designated entry will be deleted during the next save. |
| VLAN ID | The VLAN ID of the entry. |
| IGMP Snooping Enabled | Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping. |
| Querier Election | Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier. |
| Querier Address | Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1. |
| Compatibility | Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto. |
| PRI | Priority of Interface. It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0. |
| RV | Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255, default robustness variable value is 2. |
| QI | Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds. |
| QRI | Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds). |

| Object | Description |
|---------------------|--|
| LLQI(LMQI for IGMP) | Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second). |
| URI | Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second. |
| Add New IGMP VLAN | Click to add A new IGMP VLAN. Specify the VID and configure the new entry, then click "Apply". The specific IGMP VLAN starts working after the corresponding static VLAN is created. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Refresh | Click to refresh the table starting from VLAN input fields. |
| << | Click to update the table starting from the first entry in the VLAN Table (VLAN ID). |
| >> | Click to update the table starting with the entry after the last entry currently displayed. |

Port Filtering Profile

IGMP Snooping Port Filtering Profile Configuration

| Port | Filtering Profile |
|------|---|
| 1 |  - ▾ |
| 2 |  - ▾ |
| 3 |  - ▾ |
| 4 |  - ▾ |
| 5 |  - ▾ |
| 6 |  - ▾ |
| 7 |  - ▾ |
| 8 |  - ▾ |
| 9 |  - ▾ |
| 10 |  - ▾ |
| 11 |  - ▾ |

Apply Reset

| Object | Description |
|---------------------------|---|
| Port | The logical port for the settings. |
| Filtering Profile | Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button. |
| Profile Management Button | You can inspect the rules of the designated profile by using the following button "Eye": List the rules associated with the designated profile. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

MLD Snooping

Basic Configuration

This page provides MLD Snooping related configuration.

MLD Snooping Configuration

| Global Configuration | |
|--------------------------------------|-------------------------------------|
| Snooping Enabled | <input type="checkbox"/> |
| Unregistered IPMCv6 Flooding Enabled | <input checked="" type="checkbox"/> |
| MLD SSM Range | ff3e.. / 96 |
| Leave Proxy Enabled | <input type="checkbox"/> |
| Proxy Enabled | <input type="checkbox"/> |

Port Related Configuration

| Port | Router Port | Fast Leave | Throttling |
|------|--------------------------|--------------------------|------------|
| ^ | <input type="checkbox"/> | <input type="checkbox"/> | <> |
| 1 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited |
| 3 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited |
| 4 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited |
| 5 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited |
| 6 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited |
| 7 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited |
| 8 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited |
| 9 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited |
| 10 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited |
| 11 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited |

Apply Reset

| Object | Description |
|-------------------------------------|--|
| Snooping Enable | Enable the Global MLD Snooping. |
| Unregistered IPMCv6 Flooding Enable | Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting. |
| MLD SSM Range | SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. |
| Leave Proxy Enable | Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side. |
| Proxy Enable | Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side. |
| Router Port | Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port. |
| Fast Leave | Enable the fast leave on the port. |
| Throttling | Enable to limit the number of multicast groups to which a switch port can belong. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

VLAN Configuration

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the “entries per page” input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The “VLAN” input fields allow the user to select the starting point in the VLAN Table.

MLD Snooping VLAN Configuration Refresh | << | >>

Start from VLAN with entries per page.












| Delete | VLAN ID | Snooping Enabled | Querier Election | Compatibility | PRI | RV | QI (sec) | QRI (0.1 sec) | LLQI (0.1 sec) | URI (sec) |
|--------|---------|--------------------------|-------------------------------------|---------------|-----|----|----------|---------------|----------------|-----------|
| Delete | | <input type="checkbox"/> | <input checked="" type="checkbox"/> | MLD-Auto | 0 | 2 | 125 | 100 | 10 | 1 |

| Object | Description |
|----------------------|--|
| Delete | Check to delete the entry. The designated entry will be deleted during the next save. |
| VLAN ID | The VLAN ID of the entry. |
| MLD Snooping Enabled | Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping. |
| Querier Election | Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier. |
| Compatibility | Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is MLD-Auto, Forced MLDv1, Forced MLDv2, default compatibility value is MLD-Auto. |
| PRI | Priority of Interface. It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0. |
| RV | Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a link. The allowed range is 1 to 255, default robustness variable value is 2. |
| QI | Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds. |
| QRI | Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds). |
| LLQI | Last Listener Query Interval. The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The allowed range is 0 to 31744 in tenths of seconds, default last listener query interval is 10 in tenths of seconds (1 second). |

| Object | Description |
|------------------|---|
| URI | Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second. |
| Add New MLD VLAN | Click to add A new MLD VLAN. Specify the VID and configure the new entry, then click "Apply". The specific MLD VLAN starts working after the corresponding static VLAN is created. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Refresh | Click to refresh the table starting from VLAN input fields. |
| << | Click to update the table starting from the first entry in the VLAN Table (lowest VLAN ID). |
| >> | Click to update the table starting with the entry after the last entry currently displayed. |

Port Filtering Profile

MLD Snooping Port Filtering Profile Configuration

| Port | Filtering Profile |
|------|---|
| 1 |  - ▼ |
| 2 |  - ▼ |
| 3 |  - ▼ |
| 4 |  - ▼ |
| 5 |  - ▼ |
| 6 |  - ▼ |
| 7 |  - ▼ |
| 8 |  - ▼ |
| 9 |  - ▼ |
| 10 |  - ▼ |
| 11 |  - ▼ |

| Object | Description |
|---------------------------|---|
| Port | The logical port for the settings. |
| Filtering Profile | Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button. |
| Profile Management Button | You can inspect the rules of the designated profile by using the following button "Eye": List the rules associated with the designated profile. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

LLDP

LLDP

This page allows the user to inspect and configure the current LLDP port setting.

LLDP Configuration

LLDP Parameters

| | | |
|-------------|----|---------|
| Tx Interval | 30 | seconds |
| Tx Hold | 4 | times |
| Tx Delay | 2 | seconds |
| Tx Reinit | 2 | seconds |

LLDP Interface Configuration

| Interface | Mode | CDP aware | Optional TLVs | | | | |
|-----------|-----------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | | | Port Descr | Sys Name | Sys Descr | Sys Capa | Mgmt Addr |
| * | <> ▼ | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 1 | Enabled ▼ | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2 | Enabled ▼ | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3 | Enabled ▼ | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 4 | Enabled ▼ | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 5 | Enabled ▼ | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 6 | Enabled ▼ | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 7 | Enabled ▼ | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 8 | Enabled ▼ | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 9 | Enabled ▼ | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 10 | Enabled ▼ | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 11 | Enabled ▼ | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Apply Reset

| Object | Description |
|--------|-------------|
|--------|-------------|

LLDP Parameters

| | |
|-------------|---|
| Tx Interval | The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds. |
| Tx Hold | Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times. |
| Tx Delay | If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds. |
| Tx Reinit | When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds. |

LLDP Port Parameters

| | |
|-----------|--|
| Interface | The switch port number of the logical LLDP port. |
|-----------|--|

| Object | Description |
|------------|--|
| Mode | <p>Select LLDP mode.</p> <p>Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.</p> <p>Tx only The switch will drop LLDP information received from neighbors, but will send out LLDP information.</p> <p>Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors.</p> <p>Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbors.</p> |
| CDP Aware | <p>Select CDP awareness.</p> <p>The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled.</p> <p>Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.</p> <p>CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.</p> <p>CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table.</p> <p>CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.</p> <p>CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.</p> <p>Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.</p> <p>If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.</p> <p>Note: When CDP awareness on a port is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.</p> |
| Port Descr | Optional TLV: When checked the "port description" is included in LLDP information transmitted. |
| Sys Name | Optional TLV: When checked the "system name" is included in LLDP information transmitted. |
| Sys Descr | Optional TLV: When checked the "system description" is included in LLDP information transmitted. |
| Sys Capa | Optional TLV: When checked the "system capability" is included in LLDP information transmitted. |
| Mgmt Addr | Optional TLV: When checked the "management address" is included in LLDP information transmitted. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

PoE

This page allows the user to inspect and configure the current PoE port settings.

Power Over Ethernet Configuration

| | | | |
|------------------------------|---|---|--------------------------------|
| Reserved Power determined by | <input checked="" type="radio"/> Class | <input type="radio"/> Allocation | <input type="radio"/> LLDP-MED |
| Power Management Mode | <input type="radio"/> Actual Consumption | <input checked="" type="radio"/> Reserved Power | |
| Capacitor Detection | <input checked="" type="radio"/> Disabled | <input type="radio"/> Enabled | |

PoE Power Supply Configuration

| | |
|--------------------------|-----|
| Primary Power Supply [W] | 360 |
|--------------------------|-----|

PoE Port Configuration

| Port | PoE Mode | Priority | Maximum Power [W] |
|------|----------|----------|-------------------|
| * | <> | <> | 60 |
| 1 | PoE++ | Low | 60 |
| 2 | PoE++ | Low | 60 |
| 3 | PoE++ | Low | 60 |
| 4 | PoE++ | Low | 60 |
| 5 | PoE+ | Low | 30 |
| 6 | PoE+ | Low | 30 |
| 7 | PoE+ | Low | 30 |
| 8 | PoE+ | Low | 30 |

Apply Reset

| Object | Description |
|-------------------------------------|---|
| Reserved Power determined by | |
| Allocated mode | In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields. |
| Class mode | In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts. In this mode the Maximum Power fields have no effect. |
| LLDP-MED mode | This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode. In this mode the Maximum Power fields have no effect. |
| Power Management Mode | |
| Actual Consumption | In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down. |
| Reserved Power | In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply. |

Power Supply Configuration

| Object | Description |
|---------------------------|--|
| Power Source | For being able to determine the amount of power the PD may use, it must be defined what amount of power a power source can deliver. Valid values are in the range 0 to 360 Watts (depending on model). |
| Port Configuration | |
| Port | This is the logical port number for this row. Ports that are not PoE-capable are grayed out or not listed and thus impossible to configure PoE for. |
| PoE Mode | |
| Disable | PoE disabled for the port. |
| PoE | Enables IEEE 802.3af PoE protocol for maximum 15.4W per port. |
| PoE+ | Enables IEEE 802.3at PoE protocol for maximum 30W per port. |
| PoE++ | Enables 60W PoE per port (HO models only). |
| Forced | Enables 60W PoE Force mode per port (HO models only). |
| Priority | The priority is used in the case where the remote devices require more power than the power supply can deliver. In this case the port with the lowest priority will be turned off starting from the port with the highest port number. |
| Low | The lowest priority |
| High | The medium priority |
| Critical | The highest priority |
| Maximum Power | The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device. The maximum power for each port is 30 W or 60 W depending on model and port number. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

Warning - Please use the Forced mode feature with caution and ensure it's only enabled when a 60 W PoE device is attached. It should only be enabled if the 60 W devices fail to power up without this option enabled.

EPS

The Ethernet (Linear) Protection Switch instances are configured here.

Ethernet Protection Switching Refresh

| Delete | EPS ID | Domain | Architecture | W Flow | P Flow | W SF MEP | P SF MEP | APS MEP | Alarm |
|--------|--------|--------|--------------|--------|--------|----------|----------|---------|-------|
| Delete | 1 | Port ▼ | 1+1 ▼ | 1 | 1 | 1 | 1 | 1 | |

| Object | Description |
|--------------|---|
| Delete | This box is used to mark an EPS for deletion in next Save operation. |
| EPS ID | The ID of the EPS. Click on the ID of an EPS to enter the configuration page. |
| Domain | Port: This will create a EPS in the Port Domain. 'W/P Flow' is a Port. |
| Architecture | 1+1: This will create a 1+1 EPS. 1:1: This will create a 1:1 EPS. |
| W Flow | The working flow for the EPS - See 'Domain'. |
| P Flow | The protecting flow for the EPS - See 'Domain'. |
| W SF MEP | The working Signal Fail reporting MEP. |
| P SF MEP | The protecting Signal Fail reporting MEP. |
| APS MEP | The APS PDU handling MEP. |
| Alarm | There is an active alarm on the EPS. |
| Add New EPS | Click to add a new EPS entry. |
| Refresh | Click to refresh the page immediately. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

Ethernet Protection Switch Configuration

This page allows the user to inspect and configure the current EPS Instance.

EPS Configuration

Instance Data

| EPS ID | Domain | Architecture | W Flow | P Flow | W SF MEP | P SF MEP | APS MEP |
|--------|--------|--------------|--------|--------|----------|----------|---------|
| 1 | Port | 1+1 | 1 | 2 | 5 | 6 | 1 |

Instance Configuration

| Protection Type | APS | Revertive | WTR Time | Hold Off Time |
|------------------|--------------------------|--------------------------|----------|---------------|
| Unidirectional ▾ | <input type="checkbox"/> | <input type="checkbox"/> | 300 | 0 |

Instance Command

| Command |
|---------|
| None ▾ |

Instance State

| Protection State | W Flow | P Flow | Transmit APS r/b | Receive APS r/b | Architecture Mismatch | APS On Working | Switching Incomplete | No Aps Received |
|------------------|--------|--------|------------------|-----------------|-----------------------|----------------|----------------------|-----------------|
| Disabled | OK | OK | NR Null/Null | NR Null/Null | | | | |

| Object | Description |
|-------------------------------|---|
| Instance Data | |
| EPS ID | The ID of the EPS. Click on the ID of an EPS to enter the configuration page. |
| Domain | Port: This will create a EPS in the Port Domain. 'W/P Flow' is a Port. |
| Architecture | 1+1: This will create a 1+1 EPS. 1:1: This will create a 1:1 EPS. |
| W Flow | The working flow for the EPS - See 'Domain'. |
| P Flow | The protecting flow for the EPS - See 'Domain'. |
| W SF MEP | The working Signal Fail reporting MEP. |
| P SF MEP | The protecting Signal Fail reporting MEP. |
| APS MEP | The APS PDU handling MEP. |
| Instance Configuration | |
| Configured | Red: This EPS is only created and has not yet been configured - is not active. Green: This EPS is configured - is active. |
| Protection Type | Unidirectional: EPS in the two ends can select traffic from different working/protecting flow. This is only possible in case of 1+1. Bidirectional: EPS in the two ends is selecting traffic from the same working/protecting flow. This requires APS enabled. This is mandatory for 1:1 |
| APS | The Automatic Protection Switching protocol can be enabled/disabled. This is mandatory for 1:1. |
| Revertive | The revertive switching to working flow can be enabled/disabled. |
| WTR Time | The Wait To Restore timing value to be used in revertive switching. Range is 1 to 720 seconds. |
| Hold Off Time | The timing value to be used to make persistent check on Signal Fail before switching. This is in 100 ms. and the max value is 100 (10 sec). |
| Instance Command | |

| Object | Description |
|-----------------------|---|
| Command | <p>None: There is no active local command on this instance.</p> <p>Clear: The active local command will be cleared.</p> <p>Lock Out: This EPS is locked to working (not active). In case of 1:N (more than one EPS with same protecting flow) - when one EPS switch to protecting flow, other EPS is enforced this command</p> <p>Forced Switch: Forced switch to protecting.</p> <p>Manual Switch P: Manual switch to protecting.</p> <p>Manual Switch W: Manual switch to working. This is only allowed in case of 'non-revertive' mode</p> <p>Exercise: Exercise of the protocol - not traffic effecting. This is only allowed in case of 'Bidirectional' protection type</p> <p>Freeze: This EPS is locally frozen - ignoring all input.</p> <p>Lock Out Local: This EPS is locally "locked out" - ignoring local SF detected on working.</p> |
| Instance State | |
| Protection State | EPS state according to State Transition Tables in G.8031. |
| W Flow | <p>OK: State of working flow is ok</p> <p>SF: State of working flow is Signal Fail</p> <p>SD: State of working flow is Signal Degrade (for future use)</p> |
| P Flow | <p>OK: State of protecting flow is ok</p> <p>SF: State of protecting flow is Signal Fail</p> <p>SD: State of protecting flow is Signal Degrade (for future use)</p> |
| Transmit APS r/b | The transmitted APS according to State Transition Tables in G.8031. |
| Receive APS r/b | The received APS according to State Transition Tables in G.8031. |
| Architecture Mismatch | The architecture indicated in the received APS does not match the locally configured. |
| APS on working | APS is received on the working flow. |
| Switching Incomplete | Traffic is not selected from the same flow instance in the two ends. |
| No APS Received | APS PDU is not received from the other end. |
| Refresh | Click to refresh the page immediately. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

MEP

The Maintenance Entity Point instances are configured here.

Maintenance Entity Point

| Delete | Instance | Domain | Mode | Direction | Residence Port | Level | Flow Instance | Tagged VID | This MAC | Alarm |
|--------------------------|----------|--------|------|-----------|----------------|-------|---------------|------------|-------------------|-------|
| <input type="checkbox"/> | 1 | Port | Mep | Down | 1 | 0 | | 0 | 00-22-3B-02-07-BD | |

| Object | Description |
|----------------|--|
| Delete | This box is used to mark a MEP for deletion in next Save operation. |
| Instance | The ID of the MEP. Click on the ID of a MEP to enter the configuration page. The range is from 1 through 100. |
| Domain | Port: This is a MEP in the Port Domain. EVC: This is a MEP in the EVC Domain. 'Flow Instance' is an EVC. The EVC must be created VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. In case of Up-MEP the VLAN must be created MPLS Link: This is a MEP in the MPLS Link Domain. MPLS Tunnel: This is a MEP in the MPLS Tunnel Domain. MPLS PW: This is a MEP in the MPLS Pseudo Wires Domain. MPLS LSP: This is a MEP in the MPLS LSP Domain. |
| Mode | MEP: This is a Maintenance Entity End Point. MIP: This is a Maintenance Entity Intermediate Point. |
| Direction | Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'. Up: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'. |
| Residence Port | The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member. |
| Level | The MEG level of this MEP. |
| Flow Instance | The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP. |
| Tagged VID | Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added. EVC MEP: This is not used. VLAN MEP: This is not used. EVC MIP: On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active. |
| This MAC | The MAC of this MEP - can be used by other MEP when unicast is selected (Info only). |
| Alarm | There is an active alarm on the MEP. |
| Add New MEP | Click to add a new MEP entry. |
| Refresh | Click to refresh the page immediately. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

Maintenance Entity End Point Configuration

This page allows the user to inspect and configure the current MEP Instance.

MEP Configuration Refresh

Instance Data

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|----------|--------|------|-----------|----------------|---------------|------------|--------------|-------------------|
| 1 | Port | Mep | Down | 1 | | 0 | 0 | 00-22-38-02-07-BD |

Instance Configuration

| Level | Format | Domain Name | MEG Id | MEP Id | Tagged VID | Syslog | cLevel | cMEG | cMEP | cAIS | cLCK | cLoop | cConfig | cSSF | aBLK | aTSF |
|-------|---------|-------------|---------------|--------|------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 0 | ITU ICC | | ICC000MEC0000 | 1 | 0 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Peer MEP Configuration

| Delete | Peer MEP ID | Unicast Peer MAC | cLOC | cRDI | cPeriod | cPriority |
|-------------------|-------------|-------------------|------|------|---------|-----------|
| No Peer MEP Added | | | | | | |
| Delete | 0 | 00-00-00-00-00-00 | | | | |

Functional Configuration

| Continuity Check | | | | APS Protocol | | | | |
|--------------------------|----------|------------|--------------------------|--------------------------|----------|-------|-------|------------|
| Enable | Priority | Frame rate | TLV | Enable | Priority | Cast | Type | Last Octet |
| <input type="checkbox"/> | 0 | 1 f/sec | <input type="checkbox"/> | <input type="checkbox"/> | 0 | Multi | L-APS | 1 |

TLV Configuration

| Organization Specific TLV (Global) | | | | |
|------------------------------------|------------|-----------|----------|-------|
| OUI First | OUI Second | OUI Third | Sub-Type | Value |
| 0 | 0 | 12 | 1 | 2 |

TLV Status

| Peer MEP ID | CC Organization Specific | | | | | | CC Port Status | | CC Interface Status | |
|-------------|--------------------------|------------|-----------|----------|-------|---------|----------------|---------|---------------------|---------|
| | OUI First | OUI Second | OUI Third | Sub-Type | Value | Last RX | Value | Last RX | Value | Last RX |
| | | | | | | | | | | |

Link State Tracking

| Object | Description |
|----------------------|--|
| Instance Data | |
| MEP Instance | The ID of the MEP. |
| Domain | Port: This is a MEP in the Port Domain. EVC: This is a MEP in the EVC Domain. 'Flow Instance' is an EVC. The EVC must be created VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. In case of Up-MEP the VLAN must be created MPLS Link: This is a MEP in the MPLS Link Domain. MPLS Tunnel: This is a MEP in the MPLS Tunnel Domain. MPLS PW: This is a MEP in the MPLS Pseudo Wires Domain. MPLS LSP: This is a MEP in the MPLS LSP Domain. |
| Mode | MEP: This is a Maintenance Entity End Point. MIP: This is a Maintenance Entity Intermediate Point. |
| Direction | Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'. Up: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'. |
| Residence Port | The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member. |
| Flow Instance | The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP. |

| Object | Description |
|------------|---|
| Tagged VID | Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added. EVC MEP: This is not used. VLAN MEP: This is not used. EVC MIP: On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active. |
| This MAC | The MAC of this MEP - can be used by other MEP when unicast is selected (Info only). |

Instance Configuration

| | |
|---------------|---|
| EVC Policy ID | This is the Policy number of the relevant ECE. Policy ID is used to assure that received OAM PDU is able to hit a IS2 entry. If this value is '0' IS2 rules will be created on classified VID. If this is NOT '0' IS2 rules will be created on this Policy (PAG). This must be equal to ECE Policy Number if OAM PDU will hit the ECE ISO. This is the case if an ECE is created with 'tag_type' as 'any'. |
| EVC QoS | This is only relevant for a EVC MEP. This is the QoS of the EVC and used for getting QoS counters for Loss Measurement. |
| Level | See help on MEP create WEB. |
| Format | This is the configuration of the two possible Maintenance Association Identifier formats. ITU ICC: This is defined by ITU (Y1731 Fig. A3). 'Domain Name' is not used. 'MEG id' must be max. 13 char. IEEE String: This is defined by IEEE (802.1ag Section 21.6.5). 'Domain Name' can be max. 16 char. 'MEG id' (Short MA Name) can be max. 16 char. ITU CC ICC: This is defined by ITU (Y1731 Fig. A5). 'Domain Name' is not used. 'MEG id' must be max. 15 char. |
| Domain Name | This is the IEEE Maintenance Domain Name and is only used in case of 'IEEE String' format. This string can be empty giving Maintenance Domain Name Format 1 - Not present. This can be max 16 char. |
| MEG Id | This is either ITU MEG ID or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this must be 13 char. In case of ITU CC ICC format this must be 15 char. In case of IEEE String format this can be max 16 char. |
| MEP Id | This value will become the transmitted two byte CCM MEP ID. |
| Tagged VID | This value will be the VID of a TAG added to the OAM PDU. |
| VOE | This will attempt to utilize VOE HW for MEP implementation. Not all platforms support VOE. |
| cLevel | Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP. |
| cMEG | Fault Cause indicating that a CCM is received with a MEG ID different from configured for this MEP. |
| cMEP | Fault Cause indicating that a CCM is received with a MEP ID different from all 'Peer MEP ID' configured for this MEP. |
| cAIS | Fault Cause indicating that AIS PDU is received. |
| cLCK | Fault Cause indicating that LCK PDU is received. |
| cSSF | Fault Cause indicating that server layer is indicating Signal Fail. |
| aBLK | The consequent action of blocking service frames in this flow is active. |
| aTSF | The consequent action of indicating Trail Signal Fail to-wards protection is active. |

Peer MEP Configuration

| | |
|-------------|---|
| Delete | This box is used to mark a Peer MEP for deletion in next Save operation. |
| Peer MEP ID | This value will become an expected MEP ID in a received CCM - see 'cMEP'. |

| Object | Description |
|------------------|--|
| Unicast Peer MAC | This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP. |
| cLOC | Fault Cause indicating that no CCM has been received (in 3,5 periods) - from this peer MEP. |
| cRDI | Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP. |
| cPeriod | Fault Cause indicating that a CCM is received with a period different what is configured for this MEP - from this peer MEP. |
| cPriority | Fault Cause indicating that a CCM is received with a priority different what is configured for this MEP - from this peer MEP. |

Add New Peer MEP Click to add a new peer MEP.

Functional Configuration

Continuity Check

| | |
|------------|--|
| Enable | Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1. |
| Priority | The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same. |
| Frame rate | Selecting the frame rate of CCM PDU. This is the inverse of transmission period as described in Y.1731. This value has the following uses: <ul style="list-style-type: none"> * The transmission rate of the CCM PDU. * Fault Cause cLOC is declared if no CCM PDU has been received within 3.5 periods - see 'cLOC'. * Fault Cause cPeriod is declared if a CCM PDU has been received with different period - see 'cPeriod'. Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same. |
| TLV | Enable/disable of TLV insertion in the CCM PDU. |

APS Protocol

| | |
|-----------------------------------|--|
| Enable | Automatic Protection Switching protocol information transportation based on transmitting/receiving R-APS/L-APS PDU can be enabled/disabled. Must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured. |
| Priority | The priority to be inserted as PCP bits in TAG (if any). |
| Cast | Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. Unicast is only valid for L-APS - see 'Type'. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032. |
| Type | R-APS: APS PDU is transmitted as R-APS - this is for ERPS. L-APS: APS PDU is transmitted as L-APS - this is for ELPS. |
| Last Octet | This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031 (03/2010) a RAPS multi-cast MAC is defined as 01-19-A7-00-00-XX. In current standard the value for this last octet is '01' and the usage of other values is for further study. |
| TLV Configuration | Configuration of the OAM PDU TLV. Currently only TLV in the CCM is supported. |
| Organization Specific - OUI First | The transmitted first value in the OS TLV OUI field. |

| Object | Description |
|---------------------------------------|--|
| Organization Specific - OUI Second | The transmitted second value in the OS TLV OUI field. |
| Organization Specific - OUI Third | The transmitted third value in the OS TLV OUI field. |
| Organization Specific - Sub-Type | The transmitted value in the OS TLV Sub-Type field. |
| Organization Specific - Value | The transmitted value in the OS TLV Value field. |
| TLV Status | Display of the last received TLV. Currently only TLV in the CCM is supported. |
| CC Organization Specific - OUI First | The last received first value in the OUI field. |
| CC Organization Specific - OUI Second | The last received second value in the OS TLV OUI field. |
| CC Organization Specific - OUI Third | The last received third value in the OS TLV OUI field. |
| CC Organization Specific - Sub-Type | The last received value in the OS TLV Sub-Type field. |
| CC Organization Specific - Value | The last received value in the OS TLV Value field. |
| CC Organization Specific - Last RX | OS TLV was received in the last received CCM PDU. |
| CC Port Status - Value | The last received value in the PS TLV Value field. |
| CC Port Status - Last RX | PS TLV was received in the last received CCM PDU. |
| CC Interface Status - Value | The last received value in the IS TLV Value field. |
| CC Interface Status - Last RX | IS TLV was received in the last received CCM PDU. |
| Link State Tracking | |
| Enable | When LST is enabled in an instance, Local SF or received 'isDown' in CCM Interface Status TLV, will bring down the residence port. Only valid in Up-MEP. |
| Fault Management | Click to go to Fault Management page. |
| Performance Monitoring | Click to go to Performance Monitor page. |
| Refresh | Click to refresh the page immediately. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

MEP Fault Management Configuration

This page allows the user to inspect and configure the Fault Management of the current MEP Instance.

Note that the sub-tables of Link Trace, Link Trace State, Client, AIS and LOCK are not supported while the MEP entry is in MPLS(Link/Tunnel/PW/LSP) domain.

Fault Management - Instance 1

Loop Back

| Enable | DEI | Priority | Cast | Peer MEP | Unicast MAC | To Send | Size | Interval |
|--------------------------|--------------------------|----------|---------|----------|-------------------|---------|------|----------|
| <input type="checkbox"/> | <input type="checkbox"/> | 0 | Multi ▾ | 1 | 00-00-00-00-00-00 | 10 | 64 | 100 |

Loop Back State

| Transaction ID | Transmitted | Reply MAC | Received | Out Of Order |
|----------------|-------------|-------------------|----------|--------------|
| 1 | 0 | 00-00-00-00-00-00 | 0 | 0 |

Link Trace

| Enable | Priority | Peer MEP | Unicast MAC | Time To Live |
|--------------------------|----------|----------|-------------------|--------------|
| <input type="checkbox"/> | 0 | 1 | 00-00-00-00-00-00 | 1 |

Link Trace State

| Transaction ID | Time To Live | Mode | Direction | Forwarded | Relay | Last MAC | Next MAC |
|-----------------|--------------|------|-----------|-----------|-------|----------|----------|
| No Transactions | | | | | | | |

Test Signal

| Tx | Rx | DEI | Priority | Peer MEP | Rate | Size | Pattern | Sequence Number |
|--------------------------|--------------------------|--------------------------|----------|----------|------|------|------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 0 | 1 | 1 | 64 | All Zero ▾ | <input type="checkbox"/> |

Test Signal State

| TX frame count | RX frame count | RX rate | Test time | Clear |
|----------------|----------------|---------|-----------|--------------------------|
| 0 | 0 | 0 | 0 | <input type="checkbox"/> |

Client Configuration

| Flow | | | | | | | | | | |
|----------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| Domain | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ |
| Instance | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Level | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| AIS prio | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ |
| LCK prio | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ |

AIS

| Enable | Frame Rate | Protection |
|--------------------------|------------|--------------------------|
| <input type="checkbox"/> | 1 f/sec ▾ | <input type="checkbox"/> |

LOCK

| Enable | Frame Rate |
|--------------------------|------------|
| <input type="checkbox"/> | 1 f/sec ▾ |

| Object | Description |
|------------------------|--|
| Loop Back | |
| Enable | Loop Back based on transmitting/receiving LBM/LBR PDU can be enabled/disabled. Loop Back is automatically disabled when all 'To Send' LBM PDU has been transmitted - waiting 5 sec. for all LBR from the end. |
| DEI | The DEI to be inserted as PCP bits in TAG (if any). |
| Priority | The priority to be inserted as PCP bits in TAG (if any). |
| Cast | Selection of LBM PDU transmitted unicast or multi-cast. The unicast MAC will be configured through 'Peer MEP' or 'Unicast Peer MAC'. To-wards MIP only unicast Loop Back is possible. |
| Peer MEP | This is only used if the 'Unicast MAC' is configured to all zero. The LBM unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer. |
| Unicast MAC | This is only used if NOT configured to all zero. This will be used as the LBM PDU unicast MAC. This is the only way to configure Loop Back to-wards a MIP. |
| MPLS TTL | The Time-To-Live value to be used for the MPLS OAM LBM PDU. It is insignificant when this MEP domain type is MPLS Link/Tunnel/PW/LSP. The allowed value is from 0 through 255. |
| To Send | The number of LBM PDU to send in one loop test. The value 0 indicate infinite transmission (test behaviour). This is HW based LBM/LBR and Requires VOE. |
| Size | The LBM frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing LBM OAM PDU - including CRC (four bytes). Example when 'Size' = 64=> Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + LBM PDU LENGTH(46) + CRC(4) = 64 bytes The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC. There are two frame MAX sizes to consider. Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 96009600 Bytes CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 15261526 Bytes Consider that the Peer MEP must be able to handle the selected frame size. Consider that In case of SW based MEP, the received LBR PDU must be copied to CPU Warning will be given if selected frame size exceeds the CPU RX frame MAX size Frame MIN Size is 64 Bytes. |
| Interval | The interval between transmitting LBM PDU. In 10ms. in case 'To Send' != 0 (max 100 - '0' is as fast as possible) In 1us. in case 'To Send' == 0 (max 10.000)", |
| Loop Back State | |
| Transaction ID | The transaction id of the first LBM transmitted. For each LBM transmitted the transaction id in the PDU is incremented. |
| Transmitted | The total number of LBM PDU transmitted. |
| Reply MAC | The MAC of the replying MEP/MIP. In case of multi-cast LBM, replies can be received from all peer MEP in the group. This MAC is not shown in case of 'To Send' == 0. |
| Received | The total number of LBR PDU received from this 'Reply MAC'. |
| Out Of Order | The number of LBR PDU received from this 'Reply MAC' with incorrect 'Transaction ID'. |
| Link Trace | |
| Enable | Link Trace based on transmitting/receiving LTM/LTR PDU can be enabled/disabled. Link Trace is automatically disabled when all 5 transactions are done with 5 sec. interval - waiting 5 sec. for all LTR in the end. The LTM PDU is always transmitted as Multi-cast Class 2. |
| Priority | The priority to be inserted as PCP bits in TAG (if any). |

| Object | Description |
|--------------|---|
| Peer MEP | This is only used if the 'Unicast MAC' is configured to all zero. The Link Trace Target MAC will be taken from the 'Unicast Peer MAC' configuration of this peer. |
| Unicast MAC | This is only used if NOT configured to all zero. This will be used as the Link Trace Target MAC. This is the only way to configure a MIP as Target MAC. |
| Time To Live | This is the LTM PDU TTL value as described in Y.1731. This value is decremented each time forwarded by a MIP. Will not be forwarded reaching zero. |

Link Trace State

| | |
|----------------|--|
| Transaction ID | The transaction id is incremented for each LTM send. This value is inserted the transmitted LTM PDU and is expected to be received in the LTR PDU. Received LTR with wrong transaction id is ignored. There are five transactions in one Link Trace activated. |
| Time To Live | This is the TTL value taken from the LTM received by the MIP/MEP sending this LTR - decremented as if forwarded. |
| Mode | Indicating if it was a MEP/MIP sending this LTR. |
| Direction | Indicating if MEP/MIP sending this LTR is ingress/egress. |
| Forwarded | Indicating if MEP/MIP sending this LTR has forwarded the LTM. |
| Relay | The Relay action can be one of the following MAC: The was a hit on the LT Target MAC FDB: LTM is forwarded based on hit in the Filtering DB MFDB: LTM is forwarded based on hit in the MIP CCM DB |
| Last MAC | The MAC identifying the last sender of the LBM causing this LTR - initiating MEP or previous MIP forwarding. |
| Next MAC | The MAC identifying the next sender of the LBM causing this LTR - MIP forwarding or terminating MEP. |

Test Signal

| | |
|----------|---|
| Enable | Test Signal based on transmitting TST PDU can be enabled/disabled. |
| DEI | The DEI to be inserted as PCP bits in TAG (if any). |
| Priority | The priority to be inserted as PCP bits in TAG (if any). |
| Peer MEP | The TST frame destination MAC will be taken from the 'Unicast Peer MAC' configuration of this peer. |
| Rate | The TST frame transmission bit rate - in Mega bits pr. second. Limit is 2.5Gbps. This is the bit rate of a standard frame without any encapsulation. If 1 Mbps rate is selected in a EVC MEP, the added tag will give a higher bitrate on the wire. The TST frame transmission bit rate - in Mega bits pr. second. Limit is 400 Mbps. This is the bit rate of a standard frame without any encapsulation. If 1 Mbps rate is selected in a EVC MEP, the added tag will give a higher bitrate on the wire. The TST frame transmission bit rate - in Mega bits pr. second. Limit is 400 Mbps. This is the bit rate of a standard frame without any encapsulation. If 1 Mbps rate is selected in a EVC MEP, the added tag will give a higher bitrate on the wire. |

| Object | Description |
|-----------------------------|---|
| Size | <p>The TST frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing TST OAM PDU - including CRC (four bytes).</p> <p>Example when 'Size' = 64=> Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes</p> <p>The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.</p> <p>There are two frame MAX sizes to consider.</p> <p>Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 96009600 Bytes</p> <p>CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 15261526 Bytes</p> <p>Consider that the Peer MEP must be able to handle the selected frame size. Consider that in order to calculate the 'RX rate' a received TST PDU must be copied to CPU</p> <p>Warning will be given if selected frame size exceeds the CPU RX frame MAX size</p> <p>Frame MIN Size is 64 Bytes.</p> |
| Pattern | <p>The 'empty' TST PDU has the size of 12 bytes. In order to achieve the configured frame size a data TLV will be added with a pattern.</p> <p>Example when 'Size' = 64=> Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes</p> <p>The TST PDU needs to be 46 bytes so a pattern of 46-12=34 bytes will be added.</p> <p>All Zero: Pattern will be '00000000'</p> <p>All One: Pattern will be '11111111'</p> <p>10101010: Pattern will be '10101010'</p> |
| Test Signal State | |
| TX frame count | The number of transmitted TST frames since last 'Clear'. |
| RX frame count | The number of received TST frames since last 'Clear'. |
| RX rate | The current received TST frame bit rate in Kbps. This is calculated on a 1 s. basis, starting when first TST frame is received after 'Clear'. The frame size used for this calculation is the first received after 'Clear' |
| Test time | The number of seconds passed since first TST frame received after last 'Clear'. |
| Clear | This will clear all Test Signal State. Transmission of TST frame will be restarted. Calculation of 'Rx frame count', 'RX rate' and 'Test time' will be started when receiving first TST frame. |
| Client Configuration | |
| Domain | <p>The domain of the client layer flow.</p> <p>For a MPLS MEP, the client domain can only be EVC or LSP. For a non-MPLS MEP, the client flow domain can not be LSP. For a non-MPLS MEP, the client flow domain can not be mixed VLAN and EVC.</p> |
| Instance | Client layer flow instance numbers. |
| Level | Client layer level - AIS and LCK PDU transmitted in this client layer flow will be on this level. |
| AIS Prio | The priority to be used when transmitting AIS in each client flow. Priority resulting in highest possible PCP can be selected. |
| LCK Prio | The priority to be used when transmitting LCK in each client flow. Priority resulting in highest possible PCP can be selected. |
| AIS | |
| Enable | Insertion of AIS signal (AIS PDU transmission) in client layer flows, can be enable/disabled. |

| Object | Description |
|-------------|---|
| Frame Rate | Selecting the frame rate of AIS PDU. This is the inverse of transmission period as described in Y.1731. |
| Protection | Selecting this means that the first 3 AIS PDU is transmitted as fast as possible - in case of using this for protection in the end point. |
| LOCK | |
| Enable | Insertion of LOCK signal (LCK PDU transmission) in client layer flows, can be enable/disabled. |
| Frame Rate | Selecting the frame rate of LCK PDU. This is the inverse of transmission period as described in Y.1731.: |
| Refresh | Click to refresh the page immediately. |
| Back | Click to go back to this MEP instance main page. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

MEP Performance Monitor Configuration

This page allows the user to inspect and configure the performance monitor of the current MEP Instance.

Performance Monitor - Instance 1 Refresh

Performance Monitoring Data Set

Enable

Loss Measurement

| Enable | Priority | Frame rate | Cast | Ended | FLR Interval |
|--------------------------|----------|------------|-------|--------|--------------|
| <input type="checkbox"/> | 0 | 1 f/sec | Multi | Single | 5 |

Loss Measurement State

| Tx | Rx | Near End Loss Count | Far End Loss Count | Near End Loss Ratio | Far End Loss Ratio | Clear |
|----|----|---------------------|--------------------|---------------------|--------------------|--------------------------|
| 0 | 0 | 0 | 0 | 0 | 0 | <input type="checkbox"/> |

Delay Measurement

| Enable | Priority | Cast | Peer MEP | Ended | Tx Mode | Calc | Gap | Count | Unit | D2forD1 | Counter Overflow Action |
|--------------------------|----------|-------|----------|--------|-------------|------|-----|-------|------|--------------------------|-------------------------|
| <input type="checkbox"/> | 0 | Multi | 1 | Single | Standardize | Flow | 10 | 10 | us | <input type="checkbox"/> | Keep |

Delay Measurement State

| | Tx | Rx | Rx Timeout | Rx Error | Av Delay Tot | Av Delay last N | Delay Min. | Delay Max. | Av Delay-Var Tot | Av Delay-Var last N | Delay-Var Min. | Delay-Var Max. | Overflow | Clear |
|---------|----|----|------------|----------|--------------|-----------------|------------|------------|------------------|---------------------|----------------|----------------|----------|--------------------------|
| One-way | | | | | | | | | | | | | | |
| F-to-N | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| N-to-F | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Two-way | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input type="checkbox"/> |

Delay Measurement Bins

| Measurement Bins for FD | Measurement Bins for IFDV | Measurement Threshold |
|-------------------------|---------------------------|-----------------------|
| 3 | 3 | 5000 |

Delay Measurement Bins for FD

| | bin0 | bin1 | bin2 |
|---------|------|------|------|
| One-way | | | |
| F-to-N | 0 | 0 | 0 |
| N-to-F | 0 | 0 | 0 |
| Two-way | 0 | 0 | 0 |

Delay Measurement Bins for IFDV

| | bin0 | bin1 | bin2 |
|---------|------|------|------|
| One-way | | | |
| F-to-N | 0 | 0 | 0 |
| N-to-F | 0 | 0 | 0 |
| Two-way | 0 | 0 | 0 |

F-to-N :Far-end-to-near-end
N-to-F :Near-end-to-far-end

Performance Monitoring Data Set

Enable When enabled this MEP instance will contribute to the 'PM Data Set' gathered by the PM Session.

Loss Measurement

Enable Loss Measurement based on transmitting/receiving CCM or LMM/LMR PDU can be enabled/disabled - see 'Ended'. This is only valid with one Peer MEP configured.

Priority The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.

Frame rate Selecting the frame rate of CCM/LMM PDU. This is the inverse of transmission period as described in Y.1731. Selecting 300f/sec or 100f/sec is not valid. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.

Cast Selection of CCM or LMM PDU transmitted unicast or multicast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. In case of enable of Continuity Check and dual ended Loss Measurement both implemented on SW based CCM, 'Cast' has to be the same.

Ended Single: Single ended Loss Measurement implemented on LMM/LMR.
Dual: Dual ended Loss Measurement implemented on SW based CCM.

| | |
|---------------|--|
| FLR Interval | This is the interval in seconds where the Frame Loss Ratio is calculated. |
| Flow Counting | Traffic (service frames) are counted per flow - all priority in one. |
| Oam Counting | Loss Measurement can count OAM frames in different ways. Y1713: Loss Measurement is counting OAM frames as service frames as described in Y1731. None: Loss Measurement is NOT counting OAM frames as service frames. All: Loss Measurement is counting all OAM frames as service frames. |

Loss Measurement State

| | |
|---------------------|---|
| Near End Loss Count | The accumulated near end frame loss count - since last 'clear'. |
| Far End Loss Count | The accumulated far end frame loss count - since last 'clear'. |
| Near End Loss Ratio | The near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted - in the latest 'FLR Interval'. The result is given in percent. |
| Far End Loss Ratio | The far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted - in the latest 'FLR Interval'. The result is given in percent. |
| Clear | Set of this check and save will clear the accumulated counters and restart ratio calculation. |

Delay Measurement

| | |
|-------------------------|--|
| Enable | Delay Measurement based on transmitting 1DM/DMM PDU can be enabled/disabled. Delay Measurement based on receiving and handling 1DM/DMR PDU is always enabled. |
| Priority | The priority to be inserted as PCP bits in TAG (if any). |
| Cast | Selection of 1DM/DMM PDU transmitted unicast or multicast. The unicast MAC will be configured through 'Peer MEP'. |
| Peer MEP | This is only used if the 'Cast' is configured to Uni. The 1DM/DMR unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer. |
| Way | One-Way: One-Way Delay Measurement implemented on 1DM. Two-Way: Two-Way Delay Measurement implemented on DMM/DMR. |
| Tx Mode | Standardize: Y.1731 standardize way to transmit 1DM/DMR. Proprietary: Vitesse proprietary way with follow-up packets to transmit 1DM/DMR. |
| Calc | This is only used if the 'Way' is configured to Two-way. Round trip: The frame delay calculated by the transmitting and receiving timestamps of initiators. $\text{Frame Delay} = \text{RxTimeb} - \text{TxTimeStampf}$ Flow: The frame delay calculated by the transmitting and receiving timestamps of initiators and remotes. $\text{Frame Delay} = (\text{RxTimeb} - \text{TxTimeStampf}) - (\text{TxTimeStampb} - \text{RxTimeStampf})$ |
| Gap | The gap between transmitting 1DM/DMM PDU in 10ms. The range is 10 to 65535. |
| Count | The number of last records to calculate. The range is 10 to 2000. |
| Unit | The time resolution. |
| D2forD1 | Enable to use DMM/DMR packet to calculate one-way DM. If the option is enabled, the following action will be taken. When DMR is received, two-way delay (roundtrip or flow) and both near-end-to-far-end and far-end-to-near-end one-way delay are calculated. When DMM or 1DM is received, only far-end-to-near-end one-way delay is calculated. |
| Counter Overflow Action | The action to counter when overflow happens. |

Delay Measurement State

| | |
|------------|--|
| Tx | The accumulated transmit count - since last 'clear'. |
| Rx | The accumulated receive count - since last 'clear'. |
| Rx Timeout | The accumulated receive timeout count for two-way only - since last 'clear'. |

| | |
|-----------------------------------|--|
| Rx Error | The accumulated receive error count - since last 'clear'. This is counting if the frame delay is larger than 1 second or if far end residence time is larger than the round trip time. |
| Av Delay Tot | The average total delay - since last 'clear'. |
| Av Delay last N | The average delay of the last n packets - since last 'clear'. |
| Delay Min. | The minimum delay - since last 'clear'. |
| Delay Max. | The maximum delay - since last 'clear'. |
| Av Delay-Var Tot | The average total delay variation - since last 'clear'. |
| Av Delay-Var last N | The average delay variation of the last n packets - since last 'clear'. |
| Delay-Var Min. | The minimum delay variation - since last 'clear'. |
| Delay-Var Max. | The maximum delay variation - since last 'clear'. |
| Overflow | The number of counter overflow - since last 'clear'. |
| Clear | Set of this check and save will clear the accumulated counters. |
| Far-end-to-near-end one-way delay | The one-way delay is from remote devices to the local devices. Here are the conditions to calculate this delay. 1. 1DM received. 2. DMM received with D2forD1 enabled. 3. DMR received with D2forD1 enabled. |
| Near-end-to-far-end one-way delay | The one-way delay is from the local devices to remote devices. The only case to calculate this delay is below. DMR received with D2forD1 enabled. |

Delay Measurement Bins

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

| | |
|---------------------------|--|
| Measurement Bins for FD | Configurable number of Frame Delay Measurement Bins per Measurement Interval. The minimum number of FD Measurement Bins per Measurement Interval supported is 2. The maximum number of FD Measurement Bins per Measurement Interval supported is 10. The default number of FD Measurement Bins per Measurement Interval supported is 3. |
| Measurement Bins for IFDV | Configurable number of Inter-Frame Delay Variation Measurement Bins per Measurement Interval. The minimum number of FD Measurement Bins per Measurement Interval supported is 2. The maximum number of FD Measurement Bins per Measurement Interval supported is 10. The default number of FD Measurement Bins per Measurement Interval supported is 2. |
| Measurement Threshold | Configurable the Measurement Threshold for each Measurement Bin. The unit for a measurement threshold is in microseconds (us). The default configured measurement threshold for a Measurement Bin is an increment of 5000 us. |

Delay Measurement Bins for FD

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

| Bin | Threshold | Range |
|------|-----------|--|
| bin0 | 0 us | 0 us <= measurement < 5,000 us |
| bin1 | 5,000 us | 5,000 us <= measurement < 10,000 us |
| bin2 | 10,000 us | 10,000 us <= measurement < 15,000 us |
| bin3 | 15,000 us | 15,000 us <= measurement < infinite us |

Delay Measurement Bins for IFDV

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

| Bin | Threshold | Range |
|------------|------------------|--|
| bin0 | 0 us | 0 us <= measurement < 5,000 us |
| bin1 | 5,000 us | 5,000 us <= measurement < 10,000 us |
| bin2 | 10,000 us | 10,000 us <= measurement < 15,000 us |
| bin3 | 15,000 us | 15,000 us <= measurement < infinite us |

Refresh Click to refresh the page immediately.

Back Click to go back to this MEP instance main page.

Apply Click to apply changes.

Reset Click to undo any changes made locally and revert to previously saved values.

ERPS

The ERPS instances are configured here.

Please note that ERPS cannot be used in conjunction with Spanning Tree or Loop Protection on the same switch

Note: For an example of how to configure an ERPS ring please refer to appendix A at the rear of this document.

| Ethernet Ring Protection Switching | | | | | | | | | | | | Refresh |
|------------------------------------|---------|--------|--------|----------------|----------------|---------------|---------------|-----------|--------------------------|--------------------------|---------------|-------------------------------------|
| Delete | ERPS ID | Port 0 | Port 1 | Port 0 APS MEP | Port 1 APS MEP | Port 0 SF MEP | Port 1 SF MEP | Ring Type | Interconnected Node | Virtual Channel | Major Ring ID | Alarm |
| Delete | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Major ▼ | <input type="checkbox"/> | <input type="checkbox"/> | 0 | <input checked="" type="checkbox"/> |

| Object | Description |
|--------------------------|---|
| Delete | This box is used to mark an ERPS for deletion in next Save operation. |
| ERPS ID | The ID of the created Protection group, It must be an integer value between 1 and 64. The maximum number of ERPS Protection Groups that can be created are 64. Click on the ID of an Protection group to enter the configuration page. |
| Port 0 | This will create a Port 0 of the switch in the ring. |
| Port 1 | This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance |
| Port 0 SF MEP | The Port 0 Signal Fail reporting MEP. |
| Port 1 SF MEP | The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance. |
| Port 0 APS MEP | The Port 0 APS PDU handling MEP. |
| Port 1 APS MEP | The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance. |
| Ring Type | Type of Protecting ring. It can be either major ring or sub-ring. |
| Interconnected Node | Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected. |
| Virtual Channel | Sub-rings can either have virtual channel or not on the interconnected node. This is configured using "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring doesn't have virtual channel. |
| Major Ring ID | Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring. |
| Alarm | There is an active alarm on the ERPS. |
| Add New Protection Group | Click to add a new Protection group entry. |
| Refresh | Click to refresh the page immediately. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

Ethernet Ring Protection Switch Configuration


ERPS Configuration 1

Auto-refresh

Instance Data

| ERPS ID | Port 0 | Port 1 | Port 0 SF MEP | Port 1 SF MEP | Port 0 APS MEP | Port 1 APS MEP | Ring Type |
|---------|--------|--------|---------------|---------------|----------------|----------------|------------|
| 1 | 10 | 11 | 1 | 2 | 1 | 2 | Major Ring |

Instance Configuration

| Configured | Guard Time | WTR Time | Hold Off Time | Version | Revertive | VLAN config |
|---|------------|----------|---------------|---------|-------------------------------------|-------------|
|  | 500 | 1min | 0 | v2 | <input checked="" type="checkbox"/> | VLAN Config |




RPL Configuration

| RPL Role | RPL Port | Clear |
|----------|----------|--------------------------|
| None | None | <input type="checkbox"/> |

Instance Command

| Command | Port |
|---------|------|
| None | None |

Instance State

| Protection State | Port 0 | Port 1 | Transmit APS | Port 0 Receive APS | Port 1 Receive APS | WTR Remaining | RPL Un-blocked | No APS Received | Port 0 Block Status | Port 1 Block Status | FOP Alarm |
|------------------|--------|--------|--------------|--------------------|--------------------|---------------|---|---|---------------------|---------------------|---|
| Pending | OK | OK | | | | 0 |  |  | Blocked | Blocked |  |

| Object | Description |
|-------------------------------|---|
| Instance Data | |
| ERPS ID | The ID of the Protection group. |
| Port 0 | This will create a Port 0 of the switch in the ring. |
| Port 1 | This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance |
| Port 0 SF MEP | The Port 0 Signal Fail reporting MEP. |
| Port 1 SF MEP | The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance. |
| Port 0 APS MEP | The Port 0 APS PDU handling MEP. |
| Port 1 APS MEP | The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance. |
| Ring Type | Type of Protecting ring. It can be either major ring or sub-ring. |
| Instance Configuration | |
| Configured | Red: This ERPS is only created and has not yet been configured - is not active. Green: This ERPS is configured - is active. |
| Guard Time | Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages. The period of the guard timer can be configured in 10 ms steps between 10 ms and 2 seconds, with a default value of 500 ms |
| WTR Time | The Wait To Restore timing value to be used in revertive switching. The period of the WTR time can be configured by the operator in 1 minute steps between 5 and 12 minutes with a default value of 5 minutes. |

| Object | Description |
|---------------|---|
| Hold Off Time | The timing value to be used to make persistent check on Signal Fail before switching. The range of the hold off timer is 0 to 10 seconds in steps of 100 ms |
| Version | ERPS Protocol Version - v1 or v2 |
| Revertive | In Revertive mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL. In Non-Revertive mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared. |
| VLAN config | VLAN configuration of the Protection Group. Click on the "VLAN Config" link to configure VLANs for this protection group. |

RPL Configuration

| | |
|----------|--|
| RPL Role | It can be either RPL owner or RPL Neighbor. |
| RPL Port | This allows to select the east port or west port as the RPL block. |
| Clear | If the owner has to be changed, then the clear check box allows to clear the RPL owner for that ERPS ring. |

Sub-Ring Configuration

| | |
|-----------------|--|
| Topology Change | Clicking this checkbox indicates that the topology changes in the sub-ring are propagated in the major ring. |
|-----------------|--|

Instance Command

| | |
|---------------|---|
| Command | Administrative command. A port can be administratively configured to be in either manual switch or forced switch state. |
| Forced Switch | Forced Switch command forces a block on the ring port where the command is issued. |
| Manual Switch | In the absence of a failure or FS, Manual Switch command forces a block on the ring port where the command is issued. |
| Clear | The Clear command is used for clearing an active local administrative command (e.g., Forced Switch or Manual Switch). |
| Port | Port selection - Port0 or Port1 of the protection Group on which the command is applied. |

Instance State

| | |
|---------------------|---|
| Protection State | ERPS state according to State Transition Tables in G.8032. |
| Port 0 | OK: State of East port is ok SF: State of East port is Signal Fail |
| Port 1 | OK: State of West port is ok SF: State of West port is Signal Fail |
| Transmit APS | The transmitted APS according to State Transition Tables in G.8032. |
| Port 0 Receive APS | The received APS on Port 0 according to State Transition Tables in G.8032. |
| Port 1 Receive APS | The received APS on Port 1 according to State Transition Tables in G.8032. |
| WTR Remaining | Remaining WTR timeout in milliseconds. |
| RPL Un-blocked | APS is received on the working flow. |
| No APS Received | RAPS PDU is not received from the other end. |
| Port 0 Block Status | Block status for Port 0 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel. |
| Port 1 Block Status | Block status for Port 1 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel. |

| Object | Description |
|--------------|--|
| FOP Alarm | Failure of Protocol Defect(FOP) status. If FOP is detected, red LED glows; else green LED glows. |
| Apply | Click to apply changes. |
| Auto-refresh | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

VLAN Membership Configuration

ERPS VLAN Configuration 1

| Delete | VLAN ID |
|---------------------------------------|--------------------------------|
| <input type="button" value="Delete"/> | <input type="text" value="0"/> |

| Object | Description |
|-------------------|--|
| Delete | To delete a VLAN entry, check this box. The entry will be deleted on all stack switch units during the next Save. |
| VLAN ID | Indicates the ID of this particular VLAN. |
| Adding a New VLAN | Click "Add New Entry" to add a new VLAN ID. Legal values for a VLAN ID are 1 through 4095. The VLAN is enabled on the selected switch unit when you click on "Save". A VLAN without any port members will be deleted when you click "Save". The "Delete" button can be used to undo the addition of new VLANs. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Back | Click to go back to this MEP instance main page. |
| Refresh | Refreshes the displayed table starting from the "VLAN ID" input fields. |

MAC Table

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

MAC Address Table Configuration

Aging Configuration

| | |
|-------------------------|--------------------------|
| Disable Automatic Aging | <input type="checkbox"/> |
| Aging Time | 300 seconds |

MAC Table Learning

| | Port Members | | | | | | | | | | |
|---------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| Auto | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> |
| Disable | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Secure | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Static MAC Table Configuration

| | Port Members | | | | | | | | | | | | |
|--------|--------------|-------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Delete | VLAN ID | MAC Address | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| Delete | 1 | 00-00-00-00-00-00 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Add New Static Entry

Apply Reset

| Object | Description |
|---------------------------------------|---|
| Aging Configuration | |
| Disable Automatic Aging | Disable the automatic aging of dynamic entries by ticking the item. |
| Aging Time | Enter a value in seconds. The allowed range is 10 to 1000000 seconds. |
| MAC Table Learning | |
| Auto | Learning is done automatically as soon as a frame with unknown SMAC is received. |
| Disable | No learning is done. |
| Secure | Only static MAC entries are learned, all other frames are dropped. Note: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface. |
| Static MAC Table Configuration | |
| Delete | Check to delete the entry. It will be deleted during the next save. |
| VLAN ID | The VLAN ID of the entry. |
| MAC Address | The MAC address of the entry. |
| Port Members | Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry. |
| Adding a New Static Entry | Click "Add New Static Entry" button to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Apply". |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

VLAN Translation

Port to Group Configuration

This page allows you to configure switch Ports to use a given VLAN Translation Mapping Group. This will enable all VLAN Translation mappings of that group (if any) on the selected switch port.

The settings relate to the currently selected stack unit, as reflected by the page header.

VLAN Translation Port Configuration Auto-refresh

| Port | Group Configuration | |
|------|--------------------------|----------|
| | Default | Group ID |
| * | <input type="checkbox"/> | <> ▼ |
| 1 | <input type="checkbox"/> | 1 ▼ |
| 2 | <input type="checkbox"/> | 2 ▼ |
| 3 | <input type="checkbox"/> | 3 ▼ |
| 4 | <input type="checkbox"/> | 4 ▼ |
| 5 | <input type="checkbox"/> | 5 ▼ |
| 6 | <input type="checkbox"/> | 6 ▼ |
| 7 | <input type="checkbox"/> | 7 ▼ |
| 8 | <input type="checkbox"/> | 8 ▼ |
| 9 | <input type="checkbox"/> | 9 ▼ |
| 10 | <input type="checkbox"/> | 10 ▼ |
| 11 | <input type="checkbox"/> | 11 ▼ |

| Object | Description |
|--------------|--|
| Port | The Port column shows the list of ports for which you can configure the VLAN Translation Mapping Group. |
| Default | To set the switch port to use the default VLAN Translation Group click the checkbox. Click "Apply". |
| Group ID | <p>The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 1111.</p> <p>Note: By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.</p> |
| Auto-refresh | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally and revert to the previously saved values. |

VLAN Translation Mappings

This page displays current VLAN Translation mapping configurations. The settings can also be configured here.

VLAN Translation Mapping Table Auto-refresh

| Group ID | VID | TVID | |
|----------|-----|------|---|
| | | | + |

| Object | Description |
|----------|--|
| Group ID | The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 1111. Note: By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1. |
| VID | Indicates the VLAN of the mapping (i.e. 'source' VLAN). A valid VLAN ID ranges from 1 to 4095. |
| TVID | Indicates the VLAN ID to which VLAN ID of an ingress frame will be translated to (granted that the mapping is enabled on the ingress port that the frame arrived at). A valid VLAN ID ranges from 1 to 4095. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Cancel | Return to the previous page; any changes made locally will be undone. |

VLANs

This page allows for controlling VLAN configuration on the switch.

The page is divided into a global section and a per-port configuration section.

Global VLAN Configuration

| | |
|------------------------------|------|
| Allowed Access VLANs | 1 |
| Ethertype for Custom S-ports | 88A8 |

Port VLAN Configuration

| Port | Mode | Port VLAN | Port Type | Ingress Filtering | Ingress Acceptance | Egress Tagging | Allowed VLANs | Forbidden VLANs |
|------|--------|-----------|-----------|-------------------------------------|---------------------|----------------|---------------|-----------------|
| 1 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 2 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 3 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 4 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 5 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 6 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 7 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 8 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 9 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 10 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 11 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |

Apply Reset

Object Description

Global VLAN Configuration

Allowed Access VLANs This field shows the allowed Access VLANs, i.e. it only affects ports configured as Access ports. Ports in other modes are members of all VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.

The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300:
1,10-13,200,300.

Spaces are allowed in between the delimiters.

Ethertype for Custom S-ports This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

Port VLAN Configuration

Port This is the logical port number of this row.

| Object | Description |
|-----------|---|
| Mode | <p>The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below.</p> <p>Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question.</p> <p>Grayed out fields show the value that the port will get when the mode is applied.</p> <p>Access:</p> <p>Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:</p> <ul style="list-style-type: none"> • Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1 • Accepts untagged and C-tagged frames • Discards all frames that are not classified to the Access VLAN • On egress all frames classified to the Access VLAN are transmitted untagged. Other (dynamically added VLANs) are transmitted tagged <p>Trunk:</p> <p>Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:</p> <ul style="list-style-type: none"> • By default, a trunk port is member of all VLANs (1-4095) • The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs • Frames classified to a VLAN that the port is not a member of are discarded • By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress • Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress <p>Hybrid:</p> <p>Hybrid ports resemble trunk ports in many ways, but add additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:</p> <ul style="list-style-type: none"> • Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware • Ingress filtering can be controlled • Ingress acceptance of frames and configuration of egress tagging can be configured independently |
| Port VLAN | <p>Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1. On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0). On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.</p> <p>The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.</p> |
| Port Type | <p>Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.</p> <p>Unaware:</p> <p>On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.</p> <p>C-Port:</p> <p>On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.</p> <p>S-Port:</p> <p>On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.</p> <p>S-Custom-Port:</p> <p>On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.</p> |

| Object | Description |
|--------------------|---|
| Ingress Filtering | <p>Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.</p> <p>If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.</p> <p>If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.</p> |
| Ingress Acceptance | <p>Hybrid ports allow for changing the type of frames that are accepted on ingress.</p> <p>Tagged and Untagged- Both tagged and untagged frames are accepted.</p> <p>Tagged Only - Only tagged frames are accepted on ingress. Untagged frames are discarded.</p> <p>Untagged Only - Only untagged frames are accepted on ingress. Tagged frames are discarded.</p> |
| Egress Tagging | <p>Ports in Trunk and Hybrid mode may control the tagging of frames on egress.</p> <p>Untag Port VLAN Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.</p> <p>Tag All All frames, whether classified to the Port VLAN or not, are transmitted with a tag.</p> <p>Untag All All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.</p> |
| Allowed VLANs | <p>Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN.</p> <p>The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to 1-4095.</p> <p>The field may be left empty, which means that the port will not become member of any VLANs.</p> |
| Forbidden VLANs | <p>A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs.</p> <p>The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field. By default, the field is left blank, which means that the port may become a member of all possible VLANs.</p> |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

Private VLANs

Membership

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Private VLAN Membership Configuration Auto-refresh Refresh

| | | Port Members | | | | | | | | | | |
|--------------------------|----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Delete | PVLAN ID | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| <input type="checkbox"/> | 1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Add New Private VLAN

Apply Reset

| Object | Description |
|---------------------------|---|
| Delete | To delete a private VLAN entry, check this box. The entry will be deleted during the next save. |
| Private VLAN ID | Indicates the ID of this particular private VLAN. |
| Port Members | A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked. |
| Adding a New Private VLAN | Click "Add New Private VLAN" button to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction. The Private VLAN is enabled when you click "Apply". The "Delete" button can be used to undo the addition of new Private VLANs. |
| Auto_refresh | Check this box to automatically refresh page every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally. |

Port Isolation

This page is used for enabling or disabling port isolation on ports in a Private VLAN.

A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Port Isolation Configuration Auto-refresh

| Port Number | | | | | | | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Port Members: A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.

| | |
|--------------|---|
| Auto_refresh | Check this box to automatically refresh page every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally. |

VCL

MAC-based VLAN

The MAC address to VLAN ID mappings can be configured here. This page allows adding and deleting MAC-based VLAN Classification List entries and assigning the entries to different ports.

MAC-based VLAN Membership Configuration Auto-refresh

| Delete | MAC Address | VLAN ID | Port Members | | | | | | | | | | | | |
|---------------------------------------|-------------------|---------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | | |
| <input type="button" value="Delete"/> | 00-00-00-00-00-00 | 1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| Object | Description |
|---|---|
| Delete | To delete a MAC to VLAN ID mapping entry, check this box and press save. The entry will be deleted in the stack. |
| MAC Address | Indicates the MAC address of the mapping. |
| VLAN ID | Indicates the VLAN ID the above MAC will be mapped to. |
| Port Members | A row of check boxes for each port is displayed for each MAC to VLAN ID mapping entry. To include a port in the mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked. |
| Adding a New MAC to VLAN ID mapping entry | Click "Add New Entry" to add a new MAC to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any unicast MAC address can be used to configure the mapping. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095. The MAC to VLAN ID entry is enabled when you click on "Apply". A mapping without any port members will not be added when you click "Apply". The "Delete" button can be used to undo the addition of new mappings. The maximum possible MAC to VLAN ID mapping entries are limited to 256. |
| Auto_refresh | Check this box to automatically refresh page every 3 seconds. |
| Refresh | Click to refresh the displayed table. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally. |

Protocol-based VLAN

Protocol to Group

This page allows you to add new Protocol to Group Name (each protocol can be part of only one Group) mapping entries as well as allow you to see and delete already mapped entries for the switch.

Protocol to Group Mapping Table Auto-refresh

| Delete | Frame Type | Value | Group Name |
|---------------------------------------|------------|---------------|------------|
| <input type="button" value="Delete"/> | Ethernet ▼ | Etype: 0x0800 | |

The displayed settings are:

| Object | Description |
|------------|--|
| Delete | To delete a Protocol to Group Name map entry, check this box. The entry will be deleted from the switch during the next Save. |
| Frame Type | <p>Frame Type can have one of the following values:</p> <ol style="list-style-type: none"> 1. Ethernet 2. LLC 3. SNAP <p>Note: When changing the Frame type field, the valid value of the following text field will vary depending on the new frame type you selected.</p> |
| Value | <p>Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu.</p> <p>Below are the criteria for the three different Frame Types:</p> <ol style="list-style-type: none"> 1. Ethernet: Value in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype range between 0x0600 and 0xffff 2. LLC: Valid value in this case is comprised of two different sub-values. <ol style="list-style-type: none"> a. DSAP: 1-byte long string (0x00-0xff) b. SSAP: 1-byte long string (0x00-0xff) 3. SNAP: Valid value in this case is also comprised of two different sub-values. <ol style="list-style-type: none"> a. OUI: OUI (Organizationally Unique Identifier) is a parameter in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value ranging between 0x00 and 0xff. b. PID: PID (Protocol ID). If OUI is hexadecimal 000000, then the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. <p>In other words, if the value of OUI field is 00-00-00 then the value of PID will be etype (0x0600-0xffff) and if the value of OUI is other than 00-00-00 then valid values of PID will be any value between 0x0000 and 0xffff.</p> |
| Group Name | <p>A valid Group Name is a 16-character long string, unique for every entry, which consists of a combination of alphabets(a-z or A-Z) and integers(0-9).</p> <p>Note: Special characters and underscores (_) are not allowed.</p> |

| Object | Description |
|--|---|
| Adding a New Group to VLAN MAPPING ENTRY | Click "Add New Entry" to add a new entry in the mapping table. An empty row is added to the table, where Frame Type, Value and the Group Name can be configured as needed. The "Delete" button can be used to undo the addition of new entry. The maximum possible Protocol to Group mappings are limited to 128. |
| Auto_refresh | Check this box to automatically refresh page every 3 seconds. |
| Refresh | Click to refresh the displayed table. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally. |

Group to VLAN

This page allows you to map a Group Name (already configured or to be configured in the future) to a VLAN for the switch .

Group Name to VLAN mapping Table Auto-refresh

| Delete | Group Name | VLAN ID | Port Members | | | | | | | | | | | |
|---------------------------------------|----------------------|----------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | |
| <input type="button" value="Delete"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

The displayed settings are:

| Object | Description |
|---|--|
| Delete | To delete a Group Name to VLAN mapping, check this box. The entry will be deleted from the switch during the next Save. |
| Group Name | A valid Group Name is a string, at the most 16 characters long, which consists of a combination of alphabets (a-z or A-Z) and integers(0-9) with no special characters allowed. You may either use a Group that already includes one or more protocols (see Protocol to Group mappings), or create a Group to VLAN ID mapping that will become active the moment you add one or more protocols inside that Group. Furthermore, the Group to VLAN ID mapping is not unique, as long as the port lists of these mappings are mutually exclusive (e.g. Group1 can be mapped to VID 1 on port#1 and to VID 2 on port#2). |
| VLAN ID | Indicates the VLAN ID to which the Group Name will be mapped. A valid VLAN ID ranges from 1 to 4095. |
| Port Members | A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in the mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked. |
| Adding a New MAC to VLAN ID mapping entry | Click "Add New Entry" to add a new entry in the mapping table. An empty row is added to the table and the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The "Delete" button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings are limited to 256. |
| Auto_refresh | Check this box to automatically refresh page every 3 seconds. |
| Refresh | Click to refresh the displayed table. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally. |

IP Subnet-based VLAN

The IP subnet to VLAN ID mappings can be configured here. This page allows adding, updating and deleting IP subnet to VLAN ID mapping entries and assigning them to different ports.

IP Subnet-based VLAN Membership Configuration Auto-refresh

| Delete | IP Address | Mask Length | VLAN ID | Port Members | | | | | | | | | | | | |
|--------------------------|------------|-------------|---------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | | |
| <input type="checkbox"/> | 0.0.0.0 | 24 | 1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| Object | Description |
|-----------------------------------|--|
| Delete | To delete a mapping, check this box and press save. The entry will be deleted in the stack. |
| IP Address | Indicates the subnet's IP address (Any of the subnet's host addresses can be also provided here, the application will convert it automatically). |
| Mask Length | Indicates the subnet's mask length. |
| VLAN ID | Indicates the VLAN ID the subnet will be mapped to. IP Subnet to VLAN ID is a unique matching. |
| Port Members | A row of check boxes for each port is displayed for each IP subnet to VLAN ID mapping entry. To include a port in a mapping, simply check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members and all boxes are unchecked. |
| Adding a New IP subnet-based VLAN | Click "Add New Entry" to add a new IP subnet to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any IP address/mask can be configured for the mapping. Legal values for the VLAN ID are 1 to 4095. The IP subnet to VLAN ID mapping entry is enabled when you click on "Apply". The "Delete" button can be used to undo the addition of new mappings. The maximum possible IP subnet to VLAN ID mappings are limited to 128. |
| Auto_refresh | Check this box to automatically refresh page every 3 seconds. |
| Refresh | Click to refresh the displayed table. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally. |

Voice VLAN

Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

Voice VLAN Configuration

| | | |
|---------------|------------|---------|
| Mode | Disabled ▼ | |
| VLAN ID | 1000 | |
| Aging Time | 86400 | seconds |
| Traffic Class | 7 (High) ▼ | |

Port Configuration

| Port | Mode | Security | Discovery Protocol |
|------|------------|------------|--------------------|
| * | <> ▼ | <> ▼ | <> ▼ |
| 1 | Disabled ▼ | Disabled ▼ | OUI ▼ |
| 2 | Disabled ▼ | Disabled ▼ | OUI ▼ |
| 3 | Disabled ▼ | Disabled ▼ | OUI ▼ |
| 4 | Disabled ▼ | Disabled ▼ | OUI ▼ |
| 5 | Disabled ▼ | Disabled ▼ | OUI ▼ |
| 6 | Disabled ▼ | Disabled ▼ | OUI ▼ |
| 7 | Disabled ▼ | Disabled ▼ | OUI ▼ |
| 8 | Disabled ▼ | Disabled ▼ | OUI ▼ |
| 9 | Disabled ▼ | Disabled ▼ | OUI ▼ |
| 10 | Disabled ▼ | Disabled ▼ | OUI ▼ |
| 11 | Disabled ▼ | Disabled ▼ | OUI ▼ |

Apply Reset

| Object | Description |
|---------------|--|
| Mode | Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are: Enabled: Enable Voice VLAN mode operation. Disabled: Disable Voice VLAN mode operation. |
| VLAN ID | Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095. |
| Aging Time | Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age time; 2 * age time] interval. |
| Traffic Class | Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class. |

| Object | Description |
|-------------------------|---|
| Port Mode | Indicates the Voice VLAN port mode. Possible port modes are: Disabled: Disjoin from Voice VLAN. Auto: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically. Forced: Force join to Voice VLAN. |
| Port Security | Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are: Enabled: Enable Voice VLAN security mode operation. Disabled: Disable Voice VLAN security mode operation. |
| Port Discovery Protocol | Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are: OUI: Detect telephony device by OUI address. LLDP: Detect telephony device by LLDP. Both: Both OUI and LLDP. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

OUI

Configure VOICE VLAN OUI table on this page. The maximum number of entries is 16. Modifying the OUI table will restart auto detection of OUI process.

Voice VLAN OUI Table

| Delete | Telephony OUI | Description |
|--------------------------|---------------|---------------------------|
| <input type="checkbox"/> | 00-01-e3 | Siemens AG phones |
| <input type="checkbox"/> | 00-03-6b | Cisco phones |
| <input type="checkbox"/> | 00-0f-e2 | H3C phones |
| <input type="checkbox"/> | 00-60-b9 | Philips and NEC AG phones |
| <input type="checkbox"/> | 00-d0-1e | Pingtel phones |
| <input type="checkbox"/> | 00-e0-75 | Polycom phones |
| <input type="checkbox"/> | 00-e0-bb | 3Com phones |

Add New Entry

Apply

Reset

| Object | Description |
|---------------|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| Telephony OUI | A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit). |
| Description | The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Add New Entry | Click to add a new OUI. |

QoS

Port Classification

This page allows you to configure the basic QoS Ingress Classification settings for all switch ports.

QoS Ingress Port Classification

| Port | CoS | DPL | PCP | DEI | Tag Class. | DSCP Based | Address Mode |
|------|------|------|------|------|------------|--------------------------|--------------|
| * | <> ▾ | <> ▾ | <> ▾ | <> ▾ | | <input type="checkbox"/> | <> ▾ |
| 1 | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | Disabled | <input type="checkbox"/> | Source ▾ |
| 2 | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | Disabled | <input type="checkbox"/> | Source ▾ |
| 3 | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | Disabled | <input type="checkbox"/> | Source ▾ |
| 4 | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | Disabled | <input type="checkbox"/> | Source ▾ |
| 5 | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | Disabled | <input type="checkbox"/> | Source ▾ |
| 6 | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | Disabled | <input type="checkbox"/> | Source ▾ |
| 7 | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | Disabled | <input type="checkbox"/> | Source ▾ |
| 8 | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | Disabled | <input type="checkbox"/> | Source ▾ |
| 9 | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | Disabled | <input type="checkbox"/> | Source ▾ |
| 10 | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | Disabled | <input type="checkbox"/> | Source ▾ |
| 11 | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | Disabled | <input type="checkbox"/> | Source ▾ |

Apply Reset

| Object | Description |
|--------|---|
| Port | The port number for which the configuration below applies. |
| CoS | <p>Controls the default class of service.</p> <p>All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority.</p> <p>If the port is VLAN aware, the frame is tagged and Tag Class is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS.</p> <p>The classified CoS can be overruled by a QCL entry.</p> <p>Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.</p> |
| DPL | <p>Controls the default drop precedence level.</p> <p>All frames are classified to a drop precedence level.</p> <p>If the port is VLAN aware and the frame is tagged, then the frame is classified to a DPL that is equal to the DEI value in the tag. Otherwise the frame is classified to the default DPL.</p> <p>If the port is VLAN aware, the frame is tagged and Tag Class. Is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL.</p> <p>The classified DPL can be overruled by a QCL entry.</p> |
| PCP | <p>Controls the default PCP value.</p> <p>All frames are classified to a PCP value.</p> <p>If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.</p> |
| DEI | <p>Controls the default DEI value.</p> <p>All frames are classified to a DEI value.</p> <p>If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.</p> |

| Object | Description |
|--------------|---|
| Tag Class. | Shows the classification mode for tagged frames on this port. Disabled: Use default CoS and DPL for tagged frames. Enabled: Use mapped versions of PCP and DEI for tagged frames. Click on the mode in order to configure the mode and/or mapping. Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL. |
| DSCP Based | Click to Enable DSCP Based QoS Ingress Port Classification. |
| Address Mode | The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are: Source: Enable SMAC/SIP matching. Destination: Enable DMAC/DIP matching. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

QoS Ingress Port Classification Configuration

The classification mode for tagged frames are configured on this page.

QoS Ingress Port Tag Classification Port 1

Tagged Frames Settings

Tag Classification

(PCP, DEI) to (QoS class, DP level) Mapping

| PCP | DEI | QoS class | DP level |
|-----|-----|-----------|----------|
| * | * | <> | <> |
| 0 | 0 | 1 | 0 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 |
| 2 | 0 | 2 | 0 |
| 2 | 1 | 2 | 1 |
| 3 | 0 | 3 | 0 |
| 3 | 1 | 3 | 1 |
| 4 | 0 | 4 | 0 |
| 4 | 1 | 4 | 1 |
| 5 | 0 | 5 | 0 |
| 5 | 1 | 5 | 1 |
| 6 | 0 | 6 | 0 |
| 6 | 1 | 6 | 1 |
| 7 | 0 | 7 | 0 |
| 7 | 1 | 7 | 1 |

| Object | Description |
|---|--|
| Tag Classification | Controls the classification mode for tagged frames on this port. Disabled: Use default QoS class and Drop Precedence Level for tagged frames. Enabled: Use mapped versions of PCP and DEI for tagged frames. |
| (PCP, DEI) to (QoS class, DP level) Mapping | Controls the mapping of the classified (PCP, DEI) to (QoS class, DP level) values when Tag Classification is set to Enabled. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Cancel | Click to undo any changes made locally and return to the previous page. |

Port Policing

This page allows you to configure the Policer settings for all switch ports.

QoS Ingress Port Policers

| Port | Enable | Rate | Unit | Flow Control |
|------|--------------------------|------|--------|--------------------------|
| * | <input type="checkbox"/> | 500 | <> ▼ | <input type="checkbox"/> |
| 1 | <input type="checkbox"/> | 500 | kbps ▼ | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | 500 | kbps ▼ | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | 500 | kbps ▼ | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | 500 | kbps ▼ | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | 500 | kbps ▼ | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | 500 | kbps ▼ | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> | 500 | kbps ▼ | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> | 500 | kbps ▼ | <input type="checkbox"/> |
| 9 | <input type="checkbox"/> | 500 | kbps ▼ | <input type="checkbox"/> |
| 10 | <input type="checkbox"/> | 500 | kbps ▼ | <input type="checkbox"/> |
| 11 | <input type="checkbox"/> | 500 | kbps ▼ | <input type="checkbox"/> |

| Object | Description |
|--------------|--|
| Port | The port number for which the configuration below applies. |
| Enabled | Controls whether the policer is enabled on this switch port. |
| Rate | Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps". |
| Unit | Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps. The default value is "kbps". |
| Flow Control | If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

QoS Ingress Queue Policer Configuration

This page allows you to configure the Queue Policer settings for all switch ports.

QoS Ingress Queue Policers

| Port | Queue 0 | Queue 1 | Queue 2 | Queue 3 | Queue 4 | Queue 5 | Queue 6 | Queue 7 |
|------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| | Enable | Enable | Enable | Enable | Enable | Enable | Enable | Enable |
| * | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 9 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 10 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 11 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

The settings relate to the currently selected stack unit, as reflected by the page header.

| Object | Description |
|------------|---|
| Port | The port number for which the configuration below applies. |
| Enable (E) | Enable or disable the queue policer for this switch port. |
| Rate | Controls the rate for the queue policer. This value is restricted to 100-3276700 when "Unit" is kbps, and 1-3276 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer. This field is only shown if at least one of the queue policers are enabled. |
| Unit | Controls the unit of measure for the queue policer rate as kbps or Mbps. This field is only shown if at least one of the queue policers are enabled. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

Port Scheduler

This page provides an overview of QoS Egress Port Schedulers for all switch ports.

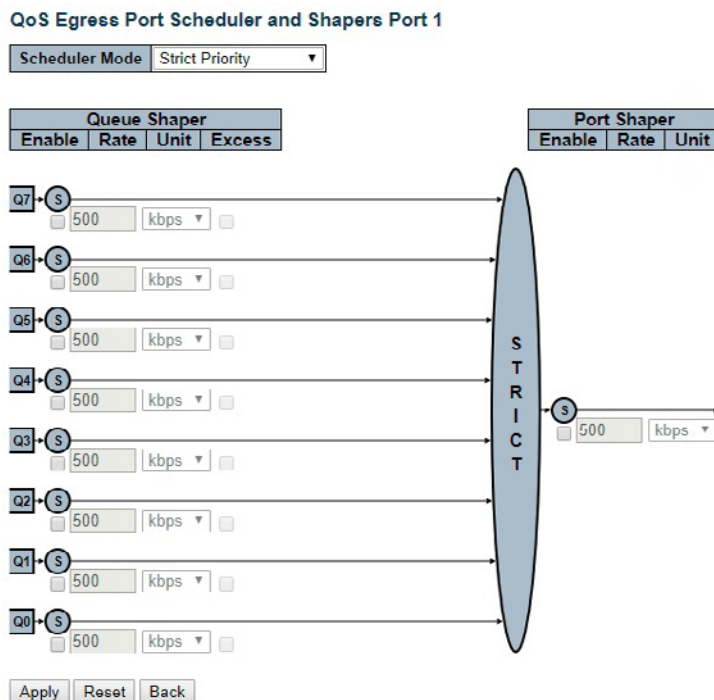
QoS Egress Port Schedulers

| Port | Mode | Weight | | | | | |
|-----------|-----------------|--------|----|----|----|----|----|
| | | Q0 | Q1 | Q2 | Q3 | Q4 | Q5 |
| <u>1</u> | Strict Priority | - | - | - | - | - | - |
| <u>2</u> | Strict Priority | - | - | - | - | - | - |
| <u>3</u> | Strict Priority | - | - | - | - | - | - |
| <u>4</u> | Strict Priority | - | - | - | - | - | - |
| <u>5</u> | Strict Priority | - | - | - | - | - | - |
| <u>6</u> | Strict Priority | - | - | - | - | - | - |
| <u>7</u> | Strict Priority | - | - | - | - | - | - |
| <u>8</u> | Strict Priority | - | - | - | - | - | - |
| <u>9</u> | Strict Priority | - | - | - | - | - | - |
| <u>10</u> | Strict Priority | - | - | - | - | - | - |
| <u>11</u> | Strict Priority | - | - | - | - | - | - |

| Object | Description |
|--------|---|
| Port | The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers. |
| Mode | Shows the scheduling mode for this port. |
| Qn | Shows the weight for this queue and port. |

QoS Egress Port Scheduler and Shapers Configuration

This page allows you to configure the Scheduler and Shapers for a specific port.



The settings relate to the currently selected stack unit, as reflected by the page header.

| Object | Description |
|-------------------------|--|
| Scheduler Mode | Controls how many of the queues are scheduled as strict and how many are scheduled as weighted on this switch port. |
| Queue Shaper Enable | Controls whether the queue shaper is enabled for this queue on this switch port. Ports in Basic or Hierarchical Scheduling Mode (HQoS setting) only have queue shapers on queue 6 and 7. |
| Queue Shaper Rate | Controls the rate for the queue shaper. This value is restricted to 100-3281943 when "Unit" is kbps, and 1-3281 when "Unit" is Mbps. Ports in Basic or Hierarchical Scheduling Mode (HQoS setting) only have queue shapers on queue 6 and 7. The rate is internally rounded up to the nearest value supported by the queue shaper. |
| Queue Shaper Unit | Controls the unit of measure for the queue shaper rate as kbps or Mbps. Ports in Basic or Hierarchical Scheduling Mode (HQoS setting) only have queue shapers on queue 6 and 7. |
| Queue Shaper Excess | Controls whether the queue is allowed to use excess bandwidth. Not shown for ports in Basic or Hierarchical Scheduling Mode (HQoS setting). |
| Queue Scheduler Weight | Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted". |
| Queue Scheduler Percent | Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted". |
| Port Shaper Enable | Controls whether the port shaper is enabled for this switch port. Only shown for Non-service configuration. |

| Object | Description |
|-----------------------------|--|
| Port Shaper Rate | Controls the rate for the port shaper. This value is restricted to 100-3281943 when "Unit" is kbps, and 1-3281 when "Unit" is Mbps. Only shown for Non-service configuration. The rate is internally rounded up to the nearest value supported by the port shaper. |
| Port Shaper Unit | Controls the unit of measure for the port shaper rate as kbps or Mbps. Only shown for Non-service configuration. |
| HQoS Shaper Enable | Controls whether the HQoS shaper is enabled for this HQoS ID. Only shown when configuring HQoS entries. |
| HQoS Shaper Rate | Controls the rate for the HQoS shaper. This value is restricted to 100-3281943 when "Unit" is kbps, and 1-3281 when "Unit" is Mbps. Only shown when configuring HQoS entries. The rate is internally rounded up to the nearest value supported by the HQoS shaper. |
| HQoS Shaper Unit | Controls the unit of measure for the HQoS shaper rate as kbps or Mbps. Only shown when configuring HQoS entries. |
| Guaranteed Bandwidth Enable | Controls whether the HQoS guaranteed bandwidth is enabled for this HQoS ID. Only shown when configuring HQoS entries. |
| Guaranteed Bandwidth Rate | Controls the rate for the guaranteed bandwidth. This value is restricted to 0-3281943 when "Unit" is kbps, and 0-3281 when "Unit" is Mbps. Only shown when configuring HQoS entries. |
| Guaranteed Bandwidth Unit | Controls the unit of measure for the guaranteed bandwidth as kbps or Mbps. Only shown when configuring HQoS entries. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Back | Click to undo any changes made locally and return to the previous page. |

Port shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports.

QoS Egress Port Shapers

| Port | Shapers | | | | | | | | Port |
|--------------------|---------|----|----|----|----|----|----|----|------|
| | Q0 | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 | |
| 1 | - | - | - | - | - | - | - | - | - |
| 2 | - | - | - | - | - | - | - | - | - |
| 3 | - | - | - | - | - | - | - | - | - |
| 4 | - | - | - | - | - | - | - | - | - |
| 5 | - | - | - | - | - | - | - | - | - |
| 6 | - | - | - | - | - | - | - | - | - |
| 7 | - | - | - | - | - | - | - | - | - |
| 8 | - | - | - | - | - | - | - | - | - |
| 9 | - | - | - | - | - | - | - | - | - |
| 10 | - | - | - | - | - | - | - | - | - |
| 11 | - | - | - | - | - | - | - | - | - |

| Object | Description |
|--------|--|
| Port | The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers. |
| Qn | Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps". |
| Port # | Shows "disabled" or actual port shaper rate - e.g. "800 Mbps". |

Port Tag Remarking

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.

QoS Egress Port Tag Remarking

| Port | Mode |
|--------------------|------------|
| 1 | Classified |
| 2 | Classified |
| 3 | Classified |
| 4 | Classified |
| 5 | Classified |
| 6 | Classified |
| 7 | Classified |
| 8 | Classified |
| 9 | Classified |
| 10 | Classified |
| 11 | Classified |

| Object | Description |
|--------|--|
| Port | The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking. |
| Mode | Shows the tag remarking mode for this port. Classified: Use classified PCP/DEI values. Default: Use default PCP/DEI values. Mapped: Use mapped versions of QoS class and DP level. |

QoS Egress Port Tag Remarking Configuration

The QoS Egress Port Tag Remarking for a specific port are configured on this page.

QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode

| Object | Description |
|---|--|
| Mode | Controls the tag remarking mode for this port. Classified: Use classified PCP/DEI values. Default: Use default PCP/DEI values. Mapped: Use mapped versions of QoS class and DP level. |
| PCP/DEI Configuration | Controls the default PCP and DEI values used when the mode is set to Default. |
| (QoS class, DP level) to (PCP, DEI) Mapping | Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to Mapped. |
| Apply | Click to apply changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Cancel | Click to undo any changes made locally and return to the previous page. |

Port DSCP

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports.

QoS Port DSCP Configuration

| Port | Ingress | | Egress |
|------|--------------------------|-----------|-----------|
| | Translate | Classify | Rewrite |
| * | <input type="checkbox"/> | <> ▼ | <> ▼ |
| 1 | <input type="checkbox"/> | Disable ▼ | Disable ▼ |
| 2 | <input type="checkbox"/> | Disable ▼ | Disable ▼ |
| 3 | <input type="checkbox"/> | Disable ▼ | Disable ▼ |
| 4 | <input type="checkbox"/> | Disable ▼ | Disable ▼ |
| 5 | <input type="checkbox"/> | Disable ▼ | Disable ▼ |
| 6 | <input type="checkbox"/> | Disable ▼ | Disable ▼ |
| 7 | <input type="checkbox"/> | Disable ▼ | Disable ▼ |
| 8 | <input type="checkbox"/> | Disable ▼ | Disable ▼ |
| 9 | <input type="checkbox"/> | Disable ▼ | Disable ▼ |
| 10 | <input type="checkbox"/> | Disable ▼ | Disable ▼ |
| 11 | <input type="checkbox"/> | Disable ▼ | Disable ▼ |

| Object | Description |
|-----------|---|
| Port | The Port column shows the list of ports for which you can configure dscp ingress and egress settings. |
| Ingress | In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: Translate Classify |
| Translate | To Enable the Ingress Translation click the checkbox. |
| Classify | Classification for a port has 4 different values. -Disable: No Ingress DSCP Classification. -DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0. -Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP. -All: Classify all DSCP. |
| Egress | Port Egress Rewriting can be one of - -Disable: No Egress rewrite. -Enable: Rewrite enabled without remapping. -Remap DP Unaware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table. -Remap DP Aware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

DSCP-Based QoS

This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.

DSCP-Based QoS Ingress Classification

| DSCP | Trust | QoS Class | DPL |
|-----------|--------------------------|-----------|------|
| * | <input type="checkbox"/> | <> ▼ | <> ▼ |
| 0 (BE) | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 1 | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 2 | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 3 | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 4 | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 5 | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 6 | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 7 | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 8 (CS1) | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 9 | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 10 (AF11) | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 11 | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 12 (AF12) | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 13 | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 14 (AF13) | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 15 | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 16 (CS2) | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 17 | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 18 (AF21) | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 19 | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 20 (AF22) | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 21 | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 22 (AF23) | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 23 | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 24 (CS3) | <input type="checkbox"/> | 0 ▼ | 0 ▼ |
| 25 | <input type="checkbox"/> | 0 ▼ | 0 ▼ |

| Object | Description |
|-----------|--|
| DSCP | Maximum number of supported DSCP values is 64. |
| Trust | Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame. |
| QoS Class | QoS class value can be any of (0-7) |
| DPL | Drop Precedence Level (0-1) |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

DSCP Translation

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

DSCP Translation

| DSCP | Ingress | | Egress | |
|-----------|-------------|--------------------------|-------------|-------------|
| | Translate | Classify | Remap DP0 | Remap DP1 |
| * | <> ▼ | <input type="checkbox"/> | <> ▼ | <> ▼ |
| 0 (BE) | 0 (BE) ▼ | <input type="checkbox"/> | 0 (BE) ▼ | 0 (BE) ▼ |
| 1 | 1 ▼ | <input type="checkbox"/> | 1 ▼ | 1 ▼ |
| 2 | 2 ▼ | <input type="checkbox"/> | 2 ▼ | 2 ▼ |
| 3 | 3 ▼ | <input type="checkbox"/> | 3 ▼ | 3 ▼ |
| 4 | 4 ▼ | <input type="checkbox"/> | 4 ▼ | 4 ▼ |
| 5 | 5 ▼ | <input type="checkbox"/> | 5 ▼ | 5 ▼ |
| 6 | 6 ▼ | <input type="checkbox"/> | 6 ▼ | 6 ▼ |
| 7 | 7 ▼ | <input type="checkbox"/> | 7 ▼ | 7 ▼ |
| 8 (CS1) | 8 (CS1) ▼ | <input type="checkbox"/> | 8 (CS1) ▼ | 8 (CS1) ▼ |
| 9 | 9 ▼ | <input type="checkbox"/> | 9 ▼ | 9 ▼ |
| 10 (AF11) | 10 (AF11) ▼ | <input type="checkbox"/> | 10 (AF11) ▼ | 10 (AF11) ▼ |
| 11 | 11 ▼ | <input type="checkbox"/> | 11 ▼ | 11 ▼ |
| 12 (AF12) | 12 (AF12) ▼ | <input type="checkbox"/> | 12 (AF12) ▼ | 12 (AF12) ▼ |
| 13 | 13 ▼ | <input type="checkbox"/> | 13 ▼ | 13 ▼ |
| 14 (AF13) | 14 (AF13) ▼ | <input type="checkbox"/> | 14 (AF13) ▼ | 14 (AF13) ▼ |
| 15 | 15 ▼ | <input type="checkbox"/> | 15 ▼ | 15 ▼ |
| 16 (CS2) | 16 (CS2) ▼ | <input type="checkbox"/> | 16 (CS2) ▼ | 16 (CS2) ▼ |
| 17 | 17 ▼ | <input type="checkbox"/> | 17 ▼ | 17 ▼ |
| 18 (AF21) | 18 (AF21) ▼ | <input type="checkbox"/> | 18 (AF21) ▼ | 18 (AF21) ▼ |
| 19 | 19 ▼ | <input type="checkbox"/> | 19 ▼ | 19 ▼ |
| 20 (AF22) | 20 (AF22) ▼ | <input type="checkbox"/> | 20 (AF22) ▼ | 20 (AF22) ▼ |
| 21 | 21 ▼ | <input type="checkbox"/> | 21 ▼ | 21 ▼ |
| 22 (AF23) | 22 (AF23) ▼ | <input type="checkbox"/> | 22 (AF23) ▼ | 22 (AF23) ▼ |
| 23 | 23 ▼ | <input type="checkbox"/> | 23 ▼ | 23 ▼ |
| 24 (CS3) | 24 (CS3) ▼ | <input type="checkbox"/> | 24 (CS3) ▼ | 24 (CS3) ▼ |
| 25 | 25 ▼ | <input type="checkbox"/> | 25 ▼ | 25 ▼ |
| 26 (AF31) | 26 (AF31) ▼ | <input type="checkbox"/> | 26 (AF31) ▼ | 26 (AF31) ▼ |
| 27 | 27 ▼ | <input type="checkbox"/> | 27 ▼ | 27 ▼ |
| 28 (AF32) | 28 (AF32) ▼ | <input type="checkbox"/> | 28 (AF32) ▼ | 28 (AF32) ▼ |
| 29 | 29 ▼ | <input type="checkbox"/> | 29 ▼ | 29 ▼ |

| Object | Description |
|-------------|--|
| DSCP | Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63. |
| Ingress | Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation : Translate Classify |
| Translation | DSCP at Ingress side can be translated to any of (0-63) DSCP values. |
| Classify | Click to enable Classification at Ingress side. |
| Egress | There are the following configurable parameters for Egress side - Remap DP0 Controls the remapping for frames with DP level 0. Remap DP1 Controls the remapping for frames with DP level 1. |
| Remap DP0 | Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63. |
| Remap DP1 | Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

DSCP Classification

This page allows you to configure the mapping of QoS class and Drop Precedence Level to DSCP value.

DSCP Classification

| QoS Class | DSCP DP0 | DSCP DP1 |
|-----------|----------|----------|
| * | <> ▼ | <> ▼ |
| 0 | 0 (BE) ▼ | 0 (BE) ▼ |
| 1 | 0 (BE) ▼ | 0 (BE) ▼ |
| 2 | 0 (BE) ▼ | 0 (BE) ▼ |
| 3 | 0 (BE) ▼ | 0 (BE) ▼ |
| 4 | 0 (BE) ▼ | 0 (BE) ▼ |
| 5 | 0 (BE) ▼ | 0 (BE) ▼ |
| 6 | 0 (BE) ▼ | 0 (BE) ▼ |
| 7 | 0 (BE) ▼ | 0 (BE) ▼ |

Apply Reset

| Object | Description |
|-----------|--|
| QoS Class | Actual QoS class. |
| DSCP DP0 | Select the classified DSCP value (0-63) for Drop Precedence Level 0. |
| DSCP DP1 | Select the classified DSCP value (0-63) for Drop Precedence Level 1. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

QoS Control List

This page shows the QoS Control List(QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch.

Click on the lowest plus sign to add a new QCE to the list.

QoS Control List Configuration

| QCE | Port | DMAC | SMAC | Tag Type | VID | PCP | DEI | Frame Type | Action | | | | |
|-----|------|------|------|----------|-----|-----|-----|------------|--------|-----|------|-----|-----|
| | | | | | | | | | CoS | DPL | DSCP | PCP | DEI |
| + | | | | | | | | | | | | | |

| Object | Description |
|----------------------|---|
| QCE | Indicates the QCE id. |
| Port | Indicates the list of ports configured with the QCE. |
| DMAC | Indicates the destination MAC address. Possible values are: Any: Match any DMAC. Unicast: Match unicast DMAC. Multicast: Match multicast DMAC. Broadcast: Match broadcast DMAC. The default value is 'Any'. |
| SMAC | Match specific source MAC address or 'Any'. If a port is configured to match on DMAC/DIP, this field indicates the DMAC. |
| Tag Type | Indicates tag type. Possible values are: Any: Match tagged and untagged frames. Untagged: Match untagged frames. Tagged: Match tagged frames. The default value is 'Any'. |
| VID | Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any' |
| PCP | Priority Code Point: Valid values of PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'. |
| DEI | Drop Eligible Indicator: Valid value of DEI is 0, 1 or 'Any'. |
| Frame Type | Indicates the type of frame. Possible values are: Any: Match any frame type. Ethernet: Match EtherType frames. LLC: Match (LLC) frames. SNAP: Match (SNAP) frames. IPv4: Match IPv4 frames. IPv6: Match IPv6 frames. |
| Action | Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are: CoS: Classify Class of Service. DPL: Classify Drop Precedence Level. DSCP: Classify DSCP value. |
| Modification Buttons | You can modify each QCE (QoS Control Entry) in the table using the following buttons: "+": Inserts a new QCE before the current row "e": Edits the QCE. "Up": Moves the QCE up the list. "Down": Moves the QCE down the list. "X": Deletes the QCE. "+": The lowest plus sign adds a new entry at the bottom of the QCE listings. |

The QCE page includes the following fields:

QCE Configuration

| Port Members | | | | | | | | | | |
|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Key Parameters

| | |
|------------|-------|
| DMAC | Any ▾ |
| SMAC | Any ▾ |
| Tag | Any ▾ |
| VID | Any ▾ |
| PCP | Any ▾ |
| DEI | Any ▾ |
| Frame Type | Any ▾ |

Action Parameters

| | |
|--------|-----------|
| CoS | 0 ▾ |
| DPL | Default ▾ |
| DSCP | Default ▾ |
| PCP | Default ▾ |
| DEI | Default ▾ |
| Policy | |

Apply Reset Cancel

| Object | Description |
|-------------------|---|
| Port Members | Check the checkbox button to include the port in the QCL entry. By default all ports are included. |
| Key Paramente | <p>Key configuration is described as below:</p> <p>DMAC Destination MAC address: Possible values are 'Unicast', 'Multicast', 'Broadcast' or 'Any'.</p> <p>SMAC Source MAC address: xx-xx-xx-xx-xx-xx or 'Any'. If a port is configured to match on DMAC/DIP, this field is the Destination MAC address.</p> <p>Tag - Value of Tag field can be 'Untagged', 'Tagged' or 'Any'.</p> <p>VID - Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.</p> <p>PCP - Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.</p> <p>DEI - Valid value of DEI can be '0', '1' or 'Any'.</p> <p>Frame Type - Frame Type can have any of the following values: Any: Allow all types of frames.</p> <p>EtherType: Ether Type Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.</p> <p>LLC: SSAP Address - Valid SSAP (Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'.</p> <p>DSAP Address - Valid DSAP (Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'.</p> <p>Control - Valid Control field can vary from 0x00 to 0xFF or 'Any'.</p> <p>SNAP: PID - Valid PID (a.k.a Ether Type) can be 0x0000-0xFFFF or 'Any'.</p> <p>IPv4: Protocol - IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.</p> <p>Source IP Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255.</p> <p>When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero. If a port is configured to match on DMAC/DIP, this field is the Destination IP address.</p> <p>IP Fragment IPv4 frame fragmented option: 'Yes', 'No' or 'Any'.</p> <p>DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.</p> <p>Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.</p> <p>Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.</p> <p>IPv6: Protocol IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.</p> <p>Source IP 32 LS bits of IPv6 source address in value/mask format or 'Any'. If a port is configured to match on DMAC/DIP, this field is the Destination IP address.</p> <p>DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.</p> <p>Sport Source TCP/UDP port :(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.</p> <p>Dport Destination TCP/UDP port :(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.</p> |
| Action Parameters | <p>CoS Class of Service: (0-7) or 'Default'.</p> <p>DP Drop Precedence Level: (0-1) or 'Default'.</p> <p>DSCP DSCP: (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.</p> <p>'Default' means that the default classified value is not modified by this QCE.</p> |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |
| Cancel | Click to return to previous values without saving. |

Storm Policing

Storm control for the switch is configured on this page.

There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch.

Global Storm Policer Configuration

| Frame Type | Enable | Rate | Unit |
|------------|--------------------------|------|-------|
| Unicast | <input type="checkbox"/> | 1 | fps ▼ |
| Multicast | <input type="checkbox"/> | 1 | fps ▼ |
| Broadcast | <input type="checkbox"/> | 1 | fps ▼ |

| Object | Description |
|------------|---|
| Frame Type | The settings in a particular row apply to the frame type listed here: Unicast, Multicast or Broadcast. |
| Enable | Enable or disable the storm control status for the given frame type. |
| Rate | The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

Mirroring & Remote Mirroring Configuration

Mirroring is a feature for switched port analyzer. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

Remote Mirroring is an extend function of Mirroring. It can extend the destination port in other switch, allowing the administrator to analyze the network traffic on the other switches.

If you want to get the tagged mirrored traffic, you have to set VLAN egress tagging as "Tag All" on the reflector port. On the other hand, if you want to get untagged mirrored traffic, you have to set VLAN egress tagging as "Untag ALL" on the reflector port.

Mirroring & Remote Mirroring Configuration

| | |
|----------------|------------|
| Mode | Disabled ▼ |
| Type | Mirror ▼ |
| VLAN ID | 200 |
| Reflector Port | Port 1 ▼ |

Source VLAN(s) Configuration

| | |
|--------------|--|
| Source VLANs | |
|--------------|--|

Port Configuration

| Port | Source | Intermediate | Destination |
|------|------------|--------------------------|--------------------------|
| 1 | Disabled ▼ | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | Disabled ▼ | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | Disabled ▼ | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | Disabled ▼ | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | Disabled ▼ | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | Disabled ▼ | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | Disabled ▼ | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | Disabled ▼ | <input type="checkbox"/> | <input type="checkbox"/> |
| 9 | Disabled ▼ | <input type="checkbox"/> | <input type="checkbox"/> |
| 10 | Disabled ▼ | <input type="checkbox"/> | <input type="checkbox"/> |
| 11 | Disabled ▼ | <input type="checkbox"/> | <input type="checkbox"/> |
| CPU | Disabled ▼ | <input type="checkbox"/> | <input type="checkbox"/> |

Apply Reset

| Object | Description |
|--------------|--|
| Mode | Enables/Disables the mirror or Remote Mirroring function. |
| Type | Select switch type. |
| Mirror | The switch is running on mirror mode. The source port(s) and destination port are located on this switch. |
| Source | The switch is a source node for monitor flow. The source port(s), reflector port and intermediate port(s) are located on this switch. |
| Intermediate | The switch is a forwarding node for monitor flow and the switch is an option node. The object is to forward traffic from source switch to destination switch. The intermediate ports are located on this switch. |

| Object | Description |
|------------------------------|--|
| Destination | The switch is an end node for monitor flow. The destination port(s) and intermediate port(s) are located on this switch. |
| VLAN ID | The VLAN ID points out where the monitor packet will copy to. The default VLAN ID is 200. |
| Reflector Port | The reflector port is a method to redirect the traffic to Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until the Remote Mirroring is disabled. In the stacking mode, you need to select switch ID to select the correct device. If you shut down a port, it cannot be a candidate for reflector port. If you shut down the port which is a reflector port, the remote mirror function cannot work. Note1: The reflector port needs to select only on Source switch type. Note2: The reflector port needs to disable MAC Table learning and STP. Note3: The reflector port only supports on pure copper ports. |
| Source VLAN(s) Configuration | The switch can supports VLAN-based Mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs on this field. Note1: The Mirroring session shall have either ports or VLANs as sources, but not both. |

Remote Mirroring Port Configuration

| | |
|--------------|--|
| Port | The logical port for the settings contained in the same row. |
| Source | Select mirror mode. Disabled Neither frames transmitted nor frames received are mirrored. Both Frames received and frames transmitted are mirrored on the Intermediate/Destination port. Rx only Frames received on this port are mirrored on the Intermediate/Destination port. Frames transmitted are not mirrored. Tx only Frames transmitted on this port are mirrored on the Intermediate/Destination port. Frames received are not mirrored. |
| Intermediate | Select intermediate port. This checkbox is designed for Remote Mirroring. The intermediate port is a switched port to connect to other switch. Note: The intermediate port needs to disable MAC Table learning. |
| Destination | Select destination port. This checkbox is designed for mirror or Remote Mirroring. The destination port is a switched port that you receive a copy of traffic from the source port. Note1: On mirror mode, the device only supports one destination port. Note2: The destination port needs to disable MAC Table learning. |

| Object | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|--|-------------|----------------|-------------------|------------------|-----------------------|------------------|-----------------------|----------------|------|--|------------|------------|--|--|-----|----------|--|------------|------------|------------|--|------------|------|--|------------|------------|--|--|---------------|------|--|------------|------------|--|--|-----------------|----------|--|------------|------------|------------|--|--------------|----------|--|--|--|--|-------------|------------|----------|--|--|--|--|-------------|------|-----|--|--|--|------------|--|------|-----|--|--|--|------------|--|--------------|----------|--|------------|------------|------------|--|------|----------|--|------------|--|------------|--|-----|----------|--|--|--|--|-------------|-----|----------|--|--------------|--------------|--------------|--|------|----------|--|------------|------------|------------|--|-----|----------|--|-------------|-------------|-------------|--|------|-----|--|--|--|------------|--|----------------|----------|--|------------|------------|--|--|---------------------|----------|--|------------|------------|--|--|------------------|----------|--|------------|------------|------------|--|------------|----------|--|------------|------------|--|--|-----|-----|--|--|--|------------|--|------|-----|--|--|--|------------|--|
| Configuration Guideline for All Features | <p>When the switch is running on Remote Mirroring mode, the administrator also needs to check whether or not other features are enabled or disabled.</p> <p>For example, the administrator is not disabled the MSTP on reflector port. All monitor traffic will be blocked on reflector port.</p> <p>All recommended settings are described as follows.</p> <table border="1"> <thead> <tr> <th></th> <th>Impact</th> <th>source port</th> <th>reflector port</th> <th>intermediate port</th> <th>destination port</th> <th>Remote Mirroring VLAN</th> </tr> </thead> <tbody> <tr> <td>arp_inspection</td> <td>High</td> <td></td> <td>* disabled</td> <td>* disabled</td> <td></td> <td></td> </tr> <tr> <td>acl</td> <td>Critical</td> <td></td> <td>* disabled</td> <td>* disabled</td> <td>* disabled</td> <td></td> </tr> <tr> <td>dhcp_relay</td> <td>High</td> <td></td> <td>* disabled</td> <td>* disabled</td> <td></td> <td></td> </tr> <tr> <td>dhcp_snooping</td> <td>High</td> <td></td> <td>* disabled</td> <td>* disabled</td> <td></td> <td></td> </tr> <tr> <td>ip_source_guard</td> <td>Critical</td> <td></td> <td>* disabled</td> <td>* disabled</td> <td>* disabled</td> <td></td> </tr> <tr> <td>ipmc/igmpsnp</td> <td>Critical</td> <td></td> <td></td> <td></td> <td></td> <td>un-conflict</td> </tr> <tr> <td>ipmc/mldsn</td> <td>Critical</td> <td></td> <td></td> <td></td> <td></td> <td>un-conflict</td> </tr> <tr> <td>lacp</td> <td>Low</td> <td></td> <td></td> <td></td> <td>o disabled</td> <td></td> </tr> <tr> <td>lldp</td> <td>Low</td> <td></td> <td></td> <td></td> <td>o disabled</td> <td></td> </tr> <tr> <td>mac learning</td> <td>Critical</td> <td></td> <td>* disabled</td> <td>* disabled</td> <td>* disabled</td> <td></td> </tr> <tr> <td>mstp</td> <td>Critical</td> <td></td> <td>* disabled</td> <td></td> <td>o disabled</td> <td></td> </tr> <tr> <td>mvr</td> <td>Critical</td> <td></td> <td></td> <td></td> <td></td> <td>un-conflict</td> </tr> <tr> <td>nas</td> <td>Critical</td> <td></td> <td>* authorized</td> <td>* authorized</td> <td>* authorized</td> <td></td> </tr> <tr> <td>psec</td> <td>Critical</td> <td></td> <td>* disabled</td> <td>* disabled</td> <td>* disabled</td> <td></td> </tr> <tr> <td>qos</td> <td>Critical</td> <td></td> <td>* unlimited</td> <td>* unlimited</td> <td>* unlimited</td> <td></td> </tr> <tr> <td>upnp</td> <td>Low</td> <td></td> <td></td> <td></td> <td>o disabled</td> <td></td> </tr> <tr> <td>mac-based vlan</td> <td>Critical</td> <td></td> <td>* disabled</td> <td>* disabled</td> <td></td> <td></td> </tr> <tr> <td>protocol-based vlan</td> <td>Critical</td> <td></td> <td>* disabled</td> <td>* disabled</td> <td></td> <td></td> </tr> <tr> <td>vlan_translation</td> <td>Critical</td> <td></td> <td>* disabled</td> <td>* disabled</td> <td>* disabled</td> <td></td> </tr> <tr> <td>voice_vlan</td> <td>Critical</td> <td></td> <td>* disabled</td> <td>* disabled</td> <td></td> <td></td> </tr> <tr> <td>mrp</td> <td>Low</td> <td></td> <td></td> <td></td> <td>o disabled</td> <td></td> </tr> <tr> <td>mvrp</td> <td>Low</td> <td></td> <td></td> <td></td> <td>o disabled</td> <td></td> </tr> </tbody> </table> <p>Note: * -- required o -- optional Impact: Critical/High/Low</p> <p>Critical 5 packets -> 0 packet High 5 packets -> 4 packets Low 5 packets -> 6 packets</p> | | Impact | source port | reflector port | intermediate port | destination port | Remote Mirroring VLAN | arp_inspection | High | | * disabled | * disabled | | | acl | Critical | | * disabled | * disabled | * disabled | | dhcp_relay | High | | * disabled | * disabled | | | dhcp_snooping | High | | * disabled | * disabled | | | ip_source_guard | Critical | | * disabled | * disabled | * disabled | | ipmc/igmpsnp | Critical | | | | | un-conflict | ipmc/mldsn | Critical | | | | | un-conflict | lacp | Low | | | | o disabled | | lldp | Low | | | | o disabled | | mac learning | Critical | | * disabled | * disabled | * disabled | | mstp | Critical | | * disabled | | o disabled | | mvr | Critical | | | | | un-conflict | nas | Critical | | * authorized | * authorized | * authorized | | psec | Critical | | * disabled | * disabled | * disabled | | qos | Critical | | * unlimited | * unlimited | * unlimited | | upnp | Low | | | | o disabled | | mac-based vlan | Critical | | * disabled | * disabled | | | protocol-based vlan | Critical | | * disabled | * disabled | | | vlan_translation | Critical | | * disabled | * disabled | * disabled | | voice_vlan | Critical | | * disabled | * disabled | | | mrp | Low | | | | o disabled | | mvrp | Low | | | | o disabled | |
| | Impact | source port | reflector port | intermediate port | destination port | Remote Mirroring VLAN | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| arp_inspection | High | | * disabled | * disabled | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| acl | Critical | | * disabled | * disabled | * disabled | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dhcp_relay | High | | * disabled | * disabled | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dhcp_snooping | High | | * disabled | * disabled | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ip_source_guard | Critical | | * disabled | * disabled | * disabled | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ipmc/igmpsnp | Critical | | | | | un-conflict | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ipmc/mldsn | Critical | | | | | un-conflict | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| lacp | Low | | | | o disabled | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| lldp | Low | | | | o disabled | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| mac learning | Critical | | * disabled | * disabled | * disabled | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| mstp | Critical | | * disabled | | o disabled | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| mvr | Critical | | | | | un-conflict | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| nas | Critical | | * authorized | * authorized | * authorized | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| psec | Critical | | * disabled | * disabled | * disabled | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| qos | Critical | | * unlimited | * unlimited | * unlimited | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| upnp | Low | | | | o disabled | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| mac-based vlan | Critical | | * disabled | * disabled | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| protocol-based vlan | Critical | | * disabled | * disabled | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| vlan_translation | Critical | | * disabled | * disabled | * disabled | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| voice_vlan | Critical | | * disabled | * disabled | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| mrp | Low | | | | o disabled | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| mvrp | Low | | | | o disabled | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Apply | Click to apply changes. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Reset | Click to undo any changes made locally and revert to previously saved values. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

UPnP

Configure UPnP on this page.

UPnP Configuration

| | |
|----------------------|------------|
| Mode | Disabled ▾ |
| TTL | 4 |
| Advertising Duration | 100 |

| Object | Description |
|----------------------|---|
| Mode | Indicates the UPnP operation mode. Possible modes are: Enabled: Enable UPnP mode operation. Disabled: Disable UPnP mode operation. When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled. |
| TTL | The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255. |
| Advertising Duration | The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

GVRP

Global Configuration

This page allows you to configure the basic GVRP Configuration settings for all switch ports.

GVRP Configuration

Enable GVRP

| Parameter | Value |
|----------------|-------|
| Join-time: | 20 |
| Leave-time: | 60 |
| LeaveAll-time: | 1000 |
| Max VLANs: | 20 |

Apply

| Object | Description |
|----------------------|---|
| GVRP Protocol timers | Join-time is a value in the range 1-20 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 20. Leave-time is a value in the range 60-300 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 60. Leave All-time is a value in the range 1000-5000 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 1000. |
| Max number of VLANs | When GVRP is enabled a maximum number of VLANs supported by GVRP is specified. By default this number is 20. This number can only be changed when GVRP is turned off. |
| Apply | Click to apply changes. |

Port Configuration

This page allows you to enable/disable a port for GVRP.

GVRP Port Configuration

| Port | Mode |
|------|------------|
| * | <> ▼ |
| 1 | Disabled ▼ |
| 2 | Disabled ▼ |
| 3 | Disabled ▼ |
| 4 | Disabled ▼ |
| 5 | Disabled ▼ |
| 6 | Disabled ▼ |
| 7 | Disabled ▼ |
| 8 | Disabled ▼ |
| 9 | Disabled ▼ |
| 10 | Disabled ▼ |
| 11 | Disabled ▼ |

| Object | Description |
|--------|--|
| Port | The logical port that is to be configured. |
| Mode | Mode can be either 'Disabled' or 'GVRP enabled'. These values turn the GVRP feature off or on respectively for the port in question. |
| Apply | Click to apply changes. |
| Reset | Click to revert to previous values. |

Monitor Menu

System

System Information

The switch system information is provided here

System Information

| System | |
|------------------|---------------------------|
| Contact | |
| Name | |
| Location | |
| Hardware | |
| MAC Address | 00-22-3b-02-07-bc |
| Time | |
| System Date | 1970-01-01T15:57:45+00:00 |
| System Uptime | 0d 15:57:45 |
| Software | |
| Software Version | Firmware Version 1.3.0 |
| Software Date | 2017-07-31T16:36:09-04:00 |

| Object | Description |
|------------------|--|
| Contact | The system contact configured in Configuration System Information System Contact. |
| Name | The system name configured in Configuration System Information System Name. |
| Location | The system location configured in Configuration System Information System Location. |
| MAC Address | The MAC Address of this switch. |
| System Date | The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any. |
| System Uptime | The period of time the device has been operational. |
| Software Version | The software version of this switch. |
| Software Date | The date when the switch software was produced. |

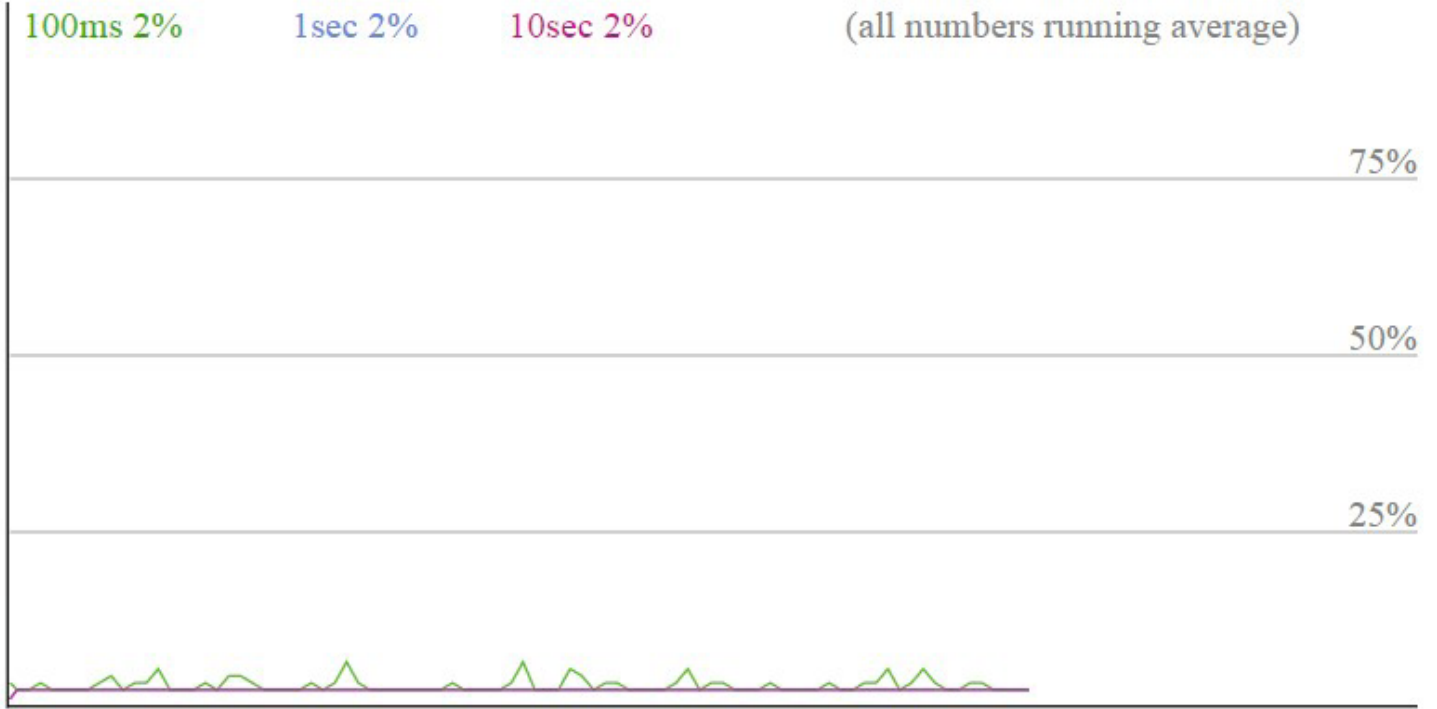
CUP Load

This page displays the CPU load, using line chart.

The load is measured as averaged over the last 100ms, 1 s and 10 seconds intervals. The last 1~256 samples (maximum 256) are graphed, and the last numbers are displayed as text as well.

CPU Load

Auto-refresh



Auto_refresh Check to refresh the page automatically every 3 seconds.

Input Power Status

This page shows the status of the 2 power inputs along with power LED's and the fault relay status.

Power Supply Status

Auto-refresh

| Power Supply 1 State | Power Supply 2 State | Alarm State | PS1 Fault LED | PS2 Fault LED |
|----------------------|----------------------|-------------|-----------------|-----------------|
| PS1 Connected | PS2 Not Connected | Fault Cond. | PS1 FLT LED OFF | PS2 FLT LED OFF |

Auto_refresh Check to refresh the page automatically every 3 seconds.

Refresh Click to refresh the displayed table starting from the input fields.

System IP Status

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbour cache (ARP cache) status.

IP Interfaces

Auto-refresh Refresh

| Interface | Type | Address | Status |
|-----------|------|----------------------------|----------------------------------|
| OS:lo | LINK | 00-00-00-00-00-00 | <UP LOOPBACK RUNNING MULTICAST> |
| OS:lo | IPv4 | 127.0.0.1/8 | |
| OS:lo | IPv6 | fe80::1/64 | |
| OS:lo | IPv6 | ::1/128 | |
| VLAN1 | LINK | 00-22-3b-02-07-bc | <UP BROADCAST RUNNING MULTICAST> |
| VLAN1 | IPv4 | 192.168.10.1/24 | |
| VLAN1 | IPv6 | fe80::222:3bff:fe02:7bc/64 | |

IP Routes

| Network | Gateway | Status |
|--------------|----------------|--------------------|
| 0.0.0.0/0 | 192.168.10.254 | <UP GATEWAY HW_RT> |
| 127.0.0.1/32 | 127.0.0.1 | <UP HOST> |
| 224.0.0.0/4 | 127.0.0.1 | <UP> |
| ::1/128 | ::1 | <UP HOST> |

Neighbour cache

| IP Address | Link Address |
|--------------------------|-------------------------|
| 192.168.10.32 | VLAN1:50-e5-49-dd-ee-c6 |
| 192.168.10.69 | VLAN1:d4-81-d7-41-11-16 |
| fe80::222:3bff:fe02:7bc | VLAN1:00-22-3b-02-07-bc |
| fe80::222:3bff:fe03:8985 | VLAN1:00-22-3b-03-89-85 |

| Object | Description |
|-----------------------|--|
| IP Interfaces | |
| Interface | The name of the interface. |
| Type | The address type of the entry. This may be LINK or IPv4. |
| Address | The current address of the interface (of the given type). |
| Status | The status flags of the interface (and/or address). |
| IP Routes | |
| Network | The destination IP network or host address of this route. |
| Gateway | The gateway address of this route. |
| Status | The status flags of the route. |
| Neighbor cache | |
| IP Address | The IP address of the entry. |
| Link Address | The Link (MAC) address for which a binding to the IP address given exist.. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Reset | Click to refresh screen without Auto_refresh. |

System Log

Each page shows up to 999 table entries, selected through the “entries per page” input field. When first visited, the web page will show the beginning entries of this table.

The “Level” input field is used to filter the display system log entries.

The “Clear Level” input field is used to specify which system log entries will be cleared.

To clear specific system log entries, select the clear level first then click the “Clear” button.

The “Start from ID” input field allow the user to change the starting point in this table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next entry match.

In addition, these input fields will upon a “Refresh” button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

The “>>” will use the last entry of the currently displayed table as a basis for the next lookup.

When the end is reached the text “No more entries” is shown in the displayed table. Use the “<<|” button to start over.

System Log Information

Auto-refresh Refresh Clear |<< << >> >>|

| | |
|-------------|-------|
| Level | All ▼ |
| Clear Level | All ▼ |

The total number of entries is 5 for the given level.

Start from ID with entries per page.

| ID | Level | Time | Message |
|----|---------------|---------------------------|--|
| 1 | Informational | 1970-01-01T00:00:01+00:00 | SYS-FIRMWARE: New firmware active: ComNetFirmware Version 1.3.0 |
| 2 | Informational | 1970-01-01T00:00:02+00:00 | SYS-BOOTING: Switch just made a cool boot. |
| 3 | Notice | 1970-01-01T00:00:02+00:00 | LINK-UPDOWN: Interface Vlan 1, changed state to down. |
| 4 | Notice | 1970-01-01T00:00:05+00:00 | LINK-UPDOWN: Interface GigabitEthernet 1/1, changed state to up. |
| 5 | Notice | 1970-01-01T00:00:07+00:00 | LINK-UPDOWN: Interface Vlan 1, changed state to up. |

| Object | Description |
|--------------|--|
| ID | The identification of the system log entry. |
| Level | The level of the system log entry. Info: The system log entry is belonged information level.“Warning: The system log entry is belonged warning level.”Error: The system log entry is belonged error level. |
| Time | The occurred time of the system log entry. |
| Message | The detail message of the system log entry. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to Updates the table entries, starting from the current entry. |
| Clear | Click to Flush the selected entries. |
| << | Click to update the table entries, starting from the first available entry. |
| << | Click to update the table entries, ending at the last entry currently displayed. |
| >> | Click to update the table entries, starting from the last entry currently displayed. |

>>| Click to update the table entries, ending at the last available entry.

System Detailed Log

The switch system detailed log information is provided here.

Detailed System Log Information

Refresh |<< << >> >>|

ID

Message

| | |
|---------|---|
| Level | Informational |
| Time | 1970-01-01T00:00:01+00:00 |
| Message | SYS-FIRMWARE: New firmware active: ComNetFirmware Version 1.3.0 |

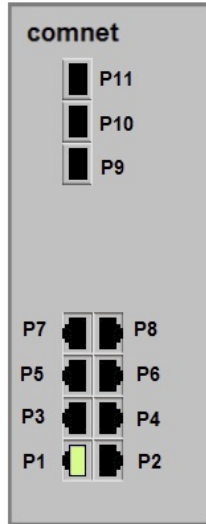
| Object | Description |
|---------|--|
| ID | The ID (>= 1) of the system log entry. |
| Message | The detailed message of the system log entry. |
| Refresh | Click to update the system log entry to the current entry ID.. |
| << | Click to update the system log entry to the first available entry ID. |
| << | Click to update the system log entry to the previous available entry ID. |
| >> | Click to update the system log entry to the next available entry ID. |
| >> | Click to update the system log entry to the last available entry ID. |

Port State

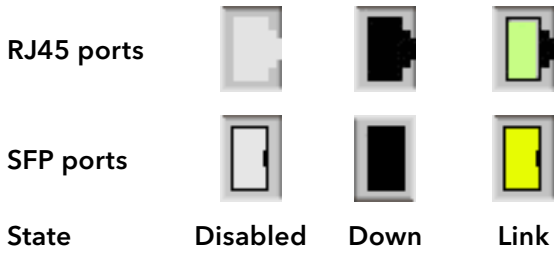
This page provides an overview of the current switch port states.

Port State Overview

Auto-refresh Refresh



The port states are illustrated as follows:



| Object | Description |
|--------------|---|
| Auto-refresh | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page. |

Green Ethernet

Port Power Savings

This page provides the current status for EEE.

Port Power Savings Status Auto refresh Refresh

| Port | Link | EEE Cap | EEE Ena | LP EEE Cap | EEE In power save | ActiPhy Savings | PerfectReach Savings |
|------|------|---------|---------|------------|-------------------|-----------------|----------------------|
| 1 | | | | | | | |
| 2 | | | | | | | |
| 3 | | | | | | | |
| 4 | | | | | | | |
| 5 | | | | | | | |
| 6 | | | | | | | |
| 7 | | | | | | | |
| 8 | | | | | | | |
| 9 | | | | | | | |
| 10 | | | | | | | |
| 11 | | | | | | | |

| Object | Description |
|----------------------|---|
| Port | This is the logical port number for this row. |
| Link | Shows if the link is up for the port (green = link up, red = link down). |
| EEE | Shows if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page). |
| LP EEE cap | Shows if the link partner is EEE capable. |
| EEE Savings | Shows if the system is currently saving power due to EEE. When EEE is enabled, the system will powered down if no frame has been received or transmitted in 5 uSec. |
| ActiPhy Saving | Shows if the system is currently saving power due to ActiPhy. |
| PerfectReach Savings | Shows if the system is currently saving power due to PerfectReach. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh screen without Auto_refresh. |

Thermal Protection

This page shows thermal status of the switch. The thermal settings are configured in Configuration > Thermal Protection

Thermal Protection Status Auto-refresh Refresh

Thermal Protection Port Status

| Port | Temperature | Port status |
|------|-------------|------------------------------|
| 1 | 40 °C | Port link operating normally |
| 2 | 38 °C | Port link operating normally |
| 3 | 38 °C | Port link operating normally |
| 4 | 39 °C | Port link operating normally |
| 5 | 39 °C | Port link operating normally |
| 6 | 38 °C | Port link operating normally |
| 7 | 38 °C | Port link operating normally |
| 8 | 38 °C | Port link operating normally |
| 9 | 39 °C | Port link operating normally |
| 10 | 38 °C | Port link operating normally |
| 11 | 38 °C | Port link operating normally |

Auto_refresh Check to refresh the page automatically every 3 seconds.

Refresh Click to refresh screen without Auto_refresh.

Ports

Traffic Overview

This page provides an overview of general traffic statistics for all switch ports.

Port Statistics Overview

Auto-refresh Refresh Clear

| Port | Packets | | Bytes | | Errors | | Drops | | Filtered |
|------|----------|-------------|----------|-------------|----------|-------------|----------|-------------|----------|
| | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received |
| 1 | 405977 | 2901 | 92460022 | 574903 | 0 | 0 | 0 | 0 | 152537 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| Object | Description |
|--------|-------------|
|--------|-------------|

| | |
|------|--|
| Port | The logical port for the settings contained in the same row. |
|------|--|

| | |
|--------|--|
| Packet | The number of received and transmitted packets per port. |
|--------|--|

| | |
|-------|--|
| Bytes | The number of received and transmitted bytes per port. |
|-------|--|

| | |
|--------|---|
| Errors | The number of frames received in error and the number of incomplete transmissions per port. |
|--------|---|

| | |
|-------|---|
| Drops | The number of frames discarded due to ingress or egress congestion. |
|-------|---|

| | |
|----------|---|
| Filtered | The number of received frames filtered by the forwarding process. |
|----------|---|

| | |
|--------------|--|
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
|--------------|--|

| | |
|---------|----------------------------|
| Refresh | Click to refresh the page. |
|---------|----------------------------|

| | |
|-------|--|
| Clear | Click to clear the counters for all ports. |
|-------|--|

QoS Statistics

This page provides statistics for the different queues for all switch ports.

Queuing Counters

Auto-refresh Refresh Clear

| Port | Q0 | | Q1 | | Q2 | | Q3 | | Q4 | | Q5 | | Q6 | | Q7 | |
|------|--------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------|
| | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx |
| 1 | 406336 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2988 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| Object | Description |
|--------------|---|
| Port | The logical port for the settings contained in the same row. |
| Qn | There are 8 QoS queues per port. Q0 is the lowest priority queue. |
| Rx/Tx | The number of received and transmitted packets per queue |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the page. |
| Clear | Click to clear the counters for all ports. |

QCL Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

QoS Control List Status

Combined ▼

 Auto-refresh

Resolve Conflict

Refresh

| User | QCE | Port | Frame Type | Action | | | | | | Conflict |
|------------|-----|------|------------|--------|-----|------|-----|-----|--------|----------|
| | | | | CoS | DPL | DSCP | PCP | DEI | Policy | |
| No entries | | | | | | | | | | |

| Object | Description |
|------------------|--|
| User | Indicates the QCL user. |
| QCE | Indicates the QCE id. |
| Port | Indicates the list of ports configured with the QCE. |
| Frame Type | Indicates the type of frame. Possible values are: Any: Match any frame type. Ethernet: Match EtherType frames. LLC: Match (LLC) frames. SNAP: Match (SNAP) frames. IPv4: Match IPv4 frames. IPv6: Match IPv6 frames |
| Action | Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are: CoS: Classify Class of Service. DPL: Classify Drop Precedence Level. DSCP: Classify DSCP value. PCP: Classify PCP value. DEI: Classify DEI value. Policy: Classify ACL Policy number. |
| Conflict | Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button. |
| Combined | Select the QCL status from this drop-down list. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Resolve Conflict | Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'. |
| Refresh | Click to refresh the page. |

Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Detailed Port Statistics Port 1 Port 1 ▼ Auto-refresh Refresh Clear

| Receive Total | | Transmit Total | |
|------------------------|----------|-------------------------|--------|
| Rx Packets | 407178 | Tx Packets | 3005 |
| Rx Octets | 92698169 | Tx Octets | 583642 |
| Rx Unicast | 643 | Tx Unicast | 1055 |
| Rx Multicast | 187224 | Tx Multicast | 1948 |
| Rx Broadcast | 219311 | Tx Broadcast | 2 |
| Rx Pause | 0 | Tx Pause | 0 |
| Receive Size Counters | | Transmit Size Counters | |
| Rx 64 Bytes | 239350 | Tx 64 Bytes | 679 |
| Rx 65-127 Bytes | 63427 | Tx 65-127 Bytes | 80 |
| Rx 128-255 Bytes | 28179 | Tx 128-255 Bytes | 2039 |
| Rx 256-511 Bytes | 38411 | Tx 256-511 Bytes | 58 |
| Rx 512-1023 Bytes | 4037 | Tx 512-1023 Bytes | 11 |
| Rx 1024-1526 Bytes | 33774 | Tx 1024-1526 Bytes | 138 |
| Rx 1527- Bytes | 0 | Tx 1527- Bytes | 0 |
| Receive Queue Counters | | Transmit Queue Counters | |
| Rx Q0 | 407178 | Tx Q0 | 0 |
| Rx Q1 | 0 | Tx Q1 | 0 |
| Rx Q2 | 0 | Tx Q2 | 0 |
| Rx Q3 | 0 | Tx Q3 | 0 |
| Rx Q4 | 0 | Tx Q4 | 0 |
| Rx Q5 | 0 | Tx Q5 | 0 |
| Rx Q6 | 0 | Tx Q6 | 0 |
| Rx Q7 | 0 | Tx Q7 | 3005 |
| Receive Error Counters | | Transmit Error Counters | |
| Rx Drops | 0 | Tx Drops | 0 |
| Rx CRC/Alignment | 0 | Tx Late/Exc. Coll. | 0 |
| Rx Undersize | 0 | | |
| Rx Oversize | 0 | | |
| Rx Fragments | 0 | | |
| Rx Jabber | 0 | | |
| Rx Filtered | 152930 | | |

| Object | Description |
|-------------------------------------|--|
| Receive Total and Transmit Total | |
| Rx and Tx Packets | The number of received and transmitted (good and bad) packets. |
| Rx and Tx Octets | The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits. |
| Rx and Tx Unicast | The number of received and transmitted (good and bad) unicast packets. |
| Rx and Tx Multicast | The number of received and transmitted (good and bad) multicast packets. |
| Rx and Tx Broadcast | The number of received and transmitted (good and bad) broadcast packets. |
| Rx and Tx Pause | A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation. |
| Receive and Transmit Size Counters | The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes. |
| Receive and Transmit Queue Counters | The number of received and transmitted packets per input and output queue. |
| Receive Error Counters | |

| Object | Description |
|-------------------------|--|
| Rx Drops | The number of frames dropped due to lack of receive buffers or egress congestion. |
| Rx CRC/Alignment | The number of frames received with CRC or alignment errors. |
| Rx Undersize | The number of short 1 frames received with valid CRC. |
| Rx Oversize | The number of long 2 frames received with valid CRC. |
| Rx Fragments | The number of short 1 frames received with invalid CRC. |
| Rx Jabber | The number of long 2 frames received with invalid CRC. |
| Rx Filtered | The number of received frames filtered by the forwarding process. 1 Short frames are frames that are smaller than 64 bytes. 2 Long frames are frames that are longer than the configured maximum frame length for this port. |
| Transmit Error Counters | |
| Tx Drops | The number of frames dropped due to output buffer congestion. |
| Tx Late/Exc. Coll | The number of frames dropped due to excessive or late collisions. |
| Port1 | Click to select the port. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Clear | Click to clear the counters for the selected port. |
| Refresh | Click to refresh the page. |

DHCP

DHCP Server

Statistics

This page displays the database counters and the number of DHCP messages sent and received by DHCP server.

DHCP Server Statistics

Auto-refresh

Database Counters

| Pool | Excluded IP Address | Declined IP Address |
|------|---------------------|---------------------|
| 0 | 0 | 0 |

Binding Counters

| Automatic Binding | Manual Binding | Expired Binding |
|-------------------|----------------|-----------------|
| 0 | 0 | 0 |

DHCP Message Received Counters

| DISCOVER | REQUEST | DECLINE | RELEASE | INFORM |
|----------|---------|---------|---------|--------|
| 0 | 0 | 0 | 0 | 0 |

DHCP Message Sent Counters

| OFFER | ACK | NAK |
|-------|-----|-----|
| 0 | 0 | 0 |

| Object | Description |
|---------------------------------------|---|
| Pool | Number of pools. |
| Excluded IP Address | Number of excluded IP address ranges. |
| Declined IP Address | Number of declined IP addresses. |
| Binding Counters | |
| Automatic Binding | Number of bindings with network-type pools. |
| Manual Binding | Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type. |
| Expired Binding | Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings. |
| DHCP Message Received Counters | |
| Discover | Number of DHCP DISCOVER messages received. |
| Request | Number of DHCP REQUEST messages received. |
| Decline | Number of DHCP DECLINE messages received. |
| Release | Number of DHCP RELEASE messages received. |
| Inform | Number of DHCP INFORM messages received. |
| DHCP Message Sent Counters | |

| Object | Description |
|--------------|--|
| Offer | Number of DHCP OFFER messages sent. |
| ACK | Number of DHCP ACK messages sent. |
| NAK | Number of DHCP NAK messages sent. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Clear | Click to clear DHCP Message Received and Sent counters. |
| Refresh | Click to refresh the page. |

Binding

This page displays bindings generated for DHCP clients.

DHCP Server Binding IP Auto-refresh

Binding IP Address

| Delete | IP | Type | State | Pool Name | Server ID |
|--------|----|------|-------|-----------|-----------|
|--------|----|------|-------|-----------|-----------|

Display all bindings.

| Object | Description |
|-----------------|---|
| IP | IP address allocated to DHCP client. |
| Type | Type of binding. Possible types are Automatic, Manual, Expired. |
| State | State of binding. Possible states are Committed, Allocated, Expired. |
| Pool Name | The pool that generates the binding. |
| Server ID | Server IP address to service the binding. CoS: Classify Class of Service. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Clear Selected | Click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to be Expired. If the selected binding is Expired, then it is freed. |
| Clear Automatic | Click to clear all Automatic bindings and Change them to Expired bindings. |
| Clear Manual | Click to clear all Manual bindings and Change them to Expired bindings. |
| Clear Expired | Click to clear all Expired bindings and free them. |
| Refresh | Click to refresh the page. |

Declined IP

This page displays declined IP addresses.

DHCP Server Declined IP

Auto-refresh

Declined IP Address

Declined IP

Declined IP: List of IP addresses declined.

Auto_refresh Check to refresh the page automatically every 3 seconds.

Refresh Click to refresh the page immediately.

Snooping Table

Each page shows up to 99 entries from the Dynamic DHCP snooping table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic DHCP snooping Table.

The "MAC address" and "VLAN" input fields allow the user to select the starting point in the Dynamic DHCP snooping Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next Dynamic DHCP snooping Table match. In addition, the two input fields will - upon a "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The ">>" will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "<<" button to start over.

Dynamic DHCP Snooping Table Auto-refresh Refresh |<< >>

Start from MAC address , VLAN with entries per page.

| MAC Address | VLAN ID | Source Port | IP Address | IP Subnet Mask | DHCP Server |
|-----------------|---------|-------------|------------|----------------|-------------|
| No more entries | | | | | |

| Object | Description |
|---------------------|--|
| MAC Address | User MAC address of the entry. |
| VLAN ID | VLAN-ID in which the DHCP traffic is permitted. |
| Source Port | Switch Port Number for which the entries are displayed. |
| IP Address | User IP address of the entry. |
| IP Subnet Mask | User IP subnet mask of the entry. |
| DHCP Server Address | DHCP Server address of the entry. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields.. |
| Clear | Click to flush all dynamic entries. |
| << | Click to update the table starting from the first entry in the Dynamic DHCP snooping Table |
| << | Click to update the table, starting with the entry after the last entry currently displayed. |

Relay Statistics

This page provides statistics for DHCP relay.

DHCP Relay Statistics

Auto-refresh Refresh Clear

Server Statistics

| Transmit to Server | Transmit Error | Receive from Server | Receive Missing Agent Option | Receive Missing Circuit ID | Receive Missing Remote ID | Receive Bad Circuit ID | Receive Bad Remote ID |
|--------------------|----------------|---------------------|------------------------------|----------------------------|---------------------------|------------------------|-----------------------|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Client Statistics

| Transmit to Client | Transmit Error | Receive from Client | Receive Agent Option | Replace Agent Option | Keep Agent Option | Drop Agent Option |
|--------------------|----------------|---------------------|----------------------|----------------------|-------------------|-------------------|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| Object | Description |
|------------------------------|---|
| Server Statistics | |
| Transmit to Server | The number of packets that are relayed from client to server. |
| Transmit Error | The number of packets that resulted in errors while being sent to clients. |
| Receive from Server | The number of packets received from server. |
| Receive Missing Agent Option | The number of packets received without agent information options. |
| Receive Missing Circuit ID | The number of packets received with the Circuit ID option missing. |
| Receive Missing Remote ID | The number of packets received with the Remote ID option missing. |
| Receive Bad Circuit ID | The number of packets whose Circuit ID option did not match known circuit ID. |
| Receive Bad Remote ID | The number of packets whose Remote ID option did not match known Remote ID. |
| Client Statistics | |
| Transmit to Client | The number of relayed packets from server to client. |
| Transmit Error | The number of packets that resulted in error while being sent to servers. |
| Receive from Client | The number of received packets from server. |
| Receive Agent Option | The number of received packets with relay agent information option. |
| Replace Agent Option | The number of packets which were replaced with relay agent information option. |
| Keep Agent Option | The number of packets whose relay agent information was retained. |
| Drop Agent Option | The number of packets that were dropped which were received with relay agent information. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the page. |
| Clear | Click to clear all statistics. |

Detailed Statistics

This page provides statistics for DHCP snooping. Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. And clear the statistics on specific port may not take effect on global statistics since it gathers the different layer overview.

DHCP Detailed Statistics Port 1 Combined ▼ Port 1 ▼ Auto-refresh Refresh Clear

| Receive Packets | | Transmit Packets | |
|-----------------------------|---|---------------------|---|
| Rx Discover | 0 | Tx Discover | 0 |
| Rx Offer | 0 | Tx Offer | 0 |
| Rx Request | 0 | Tx Request | 0 |
| Rx Decline | 0 | Tx Decline | 0 |
| Rx ACK | 0 | Tx ACK | 0 |
| Rx NAK | 0 | Tx NAK | 0 |
| Rx Release | 0 | Tx Release | 0 |
| Rx Inform | 0 | Tx Inform | 0 |
| Rx Lease Query | 0 | Tx Lease Query | 0 |
| Rx Lease Unassigned | 0 | Tx Lease Unassigned | 0 |
| Rx Lease Unknown | 0 | Tx Lease Unknown | 0 |
| Rx Lease Active | 0 | Tx Lease Active | 0 |
| Rx Discarded Checksum Error | 0 | | |
| Rx Discarded from Untrusted | 0 | | |

| Object | Description |
|-----------------------------|--|
| Rx and Tx Discover | The number of discover (option 53 with value 1) packets received and transmitted. |
| Rx and Tx Offer | The number of offer (option 53 with value 2) packets received and transmitted. |
| Rx and Tx Request | The number of request (option 53 with value 3) packets received and transmitted. |
| Rx and Tx Decline | The number of decline (option 53 with value 4) packets received and transmitted. |
| Rx and Tx ACK | The number of ACK (option 53 with value 5) packets received and transmitted. |
| Rx and Tx NAK | The number of NAK (option 53 with value 6) packets received and transmitted. |
| Rx and Tx Release | The number of release (option 53 with value 7) packets received and transmitted. |
| Rx and Tx Inform | The number of inform (option 53 with value 8) packets received and transmitted. |
| Rx and Tx Lease Query | The number of lease query (option 53 with value 10) packets received and transmitted. |
| Rx and Tx Lease Unassigned | The number of lease unassigned (option 53 with value 11) packets received and transmitted. |
| Rx and Tx Unknown | The number of lease unknown (option 53 with value 12) packets received and transmitted. |
| Rx and Tx Active | The number of lease active (option 53 with value 13) packets received and transmitted. |
| Rx Discarded checksum error | The number of discard packet that IP/UDP checksum is error. |
| Rx Discarded from Untrusted | The number of discarded packet that are coming from untrusted port. |
| Combined | Select the DHCP user from this drop-down list. |
| Port1 | Click to select the port. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Clear | Click to clear the counters for the selected port. |
| Refresh | Click to refresh the page. |

Security

Access Management Statistics

This page provides statistics for access management.

Access Management Statistics

Auto-refresh Refresh Clear

| Interface | Received Packets | Allowed Packets | Discarded Packets |
|-----------|------------------|-----------------|-------------------|
| HTTP | 0 | 0 | 0 |
| HTTPS | 0 | 0 | 0 |
| SNMP | 0 | 0 | 0 |
| TELNET | 0 | 0 | 0 |
| SSH | 0 | 0 | 0 |

| Object | Description |
|-------------------|--|
| Interface | The interface type through which the remote host can access the switch. |
| Received Packets | Number of received packets from the interface when access management mode is enabled. |
| Allowed Packets | Number of allowed packets from the interface when access management mode is enabled. |
| Discarded Packets | Number of discarded packets from the interface when access management mode is enabled. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the page. |
| Clear | Click to clear all statistics. |

Network

Port Security

Switch

This page shows the Port Security status. Port Security is a module with no direct configuration.

Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

Port Security Switch Status

Auto-refresh

User Module Legend

| User Module Name | Abbr |
|------------------|------|
| Limit Control | L |
| 802.1X | 8 |
| Voice VLAN | V |

Port Status

| Port | Users | State | MAC Count | |
|------|-------|----------|-----------|-------|
| | | | Current | Limit |
| 1 | --- | Disabled | - | - |
| 2 | --- | Disabled | - | - |
| 3 | --- | Disabled | - | - |
| 4 | --- | Disabled | - | - |
| 5 | --- | Disabled | - | - |
| 6 | --- | Disabled | - | - |
| 7 | --- | Disabled | - | - |
| 8 | --- | Disabled | - | - |
| 9 | --- | Disabled | - | - |
| 10 | --- | Disabled | - | - |
| 11 | --- | Disabled | - | - |

| Object | Description |
|---------------------------|---|
| User Module Legend | |
| User Module Name | The full name of a module that may request Port Security services. |
| Abbr | A one-letter abbreviation of the user module. This is used in the Users column in the port status table. |
| Port Status | |
| Port | The port number for which the status applies. Click the port number to see the status for this particular port. |
| Users | Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security. |
| State | Shows the current state of the port. It can take one of four values: Disabled: No user modules are currently using the Port Security service. Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive. Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in. Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page. |
| MAC Count (Current,Limit) | The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-). |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the page. |

Port

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

Port Security Port Status Port 1 Port 1 ▼ Auto-refresh Refresh

| MAC Address | VLAN ID | State | Time of Addition | Age/Hold |
|----------------------------------|---------|-------|------------------|----------|
| <i>No MAC addresses attached</i> | | | | |

| Object | Description |
|-----------------------|---|
| MAC Address & VLAN ID | The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed. |
| State | Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic. |
| Time of Addition | Shows the date and time when this MAC address was first seen on the port. |
| Age/Hold | If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown. |
| Port1 | Click to select the port. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the page. |

NAS

Switch

This page provides an overview of the current NAS port states.

Network Access Server Switch Status

Auto-refresh Refresh

| Port | Admin State | Port State | Last Source | Last ID | QoS Class | Port VLAN ID |
|-----------|------------------|-------------------|-------------|---------|-----------|--------------|
| <u>1</u> | Force Authorized | Globally Disabled | | | - | |
| <u>2</u> | Force Authorized | Globally Disabled | | | - | |
| <u>3</u> | Force Authorized | Globally Disabled | | | - | |
| <u>4</u> | Force Authorized | Globally Disabled | | | - | |
| <u>5</u> | Force Authorized | Globally Disabled | | | - | |
| <u>6</u> | Force Authorized | Globally Disabled | | | - | |
| <u>7</u> | Force Authorized | Globally Disabled | | | - | |
| <u>8</u> | Force Authorized | Globally Disabled | | | - | |
| <u>9</u> | Force Authorized | Globally Disabled | | | - | |
| <u>10</u> | Force Authorized | Globally Disabled | | | - | |
| <u>11</u> | Force Authorized | Globally Disabled | | | - | |

| Object | Description |
|--------------|--|
| Port | The switch port number. Click to navigate to detailed NAS statistics for this port. |
| Admin State | The port's current administrative state. Refer to NAS Admin State for a description of possible values. |
| Port State | The current state of the port. Refer to NAS Port State for a description of the individual states. |
| Last Source | The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication. |
| Last ID | The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication. |
| QoS Class | QoS Class assigned to the port by the RADIUS server if enabled. |
| Port VLAN ID | The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the page. |

Port

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only .

Use the port select box to select which port details to be displayed.

NAS Statistics Port 1 Port 1 ▼ Auto-refresh Refresh

Port State

| | |
|-------------|-------------------|
| Admin State | Force Authorized |
| Port State | Globally Disabled |

| Object | Description |
|--------------|--|
| Admin State | The port's current administrative state. Refer to NAS Admin State for a description of possible values. |
| Port State | The current state of the port. Refer to NAS Port State for a description of the individual states. |
| QoS Class | The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned. |
| Port VLAN ID | The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. |
| Port1 | Click to select the port. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the page. |

ACL Status

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 256 on each switch.

ACL Status

 Auto-refresh

| User | ACE | Frame Type | Action | Rate Limiter | Mirror | CPU | Counter | Conflict |
|------------|-----|------------|--------|--------------|--------|-----|---------|----------|
| No entries | | | | | | | | |

| Object | Description |
|--------------|---|
| User | Indicates the ACL user. |
| ACE | Indicates the ACE ID on local switch. |
| Frame Type | Indicates the frame type of the ACE. Possible values are: Any: The ACE will match any frame type. EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ARP: The ACE will match ARP/RARP frames. IPv4: The ACE will match all IPv4 frames. IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol. IPv4/UDP: The ACE will match IPv4 frames with UDP protocol. IPv4/TCP: The ACE will match IPv4 frames with TCP protocol. IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. IPv6: The ACE will match all IPv6 standard frames. |
| Action | Indicates the forwarding action of the ACE. Permit: Frames matching the ACE may be forwarded and learned. Deny: Frames matching the ACE are dropped. Filter: Frames matching the ACE are filtered. |
| Rate limiter | Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled. |
| Mirror | Specify the mirror operation of this port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is "Disabled". |
| CPU | Forward packet that matched the specific ACE to CPU. |
| Counter | The counter indicates the number of times the ACE was hit by a frame. |
| Conflict | Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations. |
| Combined | Select the ACL user from this drop-down list. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the page. |

ARP Inspection

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The ">>" will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "<<" button to start over.

Dynamic ARP Inspection Table Auto-refresh Refresh |<< >>

Start from , VLAN , MAC address and IP address with entries per page.

| Port | VLAN ID | MAC Address | IP Address |
|-----------------|---------|-------------|------------|
| No more entries | | | |

| Object | Description |
|--------------|--|
| Port | Switch Port Number for which the entries are displayed. |
| VLAN ID | VLAN-ID in which the ARP traffic is permitted. |
| MAC Address | User MAC address of the entry. |
| IP Address | User IP address of the entry. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |
| << | Click to update the table starting from the first entry in the Dynamic ARP Inspection Table. |
| << | Click to update the table, starting with the entry after the last entry currently displayed. |

IP Source Guard

Each page shows up to 99 entries from the Dynamic IP Source Guard table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic IP Source Guard Table.

The "Start from port address", "VLAN" and "IP address" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next Dynamic IP Source Guard Table match. In addition, the two input fields will - upon a "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The ">>" will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "<<" button to start over.

Dynamic IP Source Guard Table Auto-refresh Refresh |<< >>

Start from , VLAN and IP address with entries per page.

| Port | VLAN ID | IP Address | MAC Address |
|-----------------|---------|------------|-------------|
| No more entries | | | |

| Object | Description |
|--------------|---|
| Port | Switch Port Number for which the entries are displayed. |
| VLAN ID | VLAN-ID in which the IP traffic is permitted. |
| IP Address | User IP address of the entry. |
| MAC Address | Source MAC address. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |
| << | Click to update the table starting from the first entry in the Dynamic IP Source Guard Table. |
| << | Click to update the table, starting with the entry after the last entry currently displayed. |

AAA

RADIUS Overview

This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page.

RADIUS Server Status Overview

Auto-refresh Refresh

| # | IP Address | Authentication Port | Authentication Status | Accounting Port | Accounting Status |
|---|------------|---------------------|-----------------------|-----------------|-------------------|
| 1 | | | Disabled | | Disabled |
| 2 | | | Disabled | | Disabled |
| 3 | | | Disabled | | Disabled |
| 4 | | | Disabled | | Disabled |
| 5 | | | Disabled | | Disabled |

| Object | Description |
|-------------------------------|--|
| RADIUS Authentication Servers | |
| # | The RADIUS server number. Click to navigate to detailed statistics for this server. |
| IP Address | The IP address and UDP port number (in <IP Address> :< UDP Port> notation) of this server. |
| Status | <p>The current status of the server. This field takes one of the following values: Disabled: The server is disabled.</p> <p>Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running and the RADIUS module is ready to accept access attempts.</p> <p>Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.</p> |
| RADIUS Accounting Servers | |
| # | The RADIUS server number. Click to navigate to detailed statistics for this server. |
| IP Address | The IP address and UDP port number (in <IP Address> :< UDP Port> notation) of this server. |
| Status | <p>The current status of the server. This field takes one of the following values: Disabled: The server is disabled.</p> <p>Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running and the RADIUS module is ready to accept accounting attempts.</p> <p>Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.</p> |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |

RADIUS Details

This page provides detailed statistics for a particular RADIUS server.

RADIUS Authentication Statistics for Server #1

Server #1 ▾ Auto-refresh Refresh Clear

| Receive Packets | | Transmit Packets | |
|----------------------------|---|------------------------|---|
| Access Accepts | 0 | Access Requests | 0 |
| Access Rejects | 0 | Access Retransmissions | 0 |
| Access Challenges | 0 | Pending Requests | 0 |
| Malformed Access Responses | 0 | Timeouts | 0 |
| Bad Authenticators | 0 | | |
| Unknown Types | 0 | | |
| Packets Dropped | 0 | | |
| Other Info | | | |
| IP Address | | | |
| State | | Disabled | |
| Round-Trip Time | | 0 ms | |

RADIUS Accounting Statistics for Server #1

| Receive Packets | | Transmit Packets | |
|---------------------|---|------------------|---|
| Responses | 0 | Requests | 0 |
| Malformed Responses | 0 | Retransmissions | 0 |
| Bad Authenticators | 0 | Pending Requests | 0 |
| Unknown Types | 0 | Timeouts | 0 |
| Packets Dropped | 0 | | |
| Other Info | | | |
| IP Address | | | |
| State | | Disabled | |
| Round-Trip Time | | 0 ms | |

| Object | Description |
|---|--|
| RADIUS Authentication Statistics | |
| Packet Counters | RADIUS authentication server packet counter. There are seven receive and four transmit counters. |
| Other Info | This section contains information about the state of the server and the latest round-trip time. |
| RADIUS Accounting Statistics | |
| Packet Counters | RADIUS accounting server packet counter. There are five receive and four transmit counters. |
| Other Info | This section contains information about the state of the server and the latest round-trip time. |
| Server #1 | Select a server from this drop-down list. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the page. |
| Clear | Click to Clear the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation. |

Switch

RMON

Statistics

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

RMON Statistics Status Overview

Auto-refresh Refresh << >>

Start from Control Index 0 with 20 entries per page.

| ID | Data Source (ifIndex) | Drop | Octets | Pkts | Broad-cast | Multi-cast | CRC Errors | Under-size | Over-size | Frag. | Jabb. | Coll. | 64 Bytes | 65 ~ 127 | 128 ~ 255 | 256 ~ 511 | 512 ~ 1023 | 1024 ~ 1588 |
|-----------------|-----------------------|------|--------|------|------------|------------|------------|------------|-----------|-------|-------|-------|----------|----------|-----------|-----------|------------|-------------|
| No more entries | | | | | | | | | | | | | | | | | | |

| Object | Description |
|-----------------------|--|
| ID | Indicates the index of Statistics entry. |
| Data Source (ifIndex) | The port ID which wants to be monitored. |
| Drop | The total number of events in which packets were dropped by the probe due to lack of resources. |
| Octets | The total number of octets of data (including those in bad packets) received on the network. |
| Pkts | The total number of packets (including bad packets, broadcast packets, and multicast packets) received. |
| Broad-cast | The total number of good packets received that were directed to the broadcast address. |
| Multi-cast | The total number of good packets received that were directed to a multicast address. |
| CRC Errors | The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). |
| Under-Size | The total number of packets received that were less than 64 octets. |
| Over-size | The total number of packets received that were longer than 1518 octets. |
| Frag. | The number of frames which size is less than 64 octets received with invalid CRC. |
| Jabb. | The number of frames which size is larger than 64 octets received with invalid CRC. |
| Coll. | The best estimate of the total number of collisions on this Ethernet segment. |
| 64 | The total number of packets (including bad packets) received that were 64 octets in length. |
| 65~127 | The total number of packets (including bad packets) received that were between 65 and 127 octets in length. |
| 128~255 | The total number of packets (including bad packets) received that were between 128 and 255 octets in length. |
| 256~511 | The total number of packets (including bad packets) received that were between 256 and 511 octets in length. |
| 512~1023 | The total number of packets (including bad packets) received that were between 512 and 1023 octets in length. |

| Object | Description |
|--------------|---|
| 1024~1588 | The total number of packets (including bad packets) received that were between 1024 and 1588 octets in length. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |
| << | Click to update the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID. |
| << | Click to update the table, starting with the entry after the last entry currently displayed. |

History

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

RMON History Overview

Auto-refresh Refresh |<< >>

Start from Control Index and Sample Index with entries per page.

| History Index | Sample Index | Sample Start | Drop | Octets | Pkts | Broad-cast | Multi-cast | CRC Errors | Under-size | Over-size | Frag. | Jabb. | Coll. | Utilization |
|-----------------|--------------|--------------|------|--------|------|------------|------------|------------|------------|-----------|-------|-------|-------|-------------|
| No more entries | | | | | | | | | | | | | | |

| Object | Description |
|---------------|--|
| History Index | Indicates the index of History control entry. |
| Sample Index | Indicates the index of the data entry associated with the control entry. |
| Sample Start | The value of sysUpTime at the start of the interval over which this sample was measured. |
| Drop | The total number of events in which packets were dropped by the probe due to lack of resources. |
| Octets | The total number of octets of data (including those in bad packets) received on the network. |
| Pkts | The total number of packets (including bad packets, broadcast packets, and multicast packets) received. |
| Broadcast | The total number of good packets received that were directed to the broadcast address. |
| Multicast | The total number of good packets received that were directed to a multicast address. |
| CRCErrors | The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). |
| Undersize | The total number of packets received that were less than 64 octets. |
| Oversize | The total number of packets received that were longer than 1518 octets. |
| Frag. | The number of frames which size is less than 64 octets received with invalid CRC. |
| Jabb. | The number of frames which size is larger than 64 octets received with invalid CRC. |
| Coll. | The best estimate of the total number of collisions on this Ethernet segment. |
| Utilization | The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |

| Object | Description |
|---------|--|
| Refresh | Click to refresh the displayed table starting from the input fields. |
| << | Click to update the table starting from the first entry in the History table, i.e., the entry with the lowest History Index and Sample Index |
| << | Click to update the table, starting with the entry after the last entry currently displayed. |

Alarm

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the “entries per page” input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.

RMON Alarm Overview

Auto-refresh Refresh |<< >>

Start from Control Index with entries per page.

| ID | Interval | Variable | Sample Type | Value | Startup Alarm | Rising Threshold | Rising Index | Falling Threshold | Falling Index |
|------------------------|----------|----------|-------------|-------|---------------|------------------|--------------|-------------------|---------------|
| <i>No more entries</i> | | | | | | | | | |

| Object | Description |
|-------------------|--|
| ID | Indicates the index of Alarm control entry. |
| Interval | Indicates the interval in seconds for sampling and comparing the rising and falling threshold. |
| Variable | Indicates the particular variable to be sampled. |
| Sample Type | The method of sampling the selected variable and calculating the value to be compared against the thresholds. |
| Value | The value of the statistic during the last sampling period. |
| Startup Alarm | The alarm that may be sent when this entry is first set to valid. |
| Rising Threshold | Rising threshold value. |
| Rising Index | Rising event index. |
| Falling Threshold | Falling threshold value. |
| Falling Index | Falling event index. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |
| << | Click to update the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID. |
| << | Click to update the table, starting with the entry after the last entry currently displayed. |

Event

This page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table.

RMON Event Overview

Auto-refresh

Refresh

|<<

>>

Start from Control Index and Sample Index with entries per page.

| Event Index | LogIndex | LogTime | LogDescription |
|------------------------|----------|---------|----------------|
| <i>No more entries</i> | | | |

| Object | Description |
|----------------|---|
| Event Index | Indicates the index of the event entry. |
| Log Index | Indicates the index of the log entry. |
| Log Time | Indicates Event log time. |
| LogDescription | Indicates the Event description. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |
| << | Click to update the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index. |
| << | Click to update the table, starting with the entry after the last entry currently displayed. |

Aggregation Status

This page is used to see the status of ports in Aggregation group.

Aggregation Group Status

Aggregation Status

Auto-refresh Refresh

| Aggr ID | Name | Type | Speed | Configured Ports | Aggregated Ports |
|------------------------------|------|------|-------|------------------|------------------|
| <i>No aggregation groups</i> | | | | | |

| Object | Description |
|------------------|---|
| Aggr ID | The Aggregation ID associated with this aggregation instance. |
| Name | Name of the Aggregation group ID. |
| Type | Type of the Aggregation group(Static or LACP). |
| Speed | Speed of the Aggregation group. |
| Configured ports | Configured member ports of the Aggregation group. |
| Aggregated ports | Aggregated member ports of the Aggregation group. |
| Refresh | Click to refresh the page immediately. |
| Auto-refresh | Check to refresh the page automatically every 3 seconds. |

LACP

System Status

This page provides a status overview for all LACP instances.

| LACP System Status | | | | | |
|---|-------------------|-------------|--------------|--------------|-------------|
| Auto-refresh <input type="checkbox"/> | | | | | Refresh |
| Aggr ID | Partner System ID | Partner Key | Partner Prio | Last Changed | Local Ports |
| <i>No ports enabled or no existing partners</i> | | | | | |

| Object | Description |
|-------------------|---|
| Aggr ID | The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id' |
| Partner System ID | The system ID (MAC address) of the aggregation partner. |
| Partner Key | The Key that the partner has assigned to this aggregation ID. |
| Last Changed | The time since this aggregation changed. |
| Local Ports | Shows which ports are a part of this aggregation for this switch. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |

Port Status

This page provides a status overview for LACP status for all ports.

LACP Status Auto-refresh [Refresh](#)

| Port | LACP | Key | Aggr ID | Partner System ID | Partner Port | Partner Prio |
|------|------|-----|---------|-------------------|--------------|--------------|
| 1 | No | - | - | - | - | - |
| 2 | No | - | - | - | - | - |
| 3 | No | - | - | - | - | - |
| 4 | No | - | - | - | - | - |
| 5 | No | - | - | - | - | - |
| 6 | No | - | - | - | - | - |
| 7 | No | - | - | - | - | - |
| 8 | No | - | - | - | - | - |
| 9 | No | - | - | - | - | - |
| 10 | No | - | - | - | - | - |
| 11 | No | - | - | - | - | - |

| Object | Description |
|-------------------|---|
| Port | The switch port number. |
| LACP | 'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile its LACP status is disabled. |
| Key | The key assigned to this port. Only ports with the same key can aggregate together. |
| Aggr ID | The Aggregation ID assigned to this aggregation group. |
| Partner System ID | The partner's System ID (MAC address). |
| Partner Port | The partner's port number connected to this port. |
| Partner Prio | The partner's port priority. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |

Port Statistics

This page provides an overview for LACP statistics for all ports.

LACP Statistics Auto-refresh

| Port | LACP Received | LACP Transmitted | Discarded | |
|------|---------------|------------------|-----------|---------|
| | | | Unknown | Illegal |
| 1 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 |

| Object | Description |
|------------------|---|
| Port | The switch port number. |
| LACP Received | Shows how many LACP frames have been received at each port. |
| LACP Transmitted | Shows how many LACP frames have been sent from each port. |
| Discarded | Shows how many unknown or illegal LACP frames have been discarded at each port. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |
| Clear | Click to Clear the counters for all ports. |

Loop Protection

This page displays the loop protection port status the ports of the switch.

Loop Protection Status Auto-refresh

| Port | Action | Transmit | Loops | Status | Loop | Time of Last Loop |
|-------------------------|--------|----------|-------|--------|------|-------------------|
| <i>No ports enabled</i> | | | | | | |

| Object | Description |
|-------------------|--|
| Port | The switch port number of the logical port. |
| Action | The currently configured port action. |
| Transmit | The currently configured port transmit mode. |
| Loops | The number of loops detected on this port. |
| Status | The current loop protection status of the port. |
| Loop | Whether a loop is currently detected on the port. |
| Time of Last Loop | The time of the last loop event detected. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |

Spanning Tree

Bridge Status

This page provides a status overview of all STP bridge instances.

STP Bridges

Auto-refresh Refresh

| MSTI | Bridge ID | Root | | | Topology Flag | Topology Change Last |
|------|-------------------------|-------------------------|------|-------|---------------|----------------------|
| | | ID | Port | Cost | | |
| CIST | 32768.00-22-3B-02-07-BC | 32768.00-1F-6C-C5-A9-DE | 1 | 20000 | Steady | 0d 16:42:41 |

| Object | Description |
|----------------------|--|
| MSTI | The Bridge Instance. This is also a link to the STP Detailed Bridge Status. |
| Bridge ID | The Bridge ID of this Bridge instance. |
| Root ID | The Bridge ID of the currently elected root bridge. |
| Root Port | The switch port currently assigned the root port role. |
| Root Cost | Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge. |
| Topology Flag | The current state of the Topology Change Flag of this Bridge instance. |
| Topology Change Last | The time since last Topology Change occurred. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |

STP Detailed Bridge Status

This page provides detailed information on a single STP bridge instance, along with port state for all active ports associated.

STP Detailed Bridge Status

| STP Bridge Status | |
|-----------------------|-------------------------|
| Bridge Instance | CIST |
| Bridge ID | 32768.00-22-3B-02-07-BC |
| Root ID | 32768.00-1F-6C-C5-A9-DE |
| Root Cost | 20000 |
| Root Port | 1 |
| Regional Root | 32768.00-22-3B-02-07-BC |
| Internal Root Cost | 0 |
| Topology Flag | Steady |
| Topology Change Count | 8 |
| Topology Change Last | 2d 20:37:46 |

CIST Ports & Aggregations State

| Port | Port ID | Role | State | Path Cost | Edge | Point-to-Point | Uptime |
|------|---------|----------|------------|-----------|------|----------------|-------------|
| 1 | 128:001 | RootPort | Forwarding | 20000 | No | Yes | 2d 20:37:51 |

| Object | Description |
|--|---|
| STP Bridge Status | |
| Bridge Instance | The Bridge instance - CIST, MST1, ... |
| Bridge ID | The Bridge ID of this Bridge instance. |
| Root ID | The Bridge ID of the currently elected root bridge. |
| Root Port | The switch port currently assigned the root port role. |
| Root Cost | Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge. |
| Regional Root | The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (For the CIST instance only). |
| Internal Root Cost | The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (For the CIST instance only). |
| Topology Flag | The current state of the Topology Change Flag of this Bridge instance. |
| Topology Change Count | The number of times where the topology change flag has been set (during a one-second interval). |
| Topology Change Last | The time passed since the Topology Flag was last set. |
| CIST Ports & Aggregations State | |
| Switch ID | The Switch ID of the logical port. |
| Port | The switch port number of the logical STP port. |
| Port ID | The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port. |
| Role | The current STP port role. The port role can be one of the following values: AlternatePort BackupPort RootPort DesignatedPort. |
| State | The current STP port state. The port state can be one of the following values: Discarding Learning Forwarding. |

| Object | Description |
|----------------|--|
| Path Cost | The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value. |
| Edge | The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop. |
| Point-to-Point | The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state. |
| Uptime | The time since the bridge port was last initialized. |
| Refresh | Click to refresh the page immediately. |
| Auto-refresh | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |

Port Status

This page displays the STP CIST port status for physical ports of the switch.

STP Port Status

Auto-refresh Refresh

| Port | CIST Role | CIST State | Uptime |
|------|-----------|------------|-------------|
| 1 | RootPort | Forwarding | 0d 16:44:51 |
| 2 | Disabled | Discarding | - |
| 3 | Disabled | Discarding | - |
| 4 | Disabled | Discarding | - |
| 5 | Disabled | Discarding | - |
| 6 | Disabled | Discarding | - |
| 7 | Disabled | Discarding | - |
| 8 | Disabled | Discarding | - |
| 9 | Disabled | Discarding | - |
| 10 | Disabled | Discarding | - |
| 11 | Disabled | Discarding | - |

| Object | Description |
|--------------|--|
| Port | The switch port number of the logical STP port. |
| CIST Role | The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort BackupPort RootPort DesignatedPort Disabled. |
| CIST State | The current STP port state of the CIST port. The port state can be one of the following values: Discarding Learning Forwarding. |
| Uptime | The time since the bridge port was last initialized. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |

Port Statistics

This page displays the STP port statistics counters of bridge ports in the switch.

STP Statistics

Auto-refresh Refresh Clear

| Port | Transmitted | | | | Received | | | | Discarded | |
|------|-------------|------|-----|-----|----------|------|-------|-----|-----------|---------|
| | MSTP | RSTP | STP | TCN | MSTP | RSTP | STP | TCN | Unknown | Illegal |
| 1 | 0 | 5 | 0 | 0 | 0 | 0 | 30159 | 0 | 0 | 0 |

| Object | Description |
|-------------------|--|
| Port | The switch port number of the logical STP port. |
| MSTP | The number of MSTP BPDU's received/transmitted on the port. |
| RSTP | The number of RSTP BPDU's received/transmitted on the port. |
| STP | The number of legacy STP Configuration BPDU's received/transmitted on the port. |
| TCN | The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port. |
| Discarded Unknown | The number of unknown Spanning Tree BPDU's received (and discarded) on the port. |
| Discarded Illegal | The number of illegal Spanning Tree BPDU's received (and discarded) on the port. |

| | |
|--------------|--|
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |

MVR

Statistics

This page provides MVR Statistics information.

MVR Statistics

Auto-refresh Refresh Clear

| VLAN ID | IGMP/MLD Queries Received | IGMP/MLD Queries Transmitted | IGMPv1 Joins Received | IGMPv2/MLDv1 Reports Received | IGMPv3/MLDv2 Reports Received | IGMPv2/MLDv1 Leaves Received |
|-----------------|------------------------------|---------------------------------|--------------------------|----------------------------------|----------------------------------|---------------------------------|
| No more entries | | | | | | |

| Object | Description |
|--------------------------------|--|
| VLAN ID | The Multicast VLAN ID |
| IGMP/MLD Queries Received | The number of Received Queries for IGMP and MLD, respectively. |
| IGMP/MLD Queries Transmitted | The number of Transmitted Queries for IGMP and MLD, respectively. |
| IGMPv1 Joins Received | The number of Received IGMPv1 Join's. |
| IGMPv2/MLDv1 Report's Received | The number of Received IGMPv2 Join's and MLDv1 Report's, respectively. |
| IGMPv3/MLDv2 Report's Received | The number of Received IGMPv1 Join's and MLDv2 Report's, respectively. |
| IGMPv2/MLDv1 Leave's Received | The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |
| Clear | Click to Clears all Statistics counters. |

MVR Channel Groups

Each page shows up to 99 entries from the MVR Group table, default being 20, selected through the “entries per page” input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR Channels (Groups) Information Table.

The “Start from VLAN”, and “Group Address” input fields allow the user to select the starting point in the MVR Channels (Groups) Information Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next MVR Channels (Groups) Information Table match. In addition, the two input fields will - upon a “Refresh” button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The “>>” will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text “No more entries” is shown in the displayed table. Use the “<<” button to start over.

MVR Channels (Groups) Information Auto-refresh Refresh |<< >>

Start from VLAN and Group Address with entries per page.

| | | Port Members | | | | | | | | | | |
|-----------------|--------|--------------|---|---|---|---|---|---|---|---|----|----|
| VLAN ID | Groups | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| No more entries | | | | | | | | | | | | |

| Object | Description |
|--------------|---|
| VLAN ID | VLAN ID of the group. |
| Groups | Group ID of the group displayed. |
| Port Members | Ports under this group. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |
| << | Click to update the table starting from the first entry in the MVR Channels (Groups) Information Table. |
| >> | Click to update the table, starting with the entry after the last entry currently displayed. |

MVR SFM Information

Each page shows up to 99 entries from the MVR SFM Information Table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR SFM Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR SFM Information Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next MVR SFM Information Table match. In addition, the two input fields will - upon a "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The ">>" will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "<<" button to start over.

MVR SFM Information Auto-refresh Refresh << >>

Start from VLAN and Group Address with entries per page.

| VLAN ID | Group | Port | Mode | Source Address | Type | Hardware Filter/Switch |
|-----------------|-------|------|------|----------------|------|------------------------|
| No more entries | | | | | | |

| Object | Description |
|------------------------|--|
| VLAN ID | VLAN ID of the group. |
| Group | Group address of the group displayed. |
| Port | Switch port number. |
| Mode | Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude. |
| Source Address | IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is no any source filtering address, the text "None" is shown in the Source Address field. |
| Type | Indicates the Type. It can be either Allow or Deny. |
| Hardware Filter/Switch | Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |
| << | Click to update the table starting from the first entry in the MVR SFM Information Table. |
| >> | Click to update the table, starting with the entry after the last entry currently displayed. |

IPMC

IGMP Snooping

Status

This page provides IGMP Snooping status.

IGMP Snooping Status Auto-refresh Refresh Clear

Statistics

| VLAN ID | Querier Version | Host Version | Querier Status | Queries Transmitted | Queries Received | V1 Reports Received | V2 Reports Received | V3 Reports Received | V2 Leaves Received |
|-------------|-----------------|--------------|----------------|---------------------|------------------|---------------------|---------------------|---------------------|--------------------|
| Router Port | | | | | | | | | |
| Port | Status | | | | | | | | |
| 1 | - | | | | | | | | |
| 2 | - | | | | | | | | |
| 3 | - | | | | | | | | |
| 4 | - | | | | | | | | |
| 5 | - | | | | | | | | |
| 6 | - | | | | | | | | |
| 7 | - | | | | | | | | |
| 8 | - | | | | | | | | |
| 9 | - | | | | | | | | |
| 10 | - | | | | | | | | |
| 11 | - | | | | | | | | |

| Object | Description |
|---------------------|--|
| VLAN ID | The VLAN ID of the entry. |
| Querier Version | Working Querier Version currently. |
| Host Version | Working Host Version currently. |
| Querier Status | Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled. |
| Querier Transmitted | The number of Transmitted Queries. |
| Queries Received | The number of Received Queries. |
| V1 Report Received | The number of Received V1 Reports. |
| V2 Report Received | The number of Received V2 Reports. |
| V3 Report Received | The number of Received V3 Reports. |
| V2 Leaves Received | The number of Received V2 Leaves. |
| Router Port | Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port. |
| Port | Switch port number. |
| Status | Indicate whether specific port is a router port or not. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |
| Clear | Click to Clears all Statistics counters. |

Groups Information

Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

The "Start from VLAN ", and "group" input fields allow the user to select the starting point in the IGMP Group Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next IGMP Group Table match. In addition, the two input fields will - upon a "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The ">>" will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "|<<" button to start over.

IGMP Snooping Group Information Auto-refresh Refresh |<< >>

Start from VLAN and group address with entries per page.

| | | Port Members | | | | | | | | | | |
|------------------------|--------|--------------|---|---|---|---|---|---|---|---|----|----|
| VLAN ID | Groups | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| <i>No more entries</i> | | | | | | | | | | | | |

| Object | Description |
|--------------|--|
| VLAN ID | VLAN ID of the group. |
| Groups | Group address of the group displayed. |
| Port Members | Ports under this group. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |
| << | Click to update the table, starting with the first entry in the IGMP Group Table. |
| >> | Click to update the table, starting with the entry after the last entry currently displayed. |

IPv4 SFM Information

Each page shows up to 99 entries from the IGMP SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP SFM Information Table.

The "Start from VLAN ", and "group" input fields allow the user to select the starting point in the IGMP SFM Information Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next IGMP SFM Information Table match. In addition, the two input fields will - upon a "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The ">>" will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "<<" button to start over.

IGMP SFM Information Auto-refresh Refresh |<< >>

Start from VLAN and Group with entries per page.

| VLAN ID | Group | Port | Mode | Source Address | Type | Hardware Filter/Switch |
|-----------------|-------|------|------|----------------|------|------------------------|
| No more entries | | | | | | |

| Object | Description |
|------------------------|---|
| VLAN ID | VLAN ID of the group. |
| Group | Group address of the group displayed. |
| Port | Switch port number. |
| Mode | Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude. |
| Source Address | IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. |
| Type | Indicates the Type. It can be either Allow or Deny. |
| Hardware Filter/Switch | Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |
| << | Click to update the table starting from the first entry in the IGMP SFM Information Table. |
| >> | Click to update the table, starting with the entry after the last entry currently displayed. |

MLD Snooping

Status

This page provides MLD Snooping status.

MLD Snooping Status

Auto-refresh Refresh Clear

Statistics

| VLAN ID | Querier Version | Host Version | Querier Status | Queries Transmitted | Queries Received | V1 Reports Received | V2 Reports Received | V1 Leaves Received |
|---------|-----------------|--------------|----------------|---------------------|------------------|---------------------|---------------------|--------------------|
|---------|-----------------|--------------|----------------|---------------------|------------------|---------------------|---------------------|--------------------|

Router Port

| Port | Status |
|------|--------|
| 1 | - |
| 2 | - |
| 3 | - |
| 4 | - |
| 5 | - |
| 6 | - |
| 7 | - |
| 8 | - |
| 9 | - |
| 10 | - |
| 11 | - |

| Object | Description |
|---------------------|---|
| VLAN ID | The VLAN ID of the entry. |
| Querier Version | Working Querier Version currently. |
| Host Version | Working Host Version currently. |
| Querier Status | Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled. |
| Queries Transmitted | The number of Transmitted Queries. |
| Queries Received | The number of Received Queries. |
| V1 Report Received | The number of Received V1 Reports. |
| V2 Report Received | The number of Received V2 Reports. |
| V1 Leaves Received | The number of Received V1 Leaves. |
| Router Port | Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port. |
| Port | Switch port number. |
| status | Indicate whether specific port is a router port or not. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |
| Clear | Click to Clears all Statistics counters. |

Groups Information

Each page shows up to 99 entries from the MLD Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.

The "Start from VLAN ", and "group" input fields allow the user to select the starting point in the MLD Group Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next MLD Group Table match. In addition, the two input fields will - upon a "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The ">>" will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "|<<" button to start over.

MLD Snooping Group Information

Auto-refresh Refresh |<< >>

Start from VLAN and group address with entries per page.

| | | Port Members | | | | | | | | | | |
|-----------------|--------|--------------|---|---|---|---|---|---|---|---|----|----|
| VLAN ID | Groups | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| No more entries | | | | | | | | | | | | |

| Object | Description |
|--------------|--|
| VLAN ID | VLAN ID of the group. |
| Groups | Group address of the group displayed. |
| Port Members | Ports under this group. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |
| << | Click to update the table starting from the first entry in the MLD Groups Information Table. |
| >> | Click to update the table, starting with the entry after the last entry currently displayed. |

IPv6 SFM Information

Each page shows up to 99 entries from the MLD SFM Information table, default being 20, selected through the “entries per page” input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD SFM Information Table.

The “Start from VLAN”, and “group” input fields allow the user to select the starting point in the MLD SFM Information Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next MLD SFM Information Table match. In addition, the two input fields will upon a “Refresh” button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The “>>” will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text “No more entries” is shown in the displayed table. Use the “<<” button to start over.

MLD SFM Information Auto-refresh Refresh |<< >>

Start from VLAN and Group with entries per page.

| VLAN ID | Group | Port | Mode | Source Address | Type | Hardware Filter/Switch |
|-----------------|-------|------|------|----------------|------|------------------------|
| No more entries | | | | | | |

| Object | Description |
|------------------------|---|
| VLAN ID | VLAN ID of the group. |
| Group | Group address of the group displayed. |
| Port | Switch port number. |
| Mode | Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude. |
| Source Address | IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. |
| Type | Indicates the Type. It can be either Allow or Deny. |
| Hardware Filter/Switch | Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |
| << | Click to update the table starting from the first entry in the MLD SFM Information Table. |
| >> | Click to the table, starting with the entry after the last entry currently displayed. |

LLDP

Neighbors

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected.

LLDP Neighbor Information Auto-refresh Refresh

| LLDP Remote Device Summary | | | | | | |
|----------------------------|-------------------|---------|------------------|-------------|---------------------|----------------------|
| Local Interface | Chassis ID | Port ID | Port Description | System Name | System Capabilities | Management Address |
| 1 | 00-22-3B-0A-22-2A | 3 | Port #3 | CNGE12MS | Bridge(+) | 192.168.20.10 (IPv4) |

| Object | Description |
|---------------------|---|
| Local Interface | The port on which the LLDP frame was received. |
| Chassis ID | The Chassis ID is the identification of the neighbor's LLDP frames. |
| Port ID | The Port ID is the identification of the neighbor port. |
| Port Description | Port Description is the port description advertised by the neighbor unit. |
| System Name | System Name is the name advertised by the neighbor unit. |
| System Capabilities | System Capabilities describes the neighbor unit's capabilities. The possible capabilities are: <ol style="list-style-type: none"> 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-). |
| Management Address | Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |

PoE

This page provides a status overview for all LLDP PoE neighbors. The displayed table contains a row for each interface on which an LLDP PoE neighbor is detected. The columns hold the following information:

LLDP Neighbor Power Over Ethernet Information

Auto-refresh Refresh

| Local Interface | Power Type | Power Source | Power Priority | Maximum Power |
|-----------------------------------|------------|--------------|----------------|---------------|
| No PoE neighbor information found | | | | |

| Object | Description |
|-----------------|---|
| Local Interface | The interface for this switch on which the LLDP frame was received. |
| Power Type | The Power Type represents whether the device is a Power Sourcing Entity (PSE) or Power Device (PD). If the Power Type is unknown it is represented as "Reserved". |
| Power Source | The Power Source represents the power source being utilized by a PSE or PD device. If the device is a PSE device it can either run on its Primary Power Source or its Backup Power Source. If it is unknown whether the PSE device is using its Primary Power Source or its Backup Power Source it is indicated as "Unknown" If the device is a PD device it can either run on its local power supply or it can use the PSE as power source. It can also use both its local power supply and the PSE. If it is unknown what power supply the PD device is using it is indicated as "Unknown" |
| Power Priority | Power Power Priority represents the priority of the PD device, or the power priority associated with the PSE type device's interface that is sourcing the power. There are three levels of power priority. The three levels are: Critical, High and Low. If the power priority is unknown it is indicated as "Unknown" |
| Maximum Power | The Maximum Power Value contains a numerical value that indicates the maximum power in watts required by a PD device from a PSE device, or the minimum power a PSE device is capable of sourcing over a maximum length cable based on its current configuration. The maximum allowed value is 102.3 W. If the device indicates value higher than 102.3 W, it is represented as "reserved" |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |

EEE

The displayed table contains a row for each interface.

If the interface does not support EEE, then it displays as “EEE not supported for this interface”.

If EEE is not enabled on particular interface, then it displays as “EEE not enabled for this interface”.

If the link partner doesn't support EEE, then it displays as “Link partner is not EEE capable”.

The columns hold the following information:

LLDP Neighbors EEE Information

Auto-refresh Refresh

| Local Interface | Tx Tw | Rx Tw | Fallback Receive Tw | Echo Tx Tw | Echo Rx Tw | Resolved Tx Tw | Resolved Rx Tw | EEE in Sync |
|-----------------|-------|-------|---------------------|------------|------------|----------------|----------------|------------------------------------|
| 1 | | | | | | | | EEE not enabled for this interface |

| Object | Description |
|---------------------|--|
| Local Interface | The interface at which LLDP frames are received or transmitted. |
| TX Tw | The link partner's maximum time that transmit path can hold-off sending data after de-assertion of LPI. |
| RX Tw | The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep. |
| Fallback Receive Tw | The link partner's fallback receive Tw. A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx. "DISABLE" denotes the specific interface is administratively disabled. |
| Echo Tx Tw | The link partner's Echo Tx Tw value. The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information. |
| Echo Rx Tw | The link partner's Echo Rx Tw value. |
| Resolved Tx Tw | The resolved Tx Tw for this link. Note : NOT the link partner The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP). |
| Resolved Rx Tw | The resolved Rx Tw for this link. Note : NOT the link partner The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP). |
| EEE in Sync | Shows whether the switch and the link partner have agreed on wake times. Red - Switch and link partner have not agreed on wakeup times. Green - Switch and link partner have agreed on wakeup times. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |

Port Statistics

This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole switch, while local counters refer to per interface counters for the currently selected switch.

LLDP Global Counters Auto refresh Refresh Clear

| Global Counters | |
|------------------------------------|---|
| Clear global counters | <input checked="" type="checkbox"/> |
| Neighbor entries were last changed | 1970-01-01T16:56:25+00:00 (282 secs. ago) |
| Total Neighbors Entries Added | 1 |
| Total Neighbors Entries Deleted | 0 |
| Total Neighbors Entries Dropped | 0 |
| Total Neighbors Entries Aged Out | 0 |

LLDP Statistics Local Counters

| Local Interface | Tx Frames | Rx Frames | Rx Errors | Frames Discarded | TLVs Discarded | TLVs Unrecognized | Org. Discarded | Age-Outs | Clear |
|-----------------|-----------|-----------|-----------|------------------|----------------|-------------------|----------------|----------|-------------------------------------|
| 1 | 2044 | 10 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |

| Object | Description |
|-----------------------------------|--|
| Global Counters | |
| Neighbor entries were last change | Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected. |
| Total Neighbors Entries Added | Shows the number of new entries added since switch reboot. |
| Total Neighbors Entries Deleted | Shows the number of new entries deleted since switch reboot. |
| Total Neighbors Entries Dropped | Shows the number of LLDP frames dropped due to the entry table being full. |
| Total Neighbors Entries Aged Out | Shows the number of entries deleted due to Time-To-Live expiring. |
| Local Counters | |
| Local Port | The port on which LLDP frames are received or transmitted. |
| Tx Frames | The number of LLDP frames transmitted on the port. |
| Rx Frames | The number of LLDP frames received on the port. |
| Rx Errors | The number of received LLDP frames containing some kind of error. |
| Frames Discarded | If a LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out. |
| TLVs Discarded | Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded. |
| TLVs Unrecognized | The number of well-formed TLVs, but with an unknown type value. |
| Org. Discarded | If LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted. |

| Object | Description |
|--------------|---|
| Age-Outs | Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |
| Clear | Click to Clears the counters which have the corresponding checkbox checked. |

PoE

This page allows the user to inspect the current status for all PoE ports.

Power Over Ethernet Status Auto-refresh Refresh

| Local Port | PD class | Power Requested | Power Allocated | Power Used | Current Used | Priority | Port Status |
|------------|----------|-----------------|-----------------|------------|--------------|----------|----------------|
| 1 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 2 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 3 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 4 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 5 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 6 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 7 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 8 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| Total | | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | | |

| Object | Description |
|-----------------|---|
| Local Port | This is the logical port number for this row. |
| PD Class | Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the PDs class. Five Classes are defined: Class 0: Max. power 15.4 W Class 1: Max. power 4.0 W Class 2: Max. power 7.0 W Class 3: Max. power 15.4 W Class 4: Max. power 30.0 W |
| Power Requested | The Power Requested shows the requested amount of power the PD wants to be reserved. |
| Power Allocated | The Power Allocated shows the amount of power the switch has allocated for the PD. "DISABLE" denotes the specific interface is administratively disabled. |
| Power Used | The Power Used shows how much power the PD currently is using. |
| Current Used | The Power Used shows how much current the PD currently is using. |
| Priority | The Priority shows the port's priority configured by the user. The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP). |
| Port Status | The Port Status shows the port's status. The status can be one of the following values: PoE not available - No PoE chip found - PoE not supported for the port. PoE turned OFF - PoE disabled : PoE is disabled by user. PoE turned OFF - Power budget exceeded - The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down. No PD detected - No PD detected for the port. PoE turned OFF - PD overload - The PD has requested or used more power than the port can deliver, and is powered down. PoE turned OFF - PD is off. Invalid PD - PD detected, but is not working correctly. The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP). |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |

Note: When using the 60 W "Forced" PoE mode, the PoE statistics may not be accurately represented on this page.

MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "Start from MAC address" and "VLAN" input fields allow the user to select the starting point in the MAC Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will - upon a "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The ">>" will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "<<" button to start over.

MAC Address Table Auto-refresh

Start from VLAN and MAC address with entries per page.

| Type | VLAN | MAC Address | Port Members | | | | | | | | | | | | | | |
|---------|------|-------------------|--------------|---|---|---|---|---|---|---|---|---|----|----|--|--|--|
| | | | CPU | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | | | |
| Dynamic | 1 | 00-00-0C-42-7E-F0 | | ✓ | | | | | | | | | | | | | |
| Dynamic | 1 | 00-0C-29-05-11-3E | | ✓ | | | | | | | | | | | | | |
| Dynamic | 1 | 00-0C-29-05-11-42 | | ✓ | | | | | | | | | | | | | |
| Dynamic | 1 | 00-0C-29-05-11-43 | | ✓ | | | | | | | | | | | | | |
| Dynamic | 1 | 00-1A-62-04-4F-CF | | ✓ | | | | | | | | | | | | | |
| Dynamic | 1 | 00-21-9B-2D-5E-3D | | ✓ | | | | | | | | | | | | | |
| Dynamic | 1 | 00-21-B7-85-B7-51 | | ✓ | | | | | | | | | | | | | |
| Static | 1 | 00-22-3B-02-07-BC | ✓ | | | | | | | | | | | | | | |
| Dynamic | 1 | 00-22-3B-0A-22-2A | | ✓ | | | | | | | | | | | | | |

| Object | Description |
|--------------|---|
| Type | Indicates whether the entry is a static or a dynamic entry. |
| MAC Address | The MAC address of the entry. |
| VLAN | The VLAN ID of the entry. |
| Port Members | The ports that are members of the entry. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the displayed table starting from the input fields. |
| << | Click to update the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address. |
| >> | Click to the table, starting with the entry after the last entry currently displayed. |

VLANs

Membership

Each page shows up to 99 entries from the VLAN table (default being 20), selected through the “entries per page” input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The “VLAN” input field allows the user to select the starting point in the VLAN Table.




Clicking the “Refresh” button will update the displayed table starting from that or the closest next VLAN Table match.

The “>>” will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached, the text “No data exists for the selected user” is shown in the table. Use the “<<” button to start over.

VLAN Membership Status for Combined users Combined ▾ Auto-refresh Refresh

Start from VLAN with entries per page. |<< >>

| VLAN ID | Port Members | | | | | | | | | | |
|---------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

| Object | Description |
|--------------|--|
| VLAN User | <p>Various internal software modules may use VLAN services to configure VLAN memberships on the fly.</p> <p>The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.</p> <p>The “Combined” entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.</p> |
| VLAN ID | VLAN ID for which the Port members are displayed. |
| Port Members | <p>A row of check boxes for each port is displayed for each VLAN ID.</p> <p>If a port is included in a VLAN, the following image will be displayed: </p> <p>If a port is in the forbidden port list, the following image will be displayed: </p> <p>If a port is in the forbidden port list and at the same time attempted included in the VLAN, the following image will be displayed: . The port will not be a member of the VLAN in this case.</p> |
| Combined | Select the VLAN user from this drop-down list. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the page. |

Ports

This page shows VLAN Port Status.

VLAN Port Status for Combined users Combined ▾ Auto-refresh Refresh

| Port | Port Type | Ingress Filtering | Frame Type | Port VLAN ID | Tx Tag | Untagged VLAN ID | Conflicts |
|------|-----------|-------------------------------------|------------|--------------|-----------|------------------|-----------|
| 1 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 2 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 3 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 4 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 5 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 6 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 7 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 8 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 9 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 10 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 11 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |

| Object | Description |
|-------------------|---|
| VLAN User | <p>Various internal software modules may use VLAN services to configure VLAN port configuration on the fly.</p> <p>The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.</p> <p>If a given software modules hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table.</p> |
| Port | The logical port for the settings contained in the same row. |
| Port Type | <p>Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port.) that a given user wants to configure on the port.</p> <p>The field is empty if not overridden by the selected user.</p> |
| Ingress Filtering | Shows whether a given user wants ingress filtering enabled or not. The field is empty if not overridden by the selected user. |
| Frame Type | <p>Shows the acceptable frame types (All, Taged, Untagged) that a given user wants to configure on the port.</p> <p>The field is empty if not overridden by the selected user.</p> |
| Port VALN ID | Shows the Port VLAN ID (PVID) that a given user wants the port to have. The field is empty if not overridden by the selected user. |
| Tx Tag | <p>Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port.</p> <p>The field is empty if not overridden by the selected user.</p> |
| Untagged VLAN ID | <p>If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field will show the VLAN ID the user wants to tag or untag on egress.</p> <p>The field is empty if not overridden by the selected user.</p> |

| Object | Description |
|--------------|---|
| Conflicts | <p>Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress.</p> <p>Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list: The higher in the list, the higher priority.</p> <p>If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module.</p> <p>The "Combined" user reflects what is actually configured in hardware.</p> |
| Combined | Select the VLAN user from this drop-down list. |
| Auto_refresh | Check to refresh the page automatically every 3 seconds. |
| Refresh | Click to refresh the page. |

Diagnostics Menu

Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

ICMP Ping

| | |
|---------------|---------|
| IP Address | 0.0.0.0 |
| Ping Length | 56 |
| Ping Count | 5 |
| Ping Interval | 1 |

| Object | Description |
|---------------|---|
| IP Address | The destination IP Address. |
| Ping Length | The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes. |
| Ping Count | The count of the ICMP packet. Values range from 1 time to 60 times. |
| Ping Interval | The interval of the ICMP packet. Values range from 0 second to 30 seconds. |

Click "Start" button to start the ping test.

Ping6

This page allows you to issue ICMP PING packets to troubleshoot IPv6 connectivity issues.

ICMPv6 Ping

| | |
|------------------|-----------------|
| IP Address | 0:0:0:0:0:0:0:0 |
| Ping Length | 56 |
| Ping Count | 5 |
| Ping Interval | 1 |
| Egress Interface | |

Start

| Object | Description |
|----------------------------------|---|
| IP Address | The destination IP Address. |
| Ping Length | The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes. |
| Ping Count | The count of the ICMP packet. Values range from 1 time to 60 times. |
| Ping Interval | The interval of the ICMP packet. Values range from 0 second to 30 seconds. |
| Egress Interface (only for IPv6) | The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. When the egress interface is not given, PING6 finds the best match interface for destination. Do not specify egress interface for loopback address. Do specify egress interface for link-local or multicast address. |

Click "Start" button to start IPv6 ping test.

PHYtest

Press "Start" to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

VeriPHY Cable Diagnostics

Port

| Cable Status | | | | | | | | |
|--------------|--------|----------|--------|----------|--------|----------|--------|----------|
| Port | Pair A | Length A | Pair B | Length B | Pair C | Length C | Pair D | Length D |
| 1 | OK | 0 | OK | 0 | OK | 0 | OK | 0 |
| 2 | Open | 0 | Short | 0 | Open | 0 | Open | 0 |
| 3 | Open | 0 | Open | 0 | Open | 0 | Open | 0 |
| 4 | Open | 0 | Open | 0 | Open | 0 | Open | 0 |
| 5 | Open | 0 | Open | 0 | Open | 0 | Open | 0 |
| 6 | Open | 0 | Open | 0 | Open | 0 | Open | 0 |
| 7 | Open | 0 | Open | 0 | Open | 0 | Open | 0 |
| 8 | Open | 0 | Open | 0 | Open | 0 | Open | 0 |

| Object | Description |
|--------------|--|
| Port | The port where you are requesting VeriPHY Cable Diagnostics. |
| Cable Status | Port: Port number. Pair: The status of the cable pair. OK - Correctly terminated pair Short - Shorted pair Short A - Cross-pair short to pair A Short B - Cross-pair short to pair B Short C - Cross-pair short to pair C Short D - Cross-pair short to pair D Cross A - Abnormal cross-pair coupling with pair A Cross B - Abnormal cross-pair coupling with pair B Cross C - Abnormal cross-pair coupling with pair C Cross D - Abnormal cross-pair coupling with pair D Length: The length (in meters) of the cable pair. The resolution is 3 meters |

Click "Start" button to start the cable diagnostic test.

Maintenance Menu

Restart Device

You can restart the switch on this page. After restart, the switch will boot normally.

Restart Device

Are you sure you want to perform a Restart?

Click "Yes" Button to restart the switch. It may take up to a minute to finish restart. Click "No" button to go back to home page without resetting configurations.

Factory Defaults

You can reset the configuration of the switch on this page. Only the IP configuration is retained.

The new configuration is available immediately, which means that no restart is necessary.

Factory Defaults

Are you sure you want to reset the configuration to
Factory Defaults?

Click "Yes" button to reset the configuration to factory default. It may take up to 20 seconds to show the following message:

Configuration Factory Reset Done

The configuration has been reset. The new configuration is available immediately.

Click "No" button to go back to home page without resetting configurations.

Software

Upload

This page facilitates an update of the firmware controlling the switch.

Software Upload

No file chosen

To upload an image, click "Choose File" button. Browse to the location of a software image and click "Upload" button.

After the software image is uploaded, a page announces that the firmware update is initiated. After a few minutes, the firmware is updated and the switch restarts.

Warning - While the firmware is being updated, Web access appears to be non-responsive. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

Image Select

This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

The web page displays two tables with information about the active and alternate firmware images.

Note:

1. In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.
2. If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

Software Image Selection

| Active Image | |
|----------------|--|
| Image | C:\Users\Admin\Desktop\cnge3fe8ms[poeho]_1.3.0.dat |
| Version | ComNetFirmware Version 1.3.0 |
| Date | 2017-07-31T09:12:27-04:00 |

| Alternate Image | |
|-----------------|------------------------------|
| Image | cnge3fe8ms[poeho]_v1.1.1.dat |
| Version | ComNetFirmware Version 1.1.0 |
| Date | 2017-06-20T18:47:21-04:00 |

| Object | Description |
|--------------------------|--|
| Image | The flash index name of the firmware image. The name of primary (preferred) image is image, the alternate image is named image.bk. |
| Version | The version of the firmware image. |
| Data | The date where the firmware was produced. |
| Activate Alternate Image | Click to swap the active image to alternate image. |
| Cancel | Click to go back to home screen without change. |

Click the "Activate Alternate Image" button to swap the image and restart the switch. Click "Cancel" button to go back to home screen.

Configuration

Save Startup-configuration

Copy running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot.

Save Running Configuration to startup-config

Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

Save Configuration

Click "Save Configuration" button to save.

Download

A user can download the switch configuration files by clicking "Download Configuration" button.

Download Configuration

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

| File Name | |
|-----------------------|----------------|
| <input type="radio"/> | running-config |
| <input type="radio"/> | default-config |
| <input type="radio"/> | startup-config |

Download Configuration

Click "Download Configuration" button to download selected configuration files.

Upload

It is possible to upload a file from the web browser to all the files on the switch, except default-config, which is read-only.

Upload Configuration

File To Upload

No file chosen

Destination File

| File Name | Parameters |
|---------------------------------------|--|
| <input type="radio"/> running-config | <input checked="" type="radio"/> Replace <input type="radio"/> Merge |
| <input type="radio"/> startup-config | |
| <input type="radio"/> Create new file | |

Select the file to upload, select the destination file on the target, then click "Upload Configuration".

If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:

- Replace mode: The current configuration is fully replaced with the configuration in the uploaded file.
- Merge mode: The uploaded file is merged into running-config.

If the file system is full (i.e. contains the three system files mentioned above plus two other files), it is not possible to create new files, but an existing file must be overwritten or another deleted first.

Activate

It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.

Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will not be saved to startup-config automatically.

| File Name |
|--------------------------------------|
| <input type="radio"/> default-config |
| <input type="radio"/> startup-config |

Select the file to activate and click "Activate Configuration". This will initiate the process of completely replacing the existing configuration with that of the selected file.

Delete

It is possible to delete any of the writable files stored in flash, including startup-config. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration.

Delete Configuration File

Select configuration file to delete.

| File Name |
|--------------------------------------|
| <input type="radio"/> startup-config |

Delete Configuration File

Select "startup-config" file, and click "Delete Configuration File" button to delete the startup-config. Switch will reconfigure itself to factory default after restart.

Using Switch CLI

About CLI Management

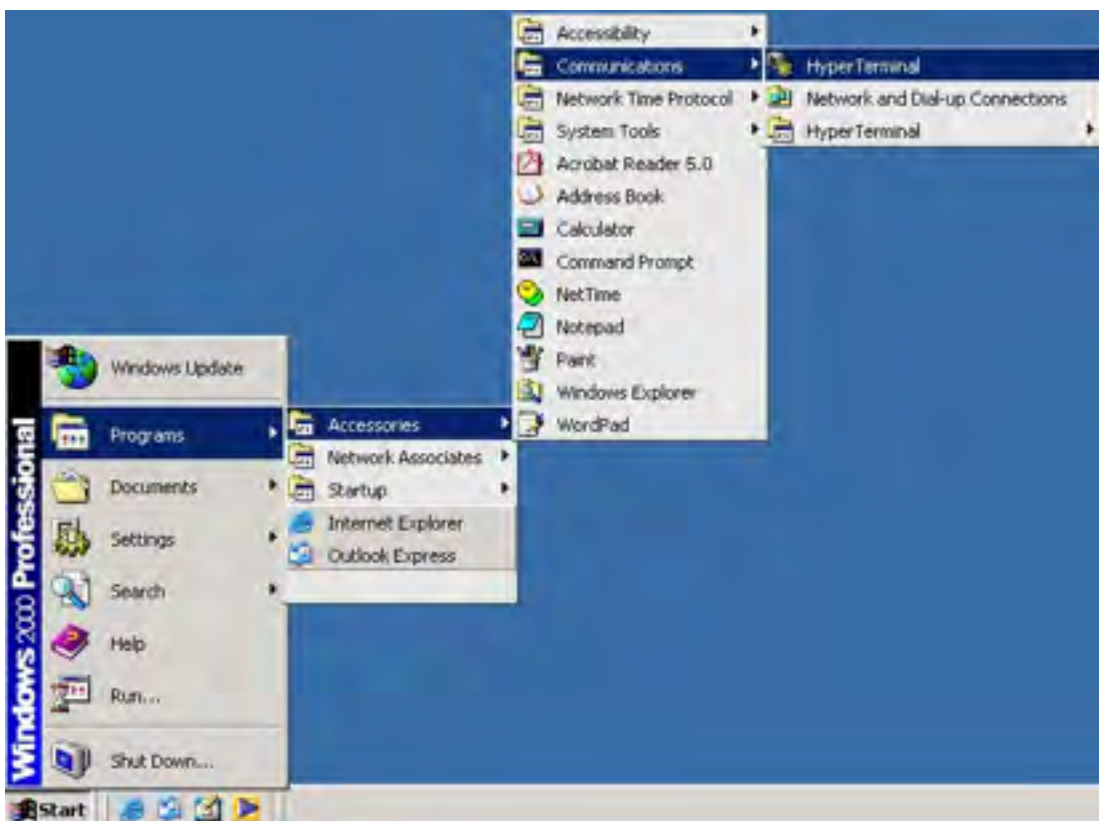
Besides WEB-base management, Comnet switch also support CLI management. You can use console or telnet to management switch by CLI.

CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)

Before Configuring RS-232 serial console, use a USB Male-A to USB Male-B cable to connect the Switches' RS-232 Console port to your PC's USB port.

Follow the steps below to access the console via RS-232 serial cable.

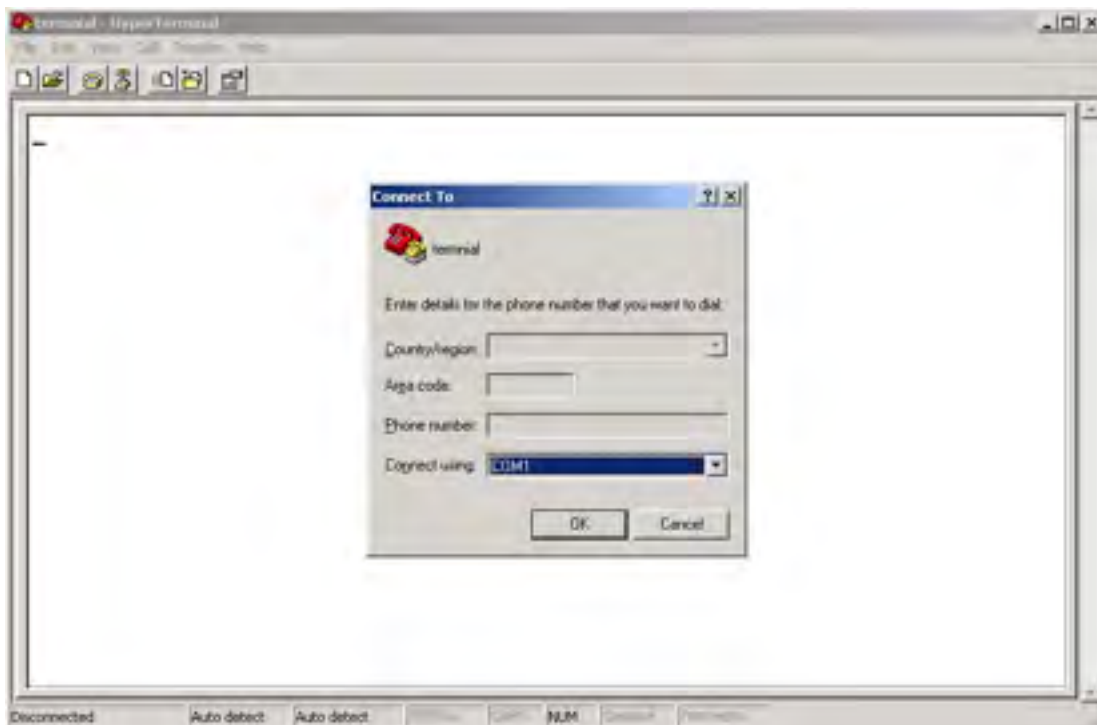
Step 1. From the Windows desktop, click on Start -> Programs -> Accessories -> Communications -> Hyper Terminal



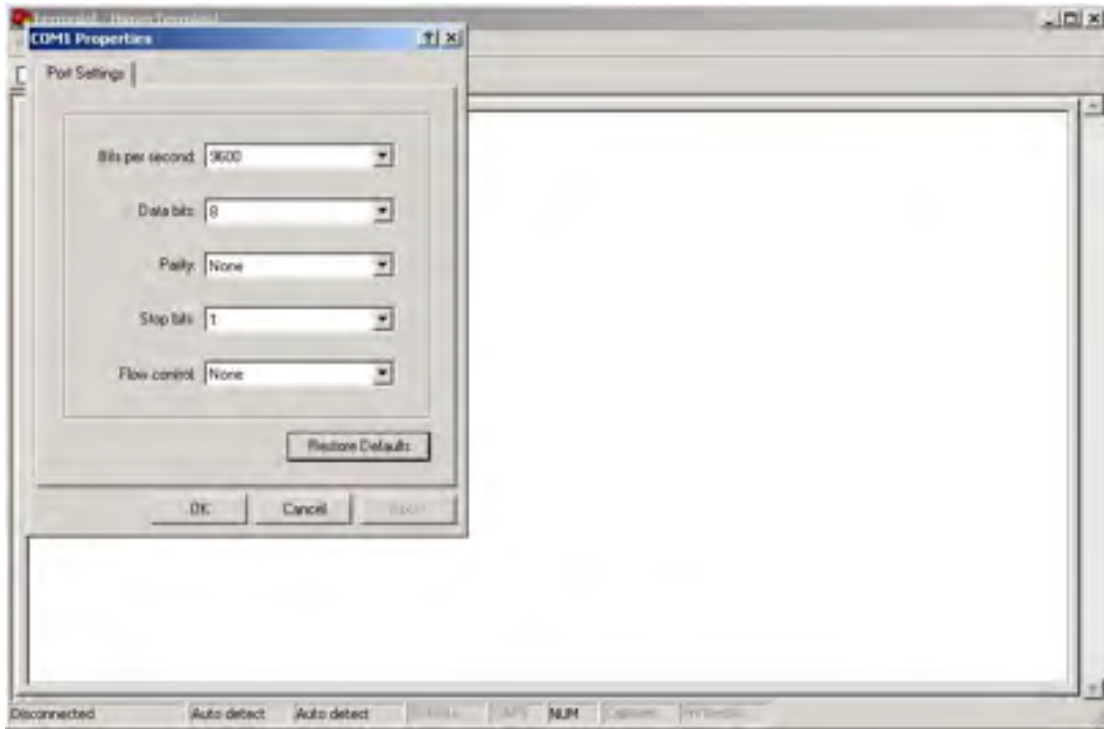
Step 2. Input a name for new connection



Step 3. Select to use COM port number



Step 4. The COM port properties setting, 115200 for Bits per second, 8 for Data bits, None for Parity, 1 for Stop bits and none for Flow control.



Step 5. The Console login screen will appear. Use the keyboard to enter the Username and Password (The same with the password for Web Browser), then press "Enter".

```
Username: admin
Password: ■
```

CLI Management by Telnet

Users can use "TELNET" to configure the switches.

The default value is as below:

IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0

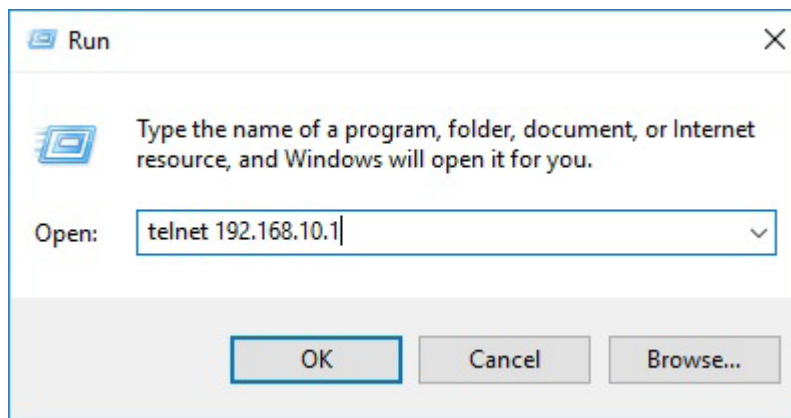
Default Gateway: 192.168.10.254

User Name: admin

Password: admin

Follow the steps below to access the console via Telnet.

Step 1. Telnet to the IP address of the switch from the Windows "Run" command (or from the MS-DOS prompt) as below.



Step 2. The Login screen will appear. Use the keyboard to enter the Username and Password (The same with the password for Web Browser), and then press "Enter"

Console login screen

Commander Groups

```
# ?
clear          Reset functions
configure     Enter configuration mode
copy          Copy from source to destination
delete        Delete one file in flash: file system
dir           Directory of all files in flash: file system
disable       Turn off privileged commands
do            To run exec commands in config mode
dot1x         IEEE Standard for port-based Network Access Control
enable        Turn on privileged commands
erps          Ethernet Ring Protection Switching
exit          Exit from EXEC mode
firmware      Firmware upgrade/swap
help          Description of the interactive help system
ip            IPv4 commands
ipv6          IPv6 configuration commands
link-oam      Link OAM configuration
logout        Exit from EXEC mode
more          Display file
no            Negate a command or set its defaults
phytest       phytest keyword
ping          Send ICMP echo messages
reload        Reload system.
send          Send a message to other tty lines
show          Show running system information
terminal      Set terminal line parameters
#
```

Typing "?" and "Enter" at any prompt, will list the valid commands with their descriptions in this mode. Typing "?" and "Enter" after a command line, will list parameters of the command line.

Quick Start

This section describes how to perform the following:

- » Log in and reset configuration to factory defaults
- » Set device hostname and admin user password
- » Set VLAN 1 IP address
- » Verify connectivity using 'ping'
- » Display the current configuration and save it to flash storage

The following assumes the device is powered on and has a functional connection to a computer using the serial console port on the device (115200 baud, no parity, 8 data bits, 1 stop bit, no flow control).

The computer must be running a terminal emulator such as TeraTerm or PuTTY on Windows, or Minicom on Linux.

Log In and Reset Configuration to Factory Default

Press Enter one or more times until the Username: prompt appears. Type admin and press Enter. At the Password: prompt press Enter as there is no password required. This completes the login sequence and displays the prompt, '#'.

```
Username: admin
```

```
Password: admin
```

```
#
```

At this point, the admin user is operating at the highest privilege level, level 15. This means full control over the device and its configuration, and it is therefore possible to reset the configuration to factory defaults. Type reload defaults and press Enter. When the prompt returns, the system has reverted to factory defaults as follows.

```
# reload defaults
```

```
% Reloading defaults. Please stand by.
```

```
#
```

Set Device Hostname and Admin User Password

The ICLI has several different modes. The current mode is called exec mode; it allows the user to perform operations related to configuration files, reloading defaults, displaying system information, etc., but it does not allow the user to change detailed configuration items. Such operations are performed while in the config mode.

To set the device hostname, first change to configuration mode by typing `configure terminal` and press Enter, then type `hostname my-device` and press Enter, where `my-device` is a suitable name for the device. Finally, type `exit` and press Enter. The sequence should appear as shown here.

```
# configure terminal
(config)# hostname my-device my-device(config)# exit
my-device#
```

The commands are executed immediately, so `hostname` changes the device hostname right away. A password should be set for the admin user.

```
my-device# configure terminal
my-device(config)# username admin privilege 15 password unencrypted very-secret
my-device(config)# exit
my-device#
```

The user, `admin`, now has the password “`very-secret`.” Other users can be added in similar fashion.

Set VLAN 1 IP Address

The objective is to assign an IP address to the device on VLAN 1. This is often sufficient for small local area networks that use Dynamic Host Configuration Protocol (DHCP) or static IP address allocation.

The system implements a DHCP client that, once enabled, will send out requests for IP address configuration. Those requests are received by a DHCP server on the network (if present and appropriately configured). The server will then search through its pool of available IP addresses, allocate one, and return it to the DHCP client. The returned information typically includes IP address, netmask, and default gateway, but may also contain other information such as Domain Name Service (DNS) server addresses.

The configuration proceeds in the same manner as setting the hostname: Enter configuration mode, input and execute configuration commands, leave configuration mode. The following commands instruct the device to use DHCP to obtain an IP address, or, if DHCP fails, to use a static fallback address. Inclusion of a fallback IP is optional and may be omitted.

```
my-device# configure terminal
```

```
my-device(config)# interface vlan 1
my-device(config-if-vlan)# ip address dhcp fallback 192.168.10.2 255.255.0.0
my-device(config-if-vlan)# exit
my-device(config)#
```

Notice how the prompt changes; the interface vlan 1 command enters a configuration sub-mode that allows, among other things, configuration of IP address.

Also note that IP addresses can only be assigned to VLAN interfaces.

After configuration is complete, the resulting IP address can be inspected. As seen below, the DHCP negotiation succeeded and the device obtained an address:

```
my-device# show ip interface brief
Vlan Address Method Status
1 192.168.10.17/16 DHCP UP my-device#
```

show ip interface brief displays all configured and active IP interfaces. The status should be UP. If it isn't, then the reason could be that there is no link on any port.

If DHCP negotiation failed, then the fallback IP of 192.168.10.2/255.255.0.0 would be assigned.

Now the most basic system configuration is complete. Management connectivity can be verified by issuing a ping command to a well-known external IP address:

```
my-device# ping ip 192.168.10.1
PING server 192.168.10.1, 56 bytes of data.
64 bytes from 192.168.10.1: icmp_seq=0,time=0ms
64 bytes from 192.168.10.1: icmp_seq=1,time=0ms
64 bytes from 192.168.10.1: icmp_seq=2,time=0ms
64 bytes from 192.168.10.1: icmp_seq=3,time=0ms
64 bytes from 192.168.10.1: icmp_seq=4,time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

```
my-device#
```

If the ping is successful, network logins can now be performed through telnet or ssh to the address on VLAN interface 1, 192.168.10.17 (or 192.168.10.2).

Display and Save Configuration to Flash

The current configuration of the device can be displayed in the form of a virtual file containing the full set of commands necessary to create an identical configuration. A few exceptions exist because certain items are not displayed, such as private SSH keys. This file is called running-config and is volatile by nature; it does not survive across reboots. It is therefore necessary to save the file to flash storage under the name startup-config, as this file is read and executed upon every boot and is therefore responsible for restoring the running configuration of the system to the state it had when the save took place.

The command show running-config will display the configuration settings as seen below. For brevity, some details were edited out. In addition, the set of interfaces is dependent on hardware capabilities.

```
my-device# show running-config
```

```
Building configuration...
```

```
hostname my-device
```

```
username admin privilege 15 password encrypted
```

```
3ad61dc090116a16a7cc9861485e60e6407c5a328015b1985b585ab353c37a4441e034172401
```

```
528229795a5c9529dfbc04c86e01
```

```
!
```

```
vlan 1,42
```

```
!
```

```
spanning-tree mst name 00-01-c1-00-ad-80 revision 0
```

```
!      [...]
```

```
!
```

```
interface GigabitEthernet 1/1
```

```
!
```

```
interface GigabitEthernet 1/2
```

```
!
```

```
!      [...]
```

```
!
```

```
interface 2.5GigabitEthernet 1/1
```

```
!
```



```
interface 2.5GigabitEthernet 1/2
!
interface vlan 1
ip address dhcp fallback 192.168.10.2 255.255.0.0
!
line console 0
!
line vty 0
!
! [...]
!
end
my-device#
```

Lines that begin with ‘!’ are comments. The file begins with the hostname command and the password for the admin user, followed by VLANs 1 and 42 and other items, such as Spanning Tree Protocol (STP). A list of all port interfaces on the device, ordered by switch ID, type, and port number comes next.

All port interfaces are at default settings, so nothing is displayed for them. As a general rule, only non-default configuration is displayed, otherwise the output would be huge and readability would suffer. There are a few exceptions that will be discussed later.

Following the physical interfaces are VLAN interfaces 1 and 42. Only the former has an IP address assigned. Finally, the line section is shown. It specifies characteristics for the serial console (line console 0) or network ICLI management connections (line vty x).

The configuration as displayed above is also what is saved to startup-config. my-device# copy running-config startup-config

Building configuration...

% Saving 1326 bytes to flash:startup-config

my-device# dir

Directory of flash:

-r- 1970-01-01 00:00:00 648 default-config

rw 1970-01-03 18:21:28 1326 startup-config

2 files, 1974 bytes total.

```
my-device# more flash:startup-config
hostname my-device
username admin privilege 15 password encrypted
3ad61dc090116a16a7cc9861485e60e6407c5a328015b1985b585ab353c37a4441e034172401
528229795a5c9529dfbc04c86e01
!
vlan 1,42
[...]
```

The dir command lists the files in the flash file system while more outputs the contents of the designated file.

The skills exercised in this section form the basis for all day-to-day work with the ICLI on the device: logging in, displaying information with the show command, working with configuration files (show running-config, copy, dir, more), working with the actual configuration (configure terminal, exit), and sub-modes (interface ...).

The configuration proceeds in the same manner as setting the hostname: Enter configuration mode, input and execute configuration commands, leave configuration mode. The following commands instruct the device to use DHCP to obtain an IP address, or, if DHCP fails, to use a static fallback address. Inclusion of a fallback IP is optional and may be omitted.

ICLI Basics

The following list shows the key ICLI characteristics:

1. It is modal (certain operations are possible or impossible in specific modes)
2. It is line-based (there are no screen editing features)
3. It executes commands instantly upon end-of-line
4. It is privilege-based (certain operations require the user to have a certain privilege level to succeed)
5. It implements industrial de-facto behavior for network equipment CLIs (structurally and behaviorally, it resembles CLIs found on other equipment while still possessing unique characteristics in some areas)

The ICLI can be accessed directly using the serial console, or over the network through telnet or ssh. In each case, the user has to log in before ICLI commands can be executed. This begins a session that lasts until logout.

Multiple sessions can co-exist at the same time, each providing separate environments: logged-in user ID, privilege level, command history, mode, and session settings. It is therefore perfectly

possible for the same user to control several concurrent sessions, such as one serial console session and one ssh session.

The user database is either local or provided by a RADIUS or TACACS+ server. In case of a local user database, passwords and privilege levels are maintained on the device.

Command Structure and Syntax

A command is a single line of text consisting of keywords and parameters, for example:

```
my-device# show vlan id 10 ...
```

```
my-device# show vlan id 20 ...
```

The keywords are show, vlan, and id; whereas 10 and 20 are parameters, something that could contain another value in another command invocation.

Keywords are not case sensitive, thus show, SHOW, and Show are identical. Conversely, parameters may either be case-sensitive or not, depending on the command and parameter in question.

Keywords and certain parameters can be abbreviated as long as they are unambiguous. For example, these commands are identical:

```
my-device# show interface GigabitEthernet 1/5 capabilities
```

```
...
```

```
my-device# sh in g 1/5 c
```

```
...
```

This works because:

- » There are many keywords that begin with 's' but only one that begins with 'sh'
- » There are several commands that begin with 'show i' but only one that begins with 'show in'
- » The show interface command takes a port type as parameter. Depending on the hardware capabilities, the options are: FastEthernet, GigabitEthernet, 2.5GigabitEthernet, 5GigabitEthernet and 10GigabitEthernet. Thus, 'g' is a unique abbreviation for GigabitEthernet
- » 1/5 identifies the interface as belonging to switch 1, port 5. This parameter cannot be abbreviated and has to be written out in full
- » The show interface GigabitEthernet 1/5 command can output different kinds of information: Capabilities, statistics, status, and several other. In this case, 'c' is a unique abbreviation for capabilities

With a bit of practice, this allows for highly efficient keyboard entry, in particular when coupled with the context-sensitive help features of the ICLI (see Context-Sensitive Help, page 9).

Syntax

A command is described by its syntax, for example:

```
show interface list { status | statistics | capabilities | switchport | veriphy }
```

and

```
show erps [ groups ] [ detail | statistics ]
```

Note: *Syntax is represented in a slightly different manner in this documentation as compared to a ICLI session.*

In this document, variable parameters are written in italics, whereas a ICLI session will display such items surrounded by '<' and '>'.

The semantics are:

- » keywords are written in bold
- » parameters are written in italics
- » [...] indicates an optional construct: It may or may not be present
- » { ... } indicates a grouping; the constructs within belong together
- » '|' indicates a choice between two or more alternatives, (example, a | b | c which reads as "a or b or c").

Thus, the first command syntax is simple: First show, then interface, then a list of interfaces, then exactly one of status, statistics, capabilities, switchport, and veriphy.

The second command is a bit more complex: show and erps are mandatory, but the remaining parameters and keywords are optional: The user may enter group IDs; the user may enter either 'statistics' or 'detail'. For example:

! Show short-form ERPS (Ethernet Ring Protection Switching) information for all

! instances:

```
my-device# show erps
```

...

! Show statistics for all instances:

```
my-device# show erps statistics
```

...

! Show details for all instances:

```
my-device# show erps detail
```

...

! But it is not allowed to show details and statistics at the same time:

my-device# show erps detail statistics

^

% Invalid word detected at '^' marker.

! Show details for specific set of instances:

my-device# show erps 1-6 detail

...

There are some slightly more complex features of the syntax that center around sequences of optional items such as [a] [b] [c].

- » Each of a, b, c may or may not be present ("a c" is valid, as is no input)
- » Order is not important ("a c" and "c a" are equivalent)
- » Each optional item can be present exactly no times or one time (not repeated)

There are variations:

- » Group of options, of which at least one must be present: { [a] [b] [c] } *1
- » Group of options, where one or more has fixed position: [a] {[b]} [c]
- » This says that 'b' is optional, but if it is present then it must follow after 'a' (if 'a' is present) and it must come before 'c' (if 'c' is present)

For example, assuming a command with this syntax:

a [b] [c] { d | e } {[f] [g]} *1 then valid input examples are:

- » 'a d f', because 'b' and 'c' are optional, 'd' is picked instead of 'e', and 'f' is chosen as the mandatory optional
- » 'a d f g', because 'b' and 'c' are optional, 'd' is picked instead of 'e', and both 'f' and 'g' are chosen in the final group of optional
- » 'a c b e g', because the 'b' optional is omitted, 'e' is picked instead of 'd', and 'g' is chosen for the mandatory optional

Ethernet Interface Naming

An Ethernet interface, or port, is identified by three pieces of information:

- » The type (FastEthernet, GigabitEthernet, 2.5GigabitEthernet, 5GigabitEthernet, 10GigabitEthernet)
- » The switch it belongs to (for non-stacking systems, this value is always 1)
- » The port number within the type and switch (numbering starts with 1 for each type, so a switch may have both GigabitEthernet 1/1 and 2.5GigabitEthernet 1/1)

Many ICLI commands accept a list of interfaces. In its simplest form, such a list is a sequence of (type, switch ID, port) information separated by whitespace. For example: GigabitEthernet 1/3 10GigabitEthernet 1/2. This allows a single list to mix different types.

The switch ID and the port numbers can be listed either as single numbers, as lists, or as sequences. A list is a comma-separated set of single port numbers or sequences, whereas a sequence is of the form: from–to.

Some examples:

- » GigabitEthernet 1/5 for the single gigabit port number 5 on switch 1
- » GigabitEthernet 1/2,4,10-12 for gigabit ports 2, 4, 10, 11, 12 on switch 1
- » GigabitEthernet 1-3/2 for gigabit port 2 on switches 1, 2 and 3

It is possible to wildcard the type and/or switch ID and/or ports to mean “all types,” “all switch IDs,” and “all ports,” respectively. A wildcard is written with an asterisk instead of type, switch ID, or port, and some further abbreviations are possible:

- » ‘*’ means “all ports of all types on all switches”
- » type ‘*’ means “all ports of the specified type on all switches”

To clarify, several examples are provided. Assume a stack with two switches, switch ID 1 and 3. Each switch has 9 gigabit ports and two 2.5 gigabit ports. Then:

- » interface * (or: interface * * *)
- » All ports of all types on all switches: GigabitEthernet 1,3/1-9 2.5GigabitEthernet 1,3/1-2
- » interface * 1/2
- » Switch 1, port number 2 of all types: GigabitEthernet 1/2 2.5GigabitEthernet 1/2
- » interface * */2
- » All switches, all types, port number 2: GigabitEthernet 1,3/2 2.5GigabitEthernet 1,3/2
- » interface * */4
- » All switches, all types, port number 4: GigabitEthernet 1,3/4

There are no 2.5 gigabit ports in the result.

- » interface GigabitEthernet 3/*
- » Switch 3, all gigabit ports: GigabitEthernet 3/1-9
- » interface 2.5GigabitEthernet * (or: interface 2.5GigabitEthernet */*)
- » All 2.5 gigabit ports on all switches: 2.5GigabitEthernet 1,3/1-2

Wildcards will include the largest possible set of ports, but may output an error message if a specific switch ID or port number doesn't exist.

For example, these sets are invalid:

interface * 2/*

- » All ports of all types on switch 2 - which isn't a member of the stack
- » interface * */100
- » There is no port 100 of any type on any switch
- » interface GigabitEthernet */* 2.5GigabitEthernet 2/*
- » Again, switch 2 doesn't exist so the entire set is considered invalid

Validity is determined per set of (type, switch ID, port) containing wildcards: The result for that set is valid if there is at least one port that matches the set. A list of sets is valid if all sets match at least one port each.

Using the Keyboard

The ICLI provides a rich set of keys to assist the user while working with the command line. The functionality is divided into:

- » Basic line editing
- » Command history
- » Context-sensitive help
- » Long lines and pagination

Basic Line Editing

Basic line editing allows the input of characters to form a command line, while also allowing cursor movement and insertion/deletion of characters and words. The following table shows the available editing functions and keys.

Table 1 - Basic Line Editing Key

| Key | Operation |
|------------------|--|
| Left/Right | Move one character left/right |
| Home/Ctrl-A | Move to start of line |
| End/Ctrl-E | Move to end of line |
| Del/Ctrl-D | Delete character at cursor |
| Backspace/Ctrl-H | Delete character to the left of cursor |
| Ctrl-N | Delete the entire current line |
| Ctrl-U/Ctrl-X | Delete all characters to the left of the cursor |
| Ctrl-K | Delete all characters under the cursor and right |
| Ctrl-W | Delete from cursor to start of word on the left |
| TAB | Complete word at end-of-line |

Command History

A session maintains a non-persistent command history of previously entered command lines. The history can be up to 32 lines long. Once full, a new line will push the oldest entry out.

Table 2 - Command History

| Key | Operation |
|-----------|----------------------------------|
| Up/Ctrl-P | Previous line in command history |
| Down | Next line in command history |

The number of lines to keep in the history for the current session is configurable between 0 and 32, where 0 disables the history altogether.

```
my-device# terminal history size 32
```

The current value is displayed as part of the output from show terminal:

```
my-device# show terminal
```

```
Line is con 0.
```

```
    * You are at this line now.
```

```
    Alive from Console.
```

```
    Default privileged level is 2.
```

```
    Command line editing is enabled
```

```
    Display EXEC banner is enabled.
```

```
    Display Day banner is enabled.
```

```
    Terminal width is 80.
```

```
        length is 24.
```

```
        history size is 32.
```

```
        exec-timeout is 10 min 0 second.
```

```
    Current session privilege is 15.
```

```
    Elapsed time is 0 day 0 hour 6 min 20 sec.
```

```
    Idle time is 0 day 0 hour 0 min 0 sec.
```

It is possible to list the history:

```
my-device# show history
```

```
    show running-config
```

```
    copy running-config startup-config
```

```
    dir
```

```
    show history
```

```
my-device#
```

The list begins with the oldest entry at top.

Context-Sensitive Help

The ICLI implements several hundred commands ranging from the very simple to the very complex. It is therefore imperative that the user can be assisted in entering syntactically correct commands as well as discovering relevant commands. These objectives are supported by the context sensitive help features.

Table 3 - Context-Sensitive Help

| Key | Operation |
|-----------|--|
| ? | Show next possible input and description |
| ??/Ctrl-Q | Show syntax of possible command(s) |
| TAB | Show next possible input without description or expand current word if it is unambiguous |

The context-sensitive help only displays commands that are accessible at the current session privilege level (see Understanding Privilege Levels, page 15).

Using Context-Sensitive Help

! Show possible next input for a command that begins with 'show a': my-device# show a?

```
aaa  Login methods
```

```
access      Access management
```

```
access-list  Access list
```

```
aggregation  Aggregation port configuration
```

! The same, but without descriptions: my-device# show a<TAB>

```
aaa  access      access-list aggregation
```

! If the user enters another 'g' the word 'aggregation' is the only possibility: my-device# show ag?

```
aggregation  Aggregation port configuration
```

```
<cr>
```

! Pressing <TAB> now expands the word fully:

```
my-device# show aggregation
```

! Possible next input is displayed with a press of '?':

```
my-device# show aggregation ?
```

```
|      Output modifiers
```

mode Traffic distribution mode

<cr>

! The syntax is displayed with another press of '?':

```
my-device# show aggregation ?
```

```
show aggregation [ mode ]
```

! This shows that there is an optional 'mode' word (square brackets indicate an option).

! Repeated presses of '?' toggles display between next possible input and syntax:

```
my-device# show aggregation ?
```

```
|      Output modifiers
```

```
mode Traffic distribution mode
```

<cr>

```
my-device# show aggregation ?
```

```
show aggregation [ mode ]
```

! Finally, the syntax display is also directly available with Ctrl-Q:

```
my-device# show aggregation ^Q
```

```
show aggregation [ mode ]
```

Long Lines and Pagination

A session has a configuration that indicates the width of the terminal in characters and the length in lines. It uses these parameters to control handling of long input lines and to control pagination of multi-line output. For details about changing these parameters, see Understanding Terminal Parameters, page 16.

Long lines come into play when a line is longer than the terminal width minus the prompt. In that case, part of the line will be hidden from display as indicated by '\$' at the beginning and/or end of the visible part of the line.

For example:

```
My-device# $there is text to the left of what is visible here my-device# there is text to the right of
what is visible here$ my-device# $there is text at both ends of what is visible here$
```

The first line has scrolled left; the second line has scrolled right; the third line has been scrolled to the middle of a quite long line.

Pagination appears each time execution of a command causes output of more lines than what has been configured as the terminal length. A typical example is the output from show running-config. After the first several lines have been output, the pagination prompt is presented:

```
! [lines of text]
```

```
-- more --, next page: Space, continue: g, quit: ^C
```

The following keys control pagination:

Table 4 - Pagination Keys

| Key | Operation |
|---------------|---|
| Enter | Display next line of output |
| Space | Display next page of output |
| G | Display remainder of output without more pagination |
| Q/Ctrl-C | Display remainder of output |
| Any other key | Display next page of output. Certain terminal keys (arrows, Home, End, etc.) may appear as multiple characters to the ICLI, leading to multiple pages being output in quick succession. |

The terminal length (also sometimes called height) can be configured for the current session using the terminal length lines command. If lines = 0 is input, pagination is disabled.

```
my-device# terminal length 0 my-device# terminal length 25
```

The same is true for setting the terminal width in characters.

Other Special Keys

One additional key is defined as a convenience. It allows the immediate return from any sub-mode to Exec mode.

Table 5 - Special Keys

| Key | Operation |
|--------|------------------------------|
| Ctrl-Z | Return directly to Exec mode |

Filtering Output

The output from commands can be filtered in most cases. It is possible to limit the output to only those lines that match/trigger a specific substring. The available filtering is:

- » Begin - display the first line that matches and all subsequent lines
- » Include - display exactly those lines that match
- » Exclude - display exactly those lines that do not match

The string is case-sensitive.

The syntax is:

command 'l' { begin | include | exclude } string

! Execute a command that generates some output; no filtering initially: my-device# show users

Line is con 0.

You are at this line now.

Connection is from Console.

User name is admin.

Privilege is 15.

Elapsed time is 0 day 21 hour 52 min 50 sec.

Idle time is 0 day 0 hour 0 min 0 sec.

! Filter to include specific word:

my-device# show users | include User

User name is admin.

! Exclude all lines that contain '0' (zero)

my-device# show users | exclude 0

* You are at this line now.

Connection is from Console.

User name is admin.

Privilege is 15.

! Begin output when specific word is matched:

```
my-device# show users | begin Elapsed
```

Elapsed time is 0 day 21 hour 53 min 29 sec.

Idle time is 0 day 0 hour 0 min 0 sec.

Understanding Modes and Sub-Modes

The ICLI implements a number of modes that control the available command set. The modes are further influenced by the privilege level of the user; some modes or commands are only accessible to administrators while others require no privileges beyond login.

There are three major modes: Exec, Privileged Exec, and Config. Under Config, there exist a number of

sub-modes. The sub-modes allow configuration of specific VLANs, Ethernet interfaces, etc.

Table 6 - Modes

| Mode | Parent Mode | Description |
|-------------------------------|-------------|---|
| Exec | | Lowest-privileged mode; used for basic system monitoring. Generally does not allow modifications to the system Command: disable Prompt: hostname> |
| Privileged Exec | Exec | Privileged mode; allows configuration and other modifications to the system Command: enable Prompt: hostname# |
| Config | Priv.Exec | Global configuration mode Command: configure terminal Prompt: hostname(config)# |
| VLAN Config | Config | Sub-mode for configuring active VLANs Command: vlan vlan_id_list Prompt: hostname(config-vlan)# |
| VLAN Interface Config | Config | Sub-mode for configuring VLAN interfaces Command: interface vlan vlan_id_list Prompt: hostname(config-if-vlan)# |
| Interface Config | Config | Sub-mode for configuring Ethernet interfaces Command: interface type switch_num/port_num Prompt: hostname(config-if)# |
| Line | Config | Sub-mode for configuring terminal lines Command: line { con vty } line_num Prompt: hostname(config-line)# |
| IPMC Profile Config | Config | Sub-mode for configuring IP Multicast profiles Command: ipmc profile profile_name Prompt: hostname(config-ipmc-profile)# |
| SNMP Server Host Config | Config | Sub-mode for configuring SNMP server host entries Command: snmp-server host host_name Prompt: hostname(config-snmps-host)# |
| STP Aggregation Config | Config | Sub-mode for configuring Spanning Tree Protocol aggregation Command: spanning-tree aggregation Prompt: hostname(config-stp-aggr)# |
| DHCP Pool Config | Config | Sub-mode for configuring DHCP client pools Command: ip dhcp pool pool_name Prompt: hostname(config-dhcp-pool)# |
| RFC2544 Profile Config | Config | Sub-mode for configuring RFC2544 profiles Command: rfc2544 profile profile_name Prompt: hostname(config-rfc2544-profile)# |
| Y.1564 Config | Config | Sub-mode for configuring Y.1564 profiles Command: y1564 profile profile_name Prompt: hostname(config-y1564-profile)# |
| JSON Notification Host Config | Config | Sub-mode for configuring JSON notification hosts Command: json notification host host_name Prompt: hostname(config-json-notif-host)# |

It is possible for a user to transition between these modes using certain commands, subject to the user's privilege level and the current session privilege level (see Understanding Privilege Levels,

page 15).

The initial mode is determined by the privilege level of the user logging in. If the privilege level is zero or one the user is unprivileged and begins in the (Unprivileged) Exec mode. If the privilege level is higher, the session begins in Privileged Exec mode.

A user can raise the Exec mode privilege level to a higher value if an enable password has been configured for that level. This elevation is done with the enable level command, where level is a value between 1 and 15. The reverse operation (lowering the privilege level) is achieved with the disable command.

Once in Privileged Exec mode, it is possible to enter into the global configuration mode by entering the command configure terminal. Exit from global configuration is achieved by typing end or exit and then pressing Enter or pressing Ctrl-Z.

Access to a configuration sub-mode (for example, Ethernet interfaces) goes through global configuration or another sub-mode. Thus, it is possible to change directly from VLAN sub-mode to Ethernet interface sub-mode, for instance.

Thus, each mode and sub-mode implements a scope for commands. Inside each mode, a particular subset of commands is available. To get to other commands, one must generally change mode/sub-mode. This is necessary because there are commands with identical prefixes in different modes. For example, there are commands that begin with 'ip' in Privileged Exec, global configuration, and VLAN Interface Configuration modes.

There are two exceptions to this:

- » While in a configuration sub-mode, access to global configuration mode commands is possible as long as there is no ambiguity. Execution of a global configuration command exits the sub-mode.
- » Exec mode commands (whether privileged or unprivileged) are accessible from within global configuration or one of the sub-modes by using the do command.

The do command takes an arbitrary command line from Exec and executes it. In the following example, the user wants to change the IP address on the VLAN 1 interface and uses do to verify the current address while in the sub-mode.

Using 'do' While in a Sub-Mode

```
my-device# configure terminal
my-device(config)# interface vlan 1
my-device(config-if-vlan)# do show ip interface brief
Vlan Address      Method Status
1 192.168.10.15/24 DHCP UP
my-device(config-if-vlan)# end
```

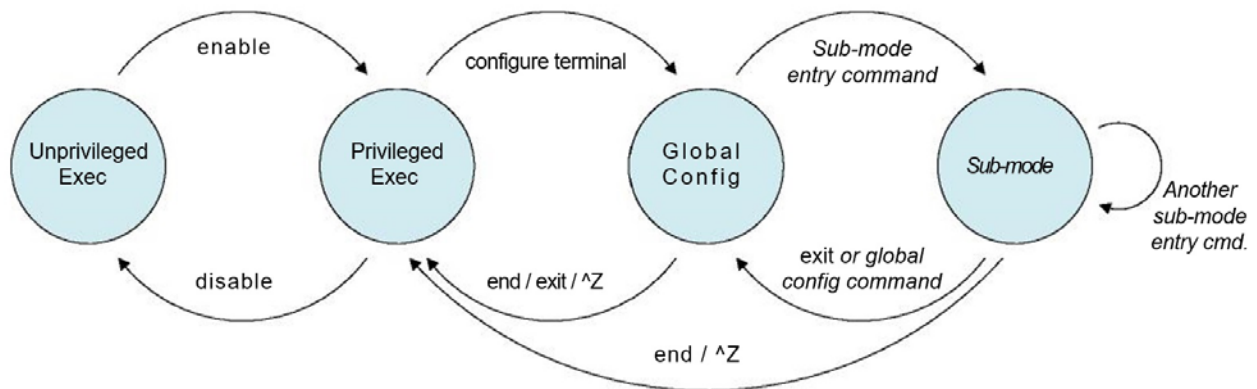
! When in Exec, no 'do' prefix is needed: my-device# show ip interface brief

```
Vlan Address      Method Status
1 192.168.10.15/24 DHCP UP
```

16.19 ICLI Mode Transitions

The following illustration shows the possible transitions between major modes and sub-modes, and some of the relevant commands.

Figure 1 - ICLI Mode Transitions



Changing Between ICLI Modes

! Initial mode for this example is Unprivileged Exec. Raise level

! (and change mode):

```
my-device> enable
```

```
Password: ***
```

```
my-device#
```

! Note how the prompt changed from '>' to '#' to indicate the privileged exec mode

! Enter global configuration mode: my-device# configure terminal

! Now create VLAN 100 and give it a name. This enters the VLAN sub-mode, as ! indicated by a new prompt: my-device(config)# vlan 100 my-device(config-vlan)# name MyVlan

! Change directly from VLAN sub-mode into Ethernet interface sub-mode for ! interface instance 4 on switch 1, and set link speed to 'auto' my-device(config-vlan)# interface GigabitEthernet 1/4

```
my-device(config-if)# speed auto
```

! Then enter a command from the global configuration mode; this leaves Ethernet ! interface sub-mode

```
my-device(config-if)# hostname my-device
```

! Exit global configuration mode and go back to Privileged Exec

```
my-device(config)# end
```

! And use 'disable' to go back to Unprivileged Exec:

```
my-device# disable
```

```
my-device>
```

Understanding Privilege Levels

A privilege level is a number in the range of 0 to 15, inclusive, with 0 being the lowest. It is assigned to a user session and used to determine access to ICLI commands. Only commands at the same or lower privilege level can be accessed.

Each user on the device has a default privilege level that is copied to the session's privilege level at login. It is, however, possible for the user to change the session privilege level by executing the enable or disable commands. This can be used, for example, as follows:

- » The user account is configured with privilege level 0
- » Whenever the user needs to perform higher-privileged commands, the user changes session priority level, executes the necessary commands, and then reverts back to the default priority level

Access to higher priority levels must be password protected by using the enable password or enable secret global configuration commands. The main difference between the two is whether passwords are displayed in clear text or encrypted form in running-config, and consequently, startup-config.

Password input can also be in encrypted or clear text form. The latter is used when an operator inputs a new password, as the operator will usually not know the encrypted form of the password.

The admin user is at level 15 by default, the highest possible privilege level.

Configuring Privilege Level Passwords

The following example configures a level 15 password using enable secret, inspects the resulting configuration, then removes it again.

```
my-device# configure terminal
```

! A secret can either be input in clear text or encrypted form; a digit indicates

! which kind follows on the command line:

```
my-device(config)# enable secret ?
```

0 Specifies an UNENCRYPTED password will follow

5 Specifies an ENCRYPTED secret will follow

! In this case: Unencrypted. Then follows either the level for which a password ! is being configured, or, if no level is given, the password for level 15: my-device(config)# enable secret 0 ?

```
<word32> Password
```

```
level Set exec level password
```

! Thus, the following two commands are semantically identical: my-device(config)# enable secret 0 my-secret

```
my-device(config)# enable secret 0 level 15 my-secret
```

! The running configuration can be inspected to see the encrypted form:

```
my-device(config)# do show running-config | include enable enable secret 5 level 15  
D29441BF847EA2DD5442EA9B1E40D4ED
```

! To remove the password use the 'no' form (the two are semantically equivalent for level 15):

```
my-device(config)# no enable secret
```

```
my-device(config)# no enable secret level 15
```

```
my-device(config)# do show running-config | include enable my-device(config)#
```

Understanding Terminal Parameters

Each system login, whether through the serial console or through telnet or ssh, creates a session. The session is initialized with settings that are configurable from the line configuration sub-mode, but most of them can also be changed from Exec mode while the session is active. Such changes are not persistent, however, and are lost when the session is terminated.

The following table lists available settings and modes where each can be configured. Table 7 • Setting and Modes

| Setting | Modes | Description |
|--------------|------------|---|
| editing | Exec, Line | Enable/disable command line scrolling |
| exec-banner | Line | Enable/disable display of the Exec banner (configured with 'banner exec ...') |
| exec-timeout | Exec, Line | Inactivity timer; automatically log out after a period of inactivity. A value of zero disables automatic logout |
| history | Exec, Line | Length of command history buffer |
| length | Exec, Line | Terminal length in lines, used for pagination. Zero disables pagination |
| location | Line | A line of text that describes the terminal location (such as "Server room") |
| motd-banner | Line | Enable/disable display of Message-Of-The-Day banner (configured with 'banner motd ...') |
| privilege | Line | Assign default privilege level |
| width | Exec, Line | Terminal width in characters, used for pagination |

The system allows one serial console session and up to 16 network sessions. The console session is called "console 0" whereas each network session is called "vty X" where vty is an abbreviation for Virtual TTY and X is a value between 0 and 15.

The configuration appears near the bottom of running-config and looks like this:

```
line console 0
exec-timeout 0
!
line vty 0
!
line vty 1
!
line vty 2
!
[...]

```

It is possible to specify different settings for each vty, but this is generally not recommended since

there is no way to associate an incoming ssh or telnet connection with a specific vty.

Changing Terminal Parameters

This example shows how to change some values for the current session, and for all future console sessions.

! First inspect current settings for this session:

```
my-device# show terminal
```

Line is con 0.

* You are at this line now.

Alive from Console.

Default privileged level is 2.

Command line editing is enabled

Display EXEC banner is enabled.

Display Day banner is enabled.

Terminal width is 80.

length is 24.

history size is 32.

exec-timeout is 10 min 0 second.

Current session privilege is 15.

Elapsed time is 0 day 0 hour 15 min 42 sec. Idle time is 0 day 0 hour 0 min 0 sec.

! Then set terminal length to zero to disable pagination, and exec-timeout to

! zero to disable automatic logout:

```
my-device# terminal length 0
```

```
my-device# terminal exec-timeout 0
```

```
my-device# show terminal
```

Line is con 0.

* You are at this line now.

Alive from Console.

Default privileged level is 2.

Command line editing is enabled

Display EXEC banner is enabled.

Display Day banner is enabled.

Terminal width is 80.

length is 0.

history size is 32.

exec-timeout is 0 min 0 second.

Current session privilege is 15.

Elapsed time is 0 day 0 hour 16 min 31 sec. Idle time is 0 day 0 hour 0 min 0 sec.

! Then we do the same, but for all future console sessions. Note how the commands

! have no 'terminal' prefix ('terminal length' vs. 'length'):

```
my-device# configure terminal
```

```
my-device(config)# line console 0
```

```
my-device(config-line)# exec-timeout 0
```

```
my-device(config-line)# length 0
```

```
my-device(config-line)# end
```

! Finally save the configuration to startup-config to make it persistent:

```
my-device# copy running-config startup-config
```

```
Building configuration...
```

```
% Saving 1287 bytes to flash:startup-config
```

```
My-device#
```


Using Banners

The system provides three different banners (text that is output as messages to the user):

- » The Message Of The Day banner (MOTD), displayed upon connection to the system or when a console login attempt has timed out
- » The Login banner, displayed before the first "Username:" login prompt
- » The Exec banner, displayed upon successful login

All of these banners are configured in a similar manner, using the banner command:

```
banner [ motd ] banner banner exec banner banner login banner
```

The banner text can be either a single line or multiple lines. The first character of the text defines a delimiter character; the actual text of the banner then follows and ends at the first appearance of the delimiter character. The delimiters are not included in the actual text.

Configuring Banners

! First configure the MOTD banner, which in this case is multi-line. '*' is

! used as delimiter character, but any printable character that isn't used in

! the message is usable:

```
my-device# configure terminal
```

```
my-device(config)# banner motd *This is the Message Of The Day Banner.
```

Enter TEXT message. End with the character '*'.

It spans multiple lines.

And one more. But now it ends.*

! Then the Login and Exec banners. Both are single-line. Note how different ! delimiters are used in each banner:

```
my-device(config)# banner login XThis is my-device.X
```

```
my-device(config)# banner exec "WARNING: Production system. Be careful." my-device(config)#
end
```

! Inspect configuration:

```
my-device# show running-config
```

Building configuration...

```
banner motd "This is the Message Of The Day Banner.
```

It spans multiple lines.

And one more. But now it ends.”

```
banner exec "WARNING: Production system. Be careful."
```

```
banner login "This is my-device."
```

```
hostname my-device
```

```
!      [...]
```

```
end
```

```
! Test it: Log out, then log in again: my-device# exit
```

This is the Message Of The Day Banner. It spans multiple lines.

And one more. But now it ends.

```
Press ENTER to get started<ENTER> This is my-device.
```

```
Username: admin
```

```
Password: admin
```

```
WARNING: Production system. Be careful. my-device#
```

```
! Finally save the configuration to startup-config to make it persistent:
```

```
my-device# copy running-config startup-config
```

```
Building configuration...
```

```
% Saving 1461 bytes to flash:startup-config
```

```
my-device#
```

Configuring the System

Changes to system configuration can only be made from the global configuration mode and its sub-modes, except when working with configuration files or reloading defaults. This is done in Privileged Exec mode. The following steps outline the sequence.

1. Raise privilege level to 15.
2. Enter global configuration mode.
3. Input appropriate configuration commands. Optionally, enter sub-modes and input appropriate commands there.
4. Exit global configuration mode.
5. Verify configuration.
6. Save configuration to flash.

Configuration Example

In this example, the hostname and VLAN 1 IP address is configured, verified, and saved. This example assumes the session is initially unprivileged.

1. Raise privilege level: > enable

Password: ***

2. Enter global configuration mode: # configure terminal

3. Input configuration commands. The IP address is set from within the

! VLAN interface submode:

```
(config)# hostname my-device
```

```
my-device(config)# interface vlan 1
```

```
my-device(config-if-vlan)# ip address dhcp fallback 192.168.10.2 255.255.0.0
```

```
my-device(config-if-vlan)# exit
```

4. Leave global configuration mode and go back to Privileged Exec: my-device(config)# end

5. Inspect and verify the configuration (some output omitted for brevity):

```
my-device# show running-config
```

```
Building configuration...
```

```
hostname my-device
```

```
username admin privilege 15 password encrypted
```

```
3ad61dc090116a16a7cc9861485e60e6407c5a328015b1985b585ab353c37a4441e034172401
528229795a5c9529dfbc04c86e01
```

```
!
```

```
vlan 1
```

```
name default
```

```
!
```

```
interface GigabitEthernet 1/1
```

```
!
```

```
interface GigabitEthernet 1/2
```

```
!
```

```
...
```

```
interface vlan 1
```

```
ip address dhcp fallback 192.168.10.2 255.255.0.0
```

```
!
```

```
... end ! More verification: Display IP interfaces and assigned IP address and status: my-device#
show ip interface brief
```

```
Vlan Address      Method Status
```

```
1 192.168.10.15/24 DHCP UP
```

```
! An address was obtained from DHCP, so the fallback wasn't used
```

```
! Try to inspect hostname:
```

```
my-device# show hostname
```

```
^
```

```
% Invalid word detected at '^' marker.
```

```
! No such command exists, but it is possible to extract a single line from
```

```
! running-config by using a filter:
```

```
my-device# show running-config | include hostname
```

```
hostname my-device
```

```
6. Save configuration to flash:
```

```
my-device# copy running-config startup-config Building configuration...
```

```
% Saving 1272 bytes to flash:startup-config
```

Resetting or Removing Configuration with “no”

It is possible to remove specific configuration items or reset them to their default values. In general, almost each configuration command has a corresponding no form. The ‘no’ form is syntactically similar (but not necessarily identical) to the configuration command, but either resets the parameters to defaults for the configurable item being addressed or removes the item altogether.

In many cases, “no” can be read as no(t) different from default settings.

Using “no” Forms

The following list shows the tasks accomplished:

- » Configure the VLAN 1 interface IP address to use DHCP
- » Configure the DNS name server to be taken from DHCP
- » Inspect the configuration
- » Remove the DNS name server
- » Remove the IP address on the VLAN 1 interface

Both “no” operations can be viewed as reset-to-default, with the defaults being no DNS name server and no IP address.

```
my-device# configure terminal
```

```
my-device(config)# interface vlan 1
```

```
my-device(config-if-vlan)# ip address dhcp my-device(config-if-vlan)# exit
```

```
my-device(config)# ip name-server dhcp my-device(config)# end
```

```
my-device# show ip interface brief
```

```
Vlan Address      Method Status
```

```
1 192.168.10.15/24 DHCP UP
```

```
my-device# show ip name-server
```

```
Current DNS server is 192.168.10.1 set by DHCP. my-device# configure terminal my-device(config)#  
no ip name-server my-device(config)# interface vlan 1 my-device(config-if-vlan)# no ip address\  
my-device(config-if-vlan)# end
```

```
device# show ip name-server Current DNS server is not set.
```

```
my-device# show ip interface brief
```

Vlan Address Method Status

my-device#

Note: The syntax of the configuration commands and their 'no' forms are different; the 'no' forms usually do not take as many parameters.

This is usually convenient but may give surprising results in certain cases. For example, an OAM MEP instance can configure Continuity Check using 'mep num cc priority ...' and reset it with 'no mep num cc'. However, because MEPs are removed using the command 'no mep num', it is possible to unintentionally remove an existing MEP by entering 'no mep 10 ccc' - the extra 'c' means that the last word isn't recognized as 'cc', leading to a match of the MEP removal command instead of the desired reset-CC command.

Managing Users

The following describes local user management on the device. RADIUS and TACACS+ user management is beyond the scope of this document.

It is possible to create several user accounts on a system. Each user account has a set of configurable attributes:

- » User name
- » Password
- » Privilege level

All attributes are configured with the same command, `username`.

```
username username privilege level password { unencrypted | encrypted } password username
username privilege level password none
```

```
no username username
```

The command `password none` is used when no password is desired. The security implications of using this should be considered carefully. Likewise, `no username` deletes the given user account.

Adding, Modifying, and Deletion Users

The following example adds two user accounts at different privilege levels, inspects configuration, and deletes one account again using 'no username'.

```
! Display current set of local user accounts: my-device# show running-
config | include username username admin privilege 15 password encrypted
3ad61dc090116a16a7cc9861485e60e6407c5a328015b1985b585ab353c37a4441e034172401
528229795a5c9529dfbc04c86e01
```

! Add two accounts, 'operator' and 'monitor'. The passwords are supplied in ! unencrypted form:

```
my-device# configure terminal
```

```
my-device(config)# username operator privilege 10 password unencrypted a-secret
```

```
my-device(config)# username monitor privilege 1 password unencrypted new-secret
```

! Verify that the configuration is correct. Note that passwords are displayed ! in encrypted form:

```
my-device(config)# do show running-config | include username
```

```
username admin privilege 15 password encrypted
```

```
3ad61dc090116a16a7cc9861485e60e6407c5a328015b1985b585ab353c37a4441e034172401  
528229795a5c9529dfbc04c86e01aaaaaaaaaaaaaaaa
```

```
Username operator privilege 10 password encrypted
```

```
015b1985b585ab353c37a4441e034172401528229795a5c9529dfbc04c86e012138abcd88dda  
222affea861485e60e6407c5a328
```

```
username monitor privilege 1 password encrypted
```

```
7cc9861485e60e6407c56a16a7cc9861485e60e6407c5a328441e034172401528229795a5c95  
229795a5c9529dfbc04c86e01abc
```

! Delete the 'operator' user and verify it is removed from the configuration: my-device(config)# no username operator

```
my-device(config)# do show running-config | include username
```

```
username admin privilege 15 password encrypted
```

```
ad61dc090116a16a7cc9861485e60e6407c5a328015b1985b585ab353c37a4441e0341724015  
28229795a5c9529dfbc04c86e01
```

```
username monitor privilege 1 password encrypted
```

```
7cc9861485e60e6407c56a16a7cc9861485e60e6407c5a328441e034172401528229795a5c95  
229795a5c9529dfbc04c86e01abc
```

Using Show Commands

The family of show commands is the cornerstone of ICLI-based system monitoring. Most features implement one or more show commands that will display a relevant mix of status and configuration.

Note: The exact set of available commands, parameters, and output format depends on the system configuration and software version, so some of the following commands and examples may not be applicable to all systems.

The show commands exist only in the two Exec modes and are subject to session privilege level enforcement. Therefore, listing the largest possible set of show commands requires the session to be at level 15.

Listing All Show Commands

The following example raises the session privilege level to 15. In this example, an enable secret has been specified, so password entry is required to proceed. Then the user inputs show and uses the context-sensitive help feature to list the possible show commands, in this case for a Carrier Ethernet system.

```
my-device> enable Password: ***
```

```
my-device# show ?
```

```
aaa    Login methods
```

```
access      Access management
```

```
access-list  Access list
```

```
aggregation Aggregation port configuration
```

```
clock       Configure time-of-day clock
```

```
dot1x       IEEE Standard for port-based Network Access Control
```

```
eps         Ethernet Protection Switching
```

```
erps        Ethernet Ring Protection Switching
```

```
evc         Ethernet Virtual Connections
```

```
green-ethernet  Green ethernet (Power reduction)
```

```
history      Display the session command history
```

```
interface    Interface status and configuration
```

```
ip           Internet Protocol
```

```
ipmc         IPv4/IPv6 multicast configuration
```

```
ipv6         IPv6 configuration commands
```

```
lacp         LACP configuration/status
```

```
line         TTY line information
```

```
link-oam     Link OAM configuration
```

```
lldp         Display LLDP neighbors information.
```

```
logging      Syslog
```

```
loop-protect Loop protection configuration
```

```
mac          Mac Address Table information
```


mep Maintenance Entity Point

mvr Multicast VLAN Registration configuration

network-clock Show selector state.

ntp Configure NTP

perf-mon Performance Monitor

platform Platform specific information

port-security Port security

privilege Display command privilege

ptp Precision time Protocol (1588)

pvlan PVLAN configuration

qos Quality of Service

radius-server RADIUS configuration

rfc2544 RFC2544 performance tests

rmon RMON statistics

running-config Show running system information

sflow Statistics flow.

snmp Display SNMP configurations

spanning-tree STP Bridge

switchport Display switching mode characteristics

tacacs-server TACACS+ configuration

terminal Display terminal configuration parameters

thermal-protect Display thermal protection status.

upnp Display UPnP configurations

users Display information about terminal lines

version System hardware and software status

vlan VLAN status

voice Voice appliance attributes

web Web

Using Context-sensitive Help for Discovery

The context-sensitive help feature for syntax display is also useful for determining the exact command to execute. In the following example, the user discovers the proper command `show ip statistics system` through exploration:

```
my-device# show ip ?
```

```
arp    Address Resolution Protocol
```

```
dhcp   Dynamic Host Configuration Protocol
```

```
http   Hypertext Transfer Protocol
```

```
igmp   Internet Group Management Protocol
```

```
interface    IP interface status and configuration
```

```
name-server  Domain Name System
```

```
route        Display the current ip routing table
```

```
source       source command
```

```
ssh          Secure Shell
```

```
statistics   Traffic statistics
```

```
verify       verify command
```

```
my-device# show ip statistics ?
```

```
|          Output modifiers
```

```
icmp        IPv4 ICMP traffic
```

```
icmp-msg    IPv4 ICMP traffic for designated message type
```

```
interface    Select an interface to configure
```

```
system       IPv4 system traffic
```

```
<cr>
```

! A repeated press of '?' displays the syntax:

```
my-device# show ip statistics ?
```

```
show ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ]
```

```
[ icmp-msg <type> ]
```

```
my-device# show ip statistics system IPv4 statistics:
```

```
Rcvd: 2768 total in 181458 bytes
```

1727 local destination, 0 forwarding
0 header error, 0 address error, 0 unknown protocol
0 no route, 0 truncated, 0 discarded
Sent: 2553 total in 180047 bytes
1512 generated, 0 forwarded
0 no route, 0 discarded
Frag: 0 reassemble (0 reassembled, 0 couldn't reassemble)
0 fragment (0 fragmented, 0 couldn't fragment)
0 fragment created
Mcast: 0 received in 0 byte
0 sent in 0 byte
Bcast: 0 received, 0 sent

Show running-config

The virtual file running-config consists of a list of commands that, taken together, result in the currently running system configuration.

This list of commands is usually not 100% identical to the list of commands a user has input to configure the device. That is because running-config is a textual representation of the system configuration that is stored in binary form in the RAM memory of the device.

Because the effective device configuration is huge, running-config in the majority of cases only lists the delta between default settings and current settings. This significantly reduces the amount of output and greatly improves readability of the configuration, but it does require the reader to know what the default settings are.

With show running-config all-defaults, it is possible to include values that are at default.

Default vs. Non-default vs. All Defaults

In this example, if the speed and duplex settings of an Ethernet interface are at default values (auto-negotiation), then nothing will be output. If the user then changes the speed to be fixed at 1 Gbps, then that value is now non-default and will be output. Duplex is also output because it is forced to 'full' when the speed is fixed at 1 Gbps.

! Display current configuration for an interface. All settings are at default:

```
my-device# show running-config interface GigabitEthernet 1/4
```

```
Building configuration...
```

```
interface GigabitEthernet 1/4
```

```
!
```

```
end
```

! Now set the speed to 1Gbps and display the configuration again: my-device# configure terminal

```
my-device(config)# interface GigabitEthernet 1/4
```

```
my-device(config-if)# speed 1000
```

```
my-device(config-if)# end
```

```
my-device# show running-config interface GigabitEthernet 1/4
```

```
Building configuration...
```

```
interface GigabitEthernet 1/4
```

```
speed 1000
```

```
duplex full
```

```
!
```

```
end
```

! Include all default settings for that interface:

```
my-device# show running-config interface GigabitEthernet 1/4 all-defaults
```

```
Building configuration...
```

```
interface GigabitEthernet 1/4
```

```
switchport voice vlan mode disable
```

```
no switchport voice vlan security
```

```
switchport voice vlan discovery-protocol oui
```

```
loop-protect
```

```
no loop-protect action
```

```
loop-protect tx-mode
```

```
switchport access vlan 1
```

```
switchport trunk native vlan 1
```

```
switchport hybrid native vlan 1
```

! ... much output omitted for brevity ...

The output of show running-config can be restricted to a specific interface. There are several such filters, described below.

Show running-config [all-defaults]

This displays the entire currently-running system configuration.

Show running-config feature feature_name [all-defaults]

Only output the commands relevant to a particular feature. The feature list depends on system configuration and software version. For example:

```
my-device# show running-config feature ?
```

```
CWORD      Valid words are 'GVRP' 'access' 'access-list' 'aggregation'
```

```
'arp-inspection' 'auth' 'clock' 'dhcp' 'dhcp-snooping' 'dhcp_server' 'dns' 'dot1x' 'eps' 'erps' 'evc'
'green-ethernet' 'http' 'icli' 'ip-igmp-snooping' 'ip-igmp-snooping-port'
```

```
'ip-igmp-snooping-vlan' 'ipmc-profile' 'ipmc-profile-range' 'ipv4' 'ipv6' 'ipv6-mld-snooping' 'ipv6-
mld-snooping-port' 'ipv6-mld-snooping-vlan' 'lACP' 'link-oam' 'lldp' 'logging' 'loop-protect' 'mac'
'mep' 'monitor' 'mstp' 'mvr' 'mvr-port' 'network-clock' 'ntp' 'perf-mon' 'phy' 'port' 'port-security'
'ptp' 'pvlan' 'qos' 'rfc2544' 'rmon' 'snmp' 'source-guard' 'ssh' 'thermal-protect' 'upnp' 'user' 'vlan'
'voice-vlan' 'web-privilege-group-level'
```

```
my-device# show running-config feature dns
```

```
Building configuration...
```

```
!
```

```
vlan 1
```

```
!
```

```
!
```

```
!
```

```
ip dns proxy
```

```
!
```

```
interface GigabitEthernet 1/1 ...
```

The structure of running-config is maintained in the output. Sub-modes such as VLANs and Ethernet interfaces are listed, but may be empty if the requested feature is irrelevant for the particular sub-mode.

Show running-config interface list [all-defaults]

By using this filter, the user can review a specific list of Ethernet interfaces. This may contain wildcards, for example:

```
My-device# show running-config interface 2.5GigabitEthernet *
Building configuration...
interface 2.5GigabitEthernet 1/1
speed 1000
duplex full
!
interface 2.5GigabitEthernet 1/2
!
end
```

In this example, there is only one VLAN on the system.

16.40 Show running-config interface vlan list [all-defaults]

It is also possible to filter the list of VLAN interface, for example:

```
my-device# show running-config interface vlan 1-10
Building configuration...
interface vlan 1
ip address dhcp fallback 192.168.10.2 255.255.0.0
!
end
```

In this example, there is only one VLAN interface on the system.

Working with Configuration Files

There are four kinds of configuration files:

- » running-config - a virtual file containing the currently running system configuration.
- » startup-config - contains the boot-time configuration. When configuration is changed, it must be copied to startup-config in order to be applied at the next boot.
- » default-config - a read-only file used when configuration is restored to defaults. This file is also used if startup-config is missing. It contains product-specific customizations to the default settings of the device.
- » User-defined - configuration files created by the user (up to 31). These are typically used for backups or variants of startup-config.

All of these except running-config are stored in the flash file system. The available operations are:
copy source destination

where source and destination can be one of:

- » running-config
- » startup-config (or flash:startup-config)
- » flash:filename
- » tftp://server[:port]/path-to-file

dir

List the contents of the flash file system. more flash: filename

Outputs the contents of the file to the terminal.

flash: filename

Erases the specific file.

Reverting to Default Configuration

It is possible to reset the system to a default configuration in two ways:

- » Deleting startup-config and rebooting
- » Instructing the software to discard the current configuration and reset to defaults without rebooting

Deleting startup-config doesn't change running-config until the system is rebooted, at which time the defaults are loaded.

Conversely, discarding the current configuration does indeed affect running-config but does not touch startup-config. An explicit copy running-config startup-config is necessary to make the change persistent.

Rebooting and resetting the default configuration is accomplished with the reload command:

```
reload cold [ sid switch_id | reload defaults [ keep-ip |
```

The reload cold version reboots the system. If the system is stacking, a specific switch can be rebooted as well by supplying its switch ID.

The second method loads configuration defaults. If the keep-ip keyword is given, then the system attempts to keep the most relevant parts of the VLAN 1 IP setup in order to maintain management connectivity (the IP address setup and the active default route).

There is no guarantee, however, that the above is sufficient for reverting to default configuration: it depends on the actual network properties and the system's total IP configuration. In some cases, it may be preferable to explicitly un-configure the system using 'no' commands, or prepare a suitable configuration and download it to the system's startup-config and reboot.

Working with Configuration Files

The following example assumes a file system that contains an additional file called backup, previously created with a copy command.

! List files in flash: my-device# dir

Directory of flash:

```
r-    1970-01-01  00:00:00    648  default-config
rw    1970-01-06  03:57:33    1313  startup-config
rw    1970-01-01  19:54:01    1237  backup
```

3 files, 3198 bytes total.

! Display the contents of the file 'backup' (output is abbreviated):

```
my-device# more flash:backup
```

```
hostname my-device
```

```
...
```

```
end
```

! Use file 'backup' for the next boot by overwriting startup-config:

```
my-device# copy flash:backup startup-config
```

```
% Saving 1237 bytes to flash:startup-config
```

! Verify that the sizes are identical: my-device# dir

Directory of flash:

```
r-    1970-01-01  00:00:00    648  default-config
rw    1970-01-06  05:30:41    1237  startup-config
rw    1970-01-01  19:54:01    1237  backup
```

3 files, 3122 bytes total.

! Regret and delete startup-config. Note how 'flash:' is required: my-device# delete flash:startup-config

```
my-device# dir
```

Directory of flash:

```
r- 1970-01-01 00:00:00    648 default-config
```

rw 1970-01-01 19:54:01 1237 backup

2 files, 1885 bytes total.

! Use the currently running config for next boot: my-device# copy running-config startup-config
Building configuration...

% Saving 1271 bytes to flash:startup-config

Using Reload Commands

! Reload defaults, but try to keep VLAN 1 configuration. First list current IP ! settings:

```
my-device# show ip interface brief
```

```
Vlan Address      Method Status
```

```
1 192.168.10.17/24 DHCP UP
```

```
my-device# reload defaults keep-ip
```

```
% Reloading defaults, attempting to keep VLAN 1 IP address. Please stand by. # show ip interface brief
```

```
Vlan Address      Method Status
```

```
1 192.168.10.17/24 DHCP UP
```

```
! Contents of flash: are unchanged: my-device# dir
```

```
Directory of flash:
```

```
r- 1970-01-01 00:00:00    648 default-config
```

```
rw 1970-01-06 05:33:18  1237 startup-config
```

```
rw 1970-01-01 19:54:01  1237 backup
```

```
3 files, 3122 bytes total.
```

```
! Reload again, but don't try to keep VLAN 1 settings:
```

```
# reload defaults
```

```
% Reloading defaults. Please stand by.
```

```
! Verify that the default IP settings have been restored:
```

```
# show ip interface brief
```

```
Vlan Address      Method Status
```

```
1 192.0.2.1/24      Manual    UP
```

```
! Reboot the system
```

```
# reload cold
```

```
% Cold reload in progress, please stand by. ! ... bootup output omitted ...
```

Working with Software Images

The system can store up to two software images in flash. The image selected for bootup is termed the Active image, while the other is termed the Alternate image.

It is possible to swap the Active and the Alternative image, and it is possible to upgrade to a new Active image. A swap simply switches the Active and Alternate designation on each image and reboots the system.

A firmware upgrade performs these steps:

- » Download new firmware using TFTP/HTTP/HTTPS/FTP and verify suitability for the system
- » Overwrite the current Alternate image with the newly downloaded image
- » Swap Active and Alternate and reboot

The result is that the old Active build becomes the Alternate, and the newly downloaded image Active. The relevant commands are:

```
show version
```

```
firmware swap
```

```
firmware upgrade protocol tftp://server[:port]/path_to_file
```

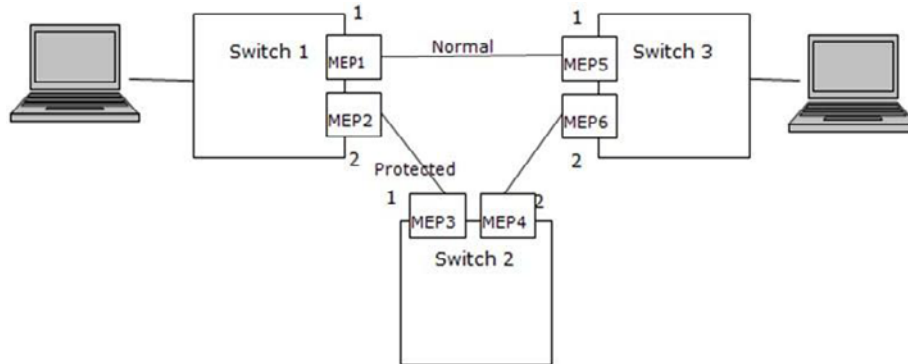
show version lists various details about the system, including the images in flash.

Appendix A

Ethernet Ring Protection Switching Example Configuration

Introduction

This section shows how to configure the Ethernet Ring Protection Switching (ERPS) for ComNet switches using the Web GUI and the CLI commands. The following figure shows a simple three switch network constructed to demonstrate these features.



Ethernet Ring Protection Switching (ERPS) Model

Configuring ERPS from the Web GUI

Initial Switch Configuration

Use the following steps to configure the ERPS features through the Web.

1. Set the proper static IP for each switch. In this example, switch 1 is 192.168.10.1, switch 2 is 192.168.10.2 and switch 3 is 192.168.10.3.
2. Connect switch 1 to switch 2 and switch 1 to switch3. Do not connect switch 2 to switch 3 to avoid creating a loop. The web client is connected to switch 1.
3. To avoid conflict with ERPS disable spanning tree on all switches if it is enabled.
4. Enable VLAN tag aware on all three switches. In VLAN configuration page, set port mode to Hybrid port and port type to C-Port on port 1 and port 2 for each of the three switches, as screen shot below.

Global VLAN Configuration

| | |
|------------------------------|------|
| Allowed Access VLANs | 1 |
| Ethertype for Custom S-ports | 88A8 |

Port VLAN Configuration

| Port | Mode | Port VLAN | Port Type | Ingress Filtering | Ingress Acceptance | Egress Tagging | Allowed VLANs | Forbidden VLANs |
|------|--------|-----------|-----------|-------------------------------------|---------------------|-----------------|---------------|-----------------|
| 1 | Hybrid | 1 | C-Port | <input type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 1-4095 | |
| 2 | Hybrid | 1 | C-Port | <input type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 1-4095 | |
| 3 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 4 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 5 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 6 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 7 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 8 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 9 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 10 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 11 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |

Apply Reset

Figure 1 - Switch 1, 2, & 3 VLAN Configuration

Creating a MEP on Switch 1

1. On switch 1, add a new MEP on port 1 and 2 by clicking MEP. Configure the MEP as shown, and click Add New MEP.

Maintenance Entity Point

| Delete | Instance | Domain | Mode | Direction | Residence Port | Level | Flow Instance | Tagged VID | This MAC | Alarm |
|--------------------------|----------|--------|------|-----------|----------------|-------|---------------|------------|-------------------|--------------------------------------|
| <input type="checkbox"/> | 1 | Port | Mep | Down | 1 | 0 | | 3001 | 00-22-3B-02-1B-25 | ● |
| <input type="checkbox"/> | 2 | Port | Mep | Down | 2 | 0 | | 3001 | 00-22-3B-02-1B-26 | ● |

Add New MEP Save Reset Refresh

Figure 2 - Switch 1 Port 1 and 2 MEP Configuration

2. Edit MEP1 by clicking 1 under Instance of the MEP table. Configure the page as shown, and click Save or Apply.

MEP Configuration Refresh

Instance Data

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|----------|--------|------|-----------|----------------|---------------|------------|--------------|-------------------|
| 1 | Port | MEP | Down | 1 | | 3001 | 1 | 00-22-38-02-10-25 |

Instance Configuration

| Level | Format | Domain Name | MEG id | MEP id | Tagged VID | Syslog | cLevel | cMEG | cMEP | cAIS | cLCK | cLoop | cConfig | cSSF | aBLK | aTSF |
|-------|---------|-------------|---------------|--------|------------|--------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 10 | ITU ICC | | ICC000MEG0000 | 1 | 3001 | | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Peer MEP Configuration

| Delete | Peer MEP ID | Unicast Peer MAC | cLOC | cRDI | cPeriod | cPriority |
|--------------------------|-------------|-------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> | 5 | 00-22-38-02-36-55 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Add New Peer MEP

Functional Configuration

| Continuity Check | | | | APS Protocol | | | | |
|-------------------------------------|----------|------------|--------------------------|-------------------------------------|----------|-------|-------|------------|
| Enable | Priority | Frame rate | TLV | Enable | Priority | Cast | Type | Last Octet |
| <input checked="" type="checkbox"/> | 0 | 300 fsec | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0 | Multi | R-APS | 1 |

Fault Management Performance Monitoring

TLV Configuration

| Organization Specific TLV (Global) | | | | |
|------------------------------------|------------|-----------|----------|-------|
| OUI First | OUI Second | OUI Third | Sub-Type | Value |
| 0 | 0 | 12 | 1 | 2 |

TLV Status

Figure 3 - Switch 1 MEP 1 Configuration

The Unicast Peer MAC can remain empty because it will be learned by receiving the CCM from the peer side. On ComNet switches, before they are learned, the CCM frame rate cannot be changed to above 100/sec. If known, enter the peer MAC address manually.

3. Edit MEP2 by clicking 2 under Instance of the MEP table. Configure the MEP as shown, and click Save or Apply.

MEP Configuration Refresh

Instance Data

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|----------|--------|------|-----------|----------------|---------------|------------|--------------|-------------------|
| 2 | Port | MEP | Down | 2 | | 3001 | 1 | 00-22-38-02-16-20 |

Instance Configuration

| Level | Format | Domain Name | MEG id | MEP id | Tagged VID | Syslog | cLevel | cMEG | cMEP | cAIS | cLCK | cLoop | cConfig | cSSF | aBLK | aTSF |
|-------|---------|-------------|---------------|--------|------------|--------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 10 | ITU ICC | | ICC000MEG0000 | 2 | 3001 | | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Peer MEP Configuration

| Delete | Peer MEP ID | Unicast Peer MAC | cLOC | cRDI | cPeriod | cPriority |
|--------------------------|-------------|-------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> | 3 | 00-22-38-02-36-49 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Add New Peer MEP

Functional Configuration

| Continuity Check | | | | APS Protocol | | | | |
|-------------------------------------|----------|------------|--------------------------|-------------------------------------|----------|-------|-------|------------|
| Enable | Priority | Frame rate | TLV | Enable | Priority | Cast | Type | Last Octet |
| <input checked="" type="checkbox"/> | 0 | 300 fsec | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0 | Multi | R-APS | 1 |

Fault Management Performance Monitoring

TLV Configuration

| Organization Specific TLV (Global) | | | | |
|------------------------------------|------------|-----------|----------|-------|
| OUI First | OUI Second | OUI Third | Sub-Type | Value |
| 0 | 0 | 12 | 1 | 2 |

TLV Status

| Peer MEP ID | CC Organization Specific | | | | | CC Port Status | | CC Interface Status | | |
|-------------|--------------------------|------------|-----------|----------|-------|-------------------------------------|-------|-------------------------------------|-------|-------------------------------------|
| | OUI First | OUI Second | OUI Third | Sub-Type | Value | Last RX | Value | Last RX | Value | Last RX |
| 3 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> | 0 | <input checked="" type="checkbox"/> | 0 | <input checked="" type="checkbox"/> |

Link State Tracking

Enable

Save Reset

Figure 4 - Switch 1 MEP 2 Configuration

Configuring Switch 2

1. Add a new MEP on port 1 and 2 of switch 2.

Maintenance Entity Point Refresh

| Delete | Instance | Domain | Mode | Direction | Residence Port | Level | Flow Instance | Tagged VID | This MAC | Alarm |
|--------------------------|----------|--------|------|-----------|----------------|-------|---------------|------------|-------------------|--------------------------------------|
| <input type="checkbox"/> | 1 | Port | Mep | Down | 1 | 0 | | 3001 | 00-22-3B-02-36-49 | ● |
| <input type="checkbox"/> | 2 | Port | Mep | Down | 2 | 0 | | 3001 | 00-22-3B-02-36-4A | ● |

Add New MEP Save Reset

Figure 5 - Switch 2 Port 1 and 2 MEP Configuration

2. Edit MEP1 of switch 2 by clicking 1 under Instance of the MEP table. Configure the MEP as shown, and click Save or Apply.

MEP Configuration Refresh

Instance Data

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|----------|--------|------|-----------|----------------|---------------|------------|--------------|-------------------|
| 1 | Port | Mep | Down | 1 | | 3001 | 1 | 00-22-3B-02-36-49 |

Instance Configuration

| Level | Format | Domain Name | MEG id | MEP id | Tagged VID | Syslog | cLevel | cMEG | cMEP | cAIS | cLCK | cLoop | cConfig | cSSF | aBLK | aTSF |
|-------|---------|-------------|---------------|--------|------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 0 | ITU ICC | | ICC000ME00000 | 3 | 3001 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Peer MEP Configuration

| Delete | Peer MEP ID | Unicast Peer MAC | cLOC | cRDI | cPeriod | cPriority |
|--------------------------|-------------|-------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> | 2 | 00-22-3B-02-1B-20 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Add New Peer MEP

Functional Configuration

| Continuity Check | | | | APS Protocol | | | | |
|-------------------------------------|----------|------------|--------------------------|-------------------------------------|----------|-------|-------|------------|
| Enable | Priority | Frame rate | TLV | Enable | Priority | Cast | Type | Last Octet |
| <input checked="" type="checkbox"/> | 0 | 300 Sec | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0 | Multi | R-APS | 1 |

Fault Management Performance Monitoring

TLV Configuration

| Organization Specific TLV (Global) | | | | | |
|------------------------------------|------------|-----------|----------|-------|--|
| OUI First | OUI Second | OUI Third | Sub-Type | Value | |
| 0 | 0 | 12 | 1 | 2 | |

TLV Status

| Peer MEP ID | CC Organization Specific | | | | | CC Port Status | | CC Interface Status | |
|-------------|--------------------------|------------|-----------|----------|-------|------------------------------------|-------|------------------------------------|--|
| | OUI First | OUI Second | OUI Third | Sub-Type | Value | Last RX | Value | Last RX | |
| 2 | 0 | 0 | 0 | 0 | 0 | ● | 0 | ● | |

Link State Tracking

Enable

Save Reset

Figure 6 - Switch 2 MEP 1 Configuration

3. Edit MEP2 of switch 2 by clicking 2 under Instance of the MEP table. Configure the MEP as shown, and click Save or Apply.

MEP Configuration Refresh

Instance Data

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|----------|--------|------|-----------|----------------|---------------|------------|--------------|-------------------|
| 2 | Port | Mep | Down | 2 | | 3001 | 1 | 00-22-3B-02-36-4A |

Instance Configuration

| Level | Format | Domain Name | MEG id | MEP id | Tagged VID | Syslog | cLevel | cMEG | cMEP | cAIS | cLCK | cLoop | cConfig | cSSF | aBLK | aTSF |
|-------|---------|-------------|---------------|--------|------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 0 | ITU ICC | | ICC000ME00000 | 4 | 3001 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Peer MEP Configuration

| Delete | Peer MEP ID | Unicast Peer MAC | cLOC | cRDI | cPeriod | cPriority |
|--------------------------|-------------|-------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> | 6 | 00-22-3B-02-36-56 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Add New Peer MEP

Functional Configuration

| Continuity Check | | | | APS Protocol | | | | |
|-------------------------------------|----------|------------|--------------------------|-------------------------------------|----------|-------|-------|------------|
| Enable | Priority | Frame rate | TLV | Enable | Priority | Cast | Type | Last Octet |
| <input checked="" type="checkbox"/> | 0 | 1 Sec | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0 | Multi | R-APS | 1 |

Fault Management Performance Monitoring

TLV Configuration

| Organization Specific TLV (Global) | | | | | |
|------------------------------------|------------|-----------|----------|-------|--|
| OUI First | OUI Second | OUI Third | Sub-Type | Value | |
| 0 | 0 | 12 | 1 | 2 | |

TLV Status

| Peer MEP ID | CC Organization Specific | | | | | CC Port Status | | CC Interface Status | |
|-------------|--------------------------|------------|-----------|----------|-------|------------------------------------|-------|------------------------------------|--|
| | OUI First | OUI Second | OUI Third | Sub-Type | Value | Last RX | Value | Last RX | |
| 6 | 0 | 0 | 0 | 0 | 0 | ● | 0 | ● | |

Link State Tracking

Enable

Save Reset

Figure 7 - Switch 2 MEP 2 Configuration

Configuring Switch 3

1. Add a new MEP on port 1 and 2 of switch 3.

Maintenance Entity Point Refresh

| Delete | Instance | Domain | Mode | Direction | Residence Port | Level | Flow Instance | Tagged VID | This MAC | Alarm |
|--------------------------|----------|--------|------|-----------|----------------|-------|---------------|------------|-------------------|--------------------------------------|
| <input type="checkbox"/> | 1 | Port | Mep | Down | 1 | 0 | | 3001 | 00-22-38-02-36-55 | ● |
| <input type="checkbox"/> | 2 | Port | Mep | Down | 2 | 0 | | 3001 | 00-22-38-02-36-56 | ● |

Add New MEP

Figure 8 - Switch 3 Port 1 and 2 MEP Configuration

2. Edit MEP1 of switch 3 by clicking 1 under Instance of the MEP table. Configure the MEP as shown, and click Save or Apply.

MEP Configuration Refresh

Instance Data

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|----------|--------|------|-----------|----------------|---------------|------------|--------------|-------------------|
| 1 | Port | Mep | Down | 1 | | 3001 | 1 | 00-22-38-02-36-55 |

Instance Configuration

| Level | Format | Domain Name | MEG id | MEP id | Tagged VID | Syslog | cLevel | cMEG | cMEP | cAIS | cLCK | cLoop | cConfig | cSSF | aBLK | aTSF |
|-------|---------|-------------|---------------|--------|------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 0 | ITU ICC | | ICC000MEG0000 | 6 | 3001 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Peer MEP Configuration

| Delete | Peer MEP ID | Unicast Peer MAC | cLOC | cRDI | cPeriod | cPriority |
|--------------------------|-------------|-------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> | 1 | 00-22-38-02-1B-25 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Add New Peer MEP

Functional Configuration

| Continuity Check | | | | APS Protocol | | | | |
|-------------------------------------|----------|------------|--------------------------|-------------------------------------|----------|------|-------|------------|
| Enable | Priority | Frame rate | TLV | Enable | Priority | Cast | Type | Last Octet |
| <input checked="" type="checkbox"/> | 0 | 300 fsec | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0 | Mult | R-APS | 1 |

Fault Management

TLV Configuration

| Organization Specific TLV (Global) | | | | | |
|------------------------------------|------------|-----------|----------|-------|--|
| OUI First | OUI Second | OUI Third | Sub-Type | Value | |
| 0 | 0 | 12 | 1 | 2 | |

TLV Status

| Peer MEP ID | CC Organization Specific | | | | | | CC Port Status | | CC Interface Status | |
|-------------|--------------------------|------------|-----------|----------|-------|------------------------------------|----------------|------------------------------------|---------------------|------------------------------------|
| | OUI First | OUI Second | OUI Third | Sub-Type | Value | Last RX | Value | Last RX | Value | Last RX |
| 1 | 0 | 0 | 0 | 0 | 0 | ● | 0 | ● | 0 | ● |

Link State Tracking

Enable

Figure 9 - Switch 3 MEP 1 Configuration

3. Edit MEP2 of switch 3 by clicking 2 and configuring the MEP as shown, and click Save or Apply.

MEP Configuration Refresh

Instance Data

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|----------|--------|------|-----------|----------------|---------------|------------|--------------|-------------------|
| 2 | Port | Mep | Down | 2 | | 3001 | 1 | 00-22-38-02-36-56 |

Instance Configuration

| Level | Format | Domain Name | MEG id | MEP id | Tagged VID | Syslog | cLevel | cMEG | cMEP | cAIS | cLCK | cLoop | cConfig | cSSF | aBLK | aTSF |
|-------|---------|-------------|---------------|--------|------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 0 | ITU ICC | | ICC000MEG0000 | 6 | 3001 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Peer MEP Configuration

| Delete | Peer MEP ID | Unicast Peer MAC | cLOC | cRDI | cPeriod | cPriority |
|--------------------------|-------------|-------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> | 4 | 00-22-38-02-36-4A | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Add New Peer MEP

Functional Configuration

| Continuity Check | | | | APS Protocol | | | | |
|-------------------------------------|----------|------------|--------------------------|-------------------------------------|----------|------|-------|------------|
| Enable | Priority | Frame rate | TLV | Enable | Priority | Cast | Type | Last Octet |
| <input checked="" type="checkbox"/> | 0 | 1 fsec | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0 | Mult | R-APS | 1 |

Fault Management

TLV Configuration

| Organization Specific TLV (Global) | | | | | |
|------------------------------------|------------|-----------|----------|-------|--|
| OUI First | OUI Second | OUI Third | Sub-Type | Value | |
| 0 | 0 | 12 | 1 | 2 | |

TLV Status

| Peer MEP ID | CC Organization Specific | | | | | | CC Port Status | | CC Interface Status | |
|-------------|--------------------------|------------|-----------|----------|-------|------------------------------------|----------------|------------------------------------|---------------------|------------------------------------|
| | OUI First | OUI Second | OUI Third | Sub-Type | Value | Last RX | Value | Last RX | Value | Last RX |
| 4 | 0 | 0 | 0 | 0 | 0 | ● | 0 | ● | 0 | ● |

Link State Tracking

Enable

Figure 10 - Switch 3 MEP 2 Configuration

Configuring ERPS on Switch 1

1. On switch 1, click ERPS to go to the Ethernet Ring Protection switching page. Add the Ring Protection Link (RPL) owner as shown, and click Add New Protection Group.

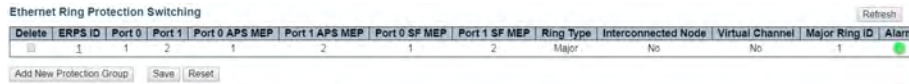


Figure 11 - Add New Protection Group (Switch 1) Configuration

2. Edit ERPS1 by clicking 1. Set the configuration as shown, and click Save or Apply.

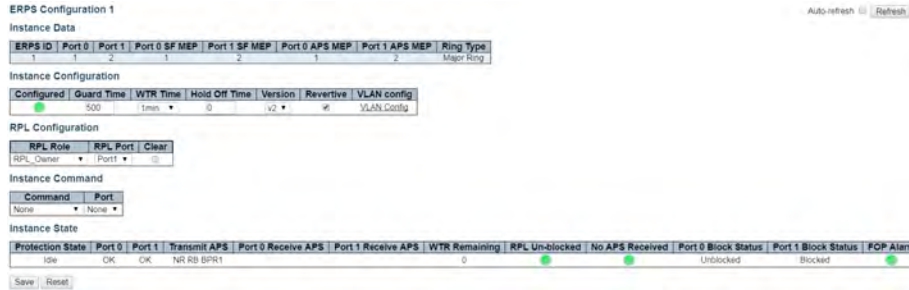


Figure 12 - ERPS 1 (Switch 1) Configuration

3. Click VLAN Config to edit the protected VLAN.

ERPS VLAN Configuration 1



Figure 13 - Protected VLAN (Switch 1) Configuration

4. After clicking Save or Apply, remember to connect switch 2 and switch 3. Because the RPL is disconnected, the user will not be able to access switch 2 from switch 1.
5. Check the MEP table on switch 1, switch 2, and switch 3. Alarms should show green.

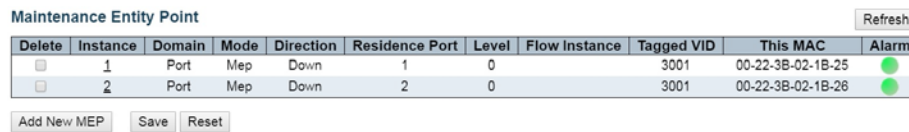


Figure 14 - MEP Status

Configuring ERPS on Switch 2, the RPL Neighbor

1. On switch 2, click ERPS followed by Add New Protection Group.

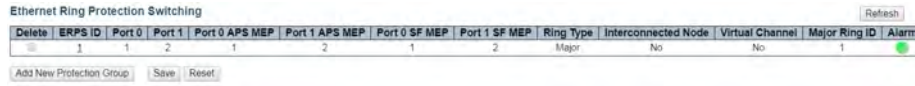


Figure 15 - Add New Protection Group (Switch 2) Configuration

2. Edit ERPS1 by clicking 1. Configure the device as shown, and click Save or Apply.



Figure 16 - ERPS 1 (Switch 2) Configuration

3. Click VLAN Config to edit the VLAN.

ERPS VLAN Configuration 1



Figure 17 - ERPS VLAN (Switch 2) Configuration

Configuring ERPS on Switch 3

1. On switch 3, click ERPS followed by Add New Protection Group.

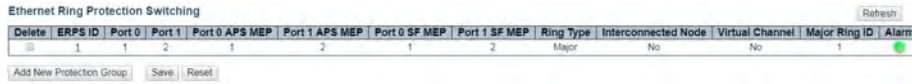


Figure 18 - Add New Protection Group (Switch3)

2. Edit ERPS1 by clicking 1. No action is required on switch 3. Keep the RPL owner at none.



Figure 19 - ERPS 1 (Switch 2) Configuration

3. Click VLAN Config to edit the VLAN.

ERPS VLAN Configuration 1



Figure 20 - ERPS VLAN (Switch 3) Configuration

Ethernet Ring Protection Switching Configuration

Verifying ERPS

1. Change the CCM rate starting from switch 3. Click on MEP > 2 and then use the frame rate pull down to select 300 f/sec.

MEP Configuration

Instance Data

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|----------|--------|------|-----------|----------------|---------------|------------|--------------|-------------------|
| 2 | Port | Meq | Down | 2 | | 3001 | 1 | 00-22-38-02-36-56 |

Instance Configuration

| Level | Format | Domain Name | MEG Id | MEP Id | Tagged VID | Syslog | cLevel | cMEG | cMEP | cAIS | cLCK | cLoop | cConfig | cSSF | aBLK | aTSF |
|-------|---------|-------------|---------------|--------|------------|--------|--------|------|------|------|------|-------|---------|------|------|------|
| 0 | ITU ICC | | ICC000MEG0000 | 6 | 3001 | | | | | | | | | | | |

Peer MEP Configuration

| Delete | Peer MEP ID | Unicast Peer MAC | cLOC | cRDI | cPeriod | cPriority |
|--------------------------|-------------|-------------------|------|------|---------|-----------|
| <input type="checkbox"/> | 4 | 00-22-38-02-36-4A | | | | |

Functional Configuration

| Continuity Check | | | | APS Protocol | | | | |
|-------------------------------------|----------|------------|-----|-------------------------------------|----------|-------|-------|------------|
| Enable | Priority | Frame rate | TLV | Enable | Priority | Cast | Type | Last Octet |
| <input checked="" type="checkbox"/> | 0 | 1 fsec | | <input checked="" type="checkbox"/> | 0 | Multi | R-APS | 1 |

TLV Configuration

| OUI First | OUI Second | OUI Third | Sub-Type | Value |
|-----------|------------|-----------|----------|-------|
| 0 | 0 | 12 | 1 | 2 |

TLV Status

| Peer MEP ID | OUI First | OUI Second | OUI Third | Sub-Type | Value | Last RX | CC Port Status Value | Last RX | CC Interface Status Value | Last RX |
|-------------|-----------|------------|-----------|----------|-------|---------|----------------------|---------|---------------------------|---------|
| 4 | 0 | 0 | 0 | 0 | 0 | | 0 | | 0 | |

Link State Tracking

Enable

Figure 21 - Edit MEP 2 CCM Rate (Switch 3)

2. Change the CCM rate for MEP 1.

MEP Configuration

Instance Data

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|----------|--------|------|-----------|----------------|---------------|------------|--------------|-------------------|
| 1 | Port | Meq | Down | 1 | | 3001 | 1 | 00-22-38-02-36-55 |

Instance Configuration

| Level | Format | Domain Name | MEG Id | MEP Id | Tagged VID | Syslog | cLevel | cMEG | cMEP | cAIS | cLCK | cLoop | cConfig | cSSF | aBLK | aTSF |
|-------|---------|-------------|---------------|--------|------------|--------|--------|------|------|------|------|-------|---------|------|------|------|
| 0 | ITU ICC | | ICC000MEG0000 | 5 | 3001 | | | | | | | | | | | |

Peer MEP Configuration

| Delete | Peer MEP ID | Unicast Peer MAC | cLOC | cRDI | cPeriod | cPriority |
|--------------------------|-------------|-------------------|------|------|---------|-----------|
| <input type="checkbox"/> | 1 | 00-22-38-02-1B-25 | | | | |

Functional Configuration

| Continuity Check | | | | APS Protocol | | | | |
|-------------------------------------|----------|------------|-----|-------------------------------------|----------|-------|-------|------------|
| Enable | Priority | Frame rate | TLV | Enable | Priority | Cast | Type | Last Octet |
| <input checked="" type="checkbox"/> | 0 | 300 fsec | | <input checked="" type="checkbox"/> | 0 | Multi | R-APS | 1 |

TLV Configuration

| OUI First | OUI Second | OUI Third | Sub-Type | Value |
|-----------|------------|-----------|----------|-------|
| 0 | 0 | 12 | 1 | 2 |

TLV Status

| Peer MEP ID | OUI First | OUI Second | OUI Third | Sub-Type | Value | Last RX | CC Port Status Value | Last RX | CC Interface Status Value | Last RX |
|-------------|-----------|------------|-----------|----------|-------|---------|----------------------|---------|---------------------------|---------|
| 1 | 0 | 0 | 0 | 0 | 0 | | 0 | | 0 | |

Link State Tracking

Enable

Figure 22 - Edit MEP 1 CCM Rate (Switch 3)

- Change the CCM rate on switch 1. Click on MEP > 1 and then use the frame rate pull down to select 300 f/sec.

MEP Configuration Refresh

Instance Data

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|----------|--------|------|-----------|----------------|---------------|------------|--------------|-------------------|
| 1 | Port | Meq | Down | 1 | | 3001 | 1 | 00-22-38-02-1B-2F |

Instance Configuration

| Level | Format | Domain Name | MEG Id | MEP Id | Tagged VID | Syslog | cLevel | cMEG | cMEP | cAIS | cCLK | cLoop | cConfig | cSSF | aBLK | aTSF |
|-------|---------|-------------|--------------|--------|------------|--------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 0 | ITU ICC | | IC0000ME0000 | 1 | 3001 | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Peer MEP Configuration

| Delete | Peer MEP ID | Unicast Peer MAC | cLOC | cRDI | cPeriod | cPriority |
|--------------------------|-------------|-------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> | 5 | 00-22-38-02-36-55 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Add New Peer MEP

Functional Configuration

| Continuity Check | | | | APS Protocol | | | | |
|-------------------------------------|----------|------------|--------------------------|-------------------------------------|----------|-------|-------|------------|
| Enable | Priority | Frame rate | TLV | Enable | Priority | Cast | Type | Last Octet |
| <input checked="" type="checkbox"/> | 0 | 300 fsec | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0 | Multi | R-APS | 1 |

Fault Management Performance Monitoring

TLV Configuration

| Organization Specific TLV (Global) | | | | |
|------------------------------------|------------|-----------|----------|-------|
| OUI First | OUI Second | OUI Third | Sub-Type | Value |
| 0 | 0 | 12 | 1 | 2 |

TLV Status

| Peer MEP ID | CC Organization Specific | | | | | | CC Port Status | | CC Interface Status | |
|-------------|--------------------------|------------|-----------|----------|-------|-------------------------------------|----------------|-------------------------------------|---------------------|-------------------------------------|
| | OUI First | OUI Second | OUI Third | Sub-Type | Value | Last RX | Value | Last RX | Value | Last RX |
| 5 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> | 0 | <input checked="" type="checkbox"/> | 0 | <input checked="" type="checkbox"/> |

Link State Tracking

Enable

Save Reset

Figure 23 - Edit MEP 1 CCM Rate (Switch 1)

- Change the CCM rate for MEP 2.

MEP Configuration Refresh

Instance Data

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|----------|--------|------|-----------|----------------|---------------|------------|--------------|-------------------|
| 2 | Port | Meq | Down | 2 | | 3001 | 1 | 00-22-38-02-1B-2E |

Instance Configuration

| Level | Format | Domain Name | MEG Id | MEP Id | Tagged VID | Syslog | cLevel | cMEG | cMEP | cAIS | cCLK | cLoop | cConfig | cSSF | aBLK | aTSF |
|-------|---------|-------------|--------------|--------|------------|--------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 0 | ITU ICC | | IC0000ME0000 | 2 | 3001 | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Peer MEP Configuration

| Delete | Peer MEP ID | Unicast Peer MAC | cLOC | cRDI | cPeriod | cPriority |
|--------------------------|-------------|-------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> | 3 | 00-22-38-02-36-49 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Add New Peer MEP

Functional Configuration

| Continuity Check | | | | APS Protocol | | | | |
|-------------------------------------|----------|------------|--------------------------|-------------------------------------|----------|-------|-------|------------|
| Enable | Priority | Frame rate | TLV | Enable | Priority | Cast | Type | Last Octet |
| <input checked="" type="checkbox"/> | 0 | 300 fsec | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0 | Multi | R-APS | 1 |

Fault Management Performance Monitoring

TLV Configuration

| Organization Specific TLV (Global) | | | | |
|------------------------------------|------------|-----------|----------|-------|
| OUI First | OUI Second | OUI Third | Sub-Type | Value |
| 0 | 0 | 12 | 1 | 2 |

TLV Status

| Peer MEP ID | CC Organization Specific | | | | | | CC Port Status | | CC Interface Status | |
|-------------|--------------------------|------------|-----------|----------|-------|-------------------------------------|----------------|-------------------------------------|---------------------|-------------------------------------|
| | OUI First | OUI Second | OUI Third | Sub-Type | Value | Last RX | Value | Last RX | Value | Last RX |
| 3 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> | 0 | <input checked="" type="checkbox"/> | 0 | <input checked="" type="checkbox"/> |

Link State Tracking

Enable

Save Reset

Figure 24 - Edit MEP 2 CCM Rate (Switch 1)

- Change the CCM rate on switch 2. Click on MEP > 1 and then use the frame rate pull down to select 300 f/sec.

MEP Configuration Refresh

Instance Data

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|----------|--------|------|-----------|----------------|---------------|------------|--------------|-------------------|
| 1 | Port | MEP | Down | 1 | | 3001 | 1 | 00-22-38-02-35-43 |

Instance Configuration

| Level | Format | Domain Name | MEG id | MEP id | Tagged VID | Syslog | cLevel | cMEG | cMEP | cAIS | cLCK | cLoop | cConfig | cSSF | aBLK | aTSF |
|-------|---------|-------------|---------------|--------|------------|--------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 0 | ITU ICC | | ICC000MEG0000 | 3 | 3001 | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Peer MEP Configuration

| Delete | Peer MEP ID | Unicast Peer MAC | cLOC | cRDI | cPeriod | cPriority |
|--------------------------|-------------|-------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> | 2 | 00-22-38-02-18-26 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Add New Peer MEP

Functional Configuration

| Continuity Check | | | | APS Protocol | | | | |
|-------------------------------------|----------|------------|--------------------------|-------------------------------------|----------|-------|-------|------------|
| Enable | Priority | Frame rate | TLV | Enable | Priority | Cast | Type | Last Octet |
| <input checked="" type="checkbox"/> | 0 | 300 f/sec | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0 | Multi | R-APS | 1 |

Fault Management Performance Monitoring

TLV Configuration

| Organization Specific TLV (Global) | | | | | |
|------------------------------------|------------|-----------|----------|-------|---|
| OUI First | OUI Second | OUI Third | Sub-Type | Value | |
| 0 | 0 | 0 | 12 | 1 | 2 |

TLV Status

| Peer MEP ID | CC Organization Specific | | | | | | CC Port Status | | CC Interface Status | |
|-------------|--------------------------|------------|-----------|----------|-------|-------------------------------------|----------------|-------------------------------------|---------------------|-------------------------------------|
| | OUI First | OUI Second | OUI Third | Sub-Type | Value | Last RX | Value | Last RX | Value | Last RX |
| 2 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> | 0 | <input checked="" type="checkbox"/> | 0 | <input checked="" type="checkbox"/> |

Link State Tracking

Enable

Save Reset

Figure 25 - Edit MEP 1 CCM Rate (Switch 2)

- Change the CCM rate for MEP 2.

MEP Configuration Refresh

Instance Data

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|----------|--------|------|-----------|----------------|---------------|------------|--------------|-------------------|
| 2 | Port | MEP | Down | 2 | | 3001 | 1 | 00-22-38-02-35-43 |

Instance Configuration

| Level | Format | Domain Name | MEG id | MEP id | Tagged VID | Syslog | cLevel | cMEG | cMEP | cAIS | cLCK | cLoop | cConfig | cSSF | aBLK | aTSF |
|-------|---------|-------------|---------------|--------|------------|--------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 0 | ITU ICC | | ICC000MEG0000 | 4 | 3001 | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Peer MEP Configuration

| Delete | Peer MEP ID | Unicast Peer MAC | cLOC | cRDI | cPeriod | cPriority |
|--------------------------|-------------|-------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> | 6 | 00-22-38-02-36-56 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Add New Peer MEP

Functional Configuration

| Continuity Check | | | | APS Protocol | | | | |
|-------------------------------------|----------|------------|--------------------------|-------------------------------------|----------|-------|-------|------------|
| Enable | Priority | Frame rate | TLV | Enable | Priority | Cast | Type | Last Octet |
| <input checked="" type="checkbox"/> | 0 | 1 f/sec | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0 | Multi | R-APS | 1 |

Fault Management Performance Monitoring

TLV Configuration

| Organization Specific TLV (Global) | | | | | |
|------------------------------------|------------|-----------|----------|-------|---|
| OUI First | OUI Second | OUI Third | Sub-Type | Value | |
| 0 | 0 | 0 | 12 | 1 | 2 |

TLV Status

| Peer MEP ID | CC Organization Specific | | | | | | CC Port Status | | CC Interface Status | |
|-------------|--------------------------|------------|-----------|----------|-------|-------------------------------------|----------------|-------------------------------------|---------------------|-------------------------------------|
| | OUI First | OUI Second | OUI Third | Sub-Type | Value | Last RX | Value | Last RX | Value | Last RX |
| 6 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> | 0 | <input checked="" type="checkbox"/> | 0 | <input checked="" type="checkbox"/> |

Link State Tracking

Enable

Save Reset

Figure 26 - Edit MEP 2 CCM Rate (Switch 2)

7. On Switch 1, check ERPS status by clicking ERPS to ensure normal link status

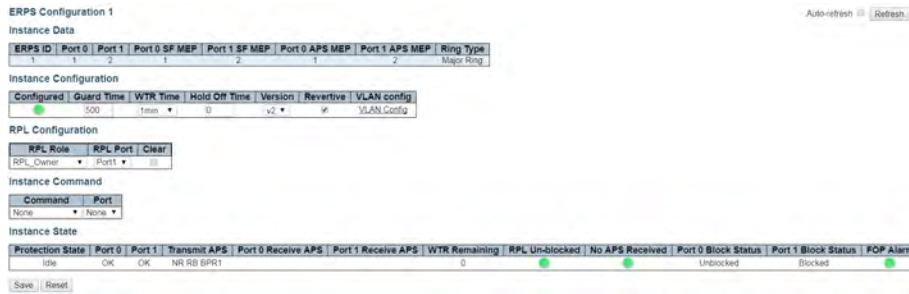


Figure 27 - Switch 1 ERPS Status

8. Disconnect the normal link for switch 1 and switch 3.

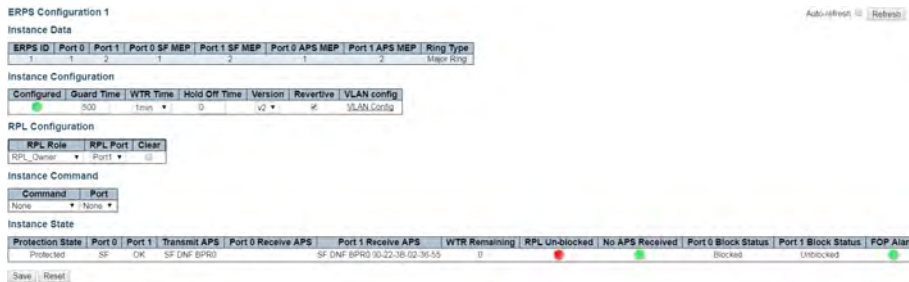


Figure 28 - Disconnect Normal Link

9. Restore the normal link for switch 1 and switch 3 to display the protection state as Pending.

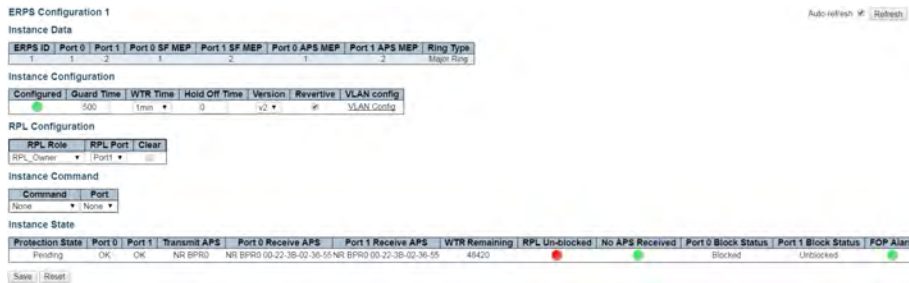


Figure 29 - Restore Normal Link

10. After WTR timeout, and clicking Refresh, it should show as Idle.

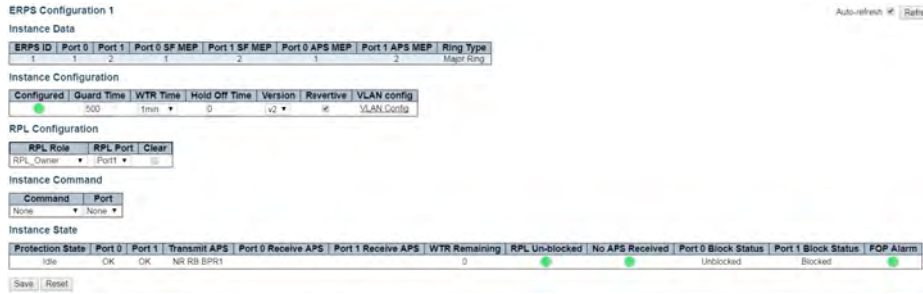


Figure 30 – Refresh ERPS Status

Configuring ERPS from the ICLI

Initial Switch Configuration

The following commands disable STP and LLDP, and they enable C-Port on Port 1 and 2 on all switches.

```
#Configure port 1-2
```

```
interface GigabitEthernet 1/1-2
```

```
#set C-Port
```

```
switchport hybrid port-type c-port
```

```
switchport mode hybrid
```

```
#disable LLDP
```

```
no lldp receive
```

```
no lldp transmit
```

```
#disable Spanning Tree Protocol
```

```
no spanning-tree
```

Configuring MEP and ERPS on Switch 1 (RPL Owner)

```
#create mep 1 on port 1
mep 1 down domain port flow 1 level 0 interface GigabitEthernet 1/1
#set vlan for MEP traffic
mep 1 vid 3001
#set id of peer mep
mep 1 peer-mep-id 5
#enable ccm, default is 1FPS
mep 1 cc 0
#enable RAPS
mep 1 aps 0 raps
mep 2 down domain port flow 2 level 0 interface GigabitEthernet 1/2
mep 2 mep-id 2
mep 2 vid 3001
mep 2 peer-mep-id 3
mep 2 cc 0
mep 2 aps 0 raps
#create erps on port 1 and port 2
erps 1 major port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet 1/2
#set MEP ID for the corresponding port
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
#set to RPL owner
erps 1 rpl owner port1\
#set protected VLAN
erps 1 vlan 1
```

Configuring MEP and ERPS on Switch 2 (RPL Neighbor)

```
mep 1 down domain port flow 1 level 0 interface GigabitEthernet 1/1
mep 1 mep-id 3
mep 1 vid 3001
mep 1 peer-mep-id 2
mep 1 cc 0
mep 1 aps 0 raps
mep 2 down domain port flow 2 level 0 interface GigabitEthernet 1/2
mep 2 mep-id 4
mep 2 vid 3001
mep 2 peer-mep-id 6
mep 2 cc 0
mep 2 aps 0 raps
erps 1 major port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet 1/2
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
#set to RPL neighbour
erps 1 rpl neighbor port0
erps 1 vlan 1
```

Configuring MEP and ERPS on Switch 3

```
mep 1 down domain port flow 1 level 0 interface GigabitEthernet 1/1
```

```
mep 1 mep-id 5
```

```
mep 1 vid 3001
```

```
mep 1 peer-mep-id 1
```

```
mep 1 cc 0
```

```
mep 1 aps 0 raps
```

```
mep 2 down domain port flow 2 level 0 interface GigabitEthernet 1/2
```

```
mep 2 mep-id 6
```

```
mep 2 vid 3001
```

```
mep 2 peer-mep-id 4
```

```
mep 2 cc 0
```

```
mep 2 aps 0 raps
```

```
erps 1 major port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet 1/2
```

```
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
```

```
erps 1 vlan 1
```

Note: *To set the CCM rate to 100FPS or 300FPS, the peer MAC address must be known as shown here, Or set it to lower rate first, until the peer MAC address is learned, and then change it to a higher rate.*

```
mep 1 peer-mep-id <peer mep id> mac <peer mac address>
```

```
mep 1 cc 0 fr300s
```

Finally, the ERPS status can be checked with the show erps command.

MECHANICAL INSTALLATION INSTRUCTIONS

ComNet Customer Service

Customer Care is ComNet Technology's global service center, where our professional staff is ready to answer your questions at any time.

Email ComNet Global Service Center: customer care@comnet.net



3 CORPORATE DRIVE | DANBURY, CT 06810 | USA

T: 203.796.5300 | F: 203.796.5303 | TECH SUPPORT: 1.888.678.9427 | INFO@COMNET.NET

8 TURNBERRY PARK ROAD | GILDERSOME | MORLEY | LEEDS, UK LS27 7LE

T: +44 (0)113 307 6400 | F: +44 (0)113 253 7462 | INFO-EUROPE@COMNET.NET