RocketLinx MP1204-XT

Industrial PoE
Managed Switch

8 - Gigabit Copper Ports
4 - Gigabit SFP Ports

User Guide

COMTROL®

Copyright Notice

First Edition, March 21, 2018

Table of Contents

Introduction

Audience

The guide is intended for system engineers or operating personnel who want to have a basic understanding of MP1204-XT.

Product Overview

The MP1204-XT is an industrial twelve port managed PoE Plus switch that provides:

- Eight Gigabit (10/100/1000BASE-T) PoE Plus ports that are IEEE 802.3af (15.4W) and IEEE 802.3at (30W)
- Four Gigabit (10/100/1000BASE-T) SFP ports

The MP1204-XT meets the high power and advanced management needs of critical PoE applications such as real-time IP video surveillance and wireless communication utilizing Wimax and IEEE 802.11 a/b/g/n access points.

Featuring a rugged design for harsh environments, web user interface, Command Line Interface (CLI), SNMP management options, power scheduling, and eight fully compliant IEEE 802.3at PoE injector ports, the MP1204-XT is easily configured to deliver up to 30W for even the most power intensive devices such as IP cameras utilizing heaters and pan/tilt/zoom controls.

In addition to functioning as a PoE power source, the MP1204-XT includes features to enhance device control, ensuring that power consumption does not exceed parameters that you define. This includes power budget control functions to limit power output on devices not reporting correct consumption rates and device priority options to guarantee power to critical devices while avoiding power supply overloads.

The MP1204-XT is equipped with full Layer 2+ management capabilities to provide the most flexible network configuration and control. Features like Link Aggregation Control Protocol (LACP) allow grouping of multiple ports to enhance bandwidth and provide load balancing while port-based VLAN with tunneling, QoS, IGMP Snooping, and Rate Control features enable optimum control over network environments. In addition to the full array of management capabilities, the MP1204-XT also supports security features that protect the network and guarantee secure, reliable data transmission. Fault relay and email notification of event alarms, DHCP supporting IP and MAC binding, IEEE 802.1x Access Control, SSH, and many other controls are included to make secure administration and management a simple task.

Detailed specifications for the MP1204-XT are available on the Comtrol web site.

System Maximum Values

Function Name	System Maximum Value
VLAN ID	4096
VLAN Limitation	1024
Privilege Level of User	15
RMON Statistic Entry	65535
RMON Alarm Entry	65
RMON Event Entry	65535

Function Name	System Maximum Value
IPMC Profile	64
IPMC Rule / Address Entry	128
ACE	256
ICMP Type / Code	255
RADIUS Server	5
TACACS+ Server	5
MAC-based VLAN Entry	256
IP subnet-based VLAN Entry	128
Protocol-based VLAN Group	125
Voice VLAN OUI	16
QCE	256
IP Interface	8
IP Route	32
Security Access Management	16
MVR VLAN	4
MAC Learning table address	8k
IGMP Group	256

Installing the Hardware

This subsection contains the following topics:

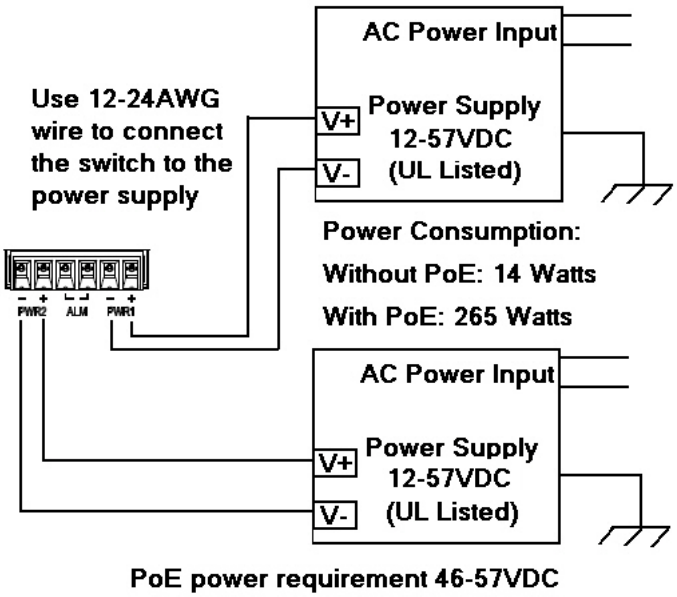
Connecting the Power Terminal Block

The MP1204-XT provides redundant power inputs (PWR 1/2), which supports reverse polarity protection, and accepts a positive or negative power source (12V – 57V). However, PWR1 and PWR2 must use the same mode.

Electrical Specifications		Value
Power Input Voltage PWR1/PWR2	IEEE 802.3af	46-57/3.1A (Max)
	IEEE 802.3at	50-57VDC/5.2A (Max)
Power Input Voltage PWR1/PWR2	IEEE 802.3af	15.4W
	IEEE 802.3at	30W
Power Budget	PWR1/PWR2	240W
Power Consumption	Without PD load (Max)	14W
	PoE with PC load (Max) IEEE 802.3af IEEE 802.3at	265W with 240W PSE 2.92A @ 48VDC [134W] 4.89A @ 53VDC [247W]

Note: *Power should be disconnected from the power supply before connecting it to the MP1204-XT. Otherwise, your screwdriver blade can inadvertently short your terminal connections to the grounded enclosure.*

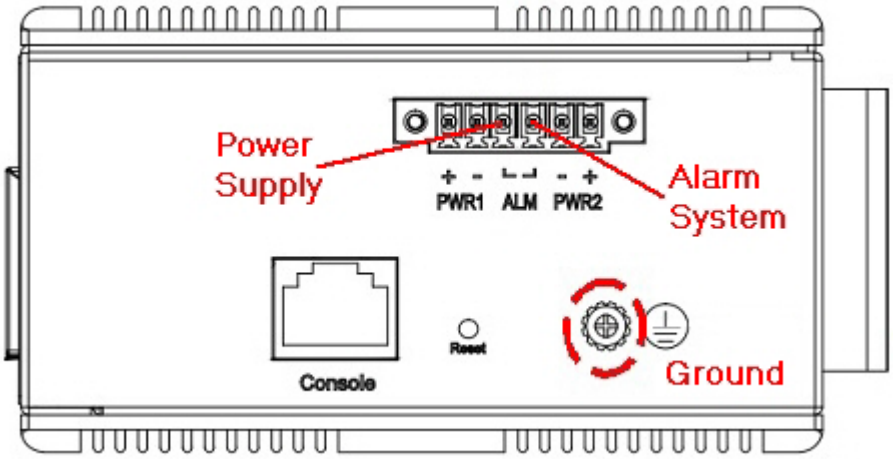
1. Insert the positive and negative wires into PWR+ and PWR- contacts. You can connect a single power supply or both power supplies depending on your requirements.
2. Tighten the wire-clamp screws to prevent the wires from coming loose.



Connect the Alarm Relay and Ground

The alarm relay output contacts are in the middle of the DC terminal block connector as shown in the figure below. The alarm relay output is *Normal Open*, and it is closed when it detects any predefined failure such as power failures or Ethernet link failures.

Note: *The relay output with current carrying capacity of 0.5A @ 24 VDC.*

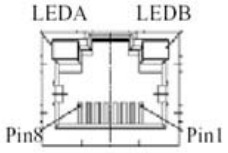


Connecting the RJ45 Cables

To connect the MP1204-XT to a PC, use straight-through or cross-over Ethernet cables. To connect the MP1204-XT to an Ethernet device, use UTP (Unshielded Twisted Pair) or STP (Shielded Twisted Pair) Ethernet cables.

The pin assignment of RJ45 connector is shown in the following figure and table.

Pin	Assignment	PoE Assignment
1, 2	T/Rx+ and T/Rx-	Positive Vport
3, 6	T/Rx+ and T/Rx-	Negative Vport
4, 5	T/Rx+ and T/Rx-	N/A
7, 8	T/Rx+ and T/Rx-	N/A

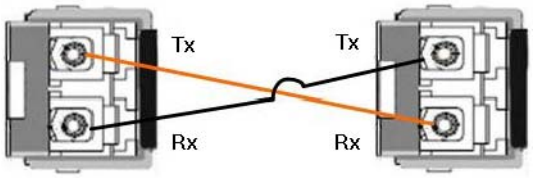


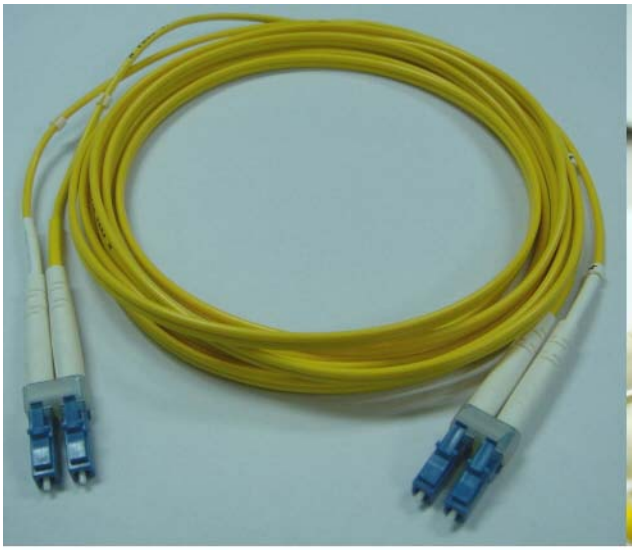
Connecting the SFPs

The SFP accepts LC connector fiber transceivers and supports both 100/1000 Mbps fiber speed connections. Comtrol recommends using Comtrol-approved SFP mini GBIC transceivers.

Note: *Never attempt to view optical connectors that might be emitting laser energy. Do not power up the laser product without connecting the laser to the optical fiber or putting the dust cover in position, as laser outputs will emit infrared laser light at this point.*

Cross-connect the transmit channel at each end to the receive channel at the opposite end as illustrated in the figure.



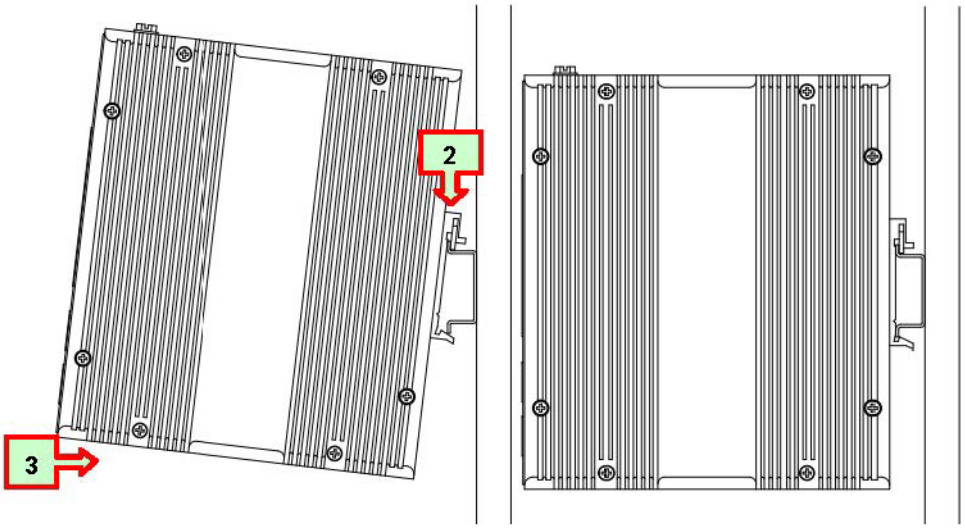


DIN Rail Mounting

Use the following procedure to mount the MP1204-XT on a DIN rail:

1. Attach the DIN clip using the screws in the accessory kit.

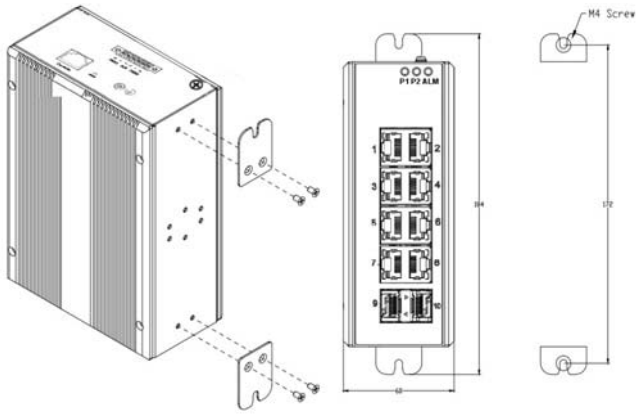
2. Hook the unit onto the DIN rail.
3. Push the bottom of the unit towards the DIN rail until it locks in place.



Wall Mounting

Use the following procedure to mount the MP1204-XT on a wall or panel:

1. Screw the wall-mount brackets with screws in the accessory kit.
2. Mount it to a wall or panel.



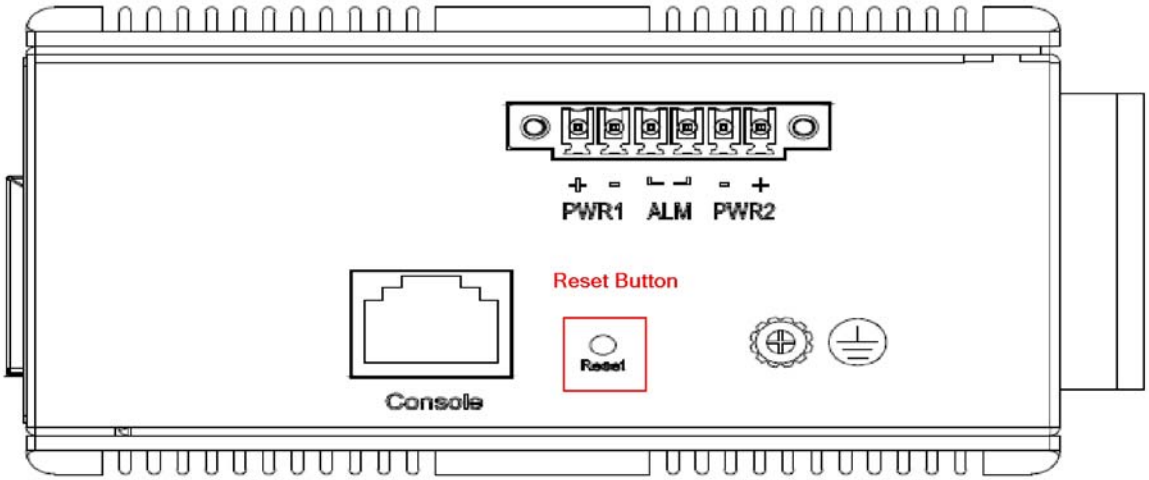
LED Status Indications

After you apply power, you can verify the state of the MP1204-XT.

LED Name	Indicator/Color	Condition
P1/P2	On Green	P1/P2 is receiving power
	Off	P1/P2 is disconnected or does not have power applied
Alarm	On Red	If configured, Ethernet link fails, alarm or power failure alarm occurs
	Off	No conditions configured or there are not any failures
Copper Port Link/Act	On Green	Ethernet link up but no traffic is detected
	Flashing Green	Ethernet link up and there is traffic detected
	Off	Ethernet link down
Copper Port Speed	On Yellow	A 1000Mbps connection is detected
	Off	No link, a 10Mbps or 100 Mbps connection is detected
SFP Port Link/Act	On Green	Ethernet link up
	Off	Ethernet link down
SFP Port Speed	On Yellow	SFP port speed 1000Mbps connection is detected
	Off	No link or a SFP port speed 100Mbps connection is detected
PoE LED	On Yellow	PoE is detected
	Off	No link
RR	Off	Not configured as the Ring-Master and ring is not configured.
	On	RR lights when the Role of the Ring is configured as the Ring-Master and Ring is enabled with the following roles. • Chain (Tail) • Balancing Chain (Central Block)
RS	Off	Ring or Chain failure not detected.
	On	Lights when a Ring (or Chain) Signal Failure is detected.

System Reset

The **Reset** button is provided to reboot the system without the need to remove power. Under normal circumstances, you will not need to reset the MP1204-XT. However, on rare occasions, the MP1204-XT may not respond and then you may need to push the **Reset** button.



Configuring the IP Address

There are two ways to configure the IP address for your network:

- Console connection through a COM port
- Telnet connection through an Ethernet cable

Using the Console Port

The Console port supports local management by using a terminal emulator or a computer with terminal emulation software, such as puTTY. The Console port is located near the power connector on the top of the MP1204-XT.

In the event that you have misplaced the cable shipped with the MP1204-XT, you can use the information in the table build a cable.

Set up the COM port with these settings:

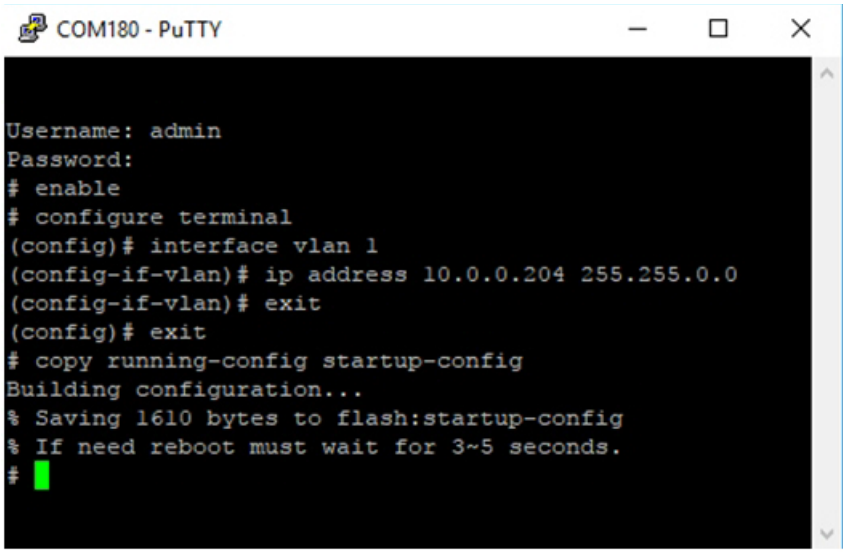
Characteristic	Setting
Baud rate	115200bps
Data bits	8
Stop bit	1
Parity	None
Flow control	None

Signal	DB9 Pins	RJ45 Pins
Rx	2	3
Tx	9	4
Gnd	5	6

Use the following procedure to configure the IP address using the Console port.

Note: *Use Ctrl+h if you need to delete a character or characters to correct a typo.*

1. Connect the RJ45 (male) connector to the MP1204-XT console port and connect the RS-232 DB9 (female) connector cable the COM port.
2. Start the terminal emulation software and configure the port as listed above.
3. You may need to press **Enter** to get the **Username** prompt depending on your software.
4. Enter **admin** as the **Username** and press the **Enter** key.
5. Enter **admin** as the **Password** and press the **Enter** key.
6. Enter **enable** and press the **Enter** key.
7. Enter **configure terminal** and press the **Enter** key.
8. Enter **interface vlan 1** and press the **Enter** key.



9. Enter **ip address ###.###.###.### ###.###.###.###** (the IP address – space – subnet mask) and press the Enter key.
10. Enter **exit** and press the **Enter** key.
11. Enter **exit** and press the **Enter** key.
12. To save the IP address to the flash, enter **copy running-config startup-config** and press the **Enter** key.

You can now open the MP1204-XT web interface to configure it for your environment.

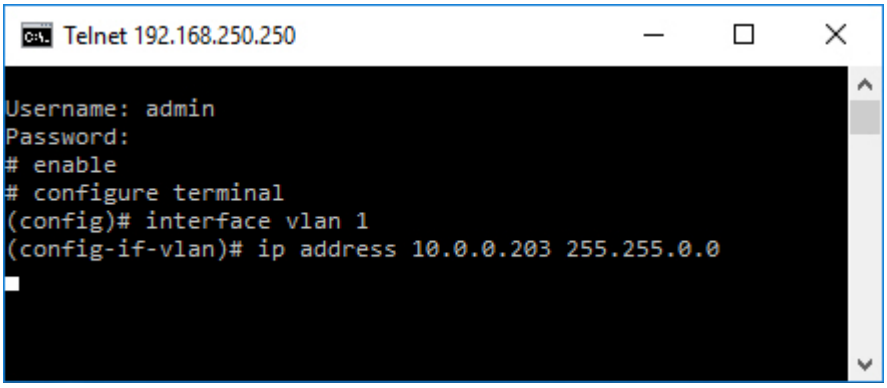
Using Telnet to Configure the IP Address

You must have the MP1204-XT connected to your network and you may need to change your IP address on your system before you can telnet into the MP1204-XT.

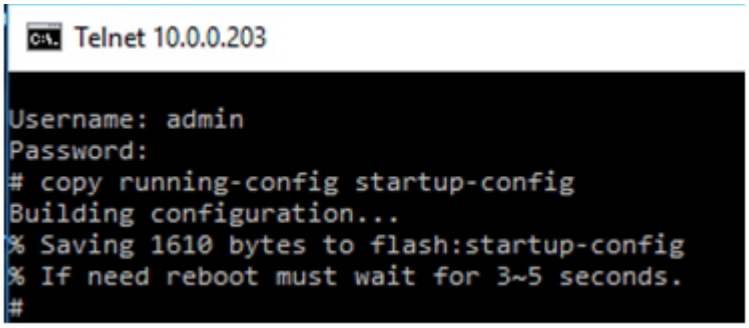
Optionally, if you change your system IP address temporarily, you can use the web interface to configure the IP address (*Using the Web Interface to Configure the IP Address* on Page 31).

Note: *The default IP address of the MP1204-XT is 192.168.250.250.*

1. Open the command prompt and enter telnet 192.168.250.250.
2. Enter **admin** as the **Username** and press the **Enter** key.
3. Enter **admin** as the **Password** and press the **Enter** key.
4. Enter **enable** and press the **Enter** key.
5. Enter **configure terminal** and press the **Enter** key.
6. Enter **interface vlan 1** and press the **Enter** key.
7. Enter **ip address ###.###.###.### ###.###.###.###** (the IP address – space – subnet mask) and press the Enter key.



8. Move the Ethernet cable the appropriate network connection.
9. Close the telnet session.
10. To save the new IP address to the flash, enter **telnet** and the new IP address.
11. Enter the **Username** and **Password**.
12. Enter **copy running-config startup-config** and press the **Enter** key.
13. If necessary, return your system IP address.



You can now open the MP1204-XT web interface to configure it for your environment.

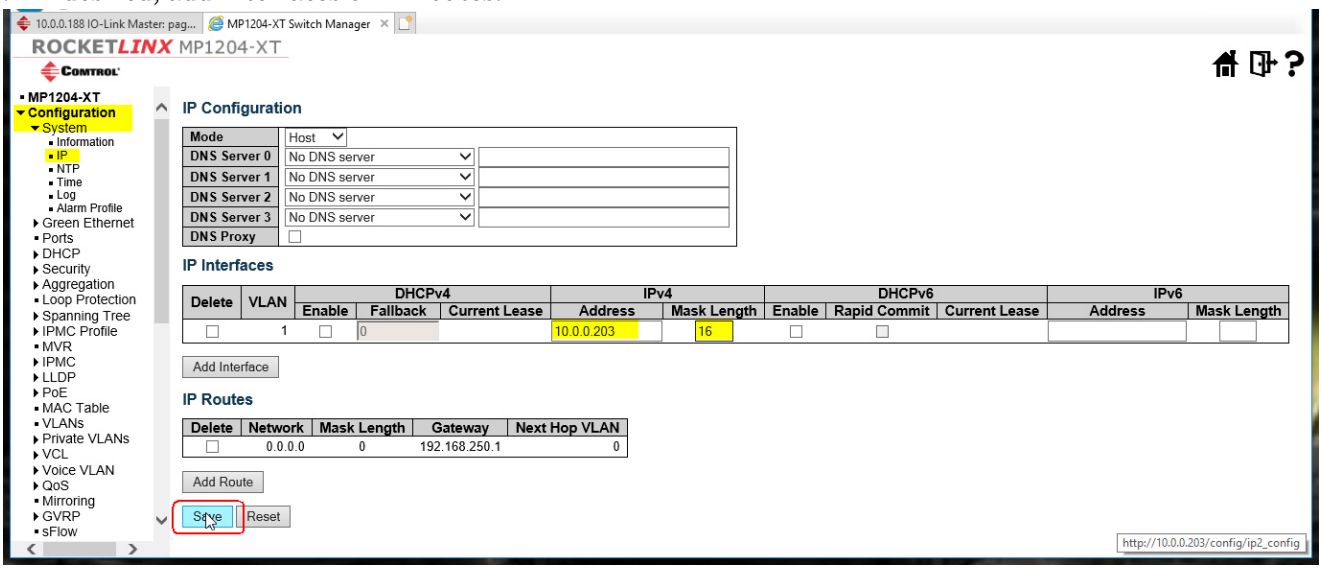
Using the Web Interface to Configure the IP Address

You must have the MP1204-XT connected to your network and you may need to change your IP address on your system before you can telnet into the MP1204-XT.

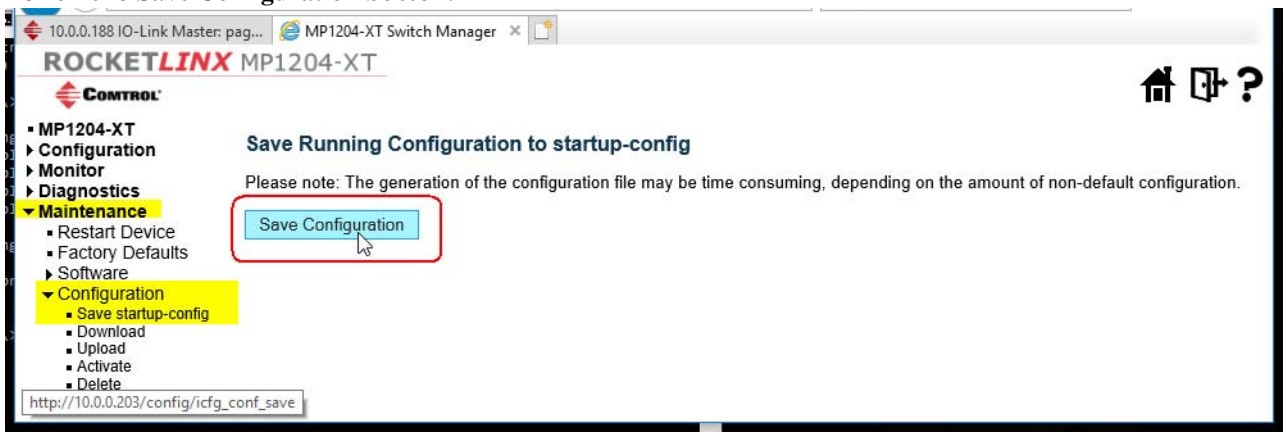
Note: *The default IP address of the MP1204-XT is 192.168.250.250.*

1. Open your browser and enter **192.168.250.250**.
2. Click **Configuration | System | IP**.
3. Select the **Mode** (**Host** or a **Router**). In **Host** mode, IP traffic between interfaces will not be routed. In **Router** mode traffic is routed between all interfaces.

   Note: *Refer to the help or* *System | IP on Page 38* *for more information about the options on this page.*
4. If applicable, select the appropriate DNS option.
5. Enter the **IP Address** and **Mask Length**.
6. If desired, add interfaces or IP routes.



7. Click the **Save** button.
8. Click **Maintenance | Configuration | Save startup-config**.
9. Click the **Save Configuration** button.



Web Interface Overview

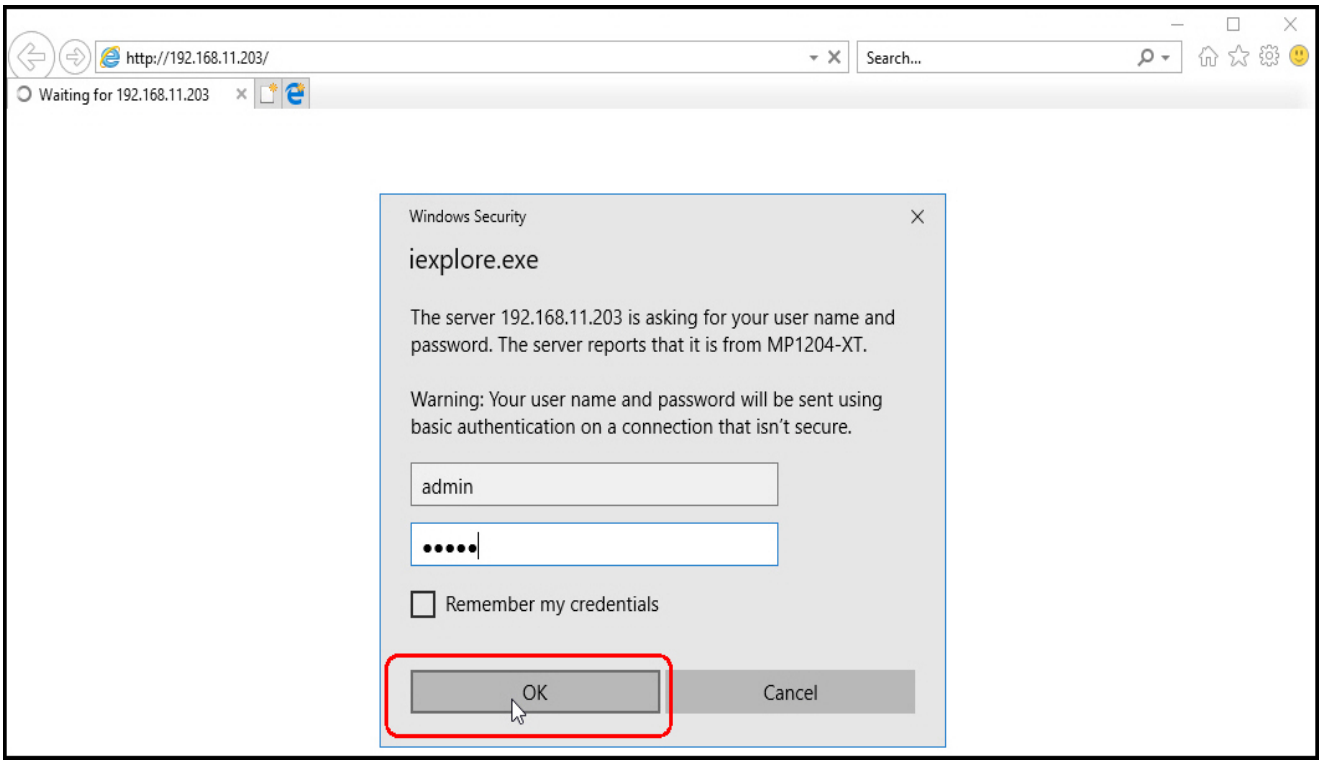
This section provides an overview of the MP1204-XT web interface.

Logging Into the MP1204-XT

After programming the IP address, you can open the web interface.

Field	Description
Username	Login user name. The maximum length is 32. Default: admin
Password	Login user password. The maximum length is 32. Default: admin

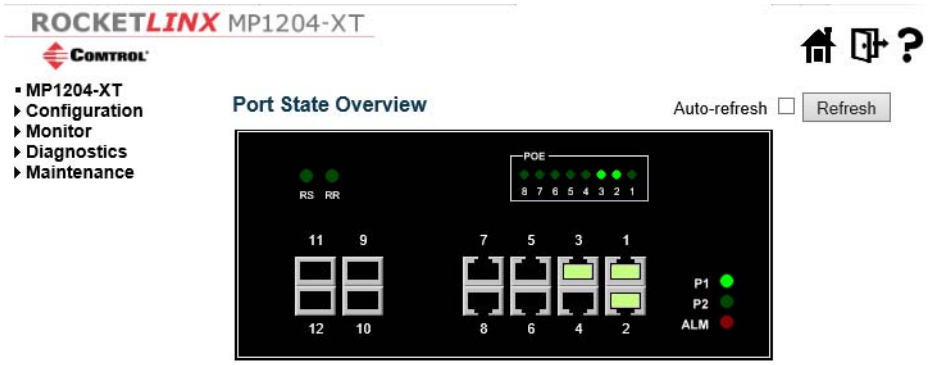
Note: *The login screen may appear under your browser, depending on your browser. If you do not see the login screen, minimize your browser and enter the user name and password.*



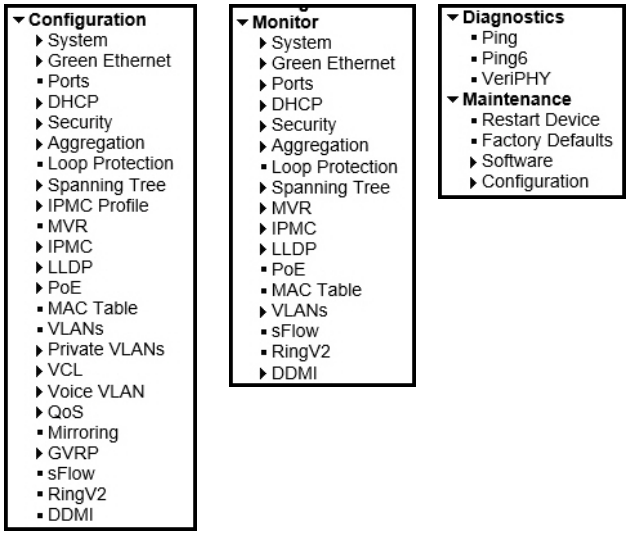
Navigational Menus

All main screens of the web interface can be reached by clicking the links in the four main menus on the left side of the screen:

- Configuration
- Monitor
- Diagnostics
- Maintenance



This illustrates the categories under the main menus.



Common Buttons

The following are not discussed in the upcoming sections because the functionality is the same across all of the pages.

Buttons	
Save	Click to save changes.
Reset	Click to revert to previously saved values.
Delete	Click to delete a setting.

Ending a Session

To end a session, close your web browser. This prevents an unauthorized user from accessing the system using your user name and password.

If you logout and leave the browser open, another user may access the MP1204-XT.

Configuration Pages

This section contains information about all **Configuration** menus.

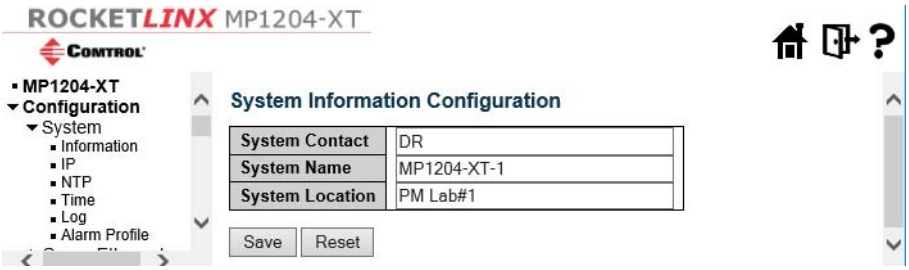
Configuration | System | Menus

The **Configuration | System** group contains these menus:

- *System | Information*
- *System | IP* on Page 38
- *System | NTP* on Page 40
- *System | Time* on Page 41
- *System | Log* on Page 44
- *System | Alarm Profile* on Page 45

System | Information

This shows the MP1204-XT system information.

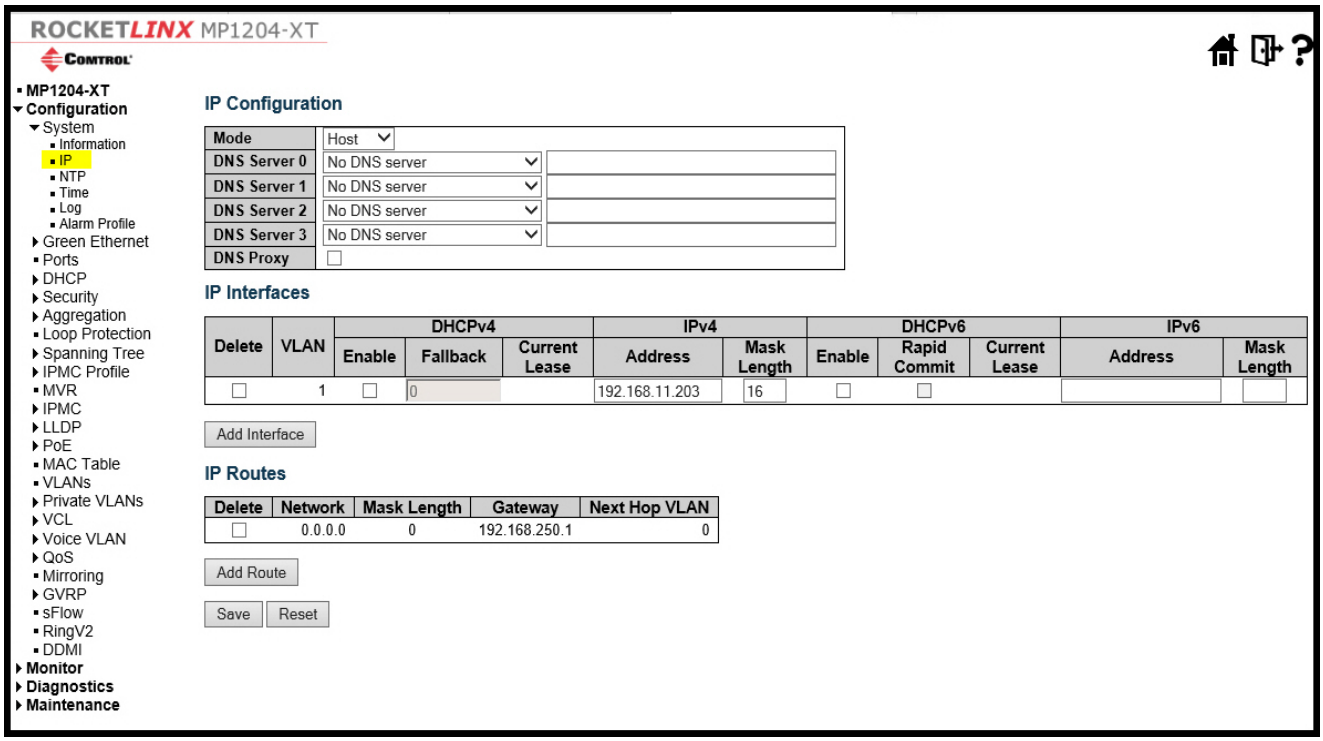


Item	Configuration | System | Information
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
System Name	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(for example,, telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

System | IP

Use this page to configure IP basic settings, control IP interfaces, and IP routes.

The maximum number of interfaces supported is eight and the maximum number of routes is 32.



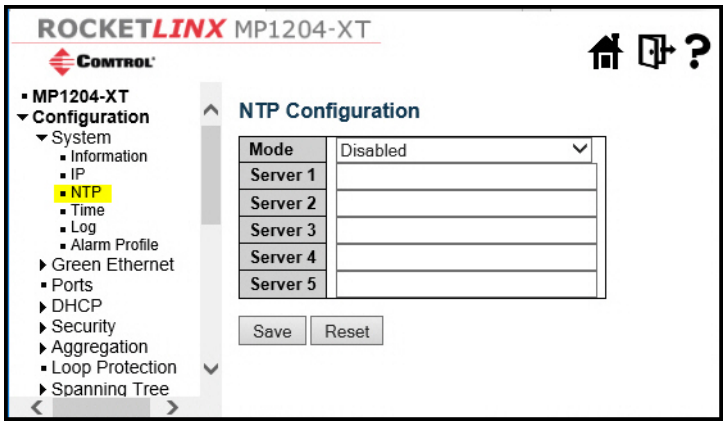
Item	Configuration | System | IP Configuration
IP Configuration	
Mode	Configure whether the IP stack should act as a Host or a Router. • In **Host** mode, IP traffic between interfaces is not routed. • In **Router** mode traffic is routed between all interfaces.
DNS Server	This setting controls the DNS name resolution done by the MP1204-XT. The following modes are supported: • **No DNS server:** No DNS server is used. • **Configured IPv4 or IPv6**: Explicitly provides the IP address of the DNS Server in dotted decimal notation. • **From any DHCPv4 interfaces**: The first DNS server offered from a DHCPv4 lease to a DHCP-enabled interface is used. • **From this DHCPv4 interface**: Specify from which DHCPv4-enabled interface a provided DNS server should be preferred. • **From any DHCPv6 interfaces**: The first DNS server offered from a DHCPv6 lease to a DHCP-enabled interface is used. • **From this DHCPv6 interface:** Specify from which DHCPv6-enabled interface a provided DNS server should be preferred.

Item	Configuration | System | IP Configuration (Continued)
DNS Proxy	When DNS proxy is enabled, the MP1204-XT relays DNS requests to the currently configured DNS server, and replies 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 are able to access the IP interface. This field is only available for input when creating an new interface.
IPv4 DHCP Enabled	Enable the DHCP client by checking this box. If this option is enabled, the system configures the IPv4 address and mask of the interface using the DHCP protocol. The DHCP client announces the configured System Name as *hostname* to provide DNS lookup.
IPv4 DHCP Fallback Timeout	This is the number of seconds to attempt to obtain a DHCP lease. After this period expires, a configured IPv4 address is used as an IPv4 interface address. A value of zero disables the fallback mechanism and DHCP keeps 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 show the current interface address, as provided by the DHCP server.
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 a 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.
IPv6 Address	The IPv6 address of the interface. A 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 a 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.

Item	Configuration | System | IP Configuration (Continued)
Network	The destination IP network or host address of this route. Valid format is dotted decimal notationor 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 has a mask length of 0 (as it matches anything).
Gateway	The IP address of the IP gateway. Valid format is dotted decimal 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 is 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.
Buttons (Other button are discussed on Page 34)	
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.

System | NTP

Use this page to configure NTP.

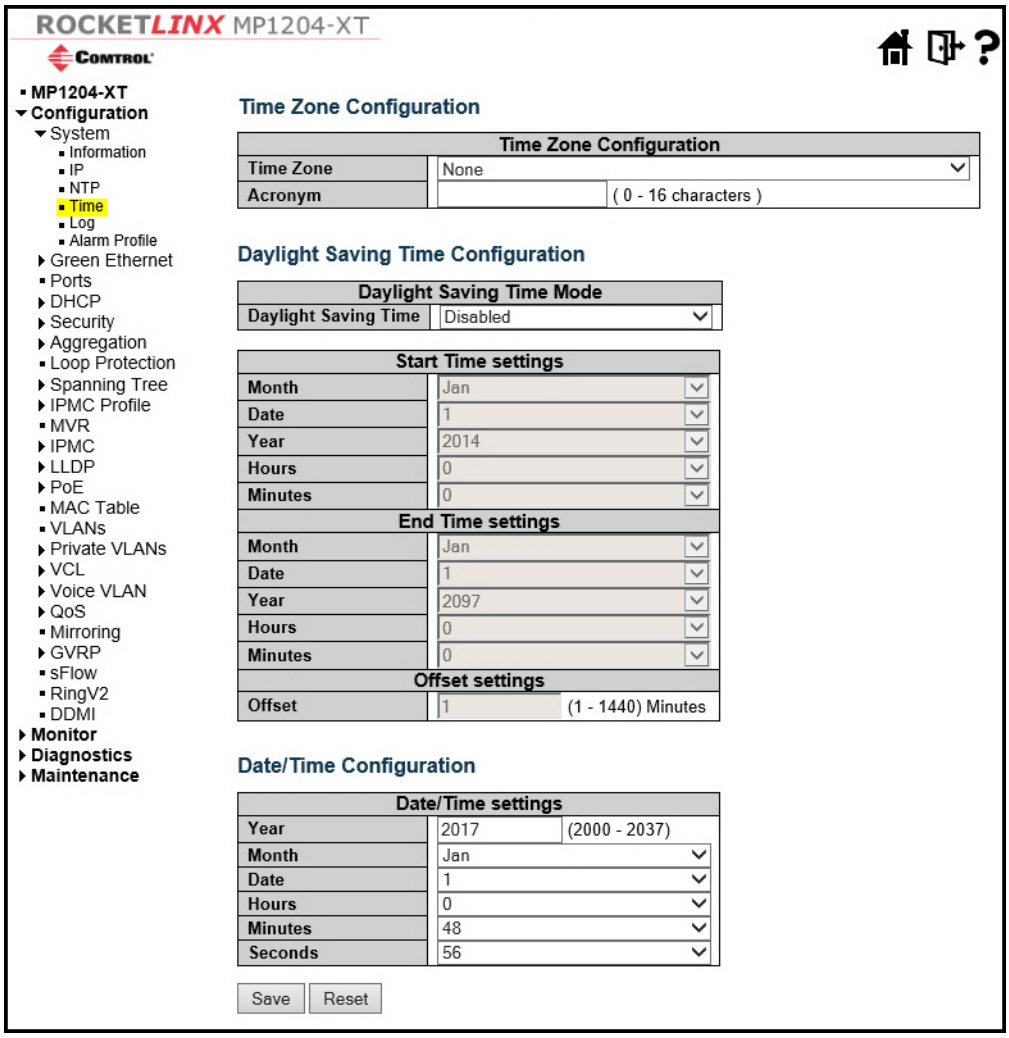


Item	Configuration | System | NTP
Mode	Indicates the NTP mode operation. Possible modes are: • **Enabled**: Enable NTP client mode operation. • **Disabled**: Disable NTP client mode operation.

Item	Configuration | System | NTP (Continued)
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'.

System | Time

Use this page to configure the MP1204-XT time zone, daylight savings, and date.

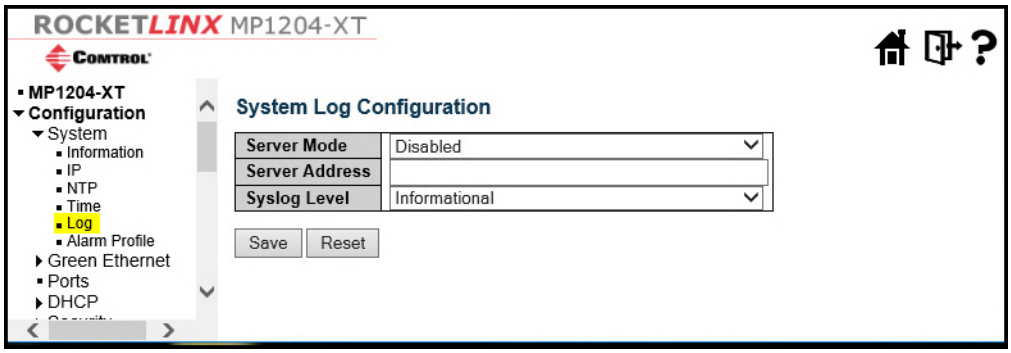


Item	Configuration | System | Time
Time Zone Configuration	
Time Zone	Lists various Time Zones worldwide. Select the appropriate Time Zone from the drop down and click **Save** to set.
Acronym	You can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range: Up to 16 characters)
Daylight Saving Time Configuration	
Daylight Saving Time	Use this option 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
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)

Item	Configuration | System | Time (Continued)
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)
Date/Time Configuration	
Date/Time Settings	
Year	Year of current date/time. (Range: 2000 to 2037)
Month	Month of current date/time.
Date	Date of current date/time.
Hours	Hour of current date/time.
Minutes	Minute of current date/time.
Seconds	Second of current date/time.

System | Log

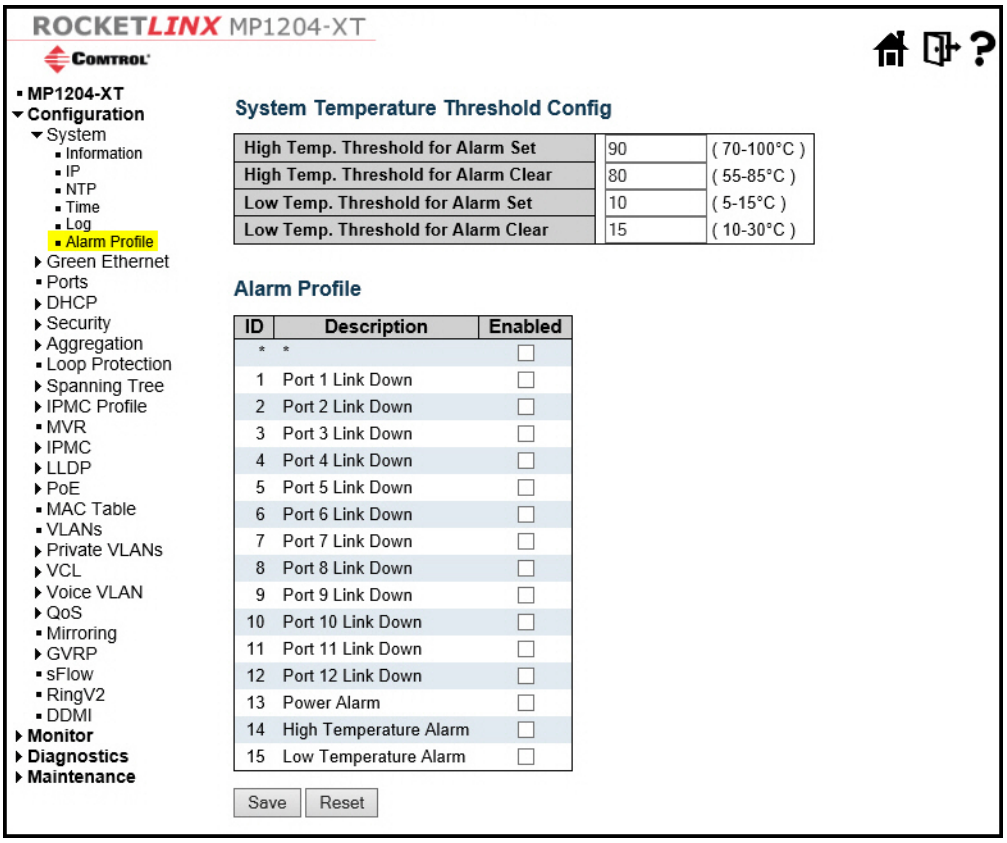
Use this page to configure the system log.



Item	Configuration | System | Log
Server Mode	Indicates the server mode operation. When the mode operation is enabled, the syslog message sends out to the syslog server. The syslog protocol is based on UDP communications and received on UDP port 514 and the syslog server does not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet always sends 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 the syslog server. If the switch supports DNS, it also can be a host name.
Syslog Level	Indicates what kind of message is sent to the syslog server. Possible modes are: • **Info**: Send informations, warnings and errors. • **Warning**: Send warnings and errors. • **Error**: Send errors.

System | Alarm Profile

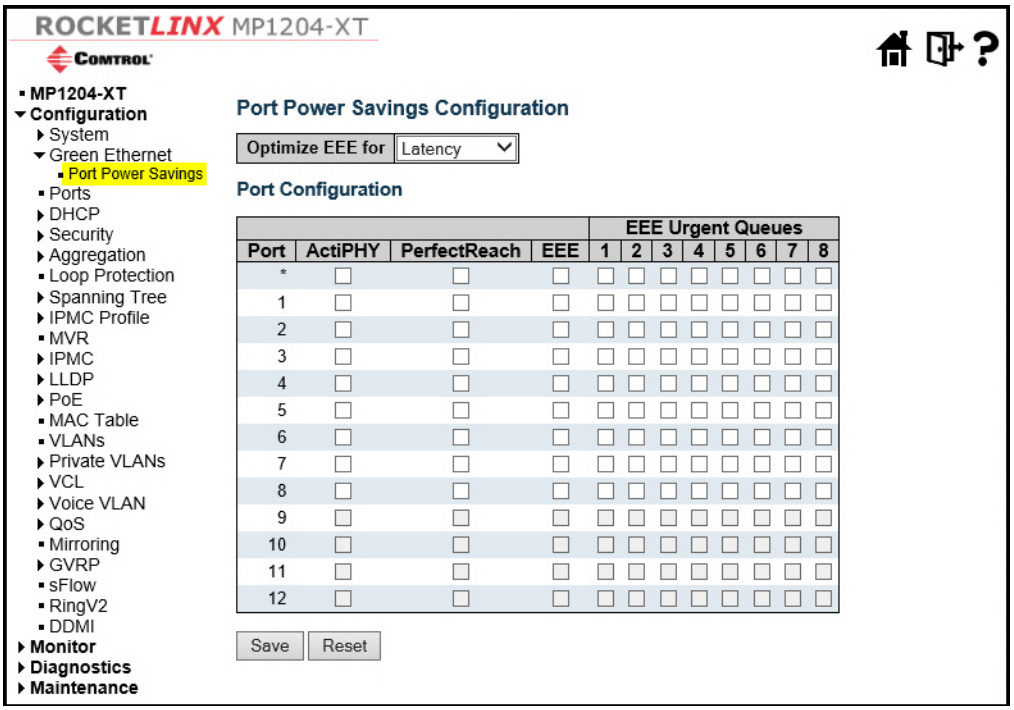
This page provides configuration to enable or disable the alarm.



Item	Configuration | System | Alarm Profile
ID	The identification of the Alarm Profile entry.
Description	Alarm Type Description.
Enabled	If alarm entry is **Enabled**, then the alarm is shown in the alarm history/current when it occurs. The Alarm LED is lit, the Alarm Relay is also enabled. SNMP trap are sent if any SNMP trap entry exists and enabled.
Disabled	If the alarm entry is **Disabled**, then the alarm is not be captured/shown in alarm history/current when an alarm occurs; then it does not trigger the Alarm LED change, Alarm Relay and SNMP trap either.
Note: *When any alarm exists, the Alarm LED is on (lighted), Alarm Output Relay is also enabled.*	

Configuration | Green Ethernet | Port Power Savings

Use this page to configure port power savings on the MP1204-XT.

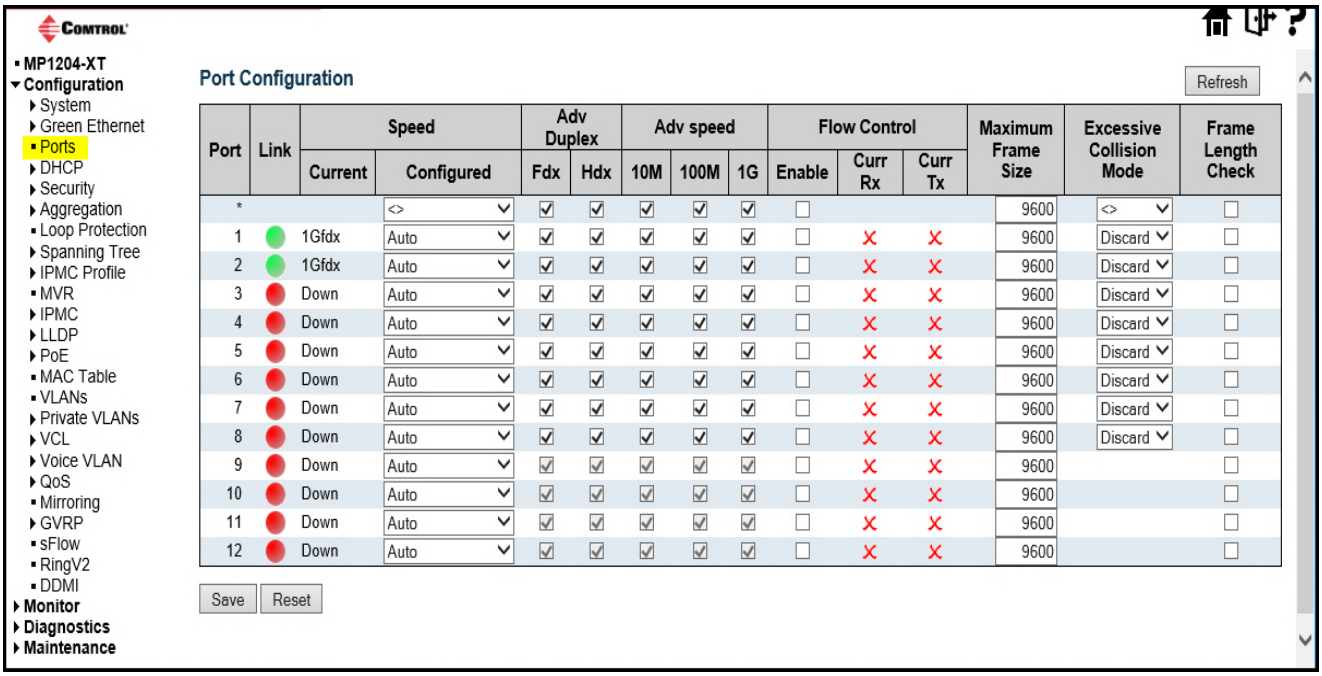


Item	Configuration | Green Ethernet| Power Savings
Port Power Savings Configuration	
Optimize EEE for	The MP1204-XT can be set to optimize EEE for either the best power savings or the least traffic latency.
Port Configuration	
Port	The MP1204-XT port number of the logical port.
ActiPHY	Link down power 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 the MP1204-XT port. For maximizing power savings, the circuit is not started immediately to transmit data ready for a port, but is instead queued until a burst of data is ready to be transmitted. This generates 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 marking the queue as an urgent queue. When an urgent queue gets the data transmitted, the circuits are powered up at once and the latency is reduced to the wakeup time.

Item	Configuration | Green Ethernet| Power Savings (Continued)
EEE Urgent Queues	Queues set activate transmission of frames as soon as data is available. Otherwise, the queue postpones transmission until a burst of frames can be transmitted.

Configuration | Ports

This page displays the current port configurations. You can also configure ports .



Item	Configuration | Ports
Port	This is the logical port number for this row.
Link	The current link state is displayed graphically. Green indicates that the link is up and red that it is down.
Current Link Speed	Provides the current link speed of the port.

Item	Configuration | Ports (Continued)
Configured Link Speed	Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are: • **Disabled** - Disables the MP1204-XT 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.
Flow Control	When **Auto Speed** is selected on a port, this section indicates the flow control capability that is advertised to the link partner. 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. Check the configured column to use flow control. This setting is related to the setting for **Configured Link Speed**.
Maximum Frame Size	Enter the maximum frame size allowed for the MP1204-XT port, including FCS.
Excessive Collision Mode	Configure port transmit collision behavior. • **Discard**: Discard frame after 16 collisions (default). • **Restart**: Restart back-off algorithm after 16 collisions.

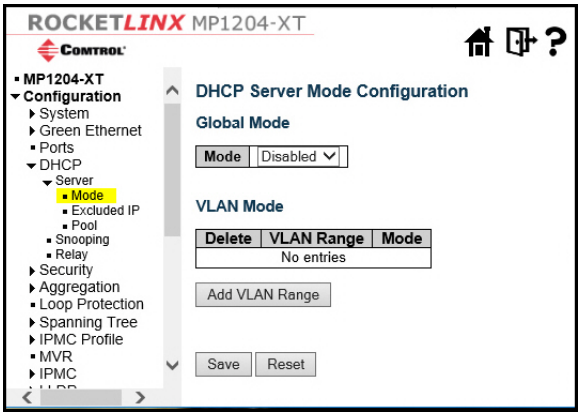
Configuration | DHCP | Menus

DHCP menus include:

- *DHCP | Server | Mode* on Page 49
- *DHCP | Server | Excluded IP* on Page 50
- *DHCP | Server | Pool* on Page 51
- *DHCP | Snooping* on Page 52
- *DHCP | Relay* on Page 53

DHCP | Server | Mode

Use this page to configure global mode and VLAN mode to enable or disable the DHCP server per system and per VLAN.

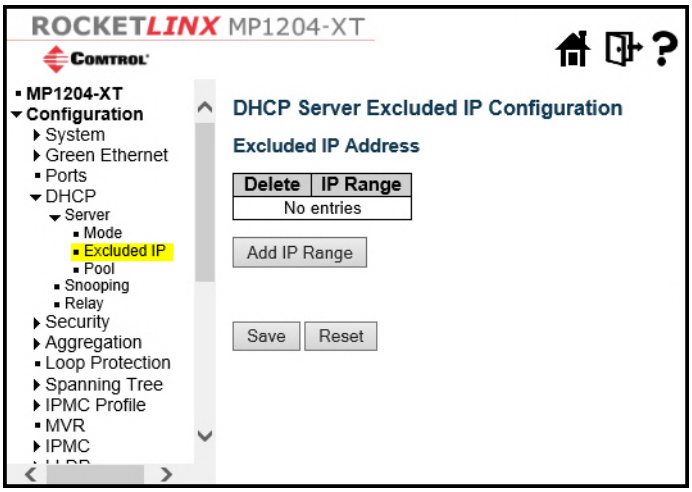


Item	Configuration | DHCP | Server | Mode
Global Mode	
Mode	Configure the operation mode per system. Possible modes are: • **Enabled**: Enable DHCP server per system • **Disabled**: Disable DHCP server per system.
VLAN Mode	
VLAN Range	Indicates the VLAN range in which the DHCP server is enabled or disabled. 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 enter it into either one of the first and second VLAN ID or both. If you want to disable an existing VLAN range, then you can follow the steps. 1. Press the **Add VLAN Range** button to add a new VLAN range. 2. Enter the VLAN range that you want to disable. 3. Choose the **Mode** option to be **Disabled**. 4. Press the **Save** button to apply the change. Note that the disabled VLAN range is removed from the **DHCP Server Mode Configuration** page.

Item	Configuration | DHCP | Server | Mode (Continued)
Mode	Indicates the operation mode per VLAN. Possible modes are: • **Enabled**: Enable DHCP server per VLAN. • **Disabled**: Disable DHCP server per VLAN.
Add VLAN Range	Click to add a new VLAN range.

DHCP | Server | Excluded IP

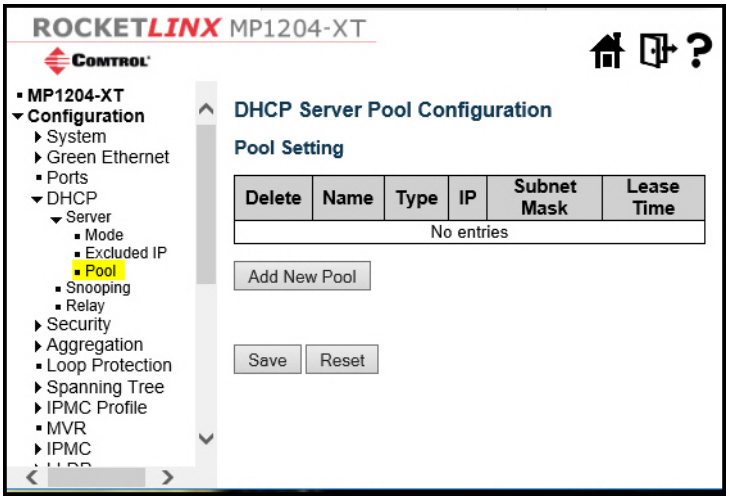
This page configures excluded IP addresses. The DHCP server does not allocate these excluded IP addresses to DHCP client.



Item	Configuration | DHCP | Server | Excluded IP
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 one 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 excluded IP address range.

DHCP | Server | Pool

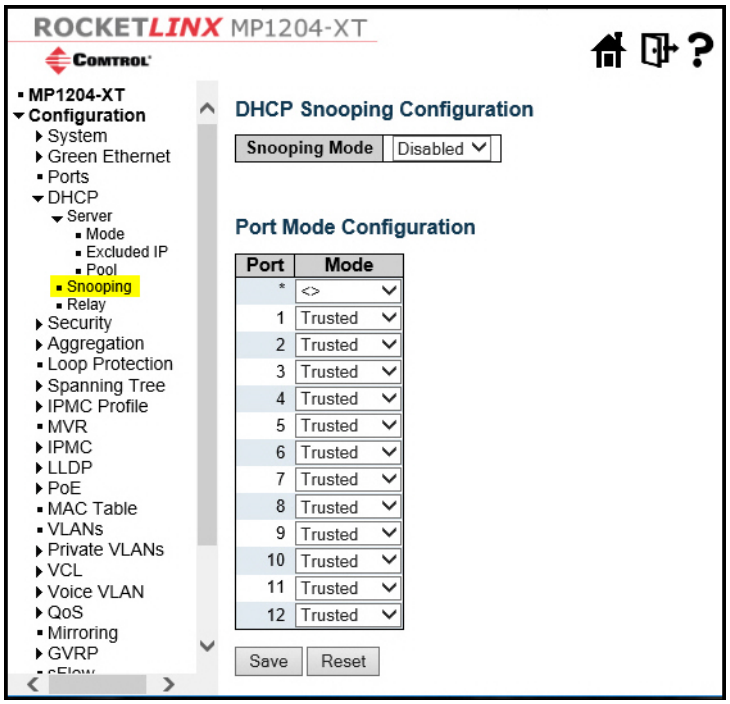
This page manages DHCP pools. According to the DHCP pool, the DHCP server allocates an IP address and delivers configuration parameters to the DHCP client.



Item	Configuration | DHCP | Server | Pool
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	Displays which type of the pool it 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	Displays the network number of the DHCP address pool. If - is displayed, it means not defined.
Subnet Mask	Displays the subnet mask of the DHCP address pool. If - is displayed, it means not defined.
Lease Time	Displays the lease time of the pool.
Add New Pool	Click to add a new DHCP pool.

DHCP | Snooping

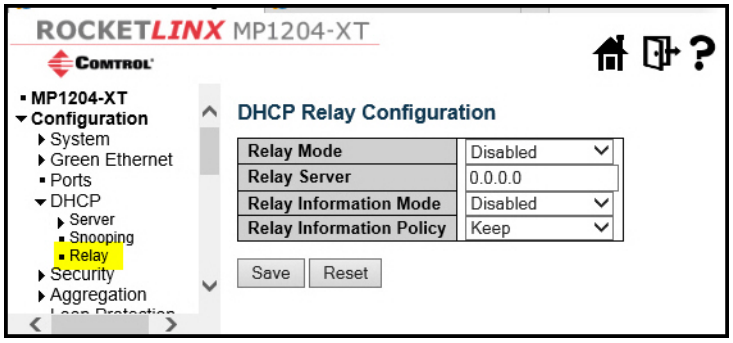
Use this page to configure DHCP snooping.



Item	Configuration | DHCP | Snooping
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 request messages are 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.

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 that the switch configuration of VLAN interface IP address and PVID (Port VLAN ID) are correct.



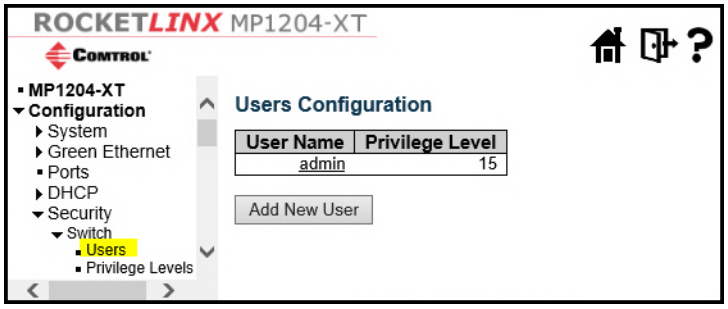
Item	Configuration | DHCP | Relay
Relay Mode	Indicates the DHCP relay mode operation. Possible modes are: • **Enabled**: Enable the DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. The DHCP broadcast message is not 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 (0), and the last two characters are the port number. For example, **00030108** means that the DHCP message was received from VLAN ID 3, switch ID 1, port No The Option 82 remote ID value is equal the switch MAC address. Possible modes are: • **Enabled**: Enable the 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 enforces the policy. The **Replace** policy is invalid when relay information mode is disabled. Possible policies are: • **Replace**: Replaces the original relay information when a DHCP message that already contains it is received. • **Keep**: Keeps the original relay information when a DHCP message that already contains it is received. • **Drop**: Drops the package when a DHCP message that already contains relay information is received.

Configuration | Security | Switch Menus

This subsection discusses the following pages:

Security | Switch | Users

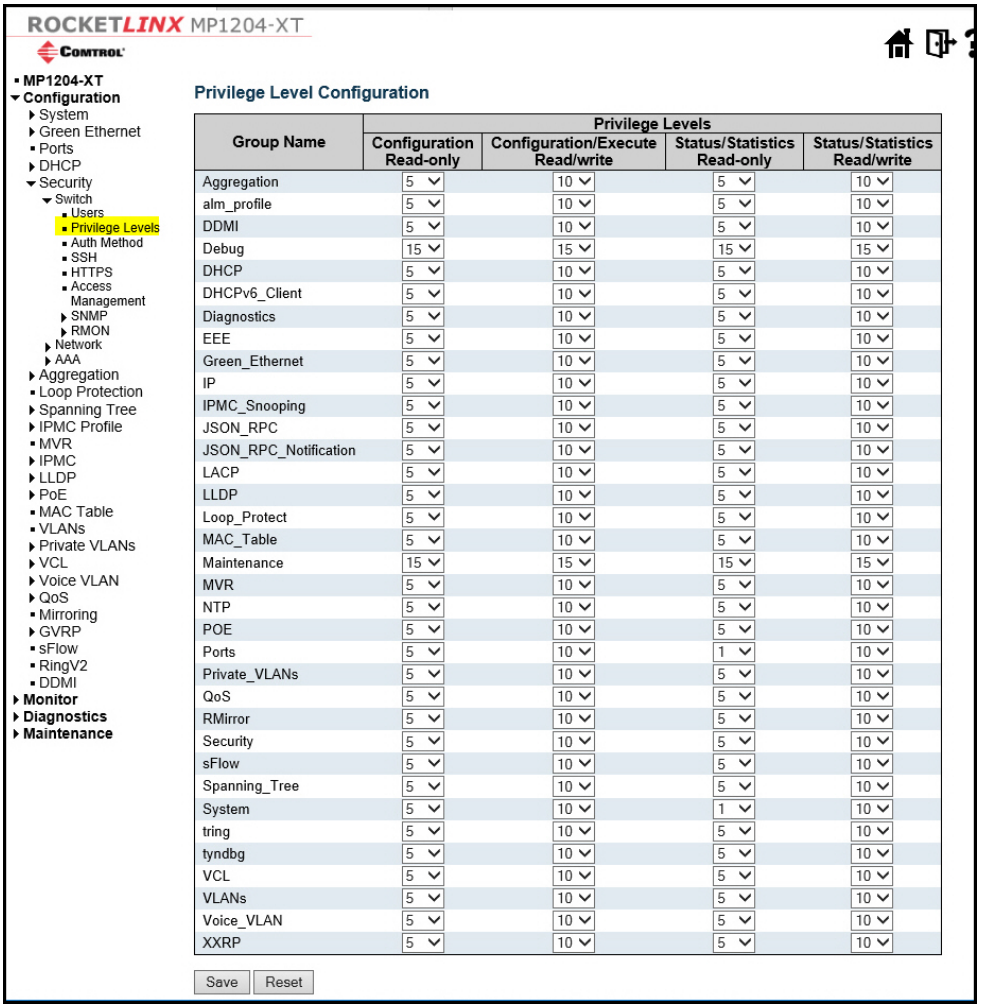
This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.



Item	Configuration | Security| Switch | Users
User Name	A string identifying the user name to which this entry should belong. 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 is 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, that is: 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 groups 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.
Delete User	Click the link for the user that you want to delete and the **Edit User** page appears. Click the **Delete User** button.

Security | Switch | Privilege Levels

This page provides an overview of the user privilege levels.



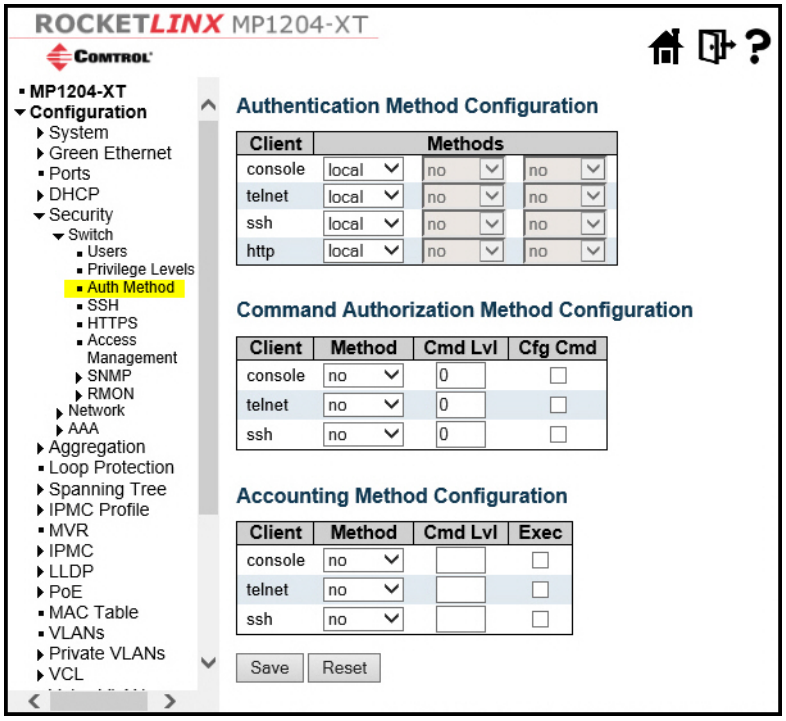
Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
alm_profile	5	10	5	10
DDMI	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
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
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
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
tring	5	10	5	10
tyndbg	5	10	5	10
VCL	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10
XXRP	5	10	5	10

Item	Configuration | Security| Switch | Privilege Levels
Group Name	The name identifying the privilege group. In most cases, a privilege level group consists of a single module (for example: LACP, RSTP or QoS), but a few of them contain 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 subgroups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (for example, clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

Security | Switch | Auth Method

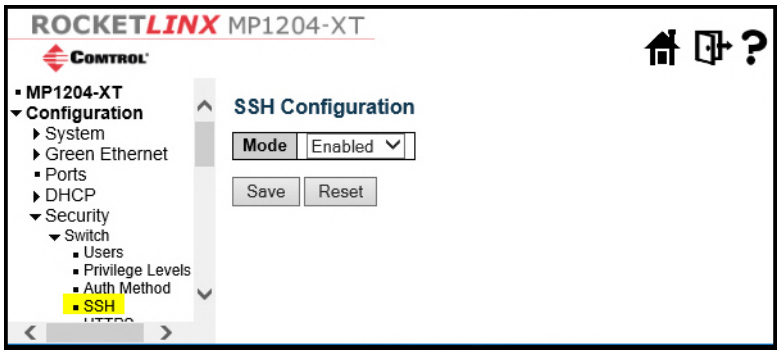
This page allows you to configure how a user is authenticated when he logs into the MP1204-XT via one of the management client interfaces.



Item	Configuration | Security| Switch | Auth Method
Client	The management client for which the configuration below applies.
Methods	Method can be set to one of the following values: • **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. Methods that involve remote servers are timed out if the remote servers are off-line. 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 enables the management client to login via the local user database if none of the configured authentication servers are alive.

Security | Switch | SSH

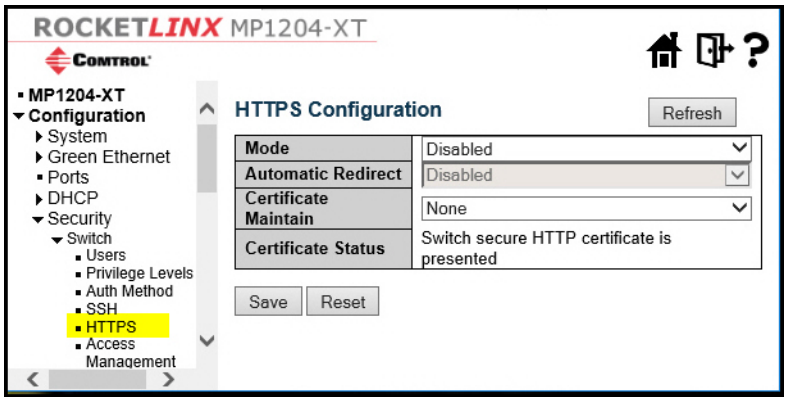
Use this page to configure SSH for the MP1204-XT.



Item	Configuration | Security| Switch | SSH
Mode	Indicates the SSH mode operation. Possible modes are: **Enabled**: Enable SSH mode operation. **Disabled**: Disable SSH mode operation.

Security | Switch | HTTPS

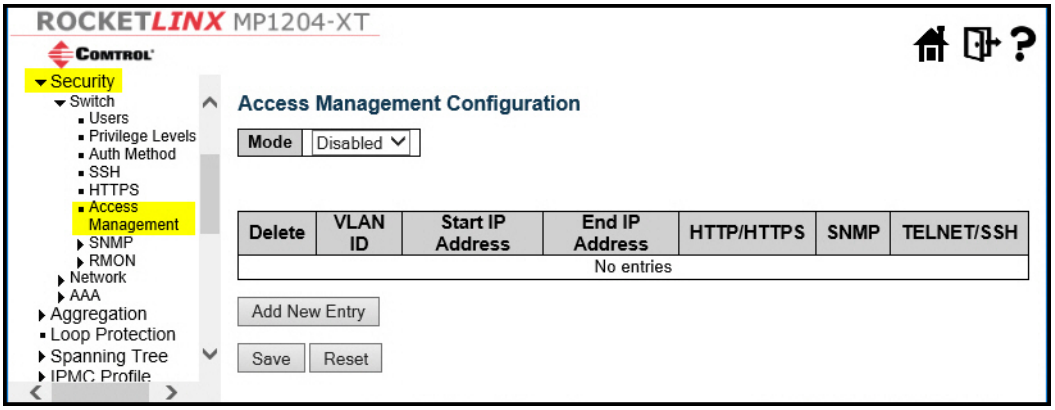
Use this page to configure https on the MP1204-XT.



Item	Configuration | Security| Switch | HTTPS
Mode	Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation automatically redirects 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.

Security | Switch | 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 allows access to the MP1204-XT.



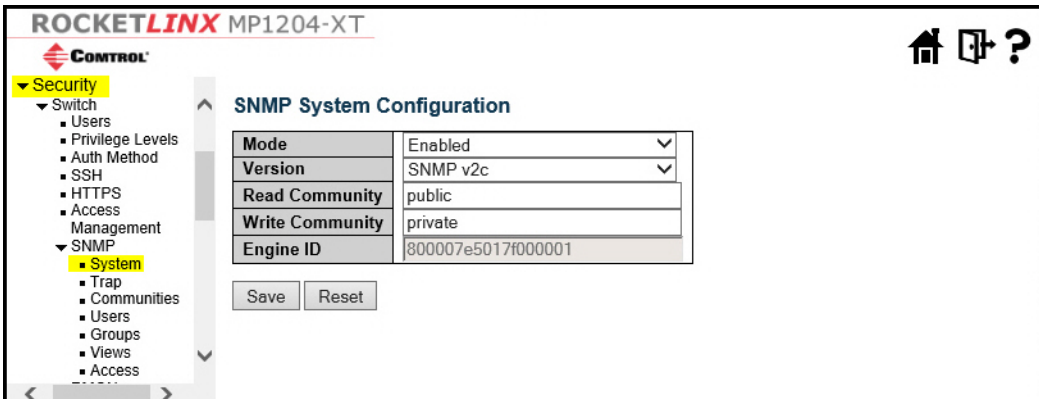
Item	Configuration | Security| Switch | Access Management
Mode	Indicates the access management mode operation. Possible modes are: • **Enabled**: Enable access management mode operation. • **Disabled**: Disable access management mode operation.
Delete	Check to delete the entry. It is deleted during the 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 MP1204-XT 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 MP1204-XT 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 MP1204-XT from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.
Add New Entry	Click to add a new access management entry.

Security | Switch | SNMP Menus

This subsection discusses **SNMP** menus under the **Security | Switch** menu.

Security | Switch | SNMP | System

Use this page to configure SNMP.

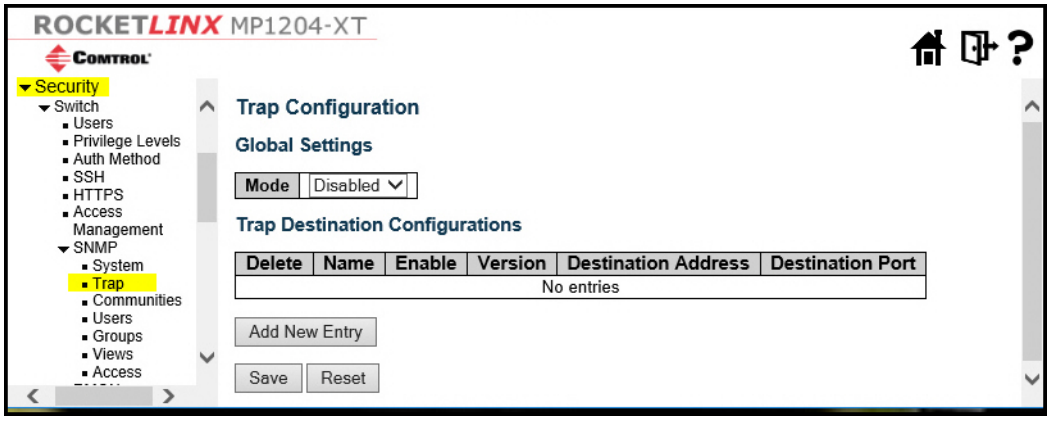


Item	Configuration | Security| Switch | SNMP | System
Mode	Indicates the SNMP mode operation. Possible modes are: • **Enabled**: Enable SNMP mode operation. • **Disabled**: Disable SNMP mode operation.
Version	Indicates the SNMP supported version. Possible versions are: • **SNMP v1**: Set SNMP supported 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. This field is applicable only when the SNMP version is SNMPv1 or SNMPv2c. If the SNMP version is SNMPv3, the community string is 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.

Item	Configuration | Security| Switch | SNMP | System (Continued)
Write Community	Indicates the community write 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. This field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If the SNMP version is SNMPv3, the community string is 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 clears all original local users.

Security | Switch | SNMP | Trap

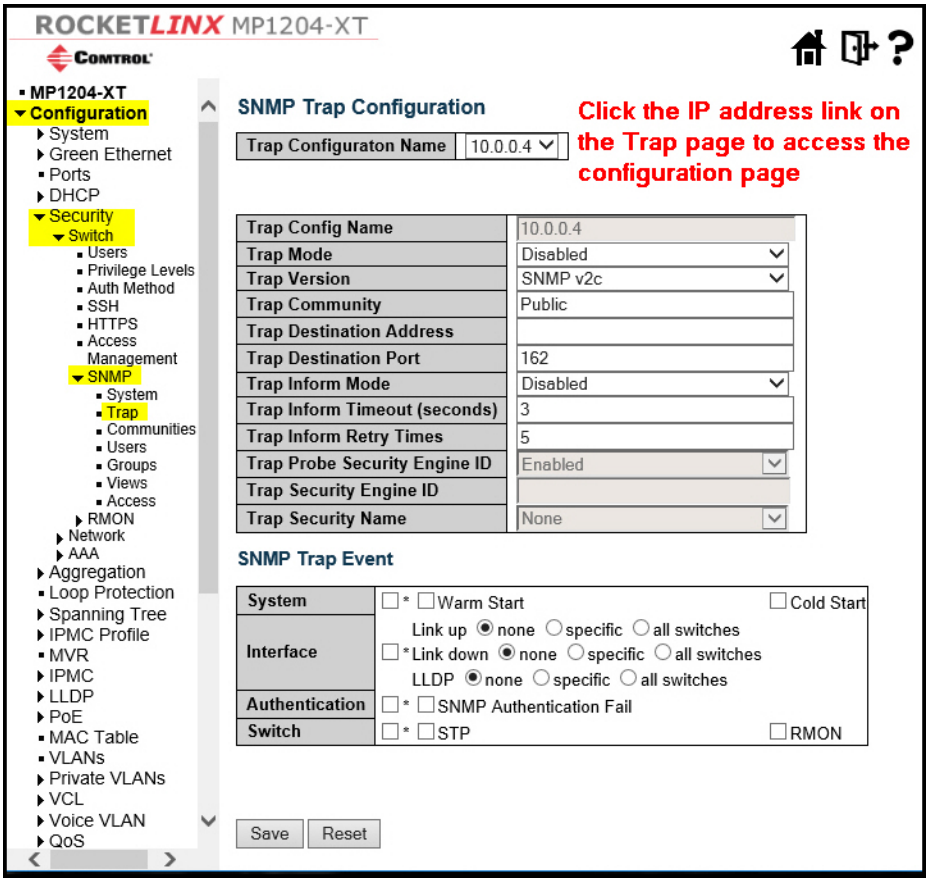
Use this page to configure SNMP traps.



Object	Configuration | Security| Switch | SNMP | Trap
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 the SNMP trap to the supported version 1. • **SNMPv2c**: Set the SNMP trap to the supported version 2c. • **SNMPv3**: Set the SNMP trap to the supported version 3.

Object	Configuration | Security| Switch | SNMP | Trap (Continued)
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 allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Z, a-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, '::192.1.2.34'.
Destination port	Indicates the SNMP trap destination port. SNMP Agent sends SNMP message through this port, the port range is 1~65535.
Add New Entry	Add a new user.

The **SNMP Trap Configuration** page includes the following fields.

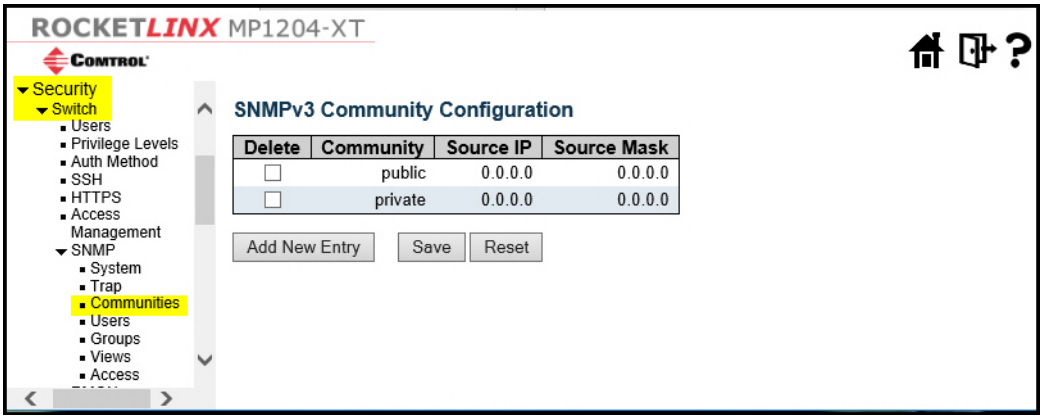


Item	Configuration | Security| Switch | SNMP | Trap Configuration
Trap Mode	Indicates the SNMP trap mode operation. Possible modes are: • **Enabled**: Enable SNMP trap mode operation. • **Disabled**: Disable SNMP trap mode operation.
Trap Version	Indicates the SNMP trap to the supported version. Possible versions are: • **SNMP v1**: Set the SNMP trap to the supported version 1. • **SNMP v2c:** Set the SNMP trap to the supported version 2c. • **SNMP v3**: Set the SNMP trap to the supported version 3.
Trap Community	Indicates the community access string when sending an 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'). It also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Z, a-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.

Item	Configuration | Security| Switch | SNMP | Trap Configuration
Trap Destination IPv6 Address	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, '::192.1.2.34'.
Trap Authentication Failure	Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible modes are: • **Enabled**: Enable SNMP trap authentication failure. • **Disabled**: Disable SNMP trap authentication failure.
Trap Link-up and Link-down	Indicates the SNMP trap link-up and link-down mode operation: • **Enabled**: Enable SNMP trap link-up and link-down mode operation. • **Disabled**: Disable SNMP trap link-up and link-down mode operation.
Trap Inform Mode	Indicates the SNMP trap inform mode operation. Possible modes are: • **Enabled**: Enable SNMP trap inform mode operation. • **Disabled**: Disable SNMP trap inform mode operation.
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 inform 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 is 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.
Add New Entry	Click to add a new user.

Security | Switch | SNMP | Communities

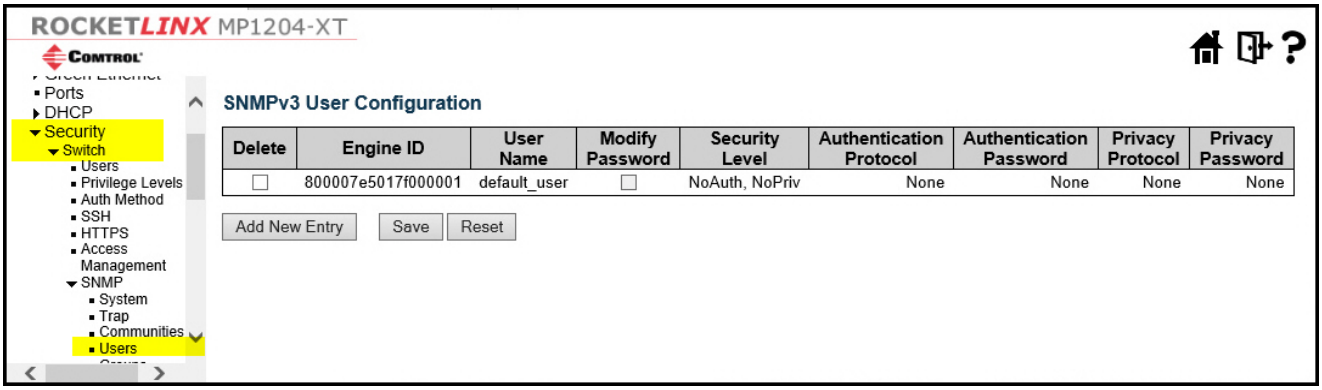
Configure SNMPv3 community table on this page. The entry index key is **Community**.



Item	Configuration | Security| Switch | SNMP | Communities
Delete	Check to delete the entry. It is 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 is treated as a security name and maps 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.
Add New Entry	Click to add a new community entry.

Security | Switch | SNMP | Users

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

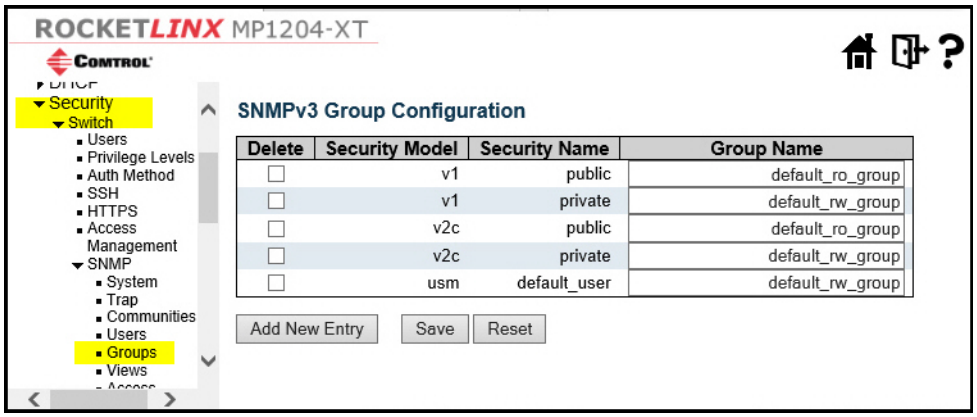


Item	Configuration | Security| Switch | SNMP | Users
Delete	Check to delete the entry. It is deleted during the next save.
Engine ID	An octet string identifying the engine ID to which this entry should belong. The string must contain an even number (in hexadecimal format) with number of digits between 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 the user engine ID equals the system engine ID then it is a local user; otherwise it's a remote user.
User name	A string identifying the user name to which this entry should belong. 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 to which this entry should belong. Possible security modes 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 to which this entry should belong. 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.

Item	Configuration | Security| Switch | SNMP | Users (Continued)
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 to which this entry should belong. 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.
Add New Entry	Click to add a new user entry.

Security | Switch | SNMP | Groups

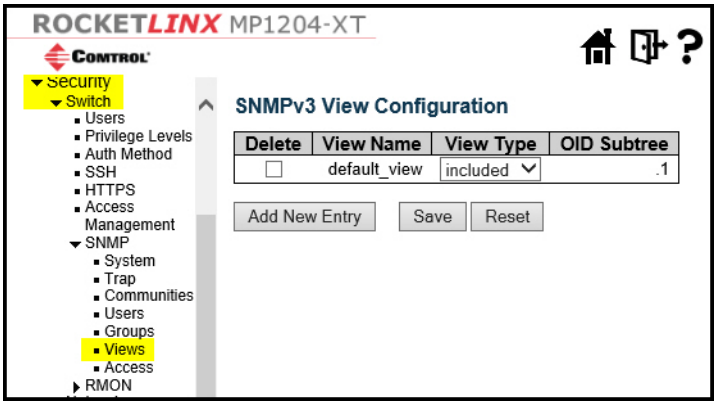
Configure the SNMPv3 group table on this page. The entry index keys are **Security Model** and **Security Name**.



Item	Configuration | Security| Switch | SNMP | Groups
Delete	Check to delete the entry. It is deleted during the next save.
Security Model	Indicates the security model to which this entry should belong. 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 to which this entry should belong. 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 to which this entry should belong. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Add New Entry	Click to add a new group entry.

Security | Switch | SNMP | Views

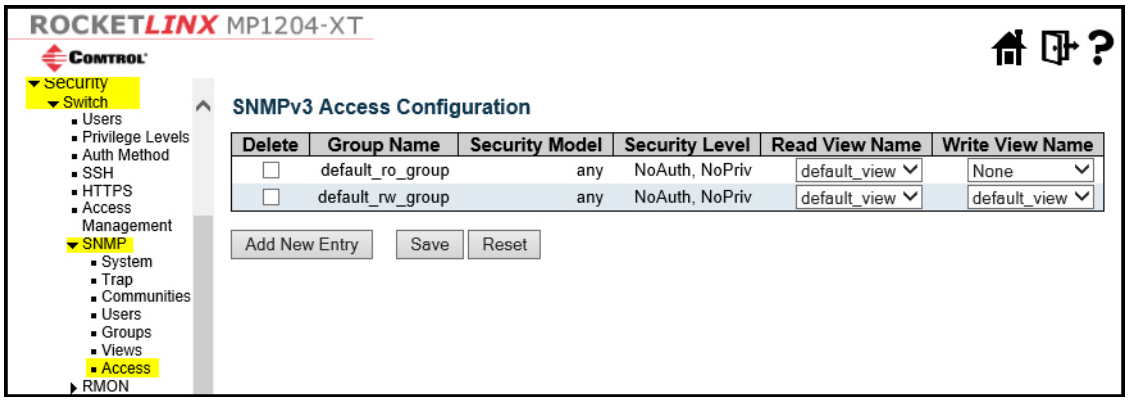
Use this page to configure the SNMPv3 view table. The entry index keys are **View Name** and **OID Subtree.**



Item	Configuration | Security | Switch | SNMP | Views
Delete	Check to delete the entry. It is 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 it's 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 (*).
Add New Entry	Click to add a new user.

Security | Switch | SNMP | Access

You can configure SNMPv3 access table on this page. The entry index keys are **Group Name**, **Security Model** and **Security Level**.



Item	Configuration | Security | Switch | SNMP | Access
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.
Add New Entry	Click to add a new view entry.

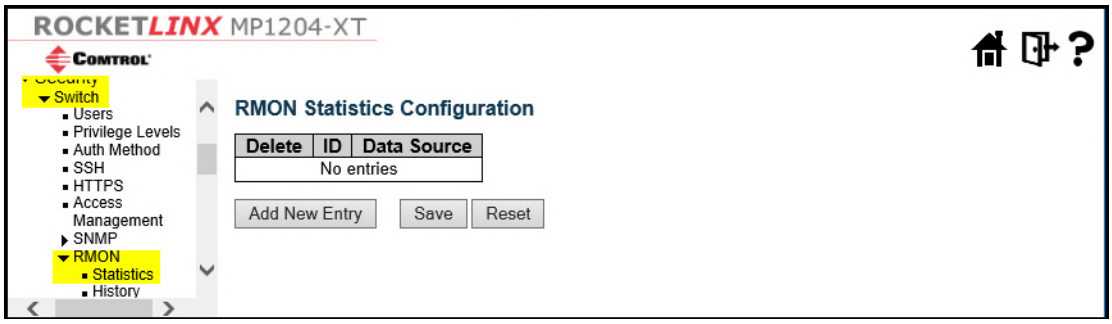
Security | Switch | RMON Menus

This subsection discusses **RMON** menus under the **Security | Switch | RMON** menu.

- *Security | Switch | RMON | Statistics* on Page 70
- *Security | Switch | RMON | History* on Page 71
- *Security | Switch | RMON | Alarm* on Page 72
- *Security | Switch | RMON | Event* on Page 73

Security | Switch | RMON | Statistics

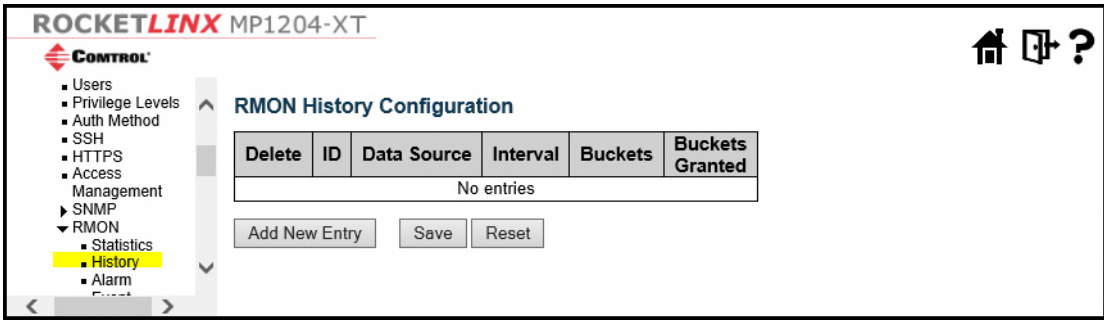
Use this page to configure the RMON Statistics table. The entry index key is **ID**.



Item	Configuration | Security | Switch | RMON | Statistics
Delete	Check to delete the entry. It is 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. If in stacking switch, the value must add 1000000* (switch ID), for example, if the port is Switch 1 Port 5, the value is 1000005; if the port is Switch 2 Port 5, the value is 2000005.
Add New Entry	Add an RMON ID.

Security | Switch | RMON | History

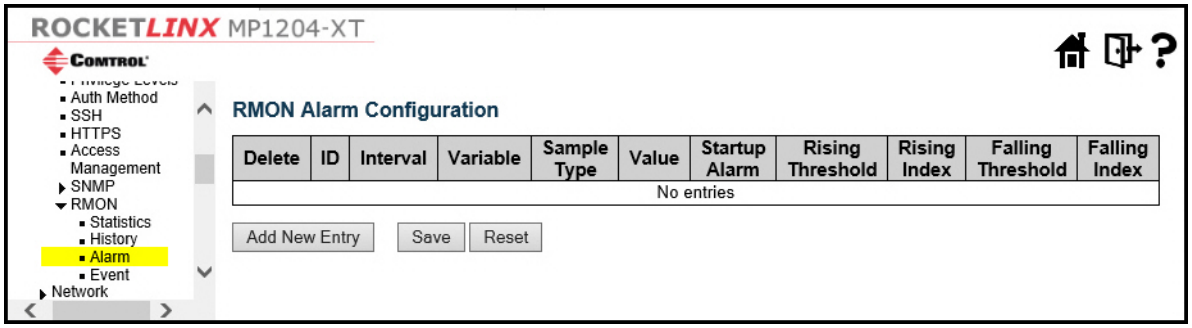
Use this page to configure RMON History table. The entry index key is **ID**.



Item	Configuration | Security | Switch | RMON | History
Delete	Check to delete the entry. It is 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. If in stacking switch, the value must add 1000* (switch ID-1), for example, if the port is Switch 3 Port 5, the value is 2005.
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.
Add New Entry	Click to add a new view entry.

Security | Switch | RMON | Alarm

Use this page to configure the **RMON Alarm** table. The entry index key is **ID**.

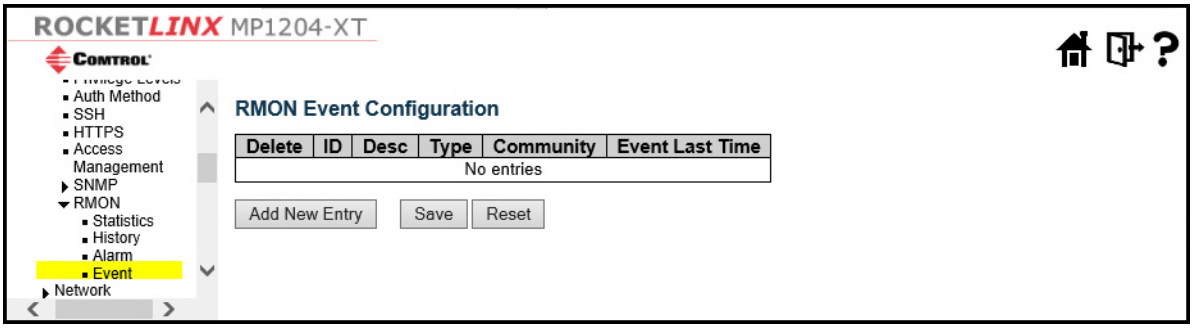


Item	Configuration | Security | Switch | RMON | Alarm
Delete	Check to delete the entry. It is deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range 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 broadcast and multicast packets that request to transmit. • **OutDiscards**: The number of outbound packets that are discarded event the packets is 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.

Item	Configuration | Security | Switch | RMON | Alarm (Continued)
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 to 2147483647).
Rising Index	Rising event index (1 to 65535).
Falling Threshold	Falling threshold value (-2147483648 to 2147483647)
Falling Index	Falling event index (1 to 65535).
Add New Entry	Click to add a new access entry.

Security | Switch | RMON | Event

Use this page to configure the RMON Event table. The entry index key is **ID**.



Item	Configuration | Security | Switch | RMON | Event
Delete	Check to delete the entry. It is 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.

Item	Configuration | Security | Switch | RMON | Event (Continued)
Add New Entry	Click to add a new community entry.

Configuration | Security | Network Menus

This subsection discusses **Network** menus and pages under the **Configuration | Security | Network** menu.

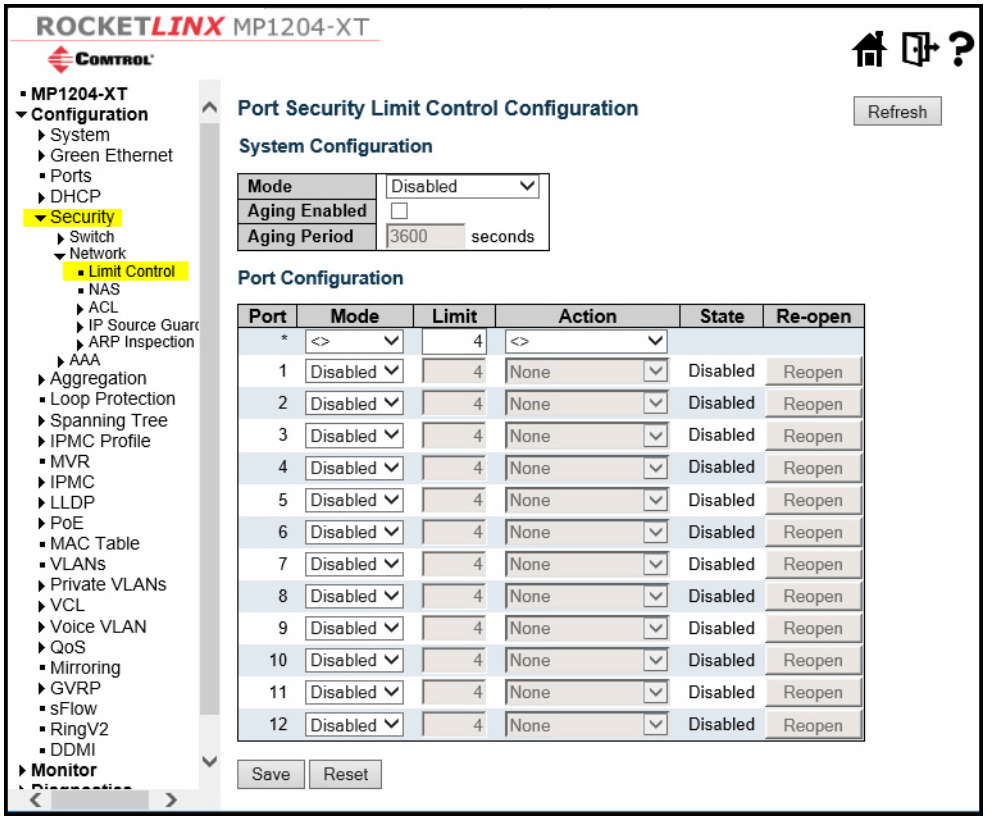
Security | Network | Limit Control

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 the table 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.



Item	Configuration | Security | Network | Limit Control
System Configuration	
Mode	Indicates if Limit Control is globally enabled or disabled on the MP1204-XT. 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 modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security uses 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 the MP1204-XT on which Limit Control is enabled. The end-host is allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it was not for aging, the end-host would still take up resources on the MP1204-XT and is 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 MP1204-XT 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 MP1204-XT.
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. Note 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 MP1204-XT 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.

Item	Configuration | Security | Network | Limit Control (Continued)
Action	If **Limit** is reached, the MP1204-XT can take one of the following actions: • **None**: Do not allow more than Limit MAC addresses on the port, but take no further action. • **Trap**: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If **Aging** is disabled, only one SNMP trap is sent, but with **Aging** enabled, new SNMP traps are 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 are removed from the port, and no new address are learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port remains shut down. There are three ways to re-open the port: 1. Reboot the switch, 2. Disable and re-enable Limit Control on the port or the MP1204-XT, 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 are 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 the **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 is only enabled if this is the case. For other methods, refer to **Shutdown** in the **Action** section. ***Note:*** *Clicking the reopen button causes the page to be refreshed, so non-committed changes are lost.*

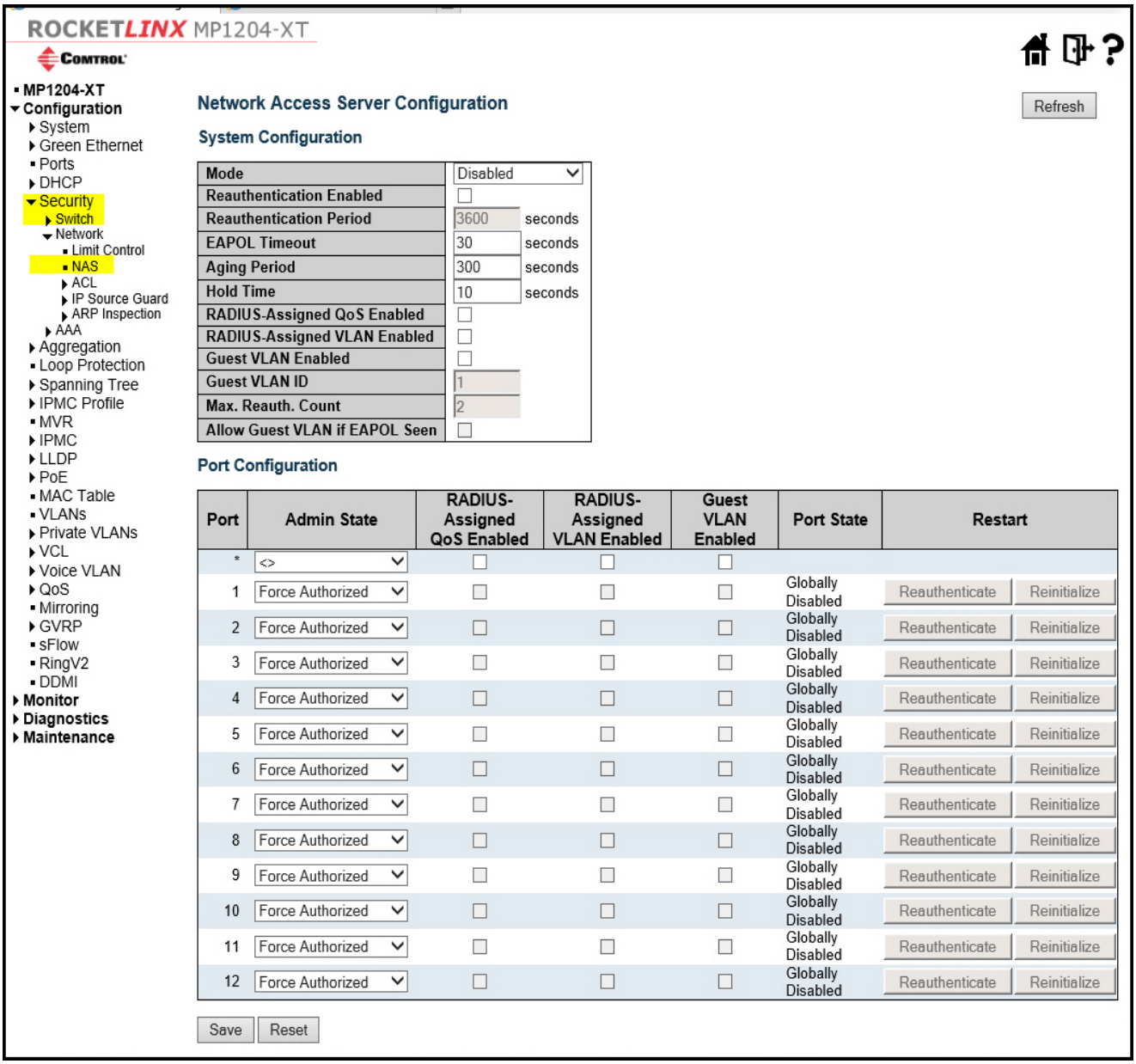
Security | Network | NAS

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 does not require the user to have special 802.1X supplicant software installed on their system. The MP1204-XT 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.



Item	Configuration | Security | Network | NAS
System Configuration	
Mode	Indicates if NAS is globally enabled or disabled on the MP1204-XT. If globally disabled, all of the 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 does not 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.
Aging Period	This setting applies to the following modes, that is, modes using the Port Security functionality to secure MAC addresses: • Single 802.1X • Multi 802.1X • MAC-Based Auth. 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. 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 get removed upon the next reauthentication, which fails. But if reauthentication is not enabled, the only way to free resources is by aging the entries. For ports in MAC-based Auth mode, reauthentication does not cause direct communication between the MP1204-XT and the client, so this does not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

Item	Configuration | Security | Network | NAS (Continued)
Hold Time	This setting applies to the following modes, that is, modes using the Port Security functionality to secure MAC addresses: • Single 802.1X • Multi 802.1X • MAC-Based Auth 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. In MAC-based Auth mode, the MP1204-XT ignores new frames coming from the client during the hold time. The **Hold Time** can be set to a number between 10 and 1000000 seconds.
RADIUS-Assigned QoS Enabled	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). The **RADIUS-Assigned QoS Enabled** check box provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports copy settings determined whether **RADIUS-assigned QoS Class** is enabled on that port. When unchecked, **RADIUS-server assigned QoS Class** is disabled on all ports.
RADIUS-Assigned VLAN Enabled	RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic is 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). The **RADIUS-Assigned VLAN Enabled** check box provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports copy settings determined whether **RADIUS-assigned VLAN** is enabled on that port. When unchecked, **RADIUS-server assigned VLAN** is disabled on all ports.
Guest VLAN Enabled	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 MP1204-XT follows a set of rules for entering and leaving the Guest VLAN as listed below. The **Guest VLAN Enabled** check box provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports copy settings determined whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.
Guest VLAN ID	This is the value that a ports **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].
Max. Reauth. Count	The number of times the MP1204-XT 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].

Item	Configuration | Security | Network | NAS (Continued)
Allow Guest VLAN if EAPOL Seen	The MP1204-XT remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the MP1204-XT considers whether to enter the Guest VLAN, it first checks to see if this option is enabled or disabled. If disabled (unchecked; default), the MP1204-XT only enters 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 MP1204-XT considers 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.
Port Configuration	
Port	The port number for which the configuration below applies.
Admin State	If NAS is globally enabled, this selection controls the ports authentication mode. The following modes are available: • **Force Authorized** In this mode, the MP1204-XT sends one EAPOL Success frame when the port link comes up, and any client on the port is allowed network access without authentication. • **Force Unauthorized** In this mode, the MP1204-XT sends one EAPOL Failure frame when the port link comes up, and any client on the port is disallowed network access. • **Port-based 802.1X** In the 802.1X-world, the user is called the supplicant, the MP1204-XT 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 MP1204-XT 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 supplicants 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 MP1204-XT) does not 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. 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 MP1204-XT uses it to open up or block traffic on the switch port connected to the supplicant. ***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 never gets authenticated, because the switch cancels on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. Since the server has not yet failed (because the X seconds have not expired), the same server is contacted upon the next backend authentication server request from the switch. This scenario loops forever. Therefore, the server timeout should be smaller than the supplicants EAPOL Start frame retransmission rate.*

Item	Configuration | Security | Network | NAS (Continued)
Admin State (continued)	• **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 are not authenticated. To overcome this security breach, use the Single 802.1X variant. 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 MP1204-XT. If more than one supplicant is connected to a port, the one that comes first when the ports link comes up is the first one considered. If that supplicant does not provide valid credentials within a certain amount of time, another supplicant gets a chance. Once a supplicant is successfully authenticated, only that supplicant is allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicants MAC address once successfully authenticated. • **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. 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 MP1204-XT. Instead, the MP1204-XT uses the supplicants 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 MP1204-XT sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the **Port Security Limit Control** functionality.

Item	Configuration | Security | Network | NAS (Continued)
Admin State (continued)	• **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 MP1204-XT acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the MP1204-XT, which in turn uses the clients 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 MP1204-XT only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the MP1204-XT to open up or block traffic for that particular client, using the Port Security module. Only then are frames from the client be forwarded on the MP1204-XT. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients do not 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.
RADIUS-Assigned QoS Enabled	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 supplicants port is classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or its invalid, or the supplicant is otherwise no longer present on the port, the ports 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). This option is only available for single-client modes: • Port-based 802.1X • Single 802.1X 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 is considered, and to be valid, it must follow this rule: • All 8 octets in the attributes 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].

Item	Configuration | Security | Network | NAS (Continued)
RADIUS-Assigned VLAN Enabled	When **RADIUS-Assigned VLAN** is both globally enabled and enabled (checked) for a given port, the MP1204-XT 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 ports **Port VLAN ID** is changed to this VLAN ID, the port is set to be a member of that VLAN ID, and the port is forced into VLAN unaware mode. Once assigned, all traffic arriving on the port is 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 its invalid, or the supplicant is otherwise no longer present on the port, the ports 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). This option is only available for single-client modes: • Port-based 802.1X • Single 802.1X For troubleshooting 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. 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: • The T**unnel-Medium-Type**, **Tunnel-Type**, and **Tunnel-Private-Group-ID** attributes must all be present at least once in the Access-Accept packet. • The MP1204-XT looks for the first set of these attributes that have the same Tag value and fulfill the following requirements (if Tag == 0 is used, the **Tunnel-Private-Group-ID** does not need to include a **Tag**): • 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 0s are discarded. The final value must be in the range [1; 4095].

Item	Configuration | Security | Network | NAS (Continued)
Guest VLAN Enabled	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: • Port-based 802.1X • Single 802.1X • Multi 802.1X For troubleshooting 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. **Guest VLAN Operation:** When a Guest VLAN enabled ports link comes up, the MP1204-XT 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 MP1204-XT 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 is now be placed in the Guest VLAN. If disabled, the MP1204-XT first checks 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 ports **Admin State** is changed), and if not, the port is placed in the Guest VLAN. Otherwise it does not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by **EAPOL Timeout**. Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The MP1204-XT does not transmit an EAPOL Success frame when entering the Guest VLAN. While in the Guest VLAN, the MP1204-XT monitors the link for EAPOL frames, and if one such frame is received, the MP1204-XT 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 is never able to go back into the Guest VLAN if the **Allow Guest VLAN if EAPOL Seen** is disabled.
Port State	The current state of the port. It can undertake one of the following values: • **Globally Disabled**: NAS is globally disabled. • **Link Down**: NAS is globally enabled, but there is no link on the port. • **Authorized**: The port is in **Force Authorized** or a single-supplicant mode and the supplicant is authorized. • **Unauthorized**: The port is in **Force Unauthorized** or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. • **X Auth/Y Unauth**: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

Item	Configuration | Security | Network | NAS (Continued)
Restart	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the ports **Admin State** is in an EAPOL-based or MAC-based mode. Clicking these buttons do not cause settings changed on the page to take effect. • **Reauthenticate**: Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication is attempted immediately. The button only has effect for successfully authenticated clients on the port and does not cause the clients to get temporarily unauthorized. • **Reinitialize**: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients transfers to the unauthorized state while the reauthentication is in progress.

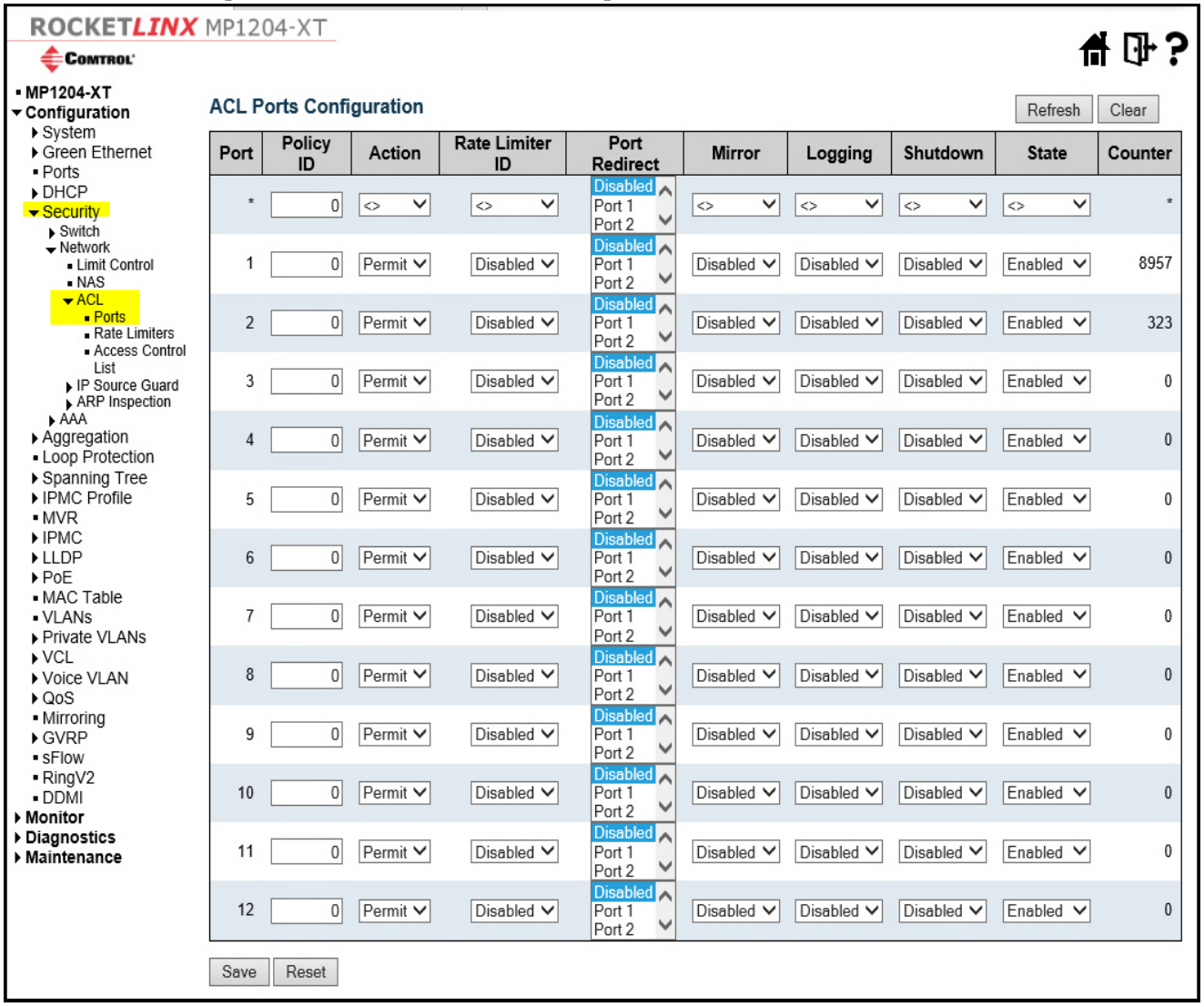
Security | Network | ACL Menus

The following pages are under the **ACL** menu.

- *Security | Network | ACL | Ports* on Page 87
- *Security | Network | ACL | Rate Limiters* on Page 89
- *Security | Network | ACL | Access Control List* on Page 90

Security | Network | ACL | Ports

Use this page to configure the ACL parameters (ACE) of each MP1204-XT port. These parameters affect frames received on a port unless the frame matches a specific ACE.



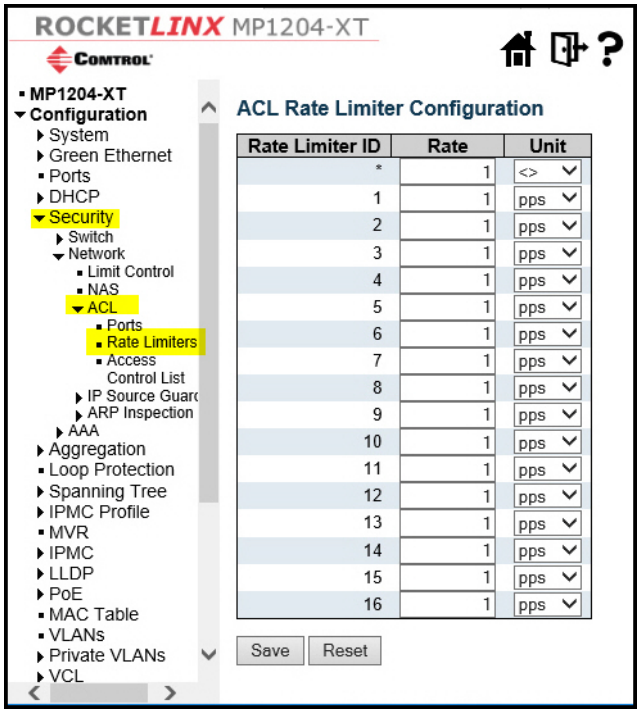
Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled / Port 1 / Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	8957
2	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	323
3	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
11	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
12	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0

Item	Configuration | Security | Network | ACL | Ports
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.

Item	Configuration | Security | Network | ACL | Ports (Continued)
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**.
Port Redirect	Select which port frames are redirected on. The allowed values are **Disabled** or a specific port number and it cannot 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 does not 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 are limited.*
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 is 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.

Security | Network | ACL | Rate Limiters

Use this page to configure the rate limiter for the ACL of the MP1204-XT.

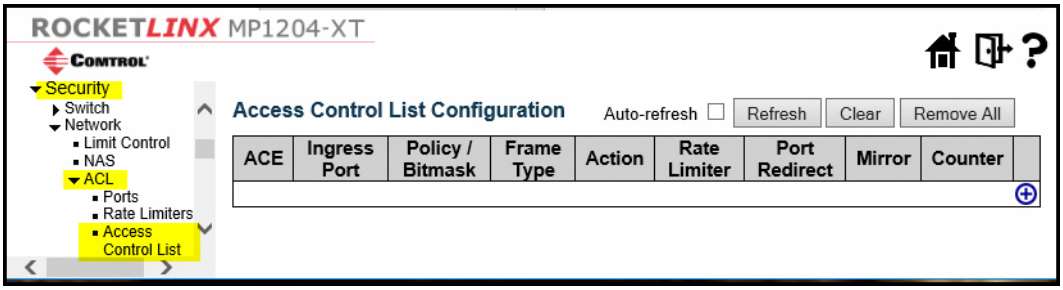


Item	Configuration | Security | Network |ACL | Rate Limiters
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate	The rate range is located 0-3276700 in pps. Or 0, 100, 200, 300, ..., 1000000 in kbps.
Unit	Specify the rate unit. The allowed values are: • **pps**: packets per second • **kbps**: Kbits per second

Security | Network | ACL | Access Control List

This page shows the Access Control List (ACL), which is made up of the ACEs defined on the MP1204-XT. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each MP1204-XT.

Click 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.



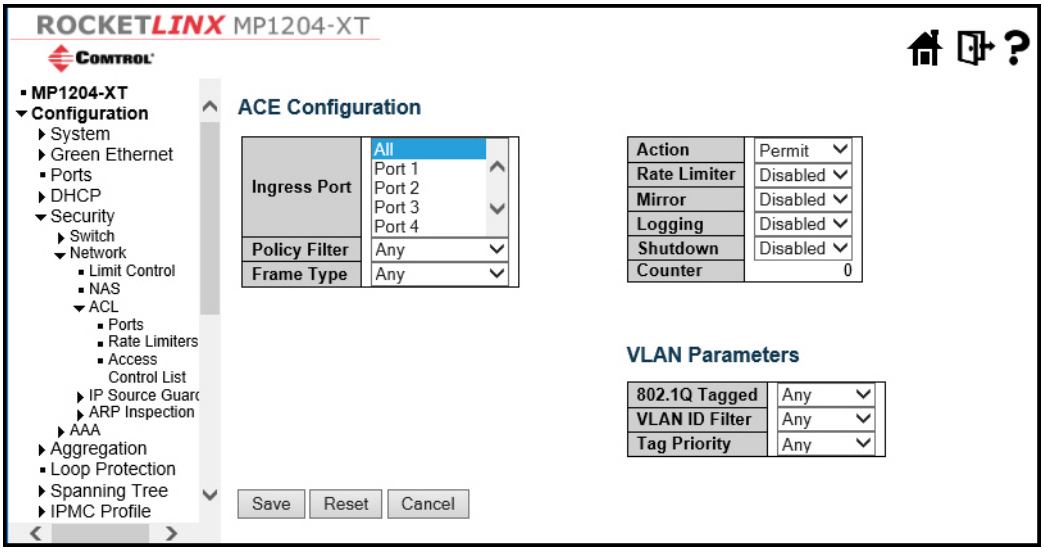
Item	Configuration | Security | Network | ACL | Access Control List
Ingress Port	Indicates the ingress port of the ACE. Possible values are: • **All**: The ACE matches all ingress port. • **Port**: The ACE matches a specific ingress port.
Policy / Bitmask	Indicates the policy number and bitmask of the ACE.
Frame Type	Indicates the frame type of the ACE. Possible values are: • **Any**: The ACE matches any frame type. • **EType**: The ACE matches Ethernet Type frames. Note that an Ethernet Type based ACE does not get matched by IP and ARP frames. • **ARP**: The ACE matches ARP/RARP frames. • **IPv4**: The ACE matches all IPv4 frames. • **IPv4/ICMP**: The ACE matches IPv4 frames with ICMP protocol. • **IPv4/UDP**: The ACE matches IPv4 frames with UDP protocol. • **IPv4/TCP**: The ACE matches IPv4 frames with TCP protocol. • **IPv4/Other**: The ACE matches IPv4 frames, which are not ICMP/UDP/TCP. • **IPv6**: The ACE matches 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.

Item	Configuration | Security | Network | ACL | Access Control List
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.

You can modify each ACE (Access Control Entry) in the table using the following modification buttons:

Button	Function
⊕	Inserts a new ACE before the current row.
ⓔ	Edits the ACE row.
⊕	Moves the ACE up the list.
⊕	Moves the ACE down the list.
⊗	Deletes the ACE.
⊕	The lowest plus sign adds a new entry at the bottom of the ACE listings.

The **ACE Configuration** page includes the following fields.



Item	Configuration | Security | Network | ACL | Access Control List | ACE Configuration
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 MP1204-XT 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 an 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.

Item	Configuration | Security | Network | ACL | Access Control List | ACE Configuration (Continued)
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.
Port Redirect	Frames that hit the ACE are redirected to the port number specified here. The rate limiter affects 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** cannot 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 does 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 does not 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 are 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 is 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	***Note:*** *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.

Item	Configuration | Security | Network | ACL | Access Control List | ACE Configuration (Continued)
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**.
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.

Item	Configuration | Security | Network | ACL | Access Control List | ACE Configuration (Continued)
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*).
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*).

Item	Configuration | Security | Network | ACL | Access Control List | ACE Configuration (Continued)
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.

Item	Configuration | Security | Network | ACL | Access Control List | ACE Configuration (Continued)
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 appears. These fields are explained later in this help file. • **UDP**: Select **UDP** to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters appears. These fields are explained later in this help file. • **TCP**: Select **TCP** to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters appears. 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 0xFFFFFFFE(bit 0 is *don't-care* bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.

Item	Configuration | Security | Network | ACL | Access Control List | ACE Configuration (Continued)
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.
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.

Item	Configuration | Security | Network | ACL | Access Control List | ACE Configuration (Continued)
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)*.
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 a 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.

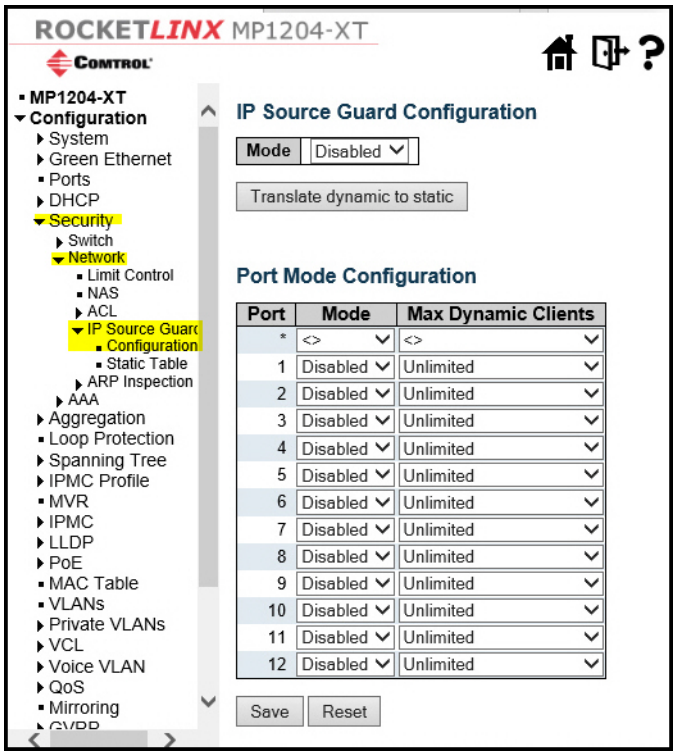
Security | Network | IP Source Guard Menus

The following pages are under the **IP Source Guard** menu.

- *Security | Network | IP Source Guard | Configuration* on Page 100
- *Security | Network | IP Source Guard | Static Table* on Page 101

Security | Network | IP Source Guard | Configuration

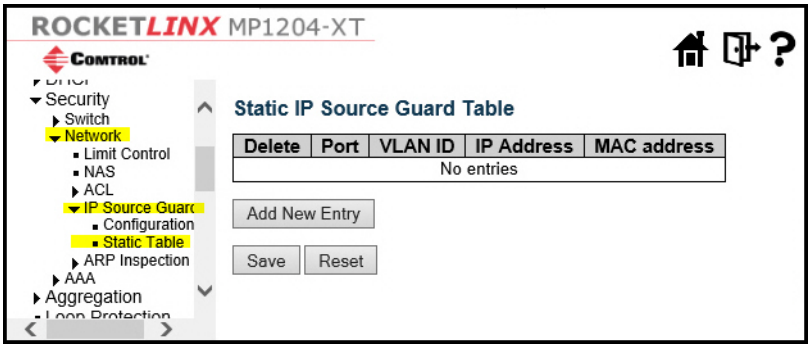
This page provides IP Source Guard related configuration.



Item	Configuration | Network | IP Source Guard | Configuration
Mode of IP Source Guard Configuration	Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs are 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.

Security | Network | IP Source Guard| Static Table

This page shows the static IP source guard rules. The maximum number of rules is 112 on the MP1204-XT.



Item	Configuration | Network | IP Source Guard | Static Table
Delete	Check to delete the entry. It is 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.

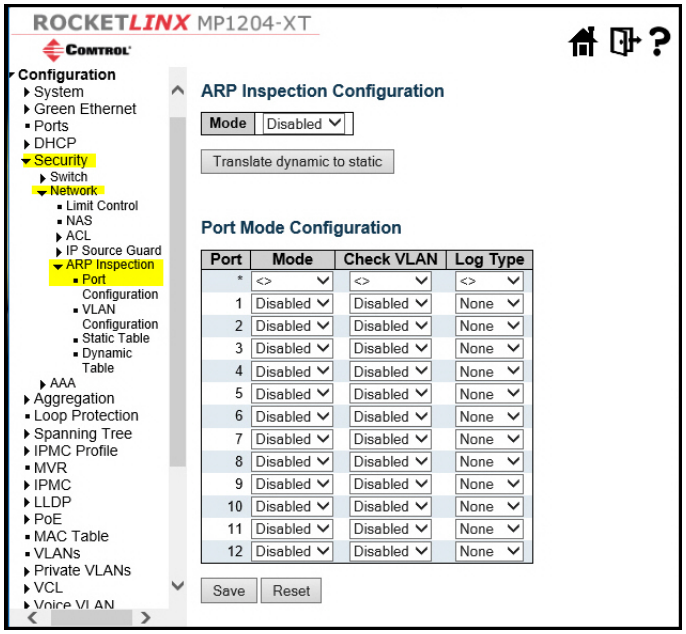
Security | Network | ARP Inspection Menus

The following pages are under the **ARP Inspection** menu.

- *Security | Network | ARP Inspection | Port Configuration* on Page 102
- *Security | Network | ARP Inspection | VLAN Configuration* on Page 103
- *Security | Network | ARP Inspection | Static Table* on Page 103
- *Security | Network | ARP Inspection | Dynamic Table* on Page 104

Security | Network | ARP Inspection | Port Configuration

This page provides ARP Inspection related configuration.



Item	Configuration | Network | ARP Inspection | Port Configuration
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 refers to the port setting. If **Check VLAN** is enabled, the log type of ARP Inspection refers 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 refers 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.
Translate dynamic to static	Click to translate all dynamic entries to static entries.

Security | Network | ARP Inspection | VLAN Configuration

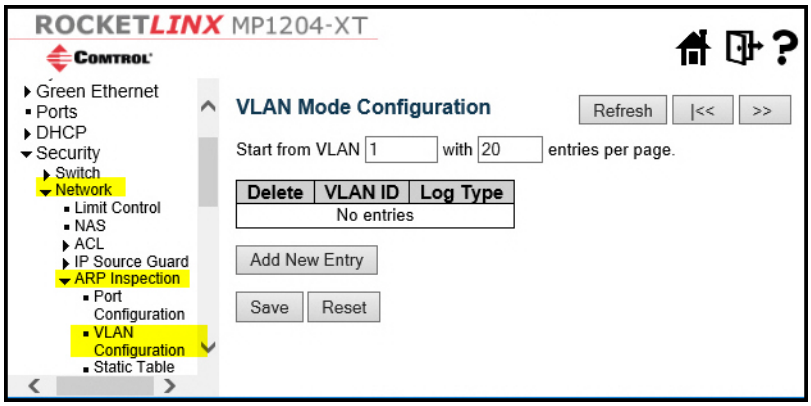
Each page shows up to 9999 entries from the VLAN table, the default is 20, selected through the **entries per page** field. When first visited, the page shows the first 20 entries from the beginning of the VLAN Table. The first displayed are the one with the lowest VLAN ID found in the VLAN Table.

The **VLAN** input fields allow you to select the starting point in the VLAN Table. Clicking the button updates the displayed table starting from that or the closest next VLAN Table match. The MP1204-XT uses 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 **Reset** button to start over.

Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration 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 is inspected on VLAN mode configuration page. The log type also can be configured on per VLAN setting.

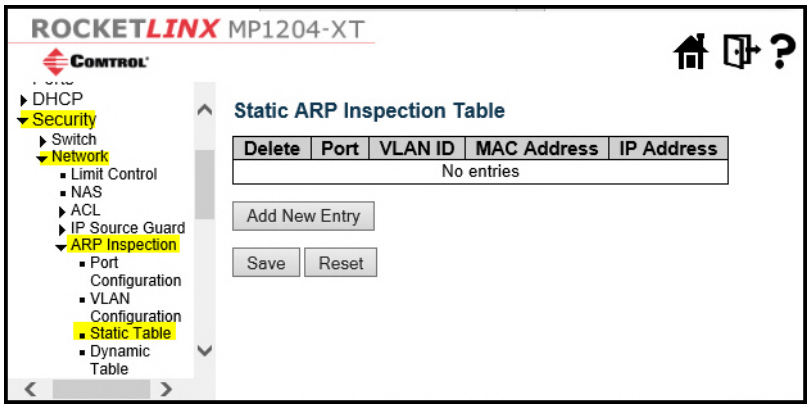
Possible types are:

- **None**: Log nothing.
- **Deny**: Log denied entries.
- **Permit**: Log permitted entries.
- **All**: Log all entries



Security | Network | ARP Inspection | Static Table

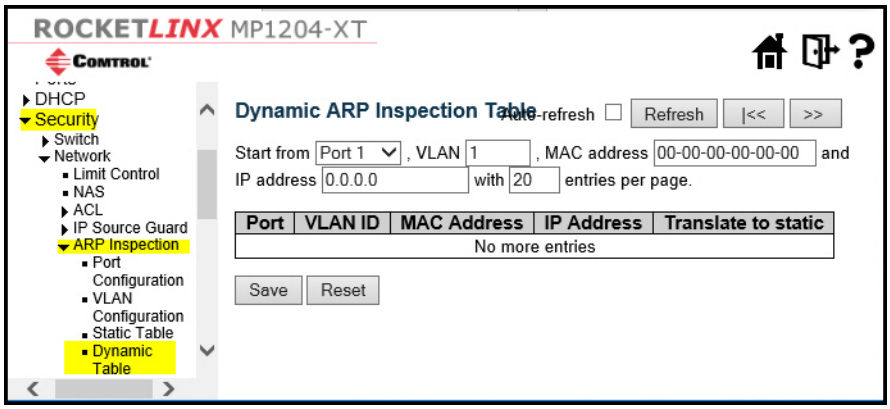
This page shows the static ARP inspection rules. The maximum number of rules is 256 on the MP1204-XT.



Item	Configuration | Security | Network | ARP Inspection | Static Table
Delete	Check to delete the entry. It is deleted during the next save.
Port	The logical port for the settings
VLAN ID	The VLAN ID for the settings.

Item	Configuration | Security | Network | ARP Inspection | Static Table
MAC Address	Allowed Source MAC address in ARP request packets.
IP Address	Allowed Source IP address in ARP request packets.
Add New Entry	Click to add a new entry in the ARP Inspection Static table.

Security | Network | ARP Inspection | Dynamic Table



Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the **entries per page** input field. Initially, the page shows 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 you to select the starting point in the Dynamic ARP Inspection Table. Clicking the **Refresh** button updates 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 that the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> button uses 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.

Item	Configuration | Security | Network | ARP Inspection | Dynamic Table
Port	MP1204-XT 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 check box to translate the entry to static entry.
|<<	Updates the table starting from the first entry in the Dynamic ARP Inspection Table.
>>	Updates the table, starting with the entry after the last entry currently displayed.

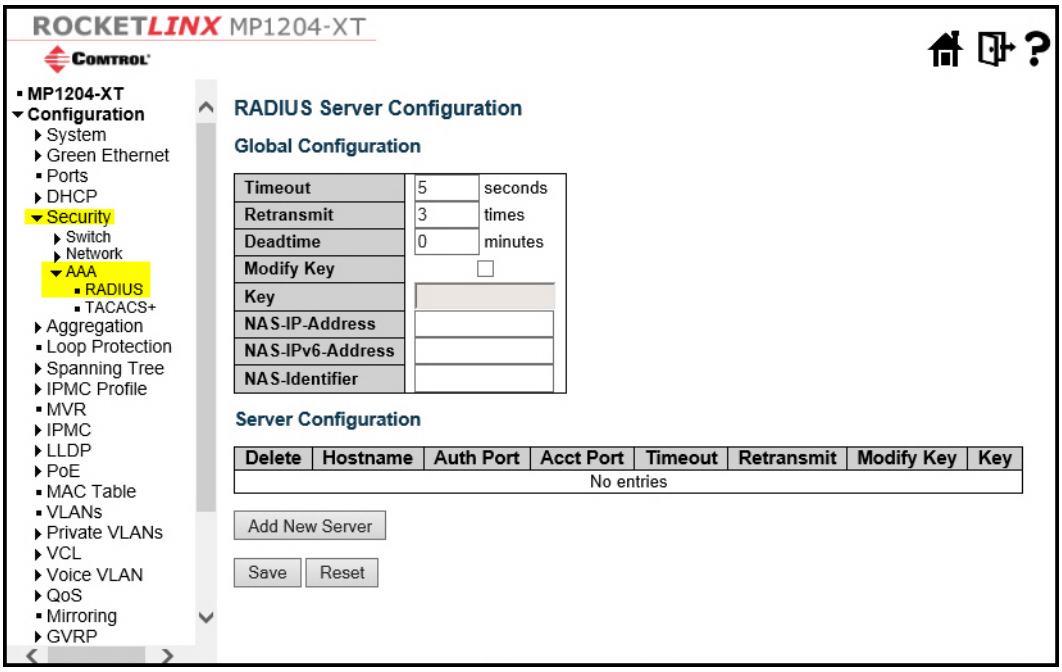
Configuration | Security | AAA Menus

The following pages are under the AAA sub-menu:

- *Security | AAA | RADIUS* on Page 105
- *Security | AAA | TACACS+* on Page 107

Security | AAA | RADIUS

Use this page to configure your RADIUS server.

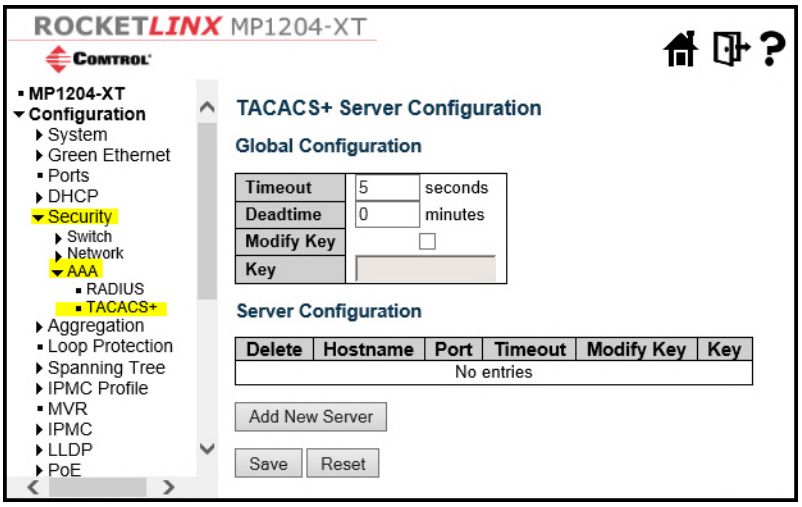


Item	Configuration | Security | AAA | RADIUS
Global Configuration	
Timeout	**Timeout** is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.
Retransmit	**Retransmit** is the number of times, in the range 1 to 1000, a RADIUS request 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 MP1204-XT does not send new requests to a server that has failed to respond to a previous request. This stops the MP1204-XT from continually trying to contact a server that it has already determined as dead. Setting the **Deadtime** to a value greater than 0 (zero) enables this feature, but only if more than one server has been configured.
Key	The secret key, up to 63 characters long is shared between the RADIUS server and the MP1204-XT.

Item	Configuration | Security | AAA | RADIUS (Continued)
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 is 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 is 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.
Timeout	This optional setting overrides the global timeout value. Leaving it blank uses the global timeout value.
Retransmit	This optional setting overrides the global retransmit value. Leaving it blank uses the global retransmit value.
Key	This optional setting overrides the global key. Leaving it blank uses the global key.
Add New Server	Click to add a new RADIUS server, up to five servers are supported.

Security | AAA | TACACS+

Use this page to configure TACACS+.



Item	Configuration | Security | AAA | TACACS+
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 MP1204-XT does not send new requests to a server that has failed to respond to a previous request. This stops the MP1204-XT from continually trying to contact a server that it has already determined as dead. Setting the **Deadtime** to a value greater than 0 (zero) enables 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 is 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 uses the global timeout value.
Key	This optional setting overrides the global key. Leaving it blank uses the global key.
Add New Server	Click to add a new TACACS+ server, up to five servers are supported.

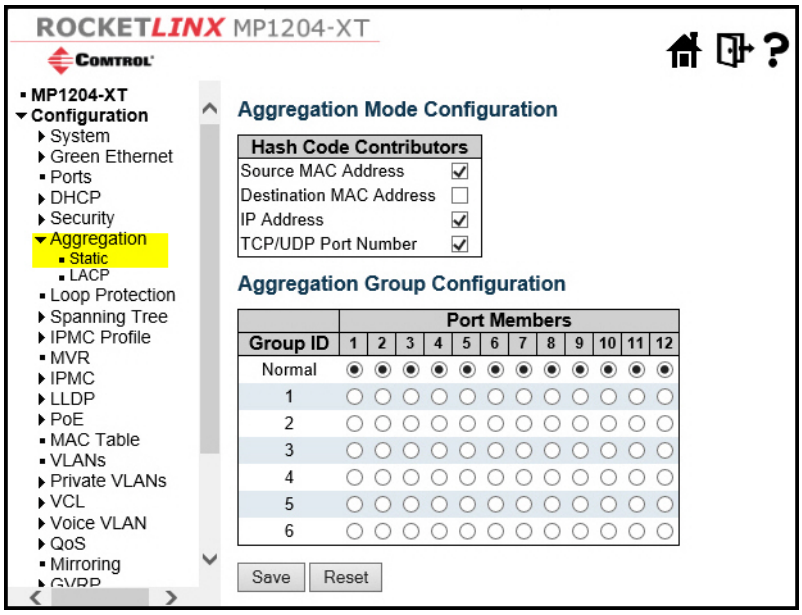
Configuration | Aggregation Menus

The following page are under the Configuration | Aggregation sub-menu.

- *Aggregation | Static* on Page 108
- *Aggregation | LACP* on Page 109

Aggregation | Static

Use this page to configure the aggregation hash mode and the aggregation group.

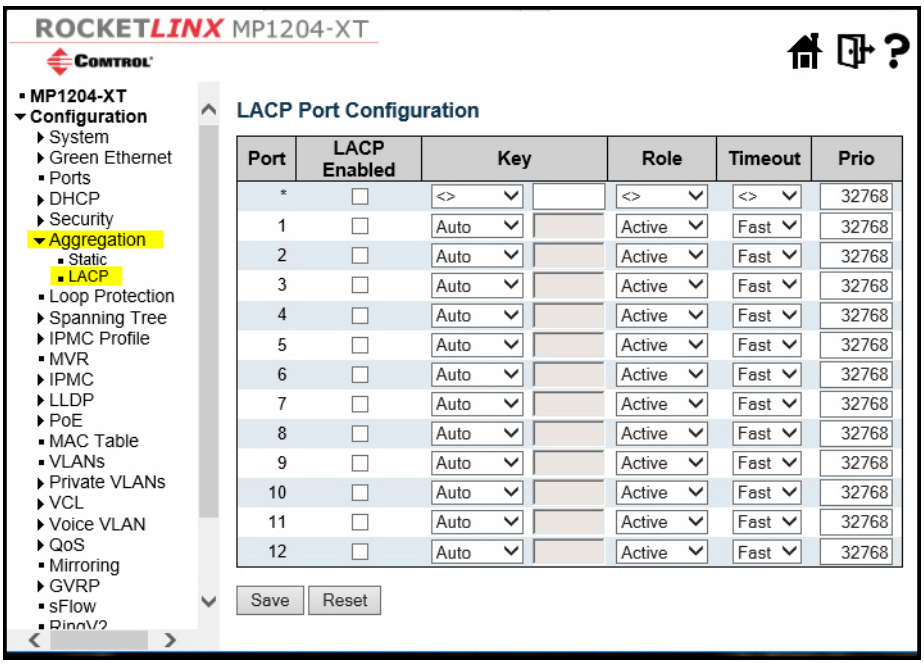


Item	Configuration | Aggregation | Static
Hash Code Contributors	
Source MAC Address	The **Source MAC Address** can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.
Destination 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.

Item	Configuration | Aggregation | Static (Continued)
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.

Aggregation | LACP

Use this page to inspect the current LACP port configuration and if necessary, make changes.

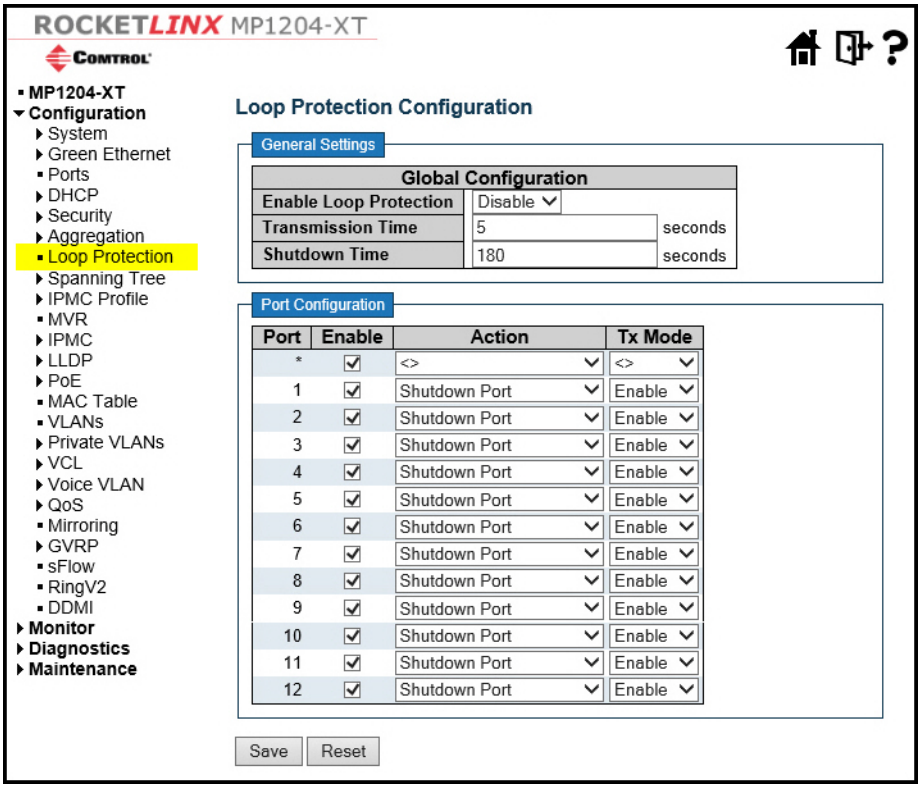


Item	Aggregation | LACP
Port	The MP1204-XT port number.
LACP Enabled	Controls whether LACP is enabled on the MP1204-XT port. LACP forms an aggregation when two or more ports are connected to the same partner.
Key	The **Key** value incurred by the port, range 1-65535. The Auto setting sets the key as 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.

Item	Aggregation | LACP (Continued)
Role	The **Role** shows the LACP activity status. The Active transmits LACP packets each second, while **Passive** waits for a LACP packet from a partner (speak if spoken to).
Timeout	The **Timeout** controls the period between BPDU transmissions. Fast transmits LACP packets each second, while **Slow** waits 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 controls which ports are active and which ports are in a backup role. The lower number, the greater the priority.

Configuration | Loop Protection

Use this page to review the current Loop Protection settings and if necessary, change them.



Item	Configuration | Loop Protection
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 is 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 keeps a port disabled (until next device restart).
Port Configuration	
Port	The MP1204-XT port number of the port.
Enable	Controls whether loop protection is enabled on the MP1204-XT 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.

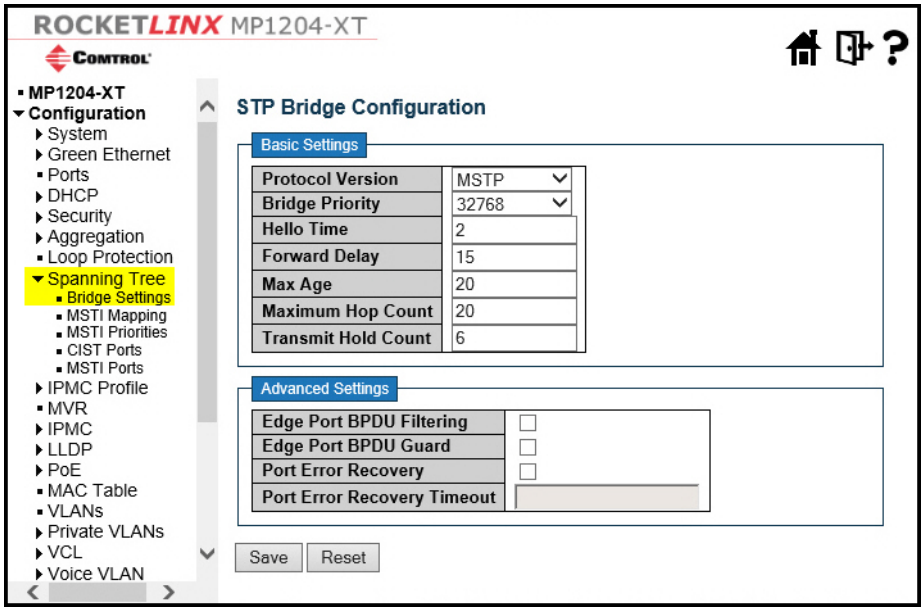
Configuration | Spanning Tree Sub-Menus

The following menus are under the **Configuration | Spanning Tree** menu:

- *Spanning Tree | Bridge Settings*
- *Spanning Tree | MSTI Mapping* on Page 114
- *Spanning Tree | MSTI Priorities* on Page 115
- *Spanning Tree | CIST Ports* on Page 116
- *Spanning Tree | MSTI Ports* on Page 118

Spanning Tree | Bridge Settings

Use this page to configure STP system settings. These settings are used by all STP Bridge instances in the MP1204-XT.

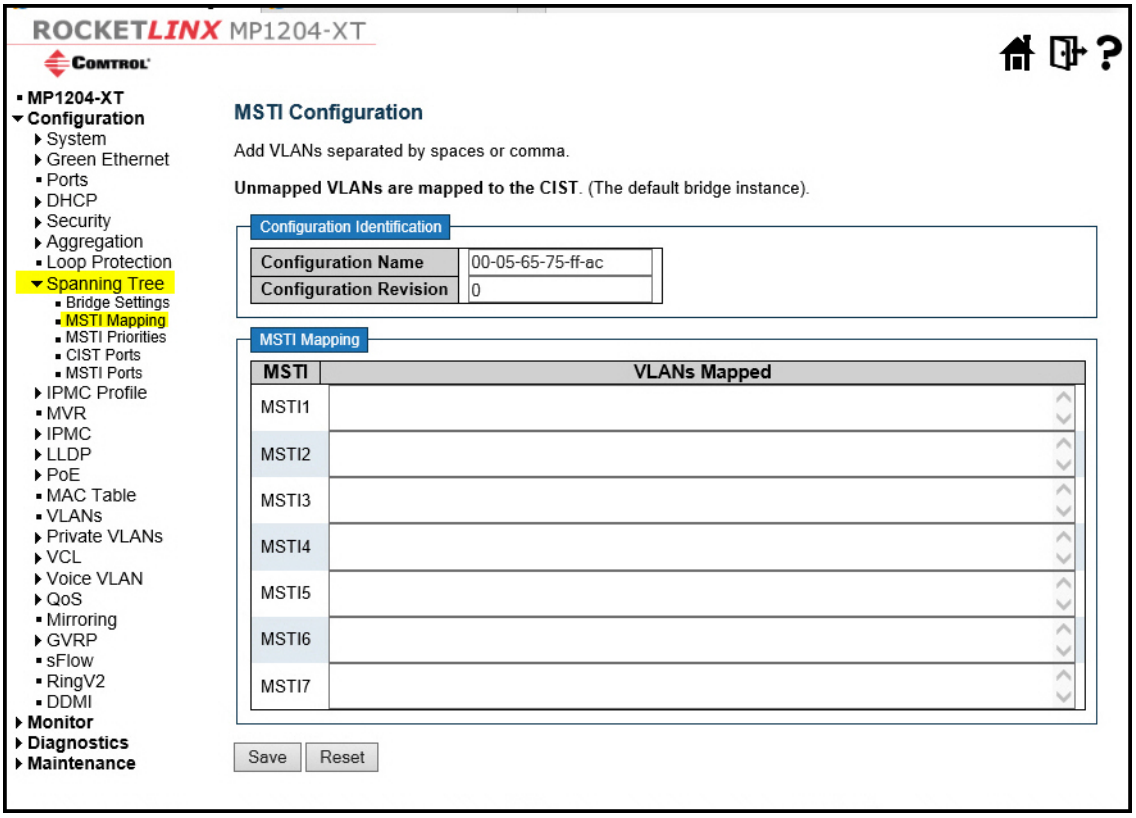


Item	Configuration | Spanning Tree | Bridge Settings
Basic Settings	
Protocol Version	The MSTP / RSTP / STP protocol version setting. Valid values are **STP**, **RSTP** and **MSTP**.
Bridge Priority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the 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 is delayed. Valid values are in the range 1 to 10 BPDU's per second.
Advanced Settings	
Edge Port BPDU Filtering	Controls whether a port explicitly configured as **Edge** transmits and receives BPDUs.

Item	Configuration | Spanning Tree | Bridge Settings (Continued)
Edge Port BPDU Guard	Controls whether a port explicitly configured as **Edge** disables itself upon reception of a BPDU. The port enters the error-disabled state, and is removed from the active topology.
Port Error Recovery	Controls whether a port in the error-disabled state automatically is 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).

Spanning Tree | MSTI Mapping

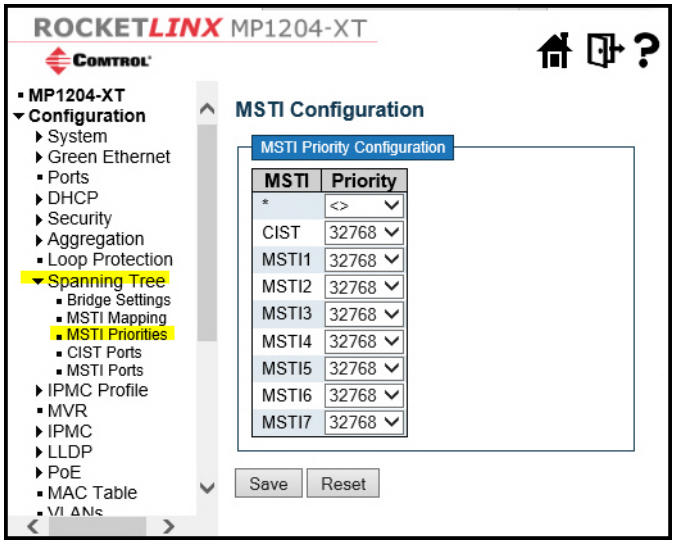
Use this page to inspect the current STP MSTI bridge instance priority configuration, and if necessary make changes.



Item	Configuration | Spanning Tree | MSTI Mapping
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 receives 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. Example: 2,5,20-40. An unused MSTI should just be left empty. That is, not having any VLANs mapped to it.

Spanning Tree | MSTI Priorities

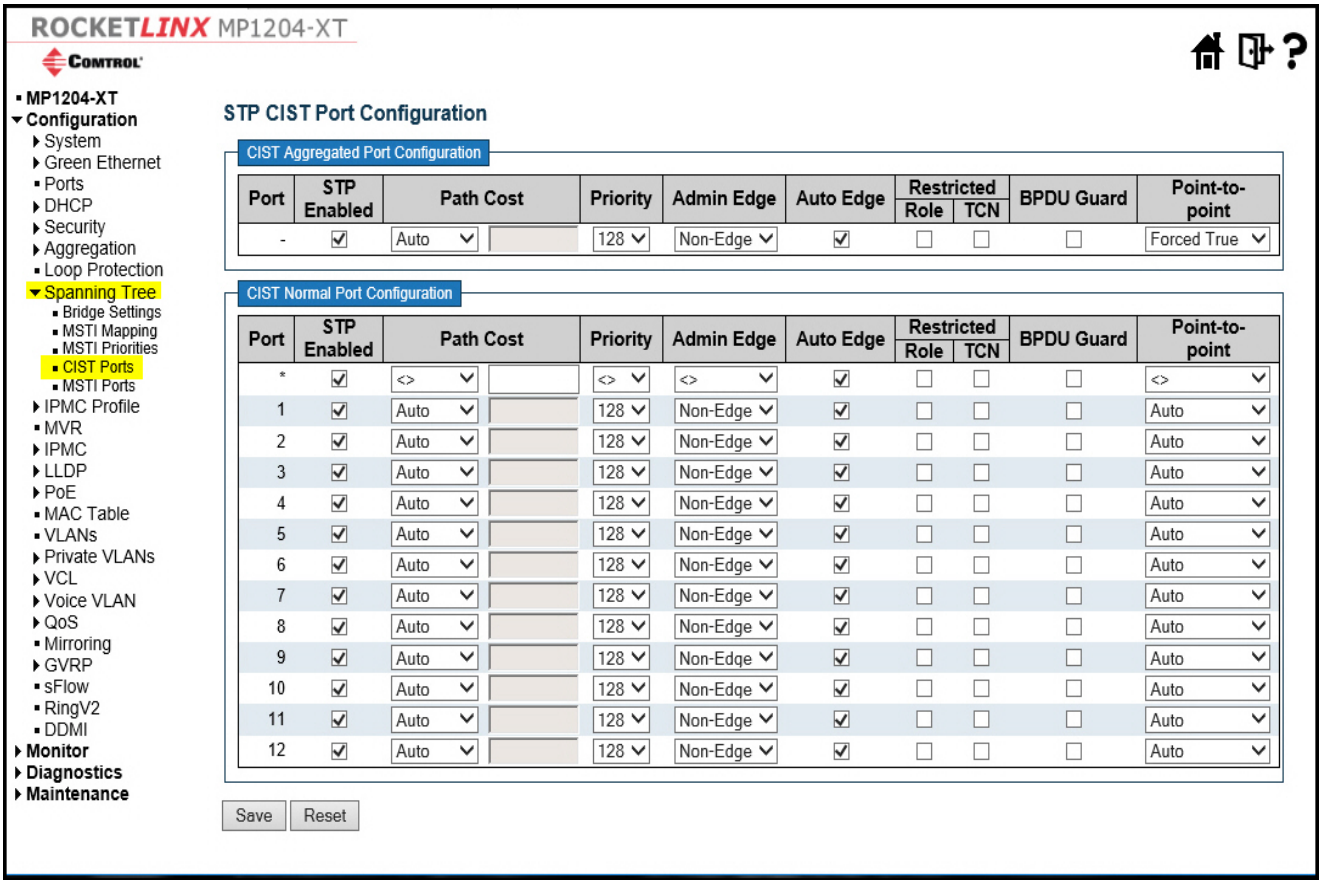
Use this pagepage to inspect the current STP MSTI bridge instance priority configuration and if necessary, make changes.



Item	Configuration | Spanning Tree |MSTI Priorities
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.

Spanning Tree | CIST Ports

Use this page to review the current STP CIST port configuration and if needed, change them. This page contains settings for physical and aggregated ports.



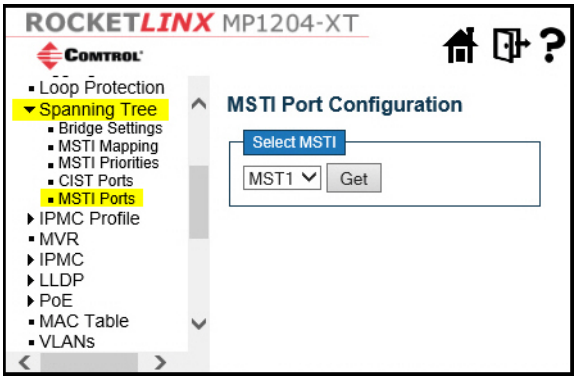
Item	Configuration | Spanning Tree | CIST Ports
Port	The MP1204-XT port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this MP1204-XT port.
Path Cost	Controls the path cost incurred by the port. The **Auto** setting sets the path cost as appropriate by the physical link 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)	This is an 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** on the **Monitor Spanning Tree | STP Detailed Bridge Status** page.

Item	Configuration | Spanning Tree | CIST Ports
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 is 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.
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.

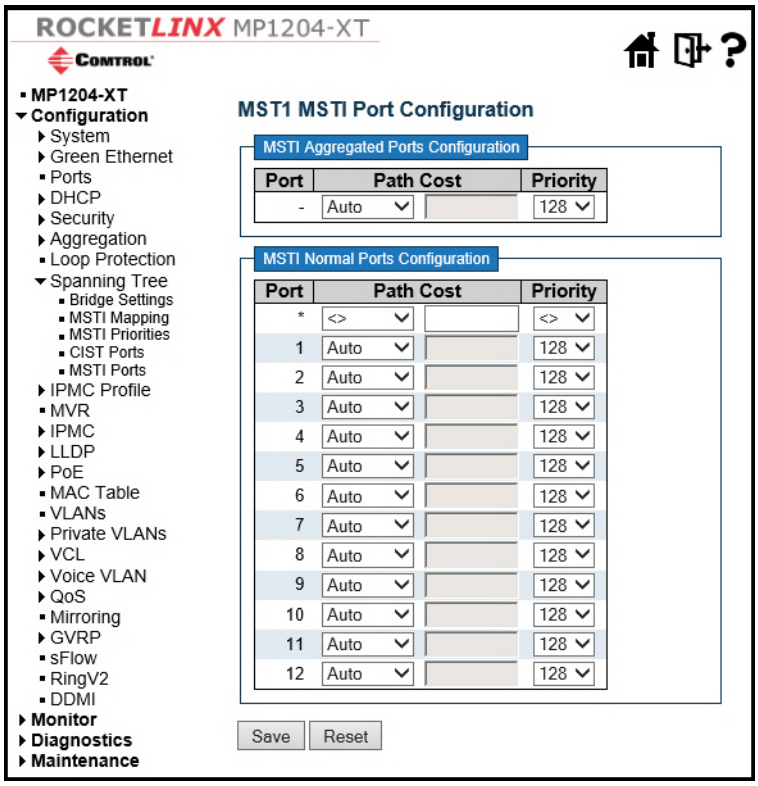
Spanning Tree | MSTI Ports

This page allows you 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.



Click the **Get** button to retrieve settings for a specific MSTI.



Item	Configuration | Spanning Tree | MSTI Ports
Port	The MP1204-XT port number of the corresponding STP CIST (and MSTI) port.
Path Cost	Controls the path cost incurred by the port. The **Auto** setting sets 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).

Configuration | IPMC Profile Menus

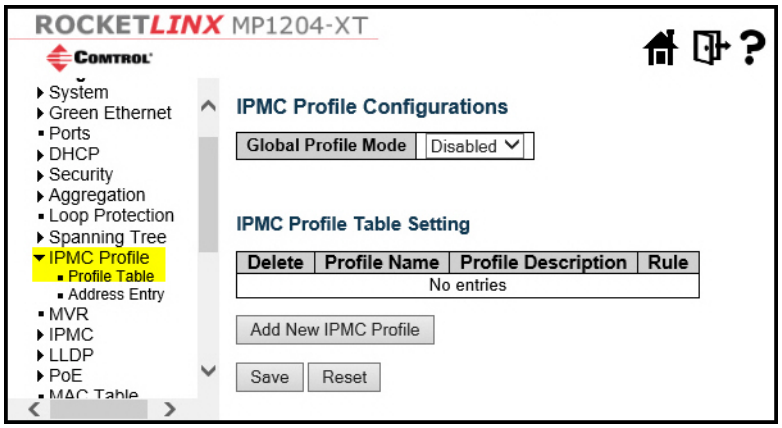
The following menus are under the **Configuration | IPMC Profile** menu.

- *IPMC Profile | Profile Table* on Page 119
- *IPMC Profile | Address Entry* on Page 120

IPMC Profile | Profile Table

Use this page to configure 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.



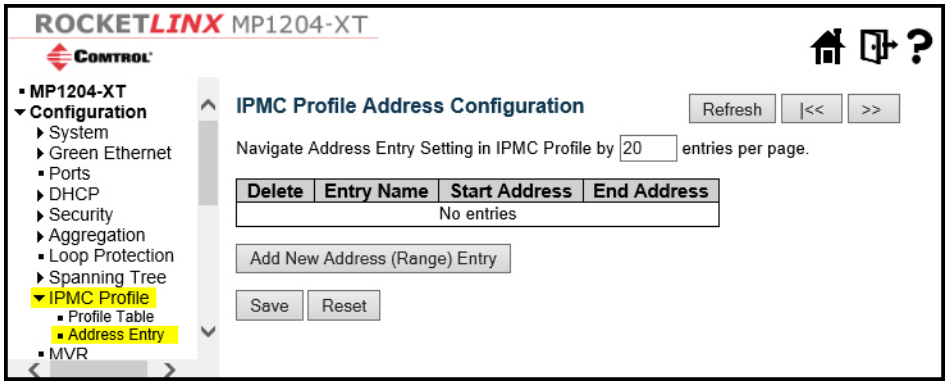
Item	Configuration | IPMC Profile | Profile Table
Global Profile Mode	Enable/Disable the Global IPMC Profile. System starts to do filtering based on profile settings only when the global profile mode is enabled.
Delete	Check to delete the entry. The designated entry is deleted during the next save.
Profile 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 an underscore (_) or a dash (-) 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. A summary about the designated profile is shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons: View the list the rules associated with the designated profile. Edit the rules associated with the designated profile.

Item	Configuration | IPMC Profile | Profile Table (Continued)
Add New IPMC Profile	Click to add a new IPMC profile. Specify the name and configure the new entry and then click **Save**.

IPMC Profile | Address Entry

Use this page to set the address range for the IPMC profile.

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



Item	Configuration | IPMC Profile | Address Entry
Delete	Check to delete the entry. The designated entry is 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 alphabetic character must be present.
Start Address	The starting IPv4/IPv6 Multicast Group Address that is used as an address range.
End Address	The ending IPv4/IPv6 Multicast Group Address that is used as an address range.
Add New Address (Range) Entry	Click to add a new address range. Specify the name and configure the addresses, and then click Save.

Configuration | MVR

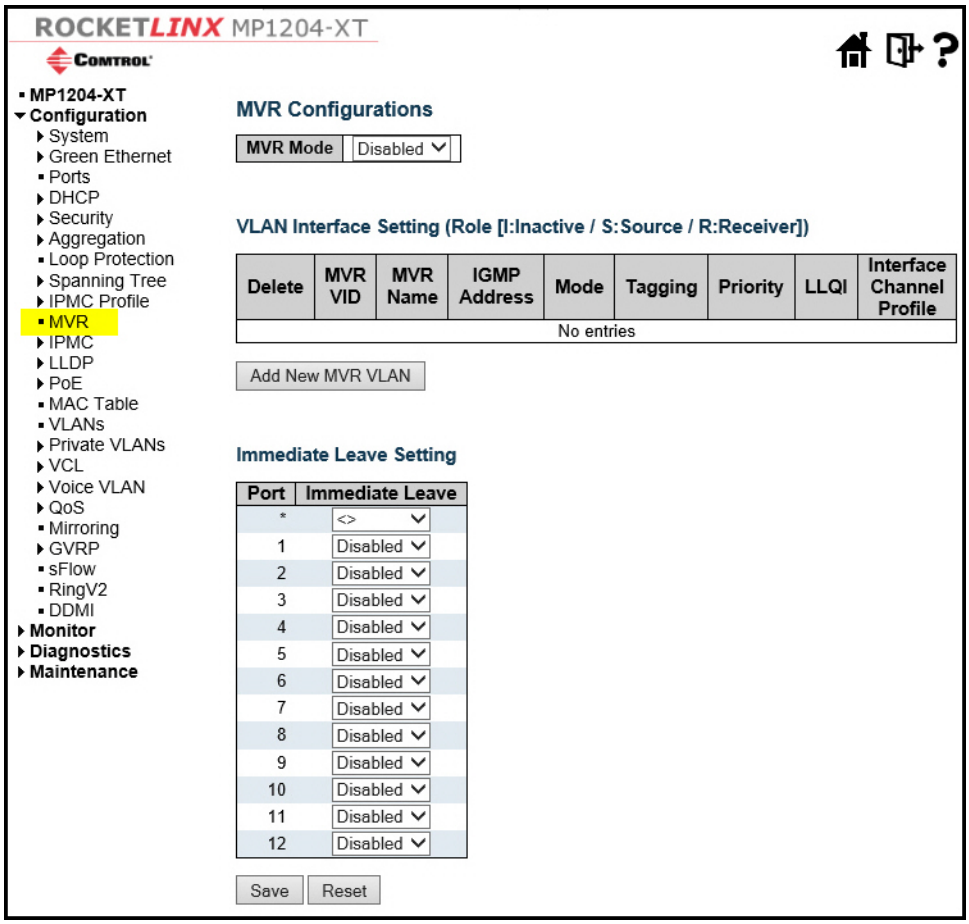
This page provides MVR related configurations.

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.

You can create a maximum of four MVR VLANs with corresponding channel profile for each Multicast VLAN.

The channel profile is defined by the IPMC Profile which provides the filtering conditions.



Item	Configuration | MVR
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 is deleted during the next save.

Item	Configuration | MVR (Continued)
MVR VID	Specify the Multicast VLAN ID. ***Note:*** *MVR source ports are not recommended to be overlapped with management VLAN ports.*
MVR Name	The 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. The MVR VLAN Name can only contain alphabetic or number characters. When the optional MVR VLAN name is given, it should contain at least one alphabetic character. The MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.
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, the MP1204-XT uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, the MP1204-XT uses the first available IPv4 management address. Otherwise, the MP1204-XT uses a pre-defined value. By default, this value is 192.168.250.250.
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 are sent as **Untagged** or **Tagged** with MVR VID. The default is **Tagged**.
Priority	Specify how the traversed IGMP/MLD control frames are 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 the multicast group membership. The value is in units of tenths of a seconds. 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. A summary about the Interface Channel Profiling (of the MVR VLAN) is shown by clicking the *view* button. The 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 *view* button: List the rules associated with the designated profile.
Port	The logical port for the settings.
Add New MVR VLAN	Click to add a new MVR VLAN. Specify the VID and configure the new entry and then click Save.

Item	Configuration | MVR (Continued)
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. ***Note:*** *MVR source ports are not recommended to be overlapped with management VLAN ports.* Select the port role by clicking the **Role** symbol to change the setting. **I** indicates Inactive; **S** indicates Source; **R** indicates Receiver The default **Port Role** is **Inactive**.
Immediate Leave	Enable the fast leave on the port. Multicast snooping **Fast Leave** processing allows the MP1204-XT to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

Configuration | IPMC Menus

The following sub-menus are under the IPMC menu.

- *IPMC | IGMP Snooping Menus* on Page 123
- *IPMC | MLD Snooping Menus* on Page 127

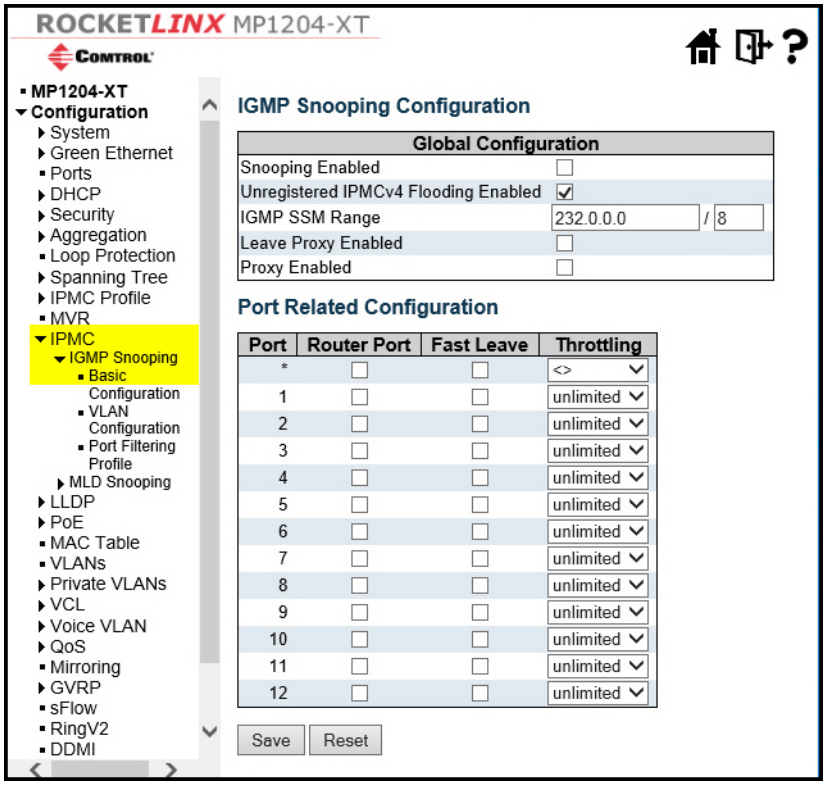
IPMC | IGMP Snooping Menus

The following pages are under the IGMP Snooping menu:

- *IPMC | IGMP Snooping | Basic Configuration* on Page 124
- *IPMC | IGMP Snooping | VLAN Configuration* on Page 125
- *IPMC | IGMP Snooping | Port Filtering Profile* on Page 126

IPMC | IGMP Snooping | Basic Configuration

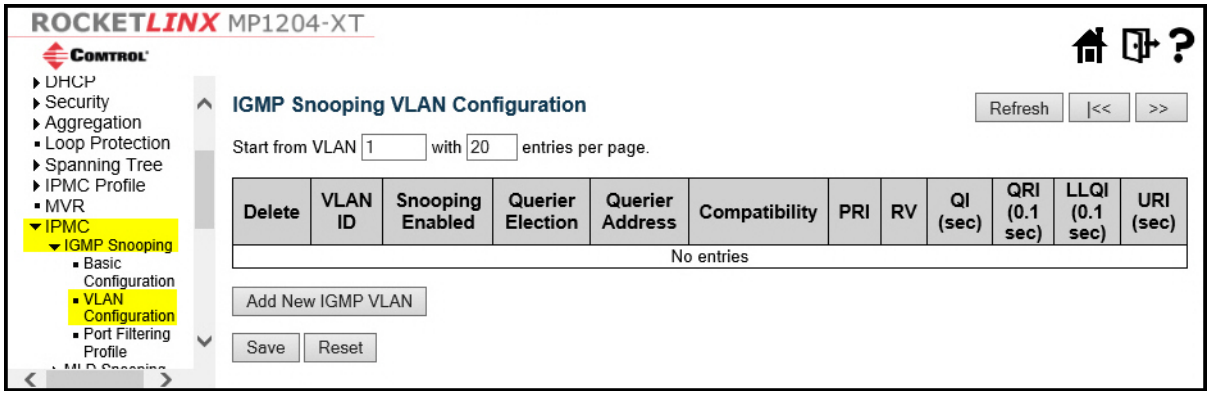
Use this page to configure IGMP Snooping for the MP1204-XT.



Item	Configuration | IPMC | IGMP Snooping | Basic Configuration
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 on the router side.
Proxy Enabled	Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages on 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 acts 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.

IPMC | IGMP Snooping | VLAN Configuration

Each IGMP Snooping VLAN Configuration 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 page shows the first 20 entries from the beginning of the VLAN Table. The first displayed are the ones with the lowest VLAN ID found in the VLAN Table.

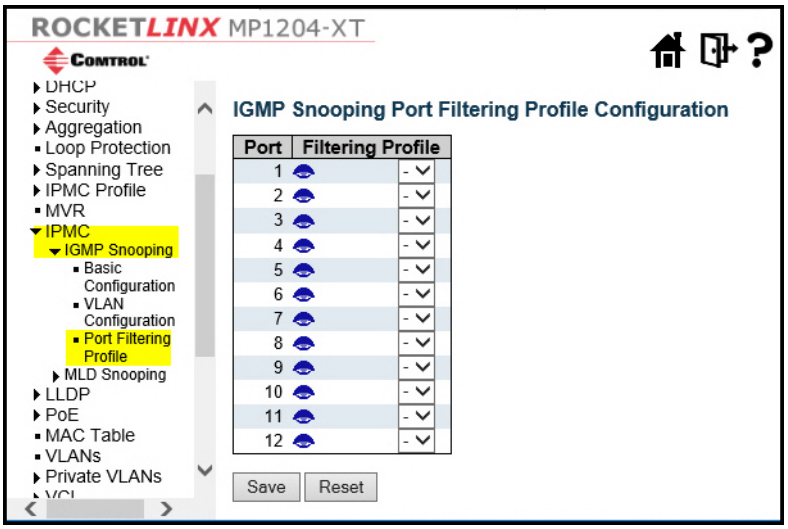


Item	Configuration | IPMC | IGMP Snooping | VLAN Configuration
Delete	Check to delete the entry. The designated entry is deleted during the next save.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enabled	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
Querier Election	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 is 192.168.250.250.
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 MP1204-XT. 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 that 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 (QI) is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.

Item	Configuration | IPMC | IGMP Snooping | VLAN Configuration (Continued)
QRI	Query Response Interval (QRI) is 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 (LMQI for IGMP)	LLQI is the Last Member Query Time, which 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	URI is the Unsolicited Report Interval, which 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 and then click Save. The specific VLAN starts working after the corresponding static VLAN is also created.

IPMC | IGMP Snooping | Port Filtering Profile

Use this page to configure a Port Filtering Profile for IGMP Snooping.



Item	Configuration | IPMC | IGMP Snooping | Port Filtering Profile
Port	The logical port for the settings.
Filtering Profile	Select the IPMC Profile as the filtering condition for the specific port. a summary about the designated profile is shown by clicking the view button.
Profile Management Button	You can inspect the rules of the designated profile by using the following button: View the list of the rules associated with the designated profile.

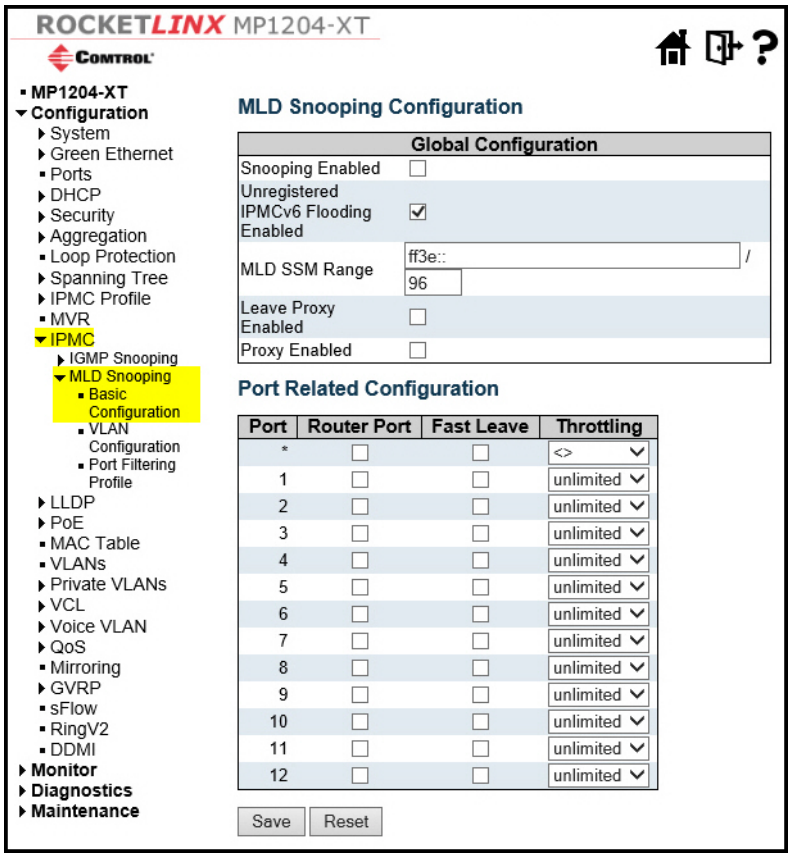
IPMC | MLD Snooping Menus

The following pages are under the MLD Snooping menu:

- *IPMC | MLD Snooping | Basic Configuration* on Page 127
- *IPMC | MLD Snooping | VLAN Configuration* on Page 128
- *IPMC | MLD Snooping | Port Filtering Profile* on Page 130

IPMC | MLD Snooping | Basic Configuration

Use this page to configure basic MLD Snooping.



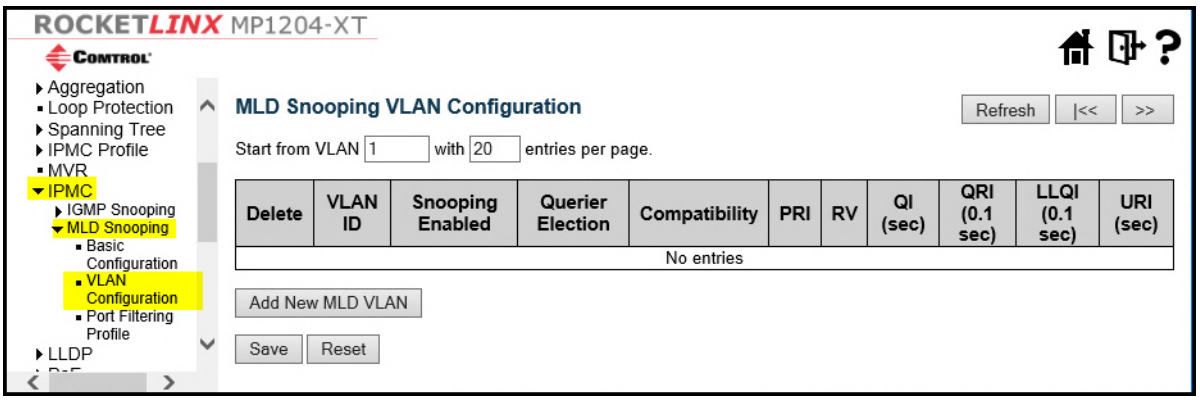
Item	Configuration | IPMC | MLD Snooping | Basic Configuration
Snooping Enable	Enable the Global MLD Snooping.
Unregistered IPMCv6 Flooding Enable	Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered 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.

Item	Configuration | IPMC | MLD Snooping | Basic Configuration (Continued)
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 acts as a router port.
Fast Leave	Enable the fast leave feature on the port.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

IPMC | MLD Snooping | 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 page shows the first 20 entries from the beginning of the VLAN Table. The first displayed are the ones with the lowest VLAN ID found in the VLAN Table.

The **VLAN** input fields allow you to select the starting point in the VLAN Table.

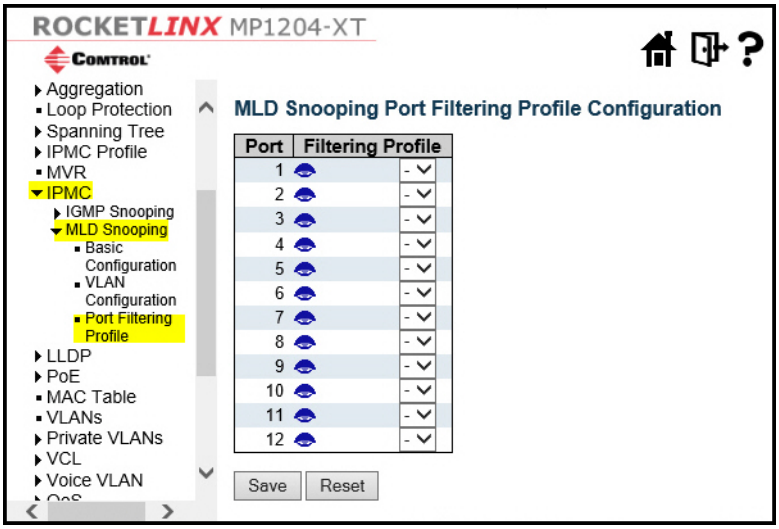


Item	Configuration | IPMC | MLD Snooping | VLAN Configuration
Delete	Check to delete the entry. The designated entry is deleted during the next save.
VLAN ID	The VLAN ID of the entry.
MLD Snooping Enabled	Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.
Querier Election	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**, the default compatibility value is **MLD-Auto**. It indicates the MLD control frame priority level generated by the MP1204-XT. These values can be used to prioritize different classes of traffic.

Item	Configuration | IPMC | MLD Snooping | VLAN Configuration (Continued)
PRI	Priority of Interface. The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.
RV	**RV** (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	**QI** (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	**QRI** (Query Response Interval) is 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	**LLQI** (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).
URI	**URI** (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 and then click save. The specific MLD VLAN starts working after the corresponding static VLAN is also created.

IPMC | MLD Snooping | Port Filtering Profile

Use this page to configure a Port Filtering Profile for MLD Snooping.



Item	Configuration | IPMC | MLD Snooping | Port Filtering Profile
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 is shown by clicking the view button.
Profile Management Button	You can inspect the rules of the designated profile by using the view button: View the rules associated with the designated profile.

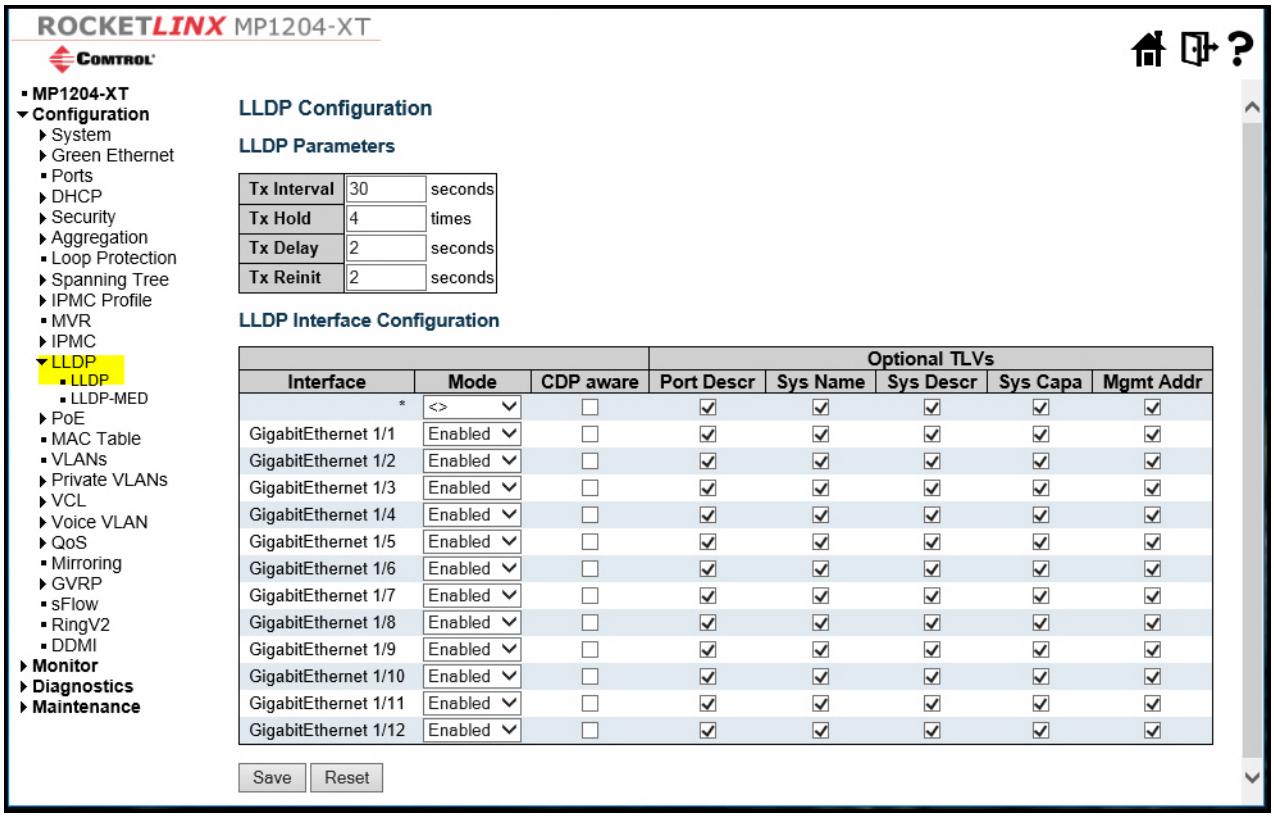
Configuration | LLDP Menus

The following pages are under the LLDP menu.

- *LLDP | LLDP* on Page 131
- *LLDP | LLDP-MED* on Page 134

LLDP | LLDP

Use this page to view current settings and if necessary, configure LLDP settings to suit your environment.



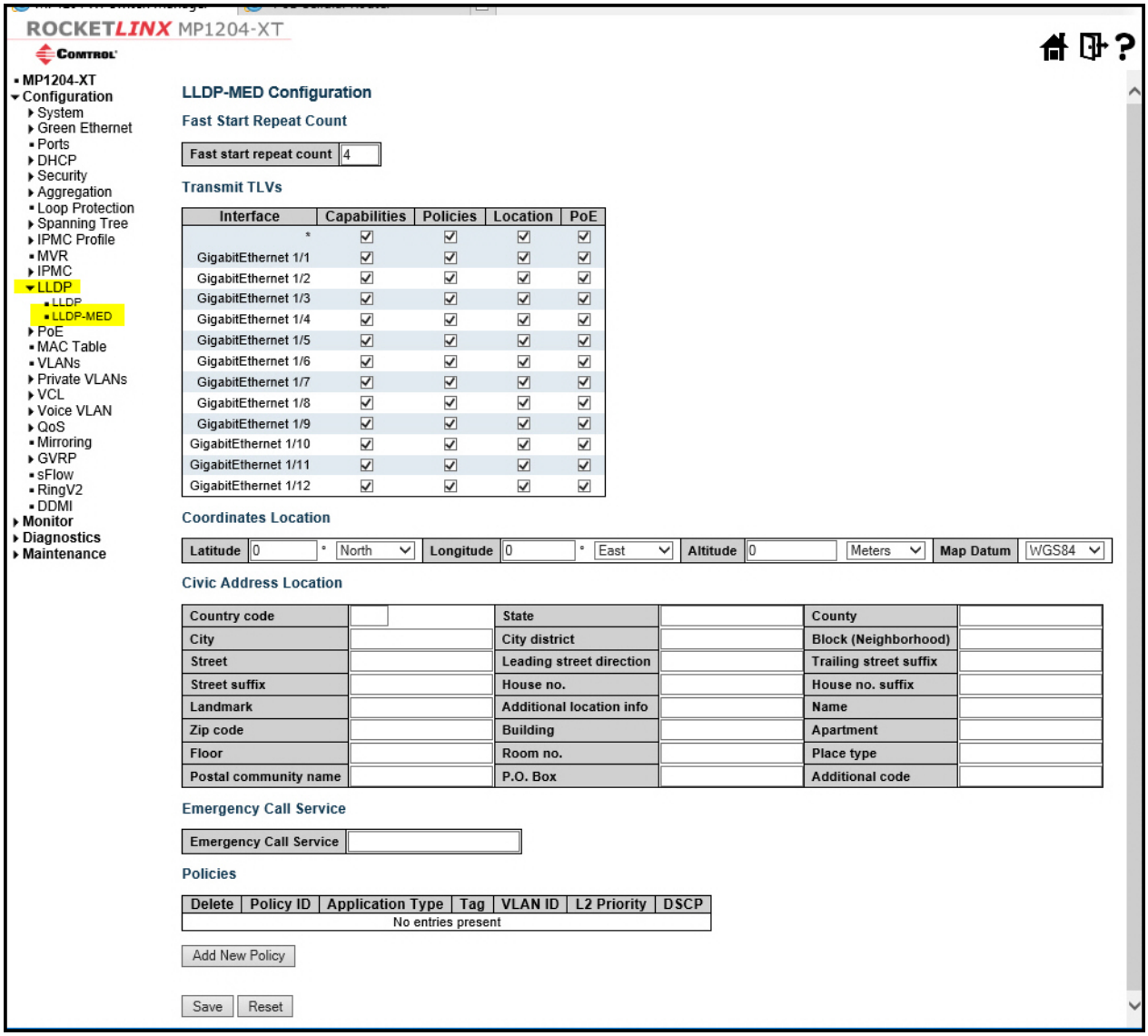
Item	Configuration | LLDP |LLDP
LLDP Parameters	
Tx Interval	The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds.
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.

Item	Configuration | LLDP |LLDP (Continued)
Tx Delay	If some configuration is changed (for example, the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames is always 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, signalling 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	
Port	The switch port number of the logical LLDP port.
Mode	Select LLDP mode. • **Rx only** The MP1204-XT does not send out LLDP information, but LLDP information from neighbor units is analyzed. • **Tx only** The MP1204-XT drops the LLDP information received from neighbors, but sends out LLDP information. • **Disabled** The MP1204-XT does not send out LLDP information, and drops the LLDP information received from neighbors. • **Enabled** The MP1204-XT sends out LLDP information, and analyzes the LLDP information received from neighbors.
CDP Aware	Select CDP awareness. 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. 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. CDP TLV **Device ID** is mapped to the LLDP **Chassis ID** field. 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. CDP TLV **Port ID** is mapped to the LLDP **Port ID** field. CDP TLV **Version** and **Platform** is mapped to the LLDP **System Description** field. 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.

Item	Configuration | LLDP |LLDP (Continued)
CDP Aware (continued)	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. ***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.*
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.

LLDP | LLDP-MED

This page allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.



Item	Configuration | LLDP | LLDP-MED
Fast start repeat count	
Fast start repeat count	Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy. With this in mind, LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device only transmits LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application temporarily speeds up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors. Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With **Fast start repeat count** it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval are transmitted, when an LLDP frame with new information is received. It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.
Coordinates Location	
Latitude	**Latitude** SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.
Longitude	**Longitude** SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.
Altitude	**Altitude** SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters). • **Meters**: Representing meters of Altitude defined by the vertical datum specified. • **Floors**: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

Item	Configuration | LLDP | LLDP-MED (Continued)
Map Datum	The **Map Datum** is used for the coordinates given in these options: • **WGS84**: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich. • **NAD83/NAVD88**: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW). • **NAD83/MLLW**: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.
Civic Address Location	
Country code	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
State	National subdivisions (state, canton, region, province, prefecture).
County	County, parish, gun (Japan), district.
City	City, township, shi (Japan) - Example: Copenhagen.
City district	City division, borough, city district, ward, chou (Japan).
Block (Neighborhood)	Neighborhood, block.
Street	Street - Example: Riverview.
Leading street direction	Leading street direction - Example: N.
Trailing street suffix	Trailing street suffix - Example: SW.
Street suffix	Street suffix - Example: Ave, Blvd.
House no.	House number - Example: 1121.
House no. suffix	House number suffix - Example: A, 1/2.
Landmark	Landmark or vanity address - Example: Columbia University.
Additional location info	Additional location info - Example: South Wing.
Name	Name (residence and office occupant) - Example: Smith, John.
Zip code	Postal/zip code - Example: 2791.
Building	Building (structure) - Example: Low Library.
Apartment	Unit (Apartment, suite) - Example: Apt 42.
Floor	Floor - Example: 4.
Room no.	Room number - Example: 450F.

Item	Configuration | LLDP | LLDP-MED (Continued)
Place type	Place type - Example: Office.
Postal community name	Postal community name - Example: Leonia.
P.O. Box	Post office box (P.O. BOX) - Example: 12345.
Additional code	Additional code - Example: 1320300003.
Emergency Call Service	
Emergency Call Service	**Emergency Call Service** ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.
Policies	
Delete	Check to delete the policy. It is deleted during the next save.
Policy ID	ID for the policy. This is auto generated and shall be used when selecting the policies that shall be mapped to the specific ports.
Application Type	Intended use of the application types: 1. **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. 2. **Voice Signaling** (conditional) - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy. 3. **Guest Voice** - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. 4. **Guest Voice Signaling** (conditional) - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy. 5. **Softphone Voice** - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance. 6. **Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. 7. **Streaming Video** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. 8. **Video Signaling** (conditional) - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.

Item	Configuration | LLDP | LLDP-MED (Continued)
Tag	**Tag** indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN. **Untagged** indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance. **Tagged** indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.
VLAN ID	VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.
L2 Priority	**L2 Priority** is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
DSCP	**DSCP** value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.
Add New Policy	Click the **Add New Policy** button to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click **Save**. The number of policies supported is 32.
Port Policies Configuration	
Port	The port number to which the configuration applies.
Policy Id	The set of policies that shall apply to a given port. The set of policies is selected by check marking the check boxes that corresponds to the policies.

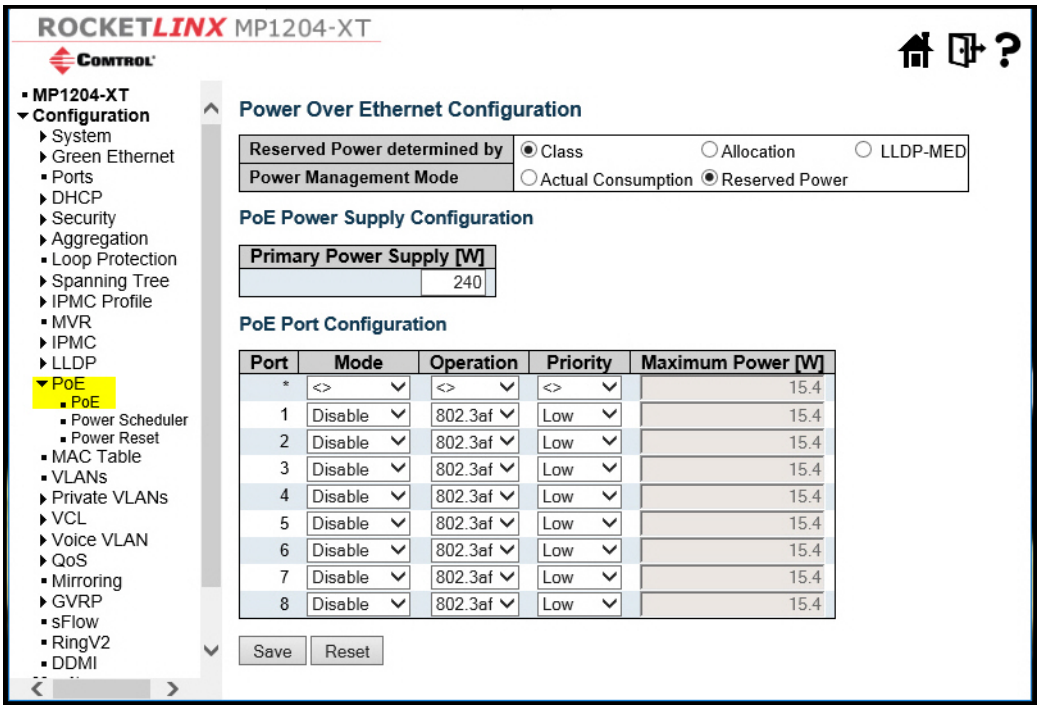
Configuration | PoE Menus

The following pages are under the **PoE** sub-menu.

- *PoE | PoE* on Page 139
- *PoE | Power Scheduler* on Page 141
- *PoE | Power Reset* on Page 142

PoE | PoE

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

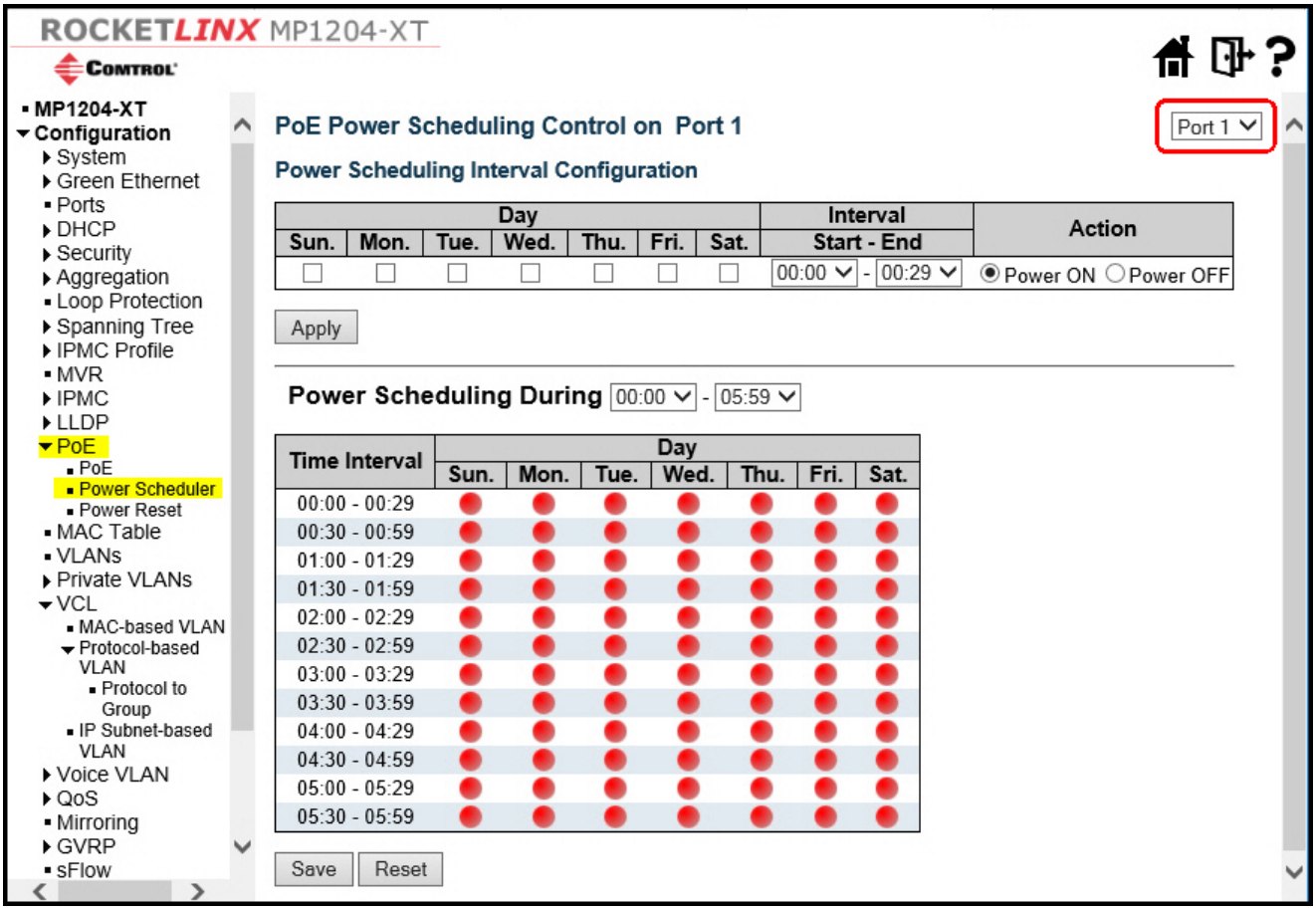


Item	Configuration | PoE | PoE
Reserved Power determined by	
Allocated mode	In this mode, you can allocate the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the **Maximum Power** fields.
Class mode	In **Class** mode, each port automatically 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 **Class** mode the **Maximum Power** fields have no effect.
LLDP-MED mode	This **LLDP-MED** 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 reserves power using the **Class** mode In **LLDP-MED** mode the **Maximum Power** fields have no effect.

Item	Configuration | PoE | PoE (Continued)
Power Management Mode	
Actual Consumption	In **Actual Consumption** 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 **Reserved Power** mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In **Reserved Power** mode the port power is not turned on if the PD requests more power than available from the power supply.
PoE Power Supply Configuration	
Primary Power Supply (W)	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 240 Watts.
PoE Port Configuration	
Port	This is the logical port number for this row.
Mode	• **Disable** - PoE disabled for the port. • **Enable** - Enables PoE for the port. • **Schedule** - Enables PoE for the port by scheduling.
Operation	• **802.3af** - Sets PoE protocol to IEEE 802.3af. • **802.3at** - Sets PoE protocol to IEEE 802.3at.
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 is 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. Valid ranges are 0 to 30 W.

PoE | Power Scheduler

This page provides power scheduling configurations. The entry is used to control the power alive interval on PoE port. You can set the specific interval to schedule power on/off in one week.



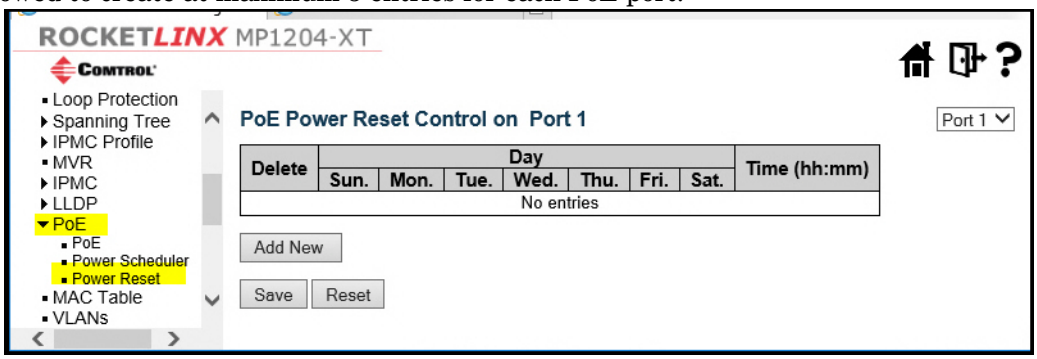
Item	Configuration | PoE | Power Scheduler
PoE Power Scheduling Control on Port #	
Port	Select the port number that you want to schedule using the drop list.
PoE Power Scheduling Interval Configuration	
Day	Check marks indicate which day are members of the set.
Interval	**Start** - Select the start hour and minute. **End** - Select the end hour and minute.
Action	**Power On** - Select the radio button to apply power on during the interval. **Power Off** - Select the radio button to apply power off during the interval.

Item	Configuration | PoE | Power Scheduler (Continued)
Power Scheduling During	
Time Interval	There are 48 time interval one day. Each interval has 30 minutes.
Day	Green indicates the power is on and red that it is off. Directly changes check marks to indicate which day are members of the time interval. Check or uncheck as needed to modify the scheduling table.

The current scheduling state is displayed graphically during the week.

PoE | Power Reset

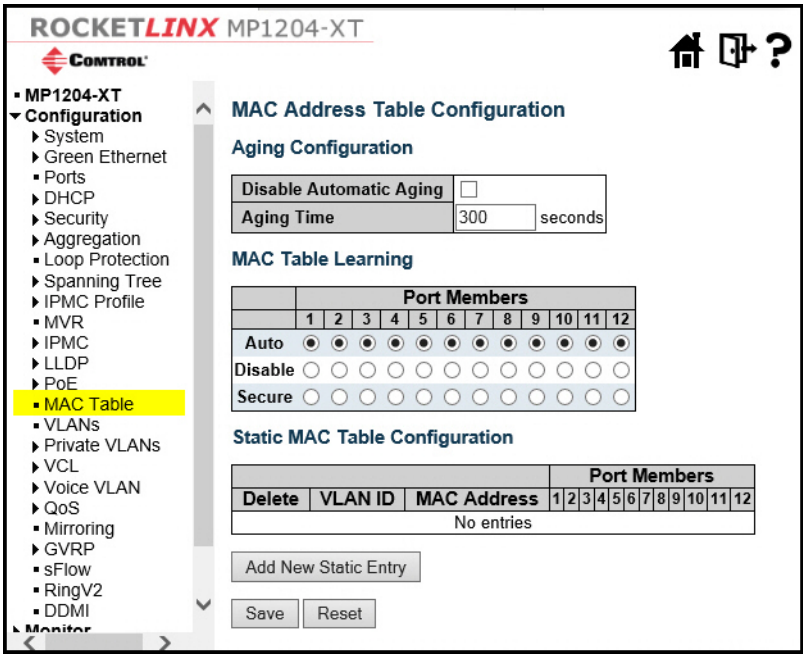
This page provides power reset entry configurations. The entry is used to control the power reset time on PoE port. It is allowed to create at maximum 5 entries for each PoE port.



Item	Configuration | PoE | PoE Reset
Delete	Check to delete the entry. The designated entry is deleted during the next save.
Day	Check marks indicate which day are members of the entry. Check or uncheck as needed to modify the entry.
Time (hh:mm)	**hh** - Select the hour. **mm** - Select the minute.
Add New	Click to add a new reset entry.

Configuration | 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.

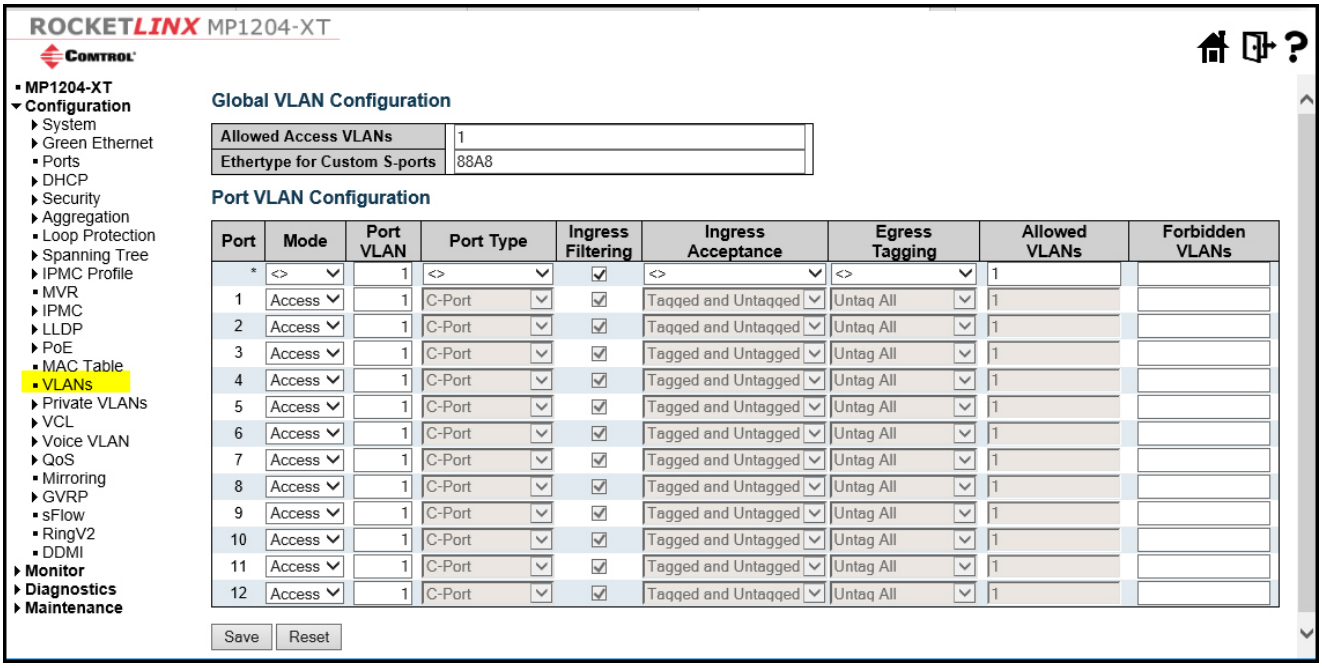


Item	Configuration | MAC Table
Aging Configuration	
Disable Automatic Aging	Disable the automatic aging of dynamic entries by ticking the item.
Aging Time	Enter a value in seconds. The allowed range is 10 to 1000000 seconds.
MAC Table Learning	
Auto	Learning is done automatically as soon as a frame with 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 Learning	
Delete	Check to delete the entry. It is deleted during the next save.
VLAN ID	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.

Item	Configuration | MAC Table (Continued)
Port Members	Check marks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Add New Static Entry	Click the **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 **Save**.

Configuration | VLANs

This page allows for controlling VLAN configuration on the MP1204-XT. The page is divided into a global section and a per-port configuration section.



Items	Configuration | VLANs
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 creates 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**.

Items	Configuration | VLANs (Continued)
Port VLAN Configuration	
Port	This is the logical port number of this row.
Mode	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. Whenever a particular mode is selected, the remaining fields in that row are either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port gets when the mode is applied. **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: • 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 **Trunk** ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics: • 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 **Hybrid** ports resemble **Trunk** ports in many ways, but adds additional port configuration features. In addition to the characteristics described for **Trunk** ports, **Hybrid** ports have these abilities: • 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	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. The Port VLAN is called an **Access VLAN** for ports in **Access** mode and Native VLAN for ports in **Trunk** or **Hybrid** mode.

Items	Configuration | VLANs (Continued)
Port Type	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. • **Unaware**: 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. • **C-Port**: 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 are tagged with a **C-tag**. • **S-Port**: 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 are tagged with an **S-tag**. • **S-Custom-Port**: 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 are tagged with the custom **S-tag**.
Ingress Filtering	**Hybrid** ports allow for changing ingress filtering. **Access** and **Trunk** ports always have ingress filtering enabled. • If ingress filtering is enabled (check box is checked), frames classified to a VLAN that the port is not a member of get discarded. • 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 never transmits frames classified to VLANs that it is not a member of.
Ingress Acceptance	**Hybrid** ports allow for changing the type of frames that are accepted on ingress. • **Tagged and Untagged** - Both tagged and untagged frames are accepted. • **Tagged Only** - Only tagged frames are accepted on ingress. Untagged frames are discarded. • **Untagged Only** - Only untagged frames are accepted on ingress. Tagged frames are discarded.
Egress Tagging	Ports in Trunk and Hybrid mode may control the tagging of frames on egress. • **Untag Port VLAN** - Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag. • **Tag All** - All frames, whether classified to the Port VLAN or not, are transmitted with a tag. • **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.
Allowed VLANs	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. The field's syntax is identical to the syntax used in the **Enabled VLANs** field. By default, a **Trunk** or **Hybrid** port becomes a member of all VLANs, and is therefore set to 1-4095. The field may be left empty, which means that the port does not become member of any VLANs.

Items	Configuration | VLANs (Continued)
Forbidden VLANs	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. 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.

Configuration | Private VLANs Menu

The following pages are under the Private VLAN menu:

- *Private VLANs | Membership* on Page 147
- *Private VLANs | Port Isolation* on Page 148

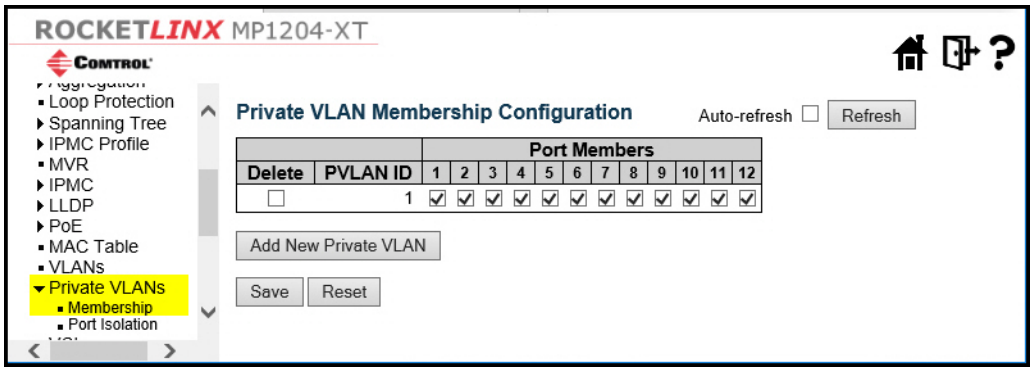
Private VLANs | Membership

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.



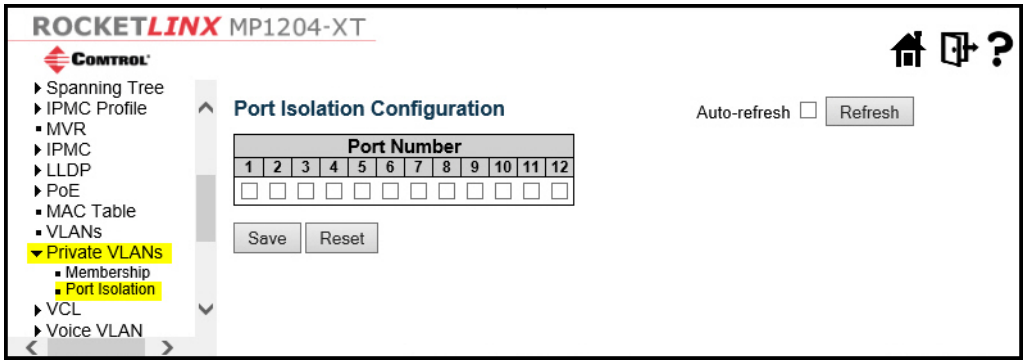
Item	Configuration | Private VLANs | Membership
Delete	To delete a private VLAN entry, check this box. The entry is deleted during the next save.
PVLAN ID	Indicates the ID of this particular private VLAN.
Port members	A row of check boxes for each port is displayed for each private VLAN ID. To include 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.

Item	Configuration | Private VLANs | Membership (Continued)
Add New Private VLAN	Click the **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 **Save**. The **Delete** button can be used to undo the addition of new Private VLANs.

Private VLANs | 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.



Item	Configuration | Private VLANs | Port Isolation
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.
Buttons	• Check the **Auto-refresh** box to refresh the page automatically. Automatic refresh occurs every 3 seconds. • Click the **Refresh** button to refresh the page immediately. • Click the **Save** button to save changes. • Click the **Reset** button to undo any changes made locally and revert to previously saved values.

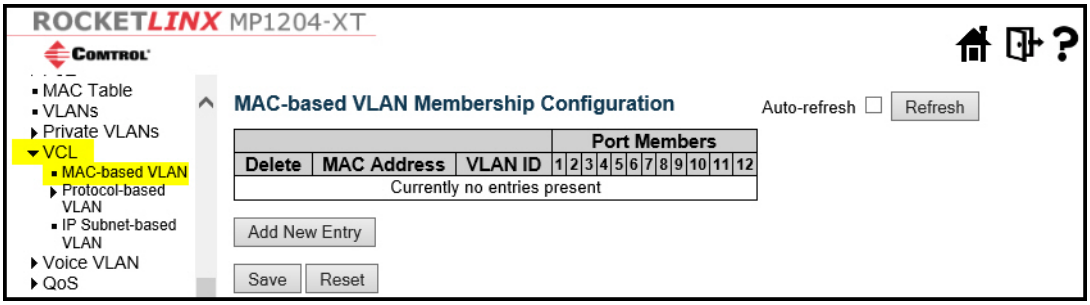
Configuration | VCL Menu

The following menus or pages are under the VCL menu.

- *VCL | MAC-Based VLAN* on Page 149
- *VCL | Protocol-Based VLAN Menu* on Page 150
- *VCL | IP Subnet-Based VLAN* on Page 152

VCL | MAC-Based VLAN

The MAC-based VLAN entries can be configured here. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries.



Item	Configuration | VCL | MAC-Based VLAN
Delete	To delete a MAC-based VLAN entry, check this box and press save. The entry is deleted in the stack.
MAC Address	Indicates the MAC address.
VLAN ID	Indicates the VLAN ID.
Port Members	A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Add New Entry	Click the **Add New Entry** button to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095. The MAC-based VLAN entry is enabled when you click the **Save** button. A MAC-based VLAN without any port members is deleted when you click **Save**. The **Delete** button can be used to undo the addition of new MAC-based VLANs. The maximum possible MAC-based VLAN entries are limited to 256.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Refreshes the displayed table.
|<<	Updates the table starting from the first entry in the MAC-based VLAN Table.
>>	Updates the table, starting with the entry after the last entry currently displayed.

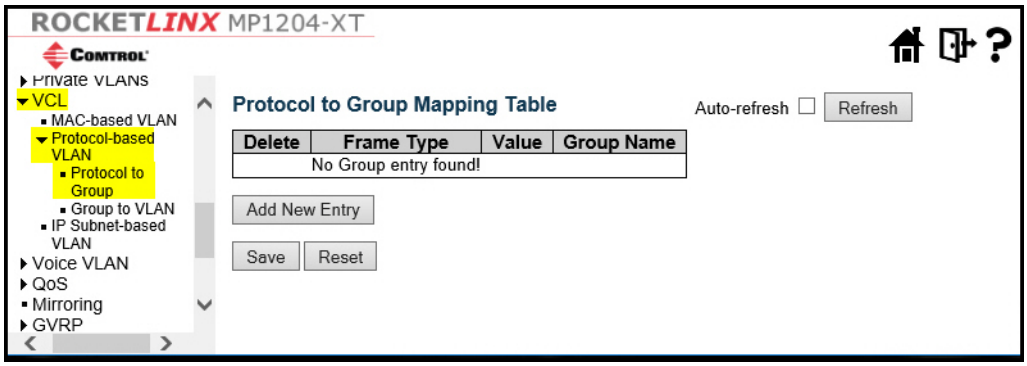
VCL | Protocol-Based VLAN Menu

The following pages are under the Protocol-Based VLAN menu

- *VCL | Protocol-Based VLAN | Protocol to Group* on Page 150
- *VCL | Protocol-Based VLAN | Group to VLAN* on Page 151

VCL | Protocol-Based VLAN | Protocol to Group

This page allows you to add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the MP1204-XT.

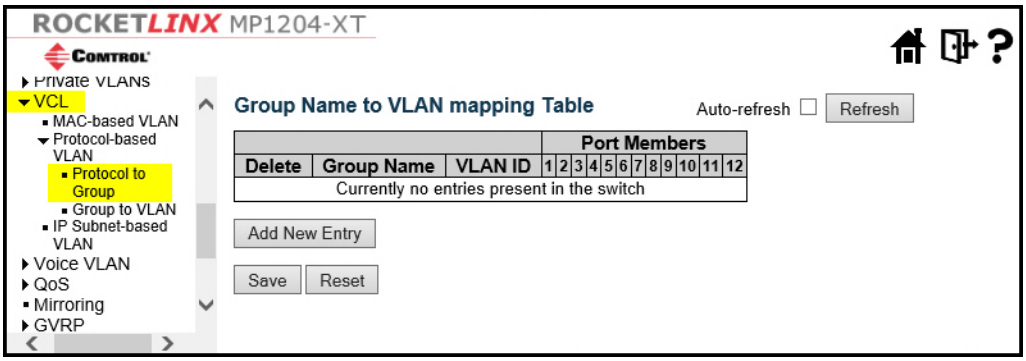


Item	Configuration | VCL | Protocol-Based VLAN | Protocol to Group
Delete	To delete a **Protocol** to **Group Name** map entry, check this box. The entry is deleted on the MP1204-XT during the next Save.
Frame Type	**Frame Type** can have one of the following values: • Ethernet • LLC • SNAP ***Note:*** *On changing the Frame type field, valid value of the following text field varies depending on the new frame type you selected.*
Value	Valid value that can be entered in this text field depends on the option selected from the preceding **Frame Type** selection menu. Below is the criteria for three different **Frame Types**: • For **Ethernet**: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff • For **LLC**: Valid value in this case is comprised of two different sub-values. - DSAP: 1-byte long string (0x00-0xff) - SSAP: 1-byte long string (0x00-0xff) • For **SNAP**: Valid value in this case also is comprised of two different sub-values. - **OUI**: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff. - **PID**: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the 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. In other words, if value of OUI field is 00-00-00 then value of PID is etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID is any value from 0x0000 to 0xffff.

Item	Configuration | VCL | Protocol-Based VLAN | Protocol to Group (Continued)
Group Name	A valid **Group Name** is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers(0-9). ***Note:*** *Special character and underscore(_) are not allowed.*
Add New Entry	Click to add a new entry in the mapping table.

VCL | Protocol-Based VLAN | Group to VLAN

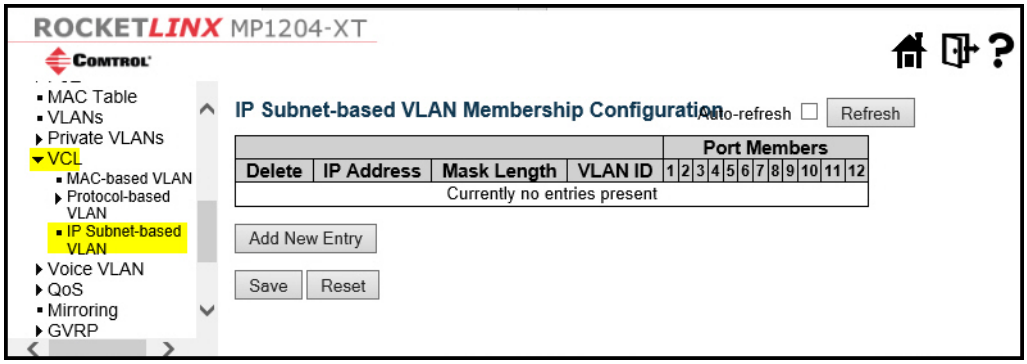
This page allows you to map a already configured Group Name to a VLAN for the MP1204-XT.



Item	Configuration | VCL | Protocol-Based VLAN | Group to VLAN
Delete	To delete a **Group Name** to VLAN map entry, check this box. The entry is deleted on the switch during the next **Save**.
Group Name	A valid **Group Name** is a string at the most 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special character is allowed. whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be pre-used by any other existing mapping entry on this page.
VLAN ID	Indicates the ID to which **Group Name** is mapped. A valid VLAN ID ranges from 1-4095.
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 a 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.
Add New Entry	Click the **Add New Entry** button to add a new entry in mapping table. An empty row is added to the table, 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 64.

VCL | IP Subnet-Based VLAN

The IP subnet-based VLAN entries can be configured here. This page allows for adding, updating and deleting IP subnet-based VLAN entries and assigning the entries to different ports. This page shows only static entries.



Item	Configuration | VCL | IP Subnet-based VLAN
Delete	To delete a IP subnet-based VLAN entry, check this box and press save. The entry is deleted in the stack.
VCE ID	Indicates the index of the entry. It is user configurable. It's value ranges from 0-128. If a VCE ID is 0, application auto-generates the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on **VCE ID.**
IP Address	Indicates the IP address.
Mask Length	Indicates the network mask length.
VLAN ID	Indicates the VLAN ID. **VLAN ID** can be changed for the existing entries.
Port Members	A row of check boxes for each port is displayed for each IP subnet-based VLAN entry. To include a port in a IP subnet-based VLAN, check the box. To remove or exclude the port from the IP subnet-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Add New Entry	Click to add a new IP subnet-based VLAN entry. Legal values for a VLAN ID are 1 through 4095.

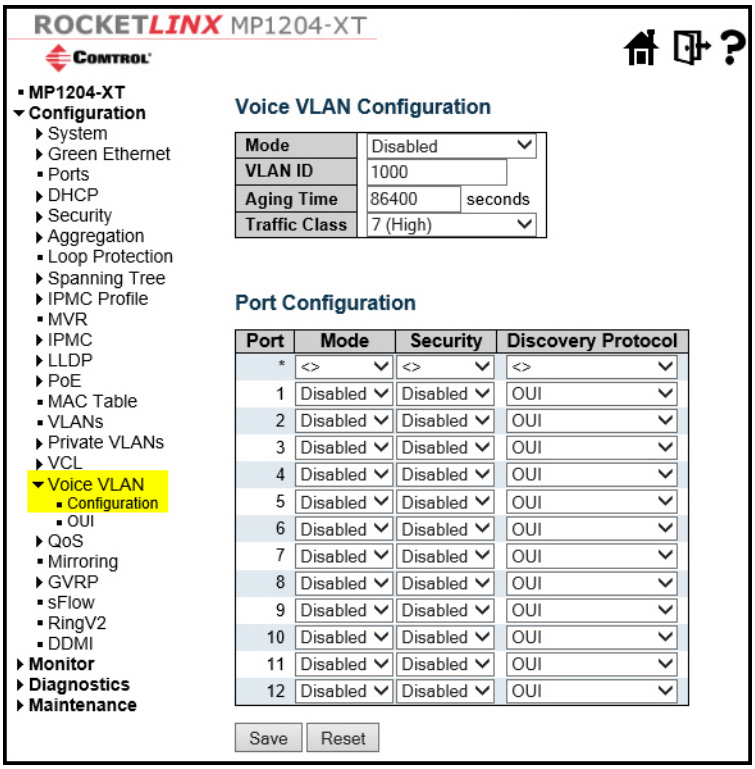
Configuration | Voice VLAN Menu

The following pages are under the Voice VLAN menu:

- *Voice VLAN | Configuration* on Page 153
- *Voice VLAN | OUI* on Page 155

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.

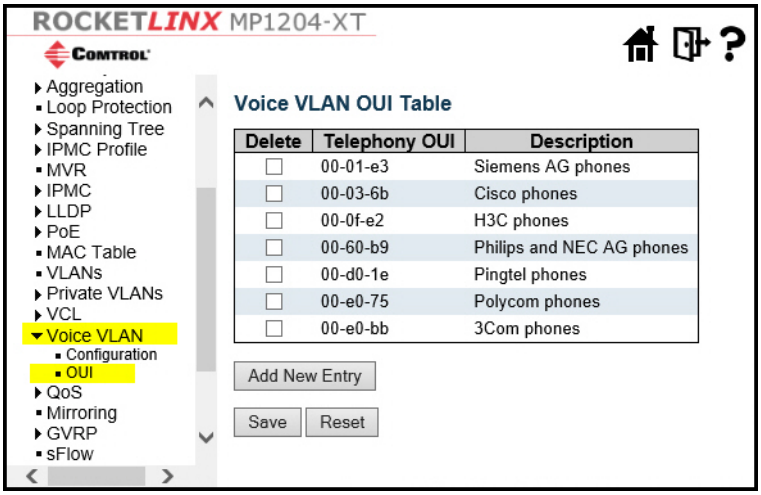


Item	Configuration | Voice VLAN | Configuration
Mode	Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are: • **Enabled**: Enable Voice VLAN mode operation. • **Disabled**: Disable Voice VLAN 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 is based on hardware aging time. The actual aging time is situated between the [age_time; 2 * age_time] interval.

Item	Configuration | Voice VLAN | Configuration (Continued)
Traffic Class	Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN is applied this class.
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 are 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 only works 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** restarts 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.

Voice VLAN | OUI

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



Item	Configuration | Voice VLAN | OUI
Delete	Check to delete the entry. It is 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.
Add New Entry	Click to add a new access management entry.

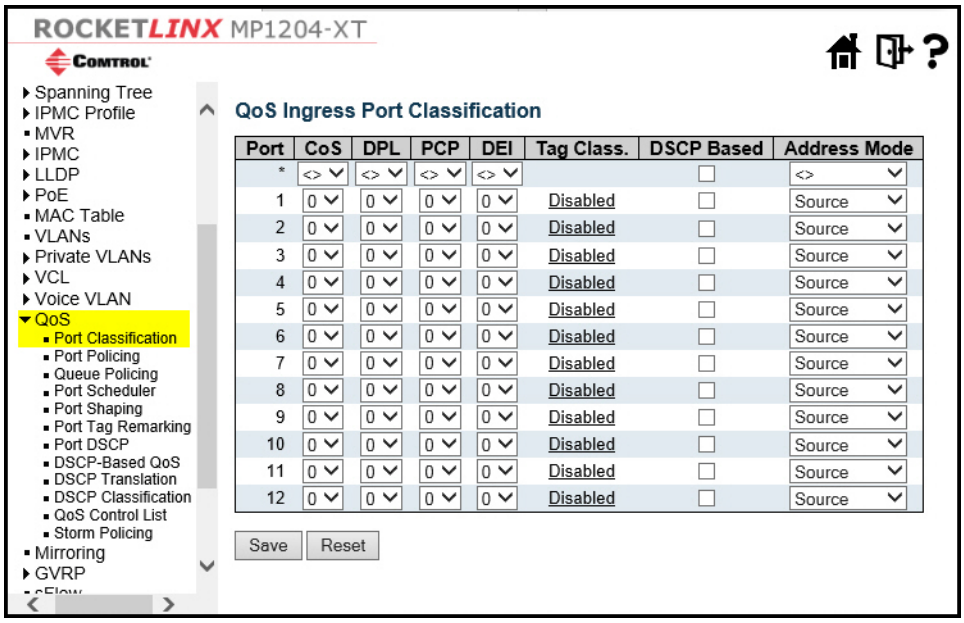
Configuration | QoS Menu

The following page are under the QoS menu.

- *QoS | Port Classification* on Page 156
- *QoS | Port Policing* on Page 157
- *QoS | Queue Policing* on Page 158
- *QoS | Port Scheduler* on Page 159
- *QoS | Port Shaping* on Page 160
- *QoS | Port Tag Remarking* on Page 161
- *QoS | Port DSCP* on Page 162
- *QoS | DSCP-Based QoS* on Page 163
- *QoS | DSCP Translation* on Page 164
- *QoS | DSCP Classification* on Page 165
- *QoS | QoS Control List* on Page 166
- *QoS | Storm Policing* on Page 170

QoS | Port Classification

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

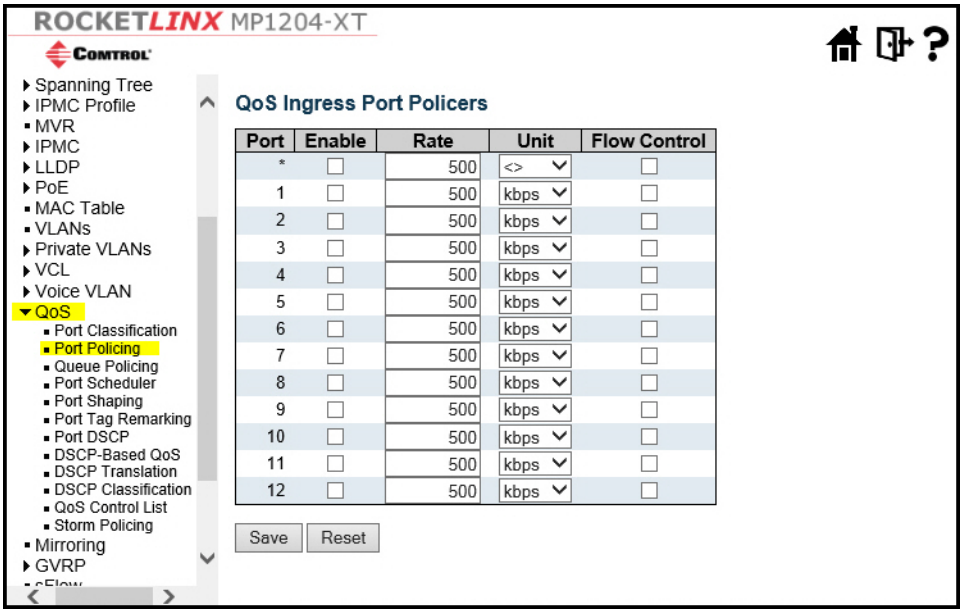


Item	Configuration | QoS | Port Classification
Port	The port number for which the configuration below applies.
CoS	Controls the default class of service. All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A **CoS** of 0 (zero) has the lowest priority. If 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**. The classified **CoS** can be overruled by a **QCL** entry. ***Note:*** *If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.*
DPL	Controls the default drop precedence level. All frames are classified to a drop precedence level. 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**. 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**. The classified **DPL** can be overruled by a **QCL** entry.
PCP	Controls the default **PCP** value. All frames are classified to a **PCP** value. 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.

Item	Configuration | QoS | Port Classification (Continued)
DEI	Controls the default **DEI** value. All frames are classified to a **DEI** value. 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.
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 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.

QoS | Port Policing

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

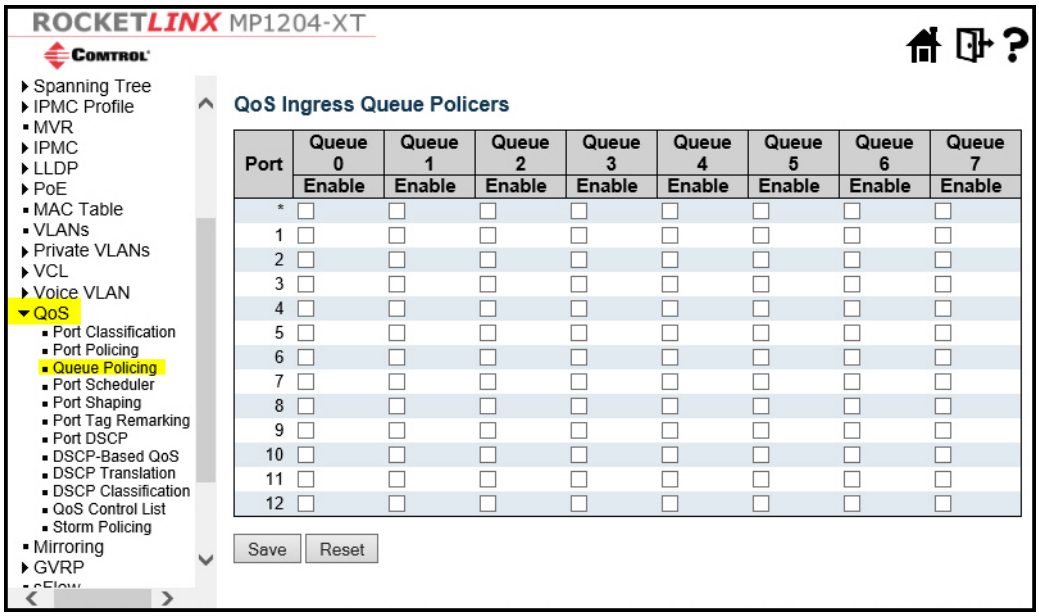


Item	Configuration | QoS | Port Policing
Port	The port number for which the configuration below applies.
Enabled	Controls whether the policer is enabled on this switch port.

Item	Configuration | QoS | Port Policing (Continued)
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.

QoS | Queue Policing

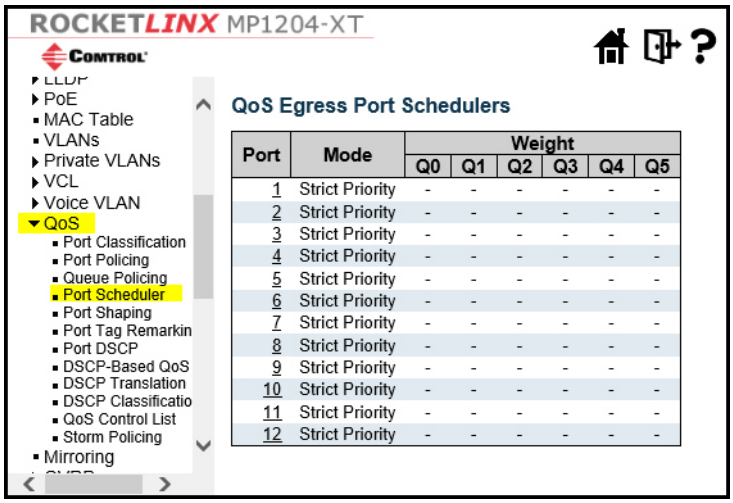
This page allows you to configure the Queue Policer settings for all switch ports.



Item	Configuration | QoS | Queue Policing
Port	The port number for which the configuration below applies.
Enable	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.

QoS | Port Scheduler

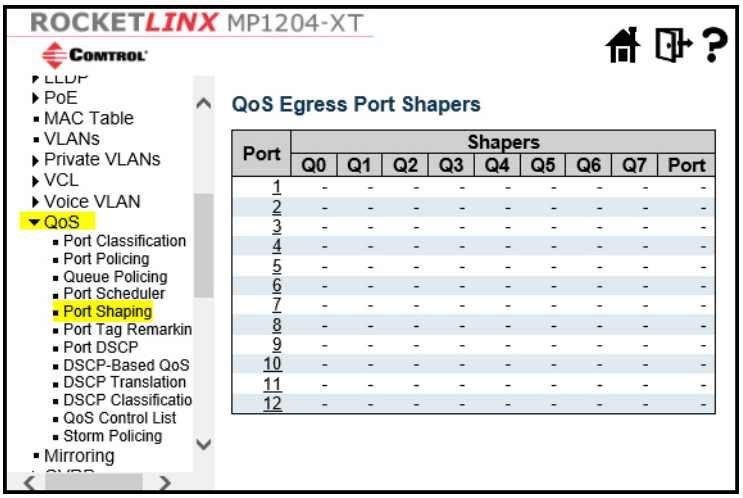
This page provides an overview of QoS Egress Port Schedulers for all switch ports.



Items	Configuration | QoS | Port Scheduler
Port	The logical port for the settings contained in the same row. Click 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 | Port Shaping

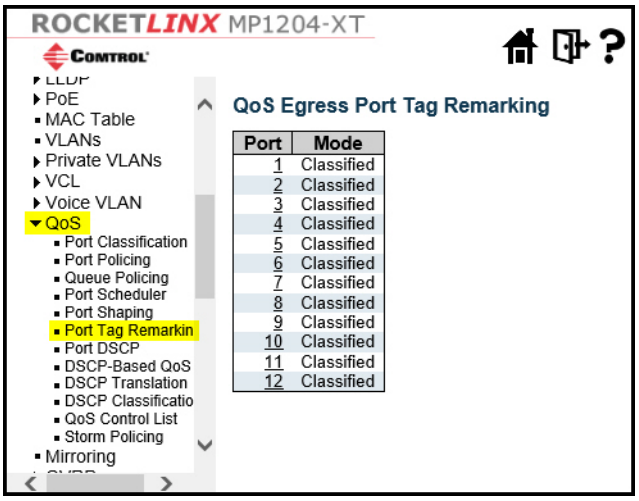
This page provides an overview of QoS Egress Port Shapers for all switch ports.



Item	Configuration | QoS | Port Shaping
Port	The logical port for the settings contained in the same row. Click the port number in order to configure the shapers.
Qn	Shows **disabled** or actual queue shaper rate - for example, **800 Mbps**.
Port #	Shows **disabled** or actual port shaper rate - for example, **800 Mbps**.

QoS | Port Tag Remarking

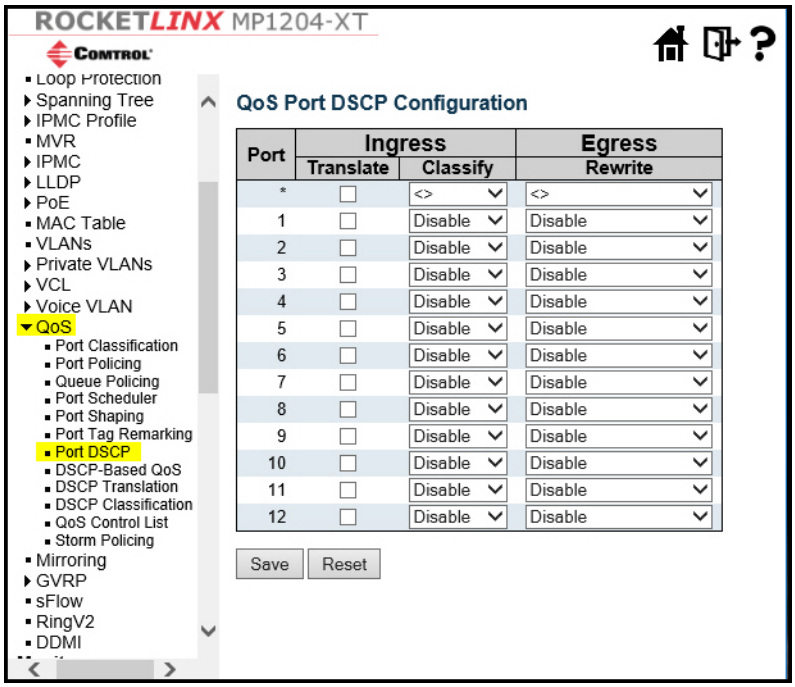
This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.



Item	Configuration | QoS |Port Tag Remarking
Port	The logical port for the settings contained in the same row. Click 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 | Port DSCP

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

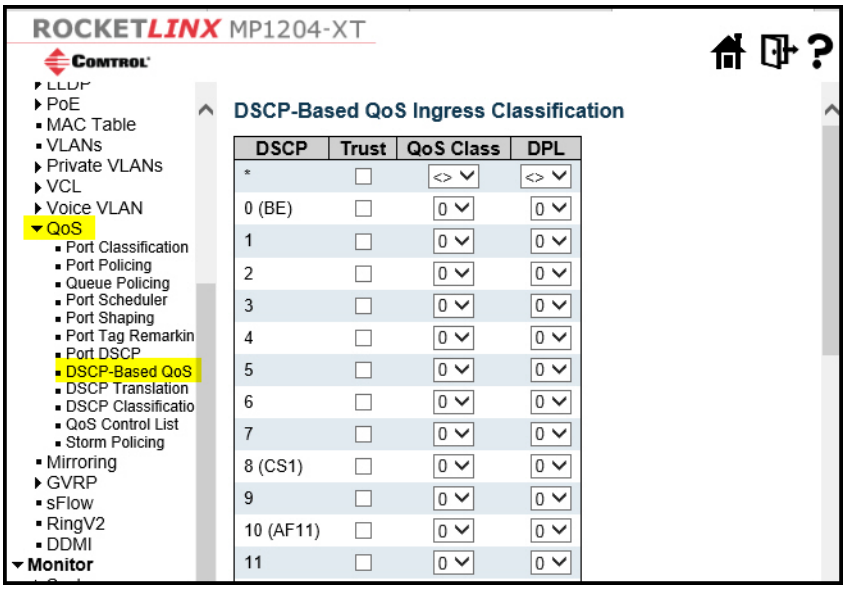


Item	Configuration | QoS | DSCP
Port	The **Port** column shows the list of ports for which you can configure DSCP ingress and egress settings.
Ingress	In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: • **Translate** • **Classify**
Translate	To enable the Ingress Translation click the check box.
Classify	Classification for a port have 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.

Item	Configuration | QoS | DSCP (Continued)
Egress	Port Egress Rewriting can be one of the following: • **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.

QoS | DSCP-Based QoS

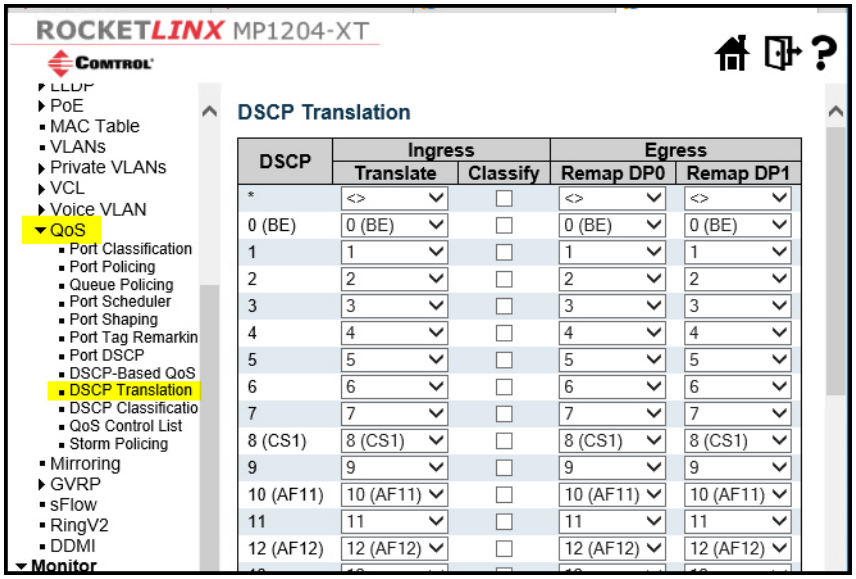
This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.



Item	Configuration | QoS | DSCP-Based QoS
DSCP	Maximum number of supported DSCP values are 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)

QoS | DSCP Translation

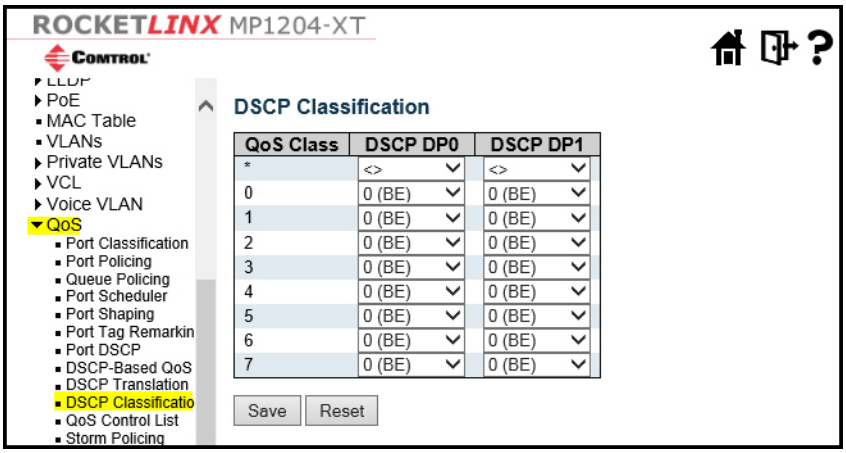
This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.



Item	Configuration | QoS | DSCP Translation
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 form 0 to 63.
Remap DP1	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

QoS | DSCP Classification

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

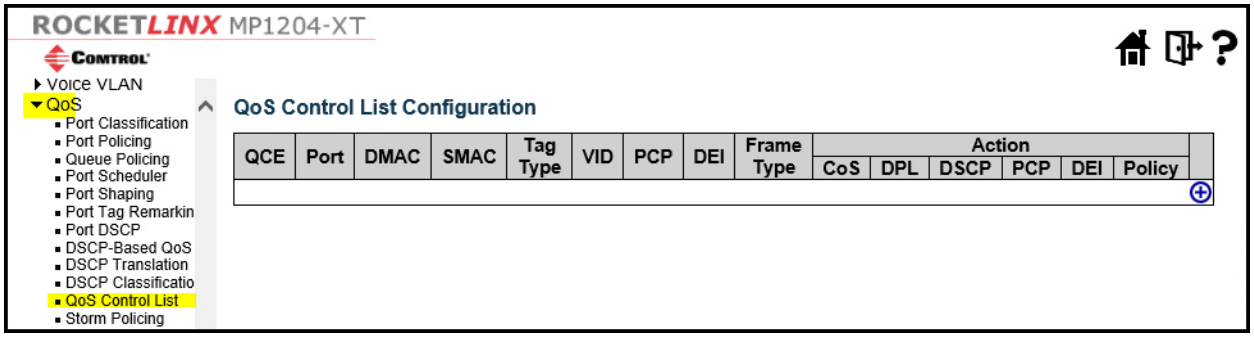


Item	Configuration | QoS | DSCP Classification
QoS Class	Actual QoS class.
DPL	Actual Drop Precedence Level.
DSCP	Select the classified DSCP value (0-63).

QoS | 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.

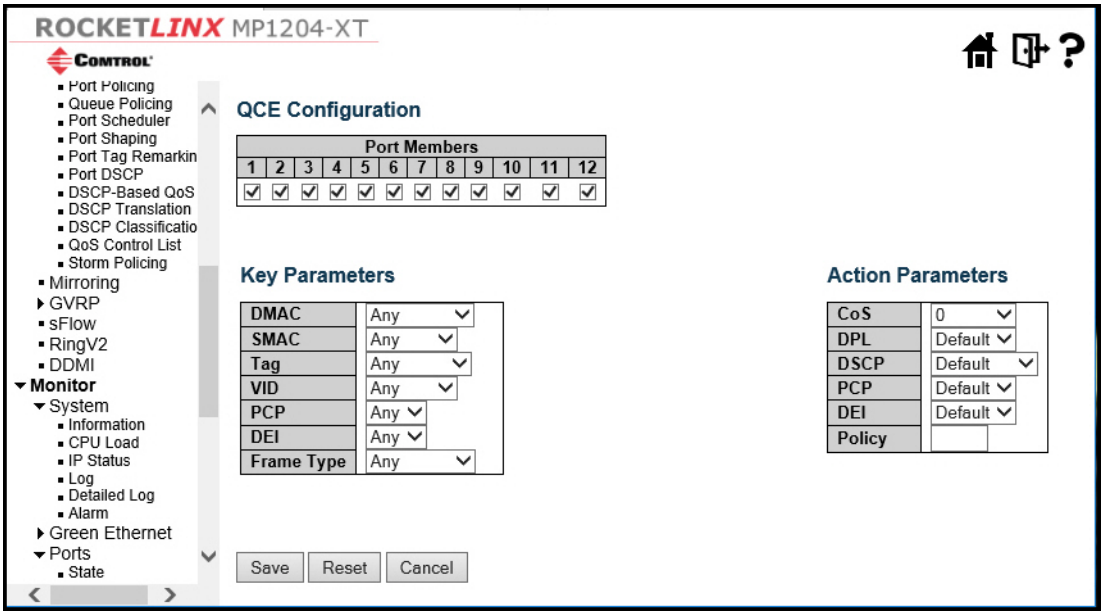
Click the lowest plus sign to add a new QCE to the list.



Item	Configuration | QoS | QoS Control List
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 are 0, 1 or **Any**.

Item	Configuration | QoS | QoS Control List (Continued)
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.
	Edits the QCE.
	Moves the QCE up the list.
	Moves the QCE down the list.
	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.



Item	Configuration | QoS | QoS Control List | QCE Configuration
Port Members	Check the checkbox button to include the port in the QCL entry. By default all ports are included.
Key parameters	Key configuration is described as below: **DMAC** Destination MAC address: Possible values are Unicast, Multicast, Broadcast or Any. **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. **Tag** Value of Tag field can be Untagged, Tagged or Any. **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. **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. **DEI** Valid value of DEI can be 0, 1 or Any. **Inner Tag** Value of Inner Tag field can be Untagged, Tagged, C-Tagged, S-Tagged or Any. **Inner VID** Valid value of Inner VLAN ID can be any value in the range: 1-4095 or Any. You can enter either a specific value or a range of VIDs. **Inner PCP** Valid value of Inner PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or a range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or Any. **Inner DEI** Valid value of Inner DEI can be 0, 1, or Any.

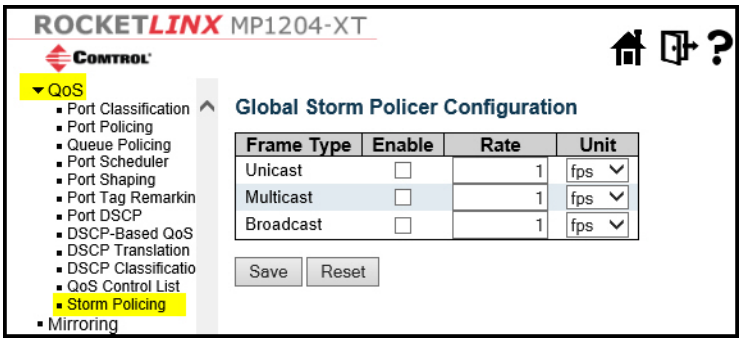
Item	Configuration | QoS | QoS Control List | QCE Configuration (Continued)
Key parameters (Continued)	**Frame Type** can have any of the following values: • **Any**: Allow all types of frames. • **EtherType**: Ether Type Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or Any. • **LLC**: SSAP Address Valid SSAP (Source Service Access Point) can vary from 0x00 to 0xFF or Any. • **DSAP** Address Valid DSAP (Destination Service Access Point) can vary from 0x00 to 0xFF or Any. • **Control** Valid Control field can vary from 0x00 to 0xFF or Any. • **SNAP**:PID Valid PID(a.k.a Ether Type) can be 0x0000-0xFFFF or Any. • **IPv4**: Protocol IP protocol number: (0-255, TCP or UDP) or Any. • **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. 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. • **IP Fragment** IPv4 frame fragmented option: Yes, No or Any. • **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. • **Sport** Source TCP/UDP port:(0-65535) or Any, specific or port range applicable for IP protocol UDP/TCP. • **Dport** Destination TCP/UDP port:(0-65535) or Any, specific or port range applicable for IP protocol UDP/TCP. • **IPv6**: Protocol IP protocol number: (0-255, TCP or UDP) or Any. • **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. • **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. • **Sport** Source TCP/UDP port:(0-65535) or Any, specific or port range applicable for IP protocol UDP/TCP. • **Dport** Destination TCP/UDP port:(0-65535) or Any, specific or port range applicable for IP protocol UDP/TCP.
Action Parameters	**CoS** Class of Service: (0-7) or Default. **DP** Drop Precedence Level: (0-1) or Default. **DSCP** DSCP: (0-63, BE, CS1-CS7, EF or AF11-AF43) or Default PCP (0-7) or Default. PCP and DEI cannot be set individually. **DEI** (0-1) or default. **Policy** ACL Policy number (0-255) or Default (empty field). Default means that the default classified value is not modified by this QCE.

QoS | 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.



Item	Configuration | QoS | Storm Policing
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.

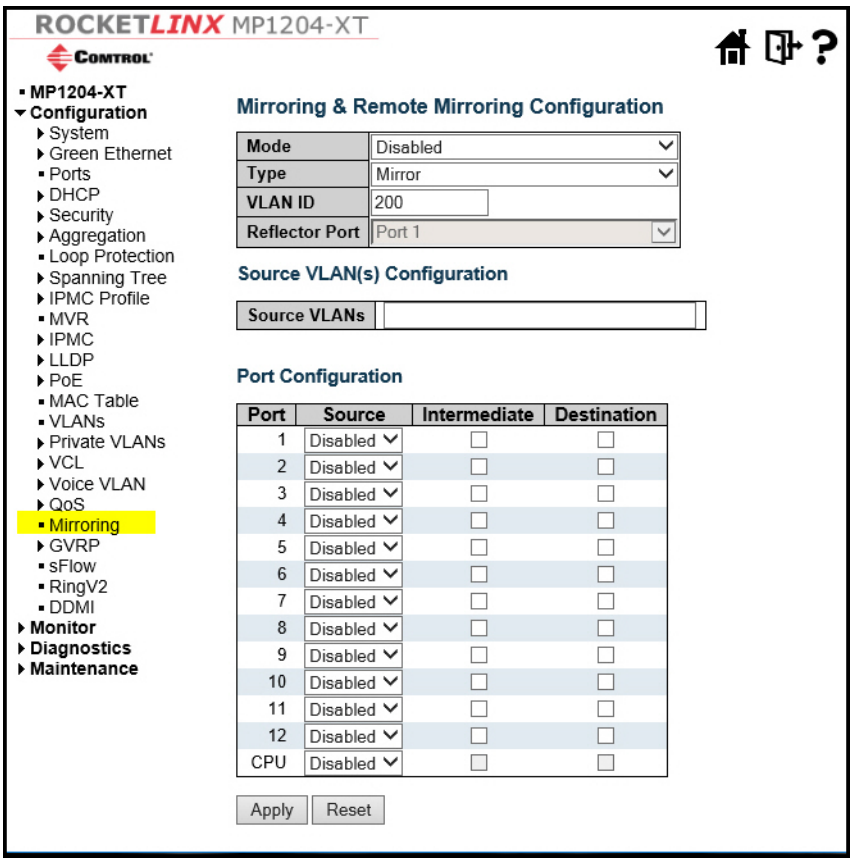
Configuration | Mirroring

Configure port Mirroring on this page.

To debug network problems, selected traffic can be copied, or mirrored, on a mirror port where a frame analyzer can be attached to analyze the frame flow.

The traffic to be copied on the mirror port is selected as follows:

- All frames received on a given port (also known as ingress or source mirroring).
- All frames transmitted on a given port (also known as egress or destination mirroring).



Item	Configuration | Mirroring
Mirroring & Remote Mirroring Configuration	
Mode	To Enabled/Disabled 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. • **Destination**: The switch is an end node for monitor flow. The destination port(s) and intermediate port(s) are located on this switch.

Item	Configuration | Mirroring (Continued)
VLAN ID	The VLAN ID points out where the monitor packet is copied 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. ***Note:*** *The reflector port needs to select only on Source switch type. The reflector port needs to disable MAC Table learning and STP. The reflector port only supports on pure copper ports.*
Source VLAN(s) Configuration	
Source VLANs	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. ***Note:*** *The Mirroring session shall have either ports or VLANs as sources, but not both.*
Port Configuration	
Port	The logical port for the settings contained in the same row.
Source	The following mirror modes are available. • **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	This check box 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	This check box 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. ***Note:*** *On mirror mode, the device only supports one destination port. The destination port needs to disable MAC Table learning.*

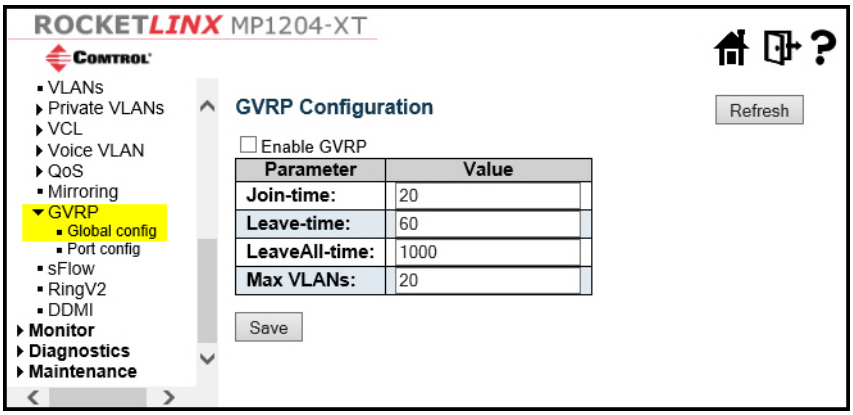
Configuration | GVRP Menu

The following pages are under the GVRP menu.

- *GVRP | Global Config* on Page 173
- *GVRP | Port Config* on Page 174

GVRP | Global Config

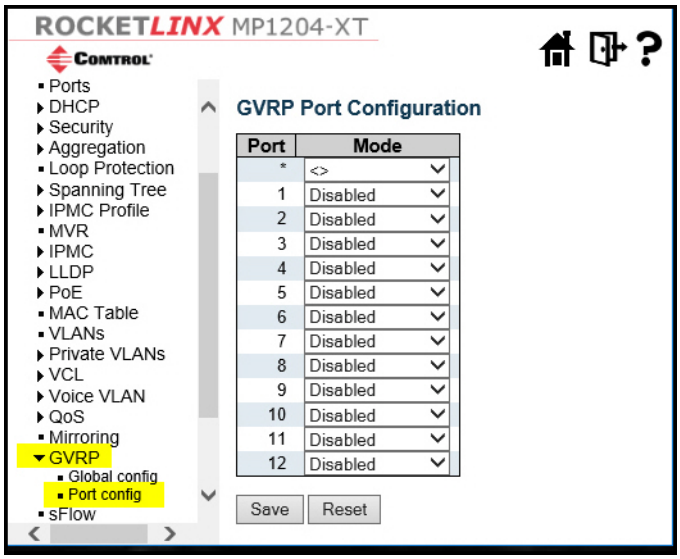
This page allows you to configure the basic GVRP Configuration settings for all switch ports.



Item	Configuration | GVRP | Global config
GVRP Protocol timers	
Join-time	**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	**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.
LeaveAll-time	**LeaveAll-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.

GVRP | Port Config

This page allows you to enable a port for GVRP.



This configuration can be performed either before or after GVRP is configured globally - the protocol operation is the same.

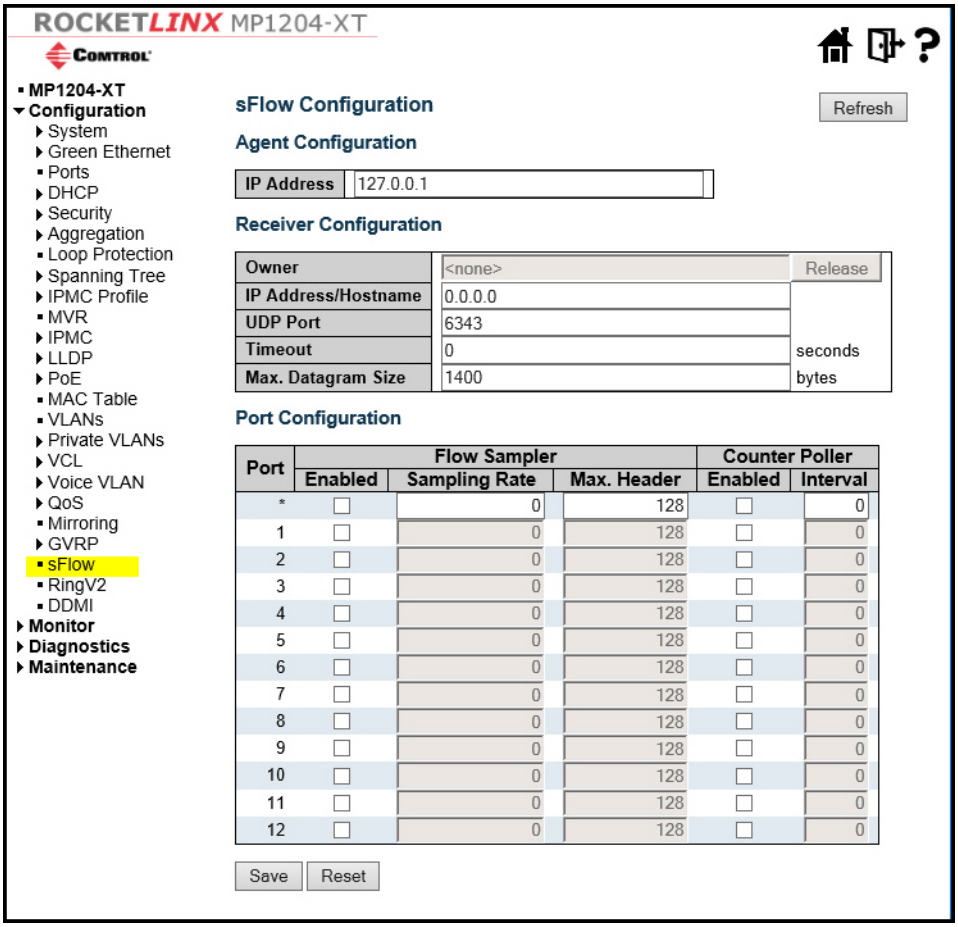
Item	Configuration | GVRP | Port Config
Port	The logical port that is to be configured.
Mode	Mode can be either Disabled or GVRP enabled. These values turn the GVRP feature off or on respectively for the port in question.

Configuration | SFlow

This page allows for configuring sFlow. The configuration is divided into two parts:

- Configuration of the sFlow receiver (also known as, sFlow collector)
- Configuration of per-port flow and counter samplers

sFlow configuration is not persisted to non-volatile memory, which means that a reboot disables sFlow sampling.



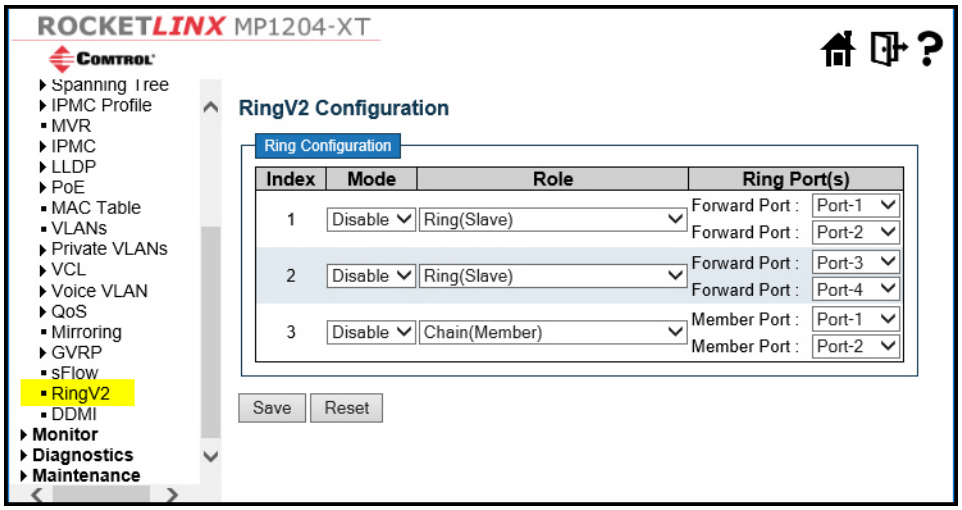
Item	Configuration | sFlow
Agent Configuration	
IP Address	The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that identifies this agent over extended periods of time. Both IPv4 and IPv6 addresses are supported.

Item	Configuration | sFlow (Continued)
Receiver Configuration	
Owner	Basically, sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows: • If sFlow is currently unconfigured/unclaimed, Owner contains **<none>**. • If sFlow is currently configured through Web or CLI, Owner contains **<Configured through local management>**. • If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver. • If sFlow is configured through SNMP, all controls - except for the **Release** button - are disabled to avoid inadvertent reconfiguration. The **Release** button allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request appears).
IP Address/ Hostname	The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.
UDP Port	The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.
Timeout	The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated by clicking the **Refresh** button. If locally managed, the timeout can be changed on the fly without affecting any other settings.
Max. Datagram Size	The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.
Port Configuration	
Port	The port number for which the configuration below applies.
Flow Sampler Enabled	Enables/disables flow sampling on this port.
Flow Sampler Sampling Rate	The statistical sampling rate for packet sampling. Set to N to sample on average 1/ Nth of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported sampling rate is requested, the MP1204-XT automatically adjusts it to the closest achievable. This is reported back in this field.
Flow Sampler Max. Header	The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.
Counter Poller Enabled	Enables/disables counter polling on this port.

Item	Configuration | sFlow (Continued)
Counter Poller Interval	With counter polling enabled, this specifies the interval - in seconds - between counter poller samples.

Configuration | RingV2

This page provides Ring related configuration.

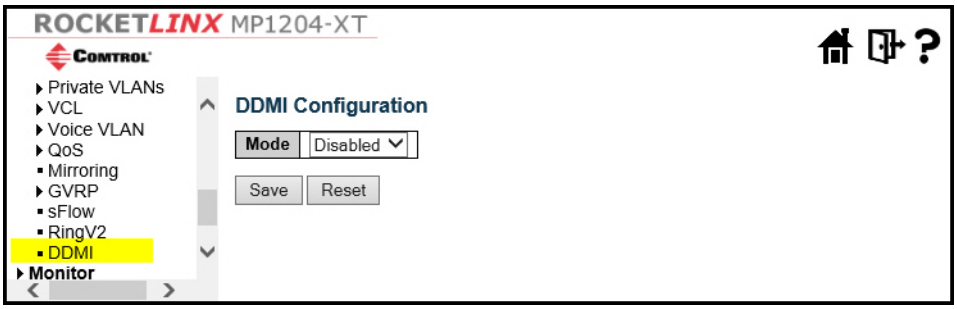


Item	Configuration | RingV2
Index	The group index. This parameter is used for easy identifying the ring when you configure it. • Group 1 (Index 1) - It supports configuration of ring. • Group 2 (Index 2) - It supports configuration of ring, coupling and dual-homing. • Group 3 (Index 3) - It supports configuration of chain and balancing-chain.
Mode	Enable Ring on the specific group. • When Group 1 or 2 is enabled, all configuration of Group 3 are reset to default. Group 3 all configuration options are locked. • To configure Group 3, both Group1 and 2 should be disabled first. When Group 3 is enabled, all configuration of Group1 and 2 are reset to default. Group 1 and 2 all configuration options are locked.

Item	Configuration | RingV2 (Continued)
Role	Configure the Ring group on this switch as specific role. **Group 1** - supports option of ring-master and ring-slave. • Ring - it could be master or slave. **Group 2** - supports configuration of the ring, coupling and dual-homing. • Ring - it could be master or slave. • Coupling - it could be primary and backup. • Dual-Homing **Group 3** - supports configuration of the chain and balancing-chain. • Chain - it could be head, tail or member. • Balancing Chain - it could be central-block, terminal-1/2 or member. ***Note:*** *Group 1 must be enabled before enable Group 2 to coupling. When Group 1 or 2 is enabled, the configuration of Group 3 are disabled. When Group 3 is enabled, the configuration of Group 1 and 2 are disabled.*
Ring Port(s)	Selecting ring port(s). Each ring port must be unique, which means that it CANNOT be configured in different groups and 2 ring ports between ring/chain CANNOT be the same. • When **Role** is ring/master, one ring port is forward port and another is block port. The block port is redundant port; it is blocking port in normal state. • When **Role** is ring/slave, both ring ports are forward port. • When **Role** is coupling/primary, only need one ring port named primary port. • When **Role** is coupling/backup, only need one ring port named backup port. This backup port is redundant port; it is blocking port in normal state. • When **Role** is dual-homing, one ring port is primary port and another is backup port. This backup port is redundant port; it is blocking port in normal state. • When **Role** is chain/head, one ring port is member port and another is head port. Both ring ports are forwarding port in normal state. • When **Role** is chain/tail, one ring port is member port and another is tail port. The tail port is redundant port; it is blocking port in normal state. • When **Role** is chain/member, both ring ports are member port. Both ring ports are forwarding port in normal state. • When **Role** is balancing-chain/central-block, one ring port is member port and another is block port. The block port is redundant port; it is blocking port in normal state. • When **Role** is balancing-chain/terminal-1/2, one ring port is member port and another is terminal port. Both ring ports are forwarding port in normal state. • When **Role** is balancing-chain/member, both ring ports are member port. Both ring ports are forwarding port in normal state.

Configuration | DDMI

Configure DDMI on this page.



Item	Configuration | DDMI
Mode	
Enabled	Enable DDMI mode operation.
Disabled	Disable DDMI mode operation.

Monitor Pages

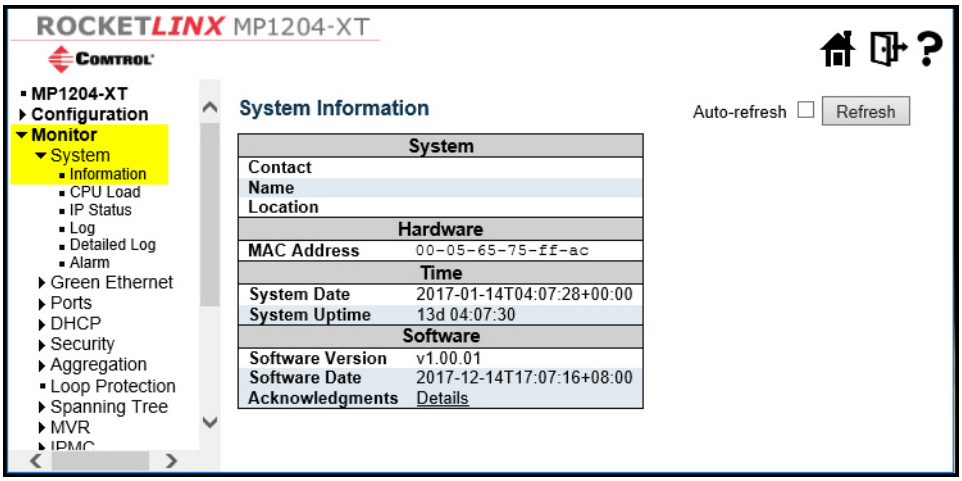
Monitor | System Menus

The following are under the **System** menu:

- System | Information on Page 181
- System | CPU Load on Page 182
- System | IP Status on Page 183
- System | Log on Page 184
- System | Detailed Log on Page 185
- System | Alarm on Page 186

System | Information

MP1204-XT system information is report on this page.



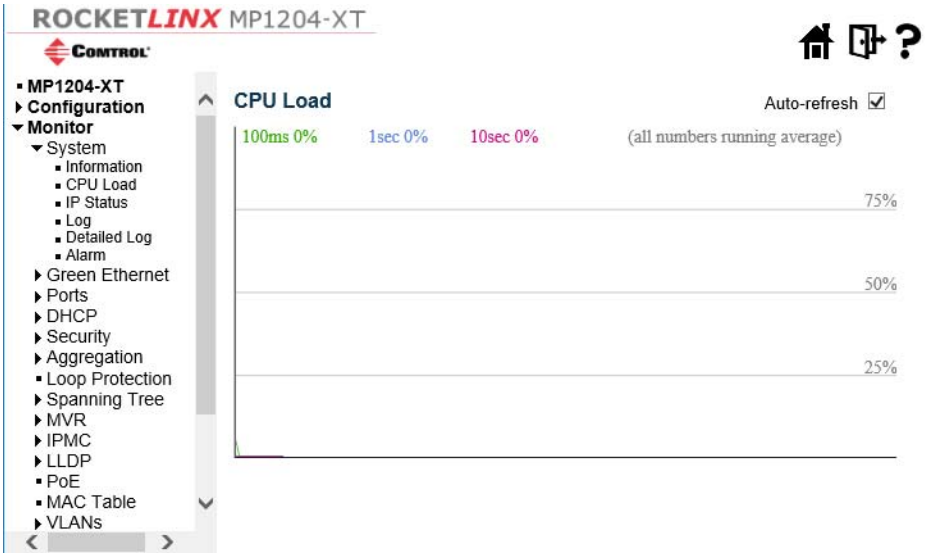
Item	Monitor | System | Information
Contact	The system contact configured in **Configuration | System | Information | System Contact**.
Name	The system name configured in **Configuration | System | Information | System Name**.
Location	The system location configured in **Configuration | System | Information | System Location**.
MAC Address	The MAC Address of this switch.
Chip ID	The Chip ID 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.

Item	Monitor | System | Information (Continued)
Software Version	The software version of this switch.
Software Date	The date when the switch software was produced.

System | CPU Load

This page displays the CPU load, using a graph.

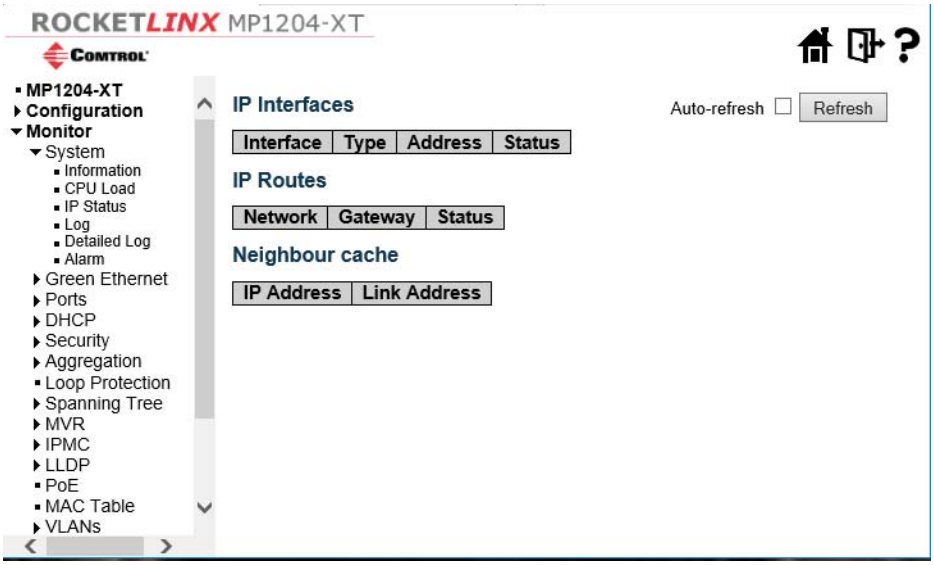
The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 1~256 samples (maximum 256) are graphed, and the last numbers are displayed as text as well.



Check the Auto-refresh box to refresh the page automatically, every 3 seconds.

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 neighbor cache (ARP cache) status.



Item	Monitor | System |
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.

System | Log

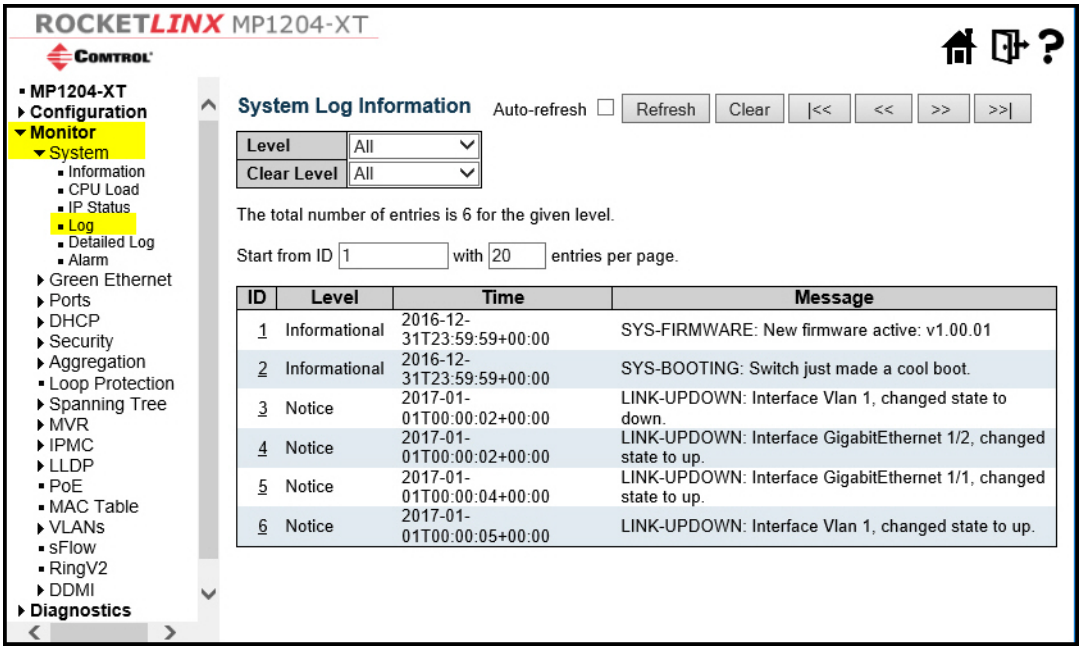
Each page shows up to 999 table entries, selected through the **entries per page** input field. When first visited, the page shows the beginning entries of this table.

- 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 are cleared.
- To clear specific system log entries, select the clear level first then click the **Clear** button.
- The **Start from ID** input field allows you to change the starting point in this table. Clicking the **Refresh** button updates 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 [>>] uses 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.

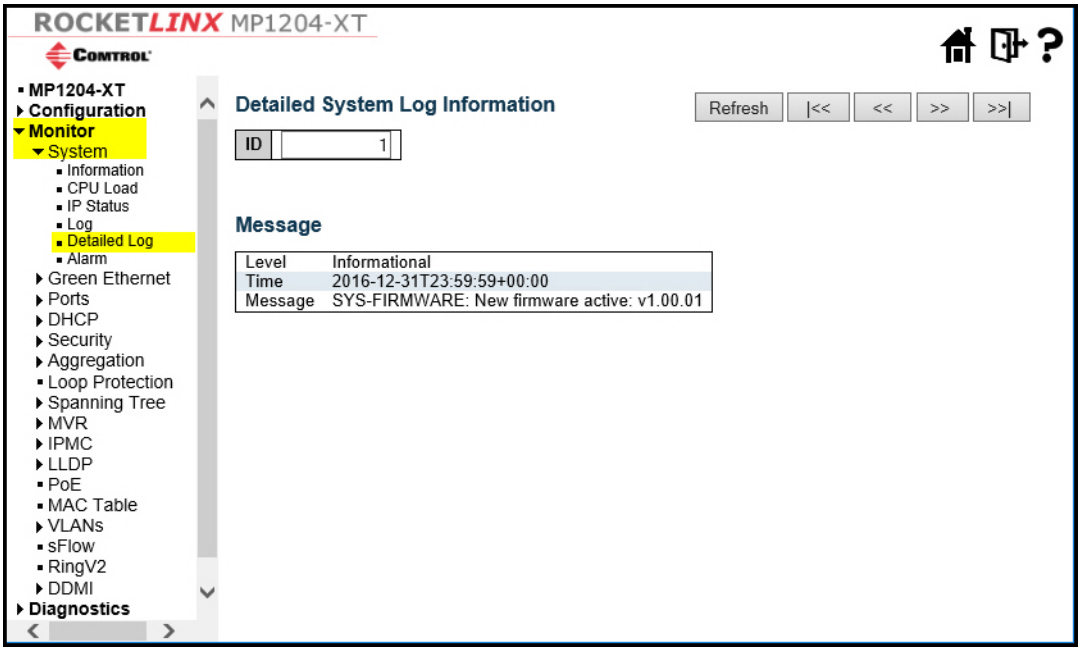


Item	Monitor | System | Log
ID	The identification of the system log entry.
Level	The level of the system log entry. • **Error**: The system log entry is belonged error level. • **Warning**: The system log entry is belonged warning level. • **Notice**: Displays port state changes • **Informational**: The system log entry is belonged information level.
Time	The occurred time of the system log entry.
Message	The detail message of the system log entry.

Item	Monitor | System | Log
|<<	Updates the table entries starting from the current entry.
<<	Updates the table entries ending at the last entry currently displayed.
>>	Updates the table entries starting from the last entry currently displayed.
>>|	Updates the table entries ending at the last available entry.

System | Detailed Log

The MP1204-XT system detailed log information is provided here.

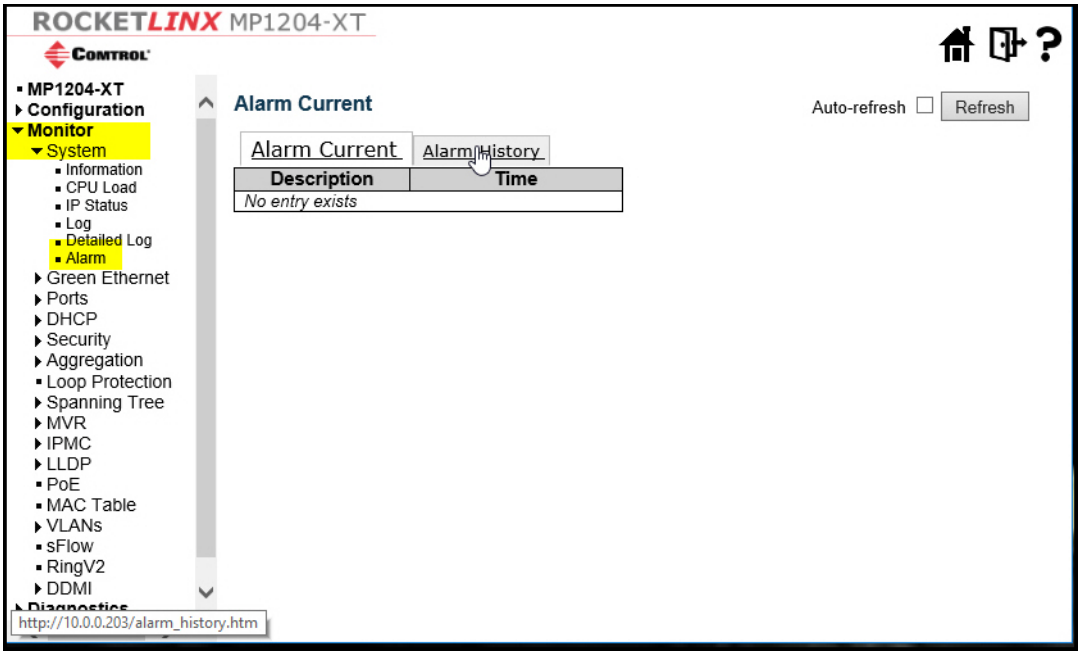


Item	Monitor | System | Detailed Log
ID	The ID (>= 1) of the system log entry.
Message	The detailed message of the system log entry.
Refresh	Updates the system log entry to the current entry ID.
|<<	Updates the system log entry to the first available entry ID.
<<	Updates the system log entry to the previous available entry ID.

Item	Monitor | System | Detailed Log
>>	Updates the system log entry to the next available entry ID.
>>|	Updates the system log entry to the last available entry ID.

System | Alarm

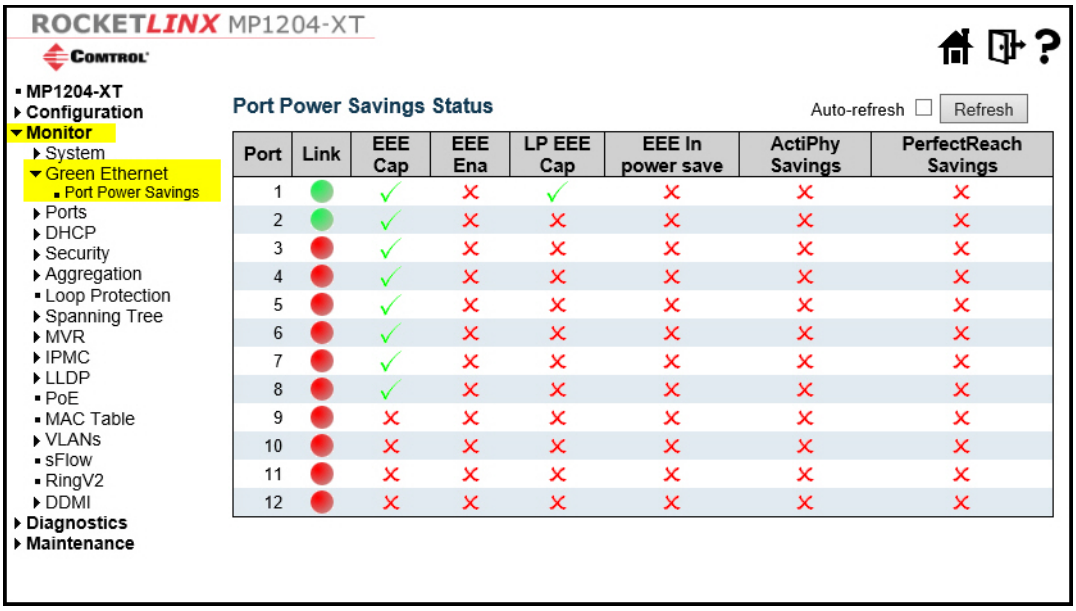
The current alarm is displayed on this page.



Item	Monitor | System | Alarm
Description	Alarm Type Description.
Time	Alarm occurrence date time.

Monitor | Green Ethernet - Port Power Savings Menu

This page displays current status for EEE.



Port	Link	EEE Cap	EEE Ena	LP EEE Cap	EEE In power save	ActiPhy Savings	PerfectReach Savings
1	green	✓	✗	✓	✗	✗	✗
2	green	✓	✗	✗	✗	✗	✗
3	red	✓	✗	✗	✗	✗	✗
4	red	✓	✗	✗	✗	✗	✗
5	red	✓	✗	✗	✗	✗	✗
6	red	✓	✗	✗	✗	✗	✗
7	red	✓	✗	✗	✗	✗	✗
8	red	✓	✗	✗	✗	✗	✗
9	red	✗	✗	✗	✗	✗	✗
10	red	✗	✗	✗	✗	✗	✗
11	red	✗	✗	✗	✗	✗	✗
12	red	✗	✗	✗	✗	✗	✗

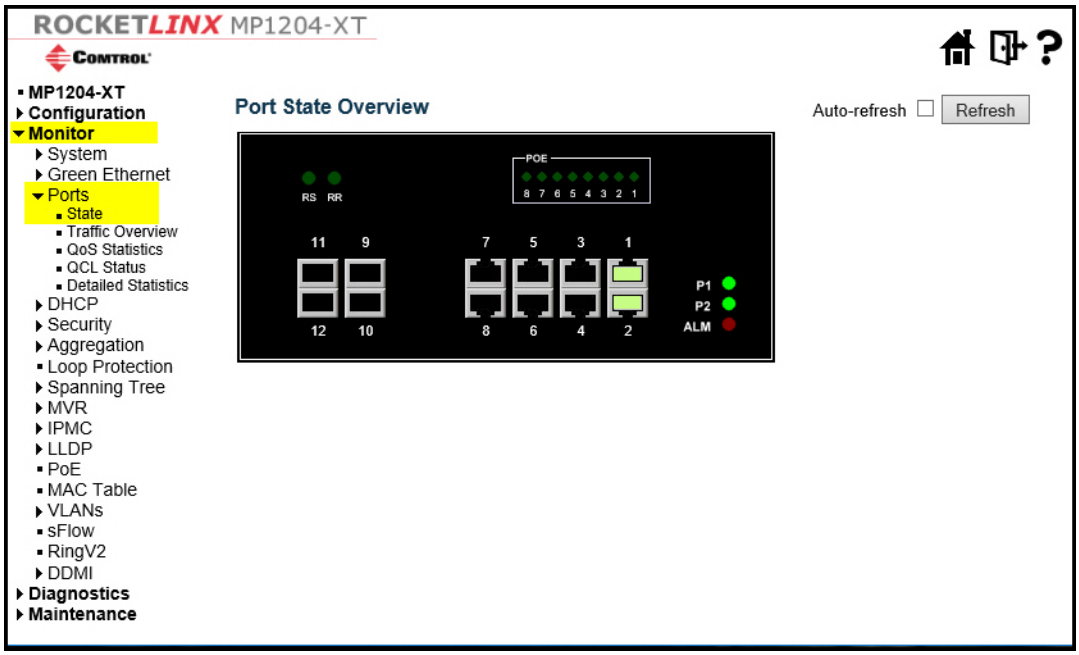
Item	Monitor | Green Ethernet | Port Power Savings
Port	This is the logical port number for this row.
Link	Shows if the link is up for the port (green = link up, red = link down).
EEE	Shows if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page).
LP EEE cap	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 MP1204-XT powers 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.

Monitor | Port Menus

The following pages are under the **Monitor | Port** menu.

Ports | State

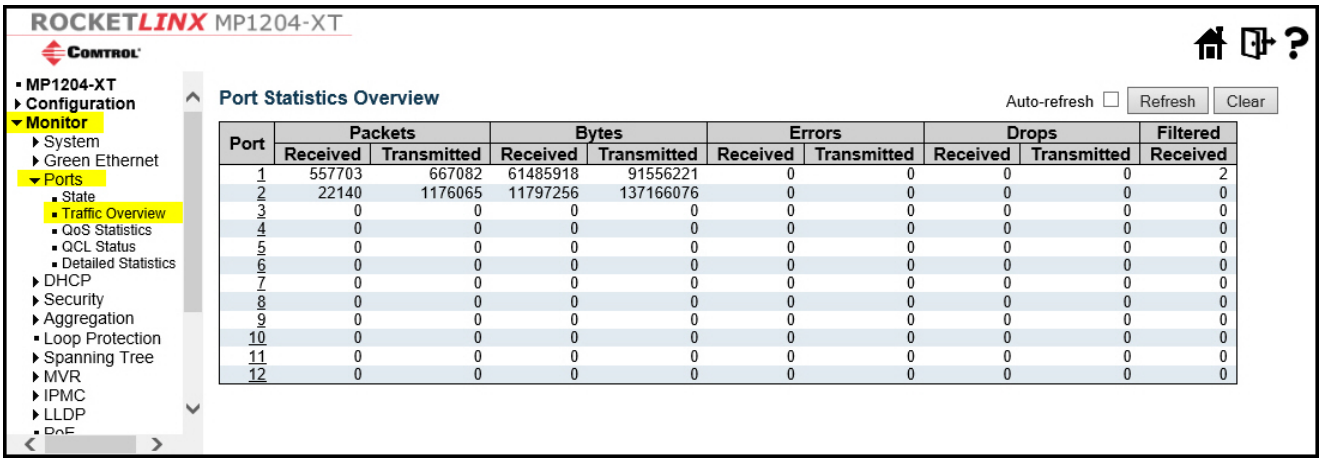
This page provides an overview of the current switch port states.



RJ45 ports			
SFP ports			
State	Disabled	Down	Link

Ports | Traffic Overview

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

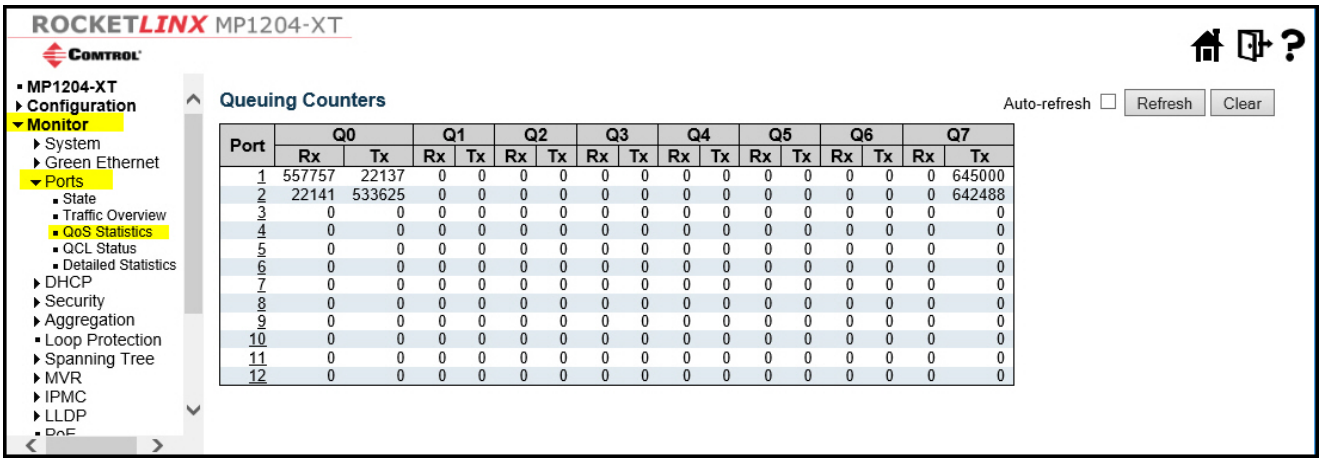


Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	557703	667082	61485918	91556221	0	0	0	0	2
2	22140	1176065	11797256	137166076	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	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
12	0	0	0	0	0	0	0	0	0

Item	Monitor | Ports | Traffic Overview
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.

Ports | QoS Statistics

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

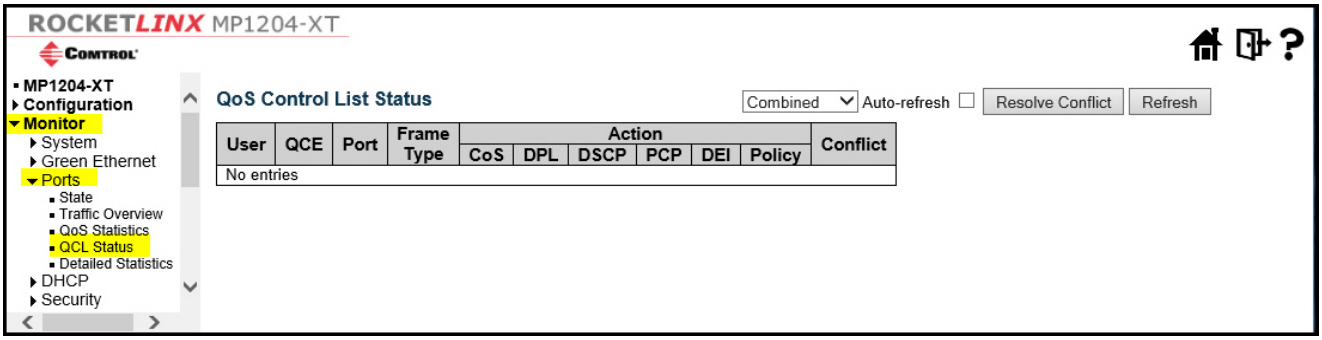


Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	557757	22137	0	0	0	0	0	0	0	0	0	0	0	0	0	645000
2	22141	533625	0	0	0	0	0	0	0	0	0	0	0	0	0	642488
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	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
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Item	Monitor | Ports | QoS Statistics
Port	The logical port for the settings contained in the same row.
Qn	There are eight QoS queues per port. Q0 is the lowest priority queue.
Rx/Tx	The number of received and transmitted packets per queue

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.



User	QCE	Port	Frame Type	Action						Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	

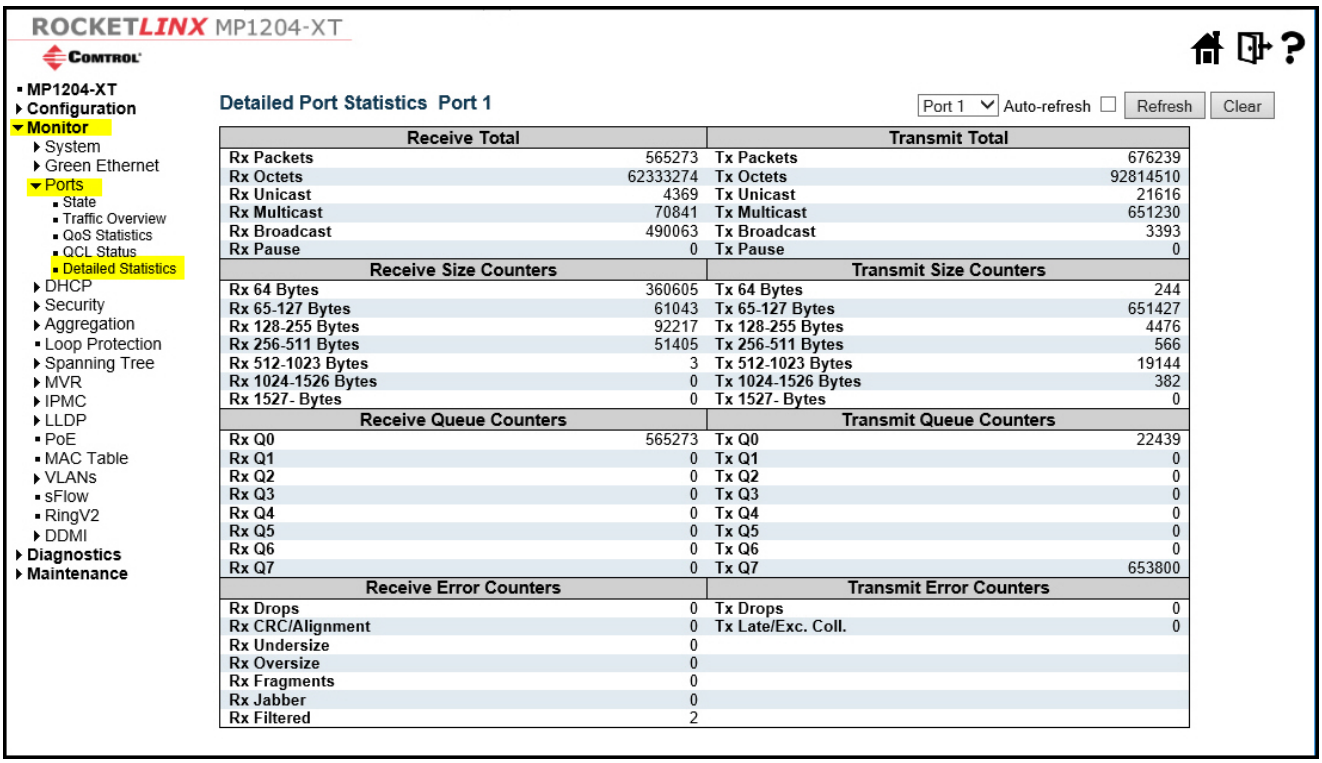
Item	Monitor | Ports | QCL Status
User	Indicates the QCL user.
QCE	Indicates the QCE id.
Port	Indicates the list of ports configured with the QCE.

Item	Monitor | Ports | QCL Status (Continued)
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.
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.

Ports | 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.



Item	Monitor | Ports | Detailed Statistics
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	TThe 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.

Item	Monitor | Ports | Detailed Statistics (Continued)
Receive Error Counters	
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. Short frames are frames that are smaller than 64 bytes. 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.

Monitor | DHCP Menus

The following pages are under the **DHCP** menu:

- DHCP | Server Sub-Menus on Page 193
- DHCP | Snooping Table on Page 196
- DHCP | Relay Statistics on Page 197
- DHCP | Detailed Statistics on Page 198

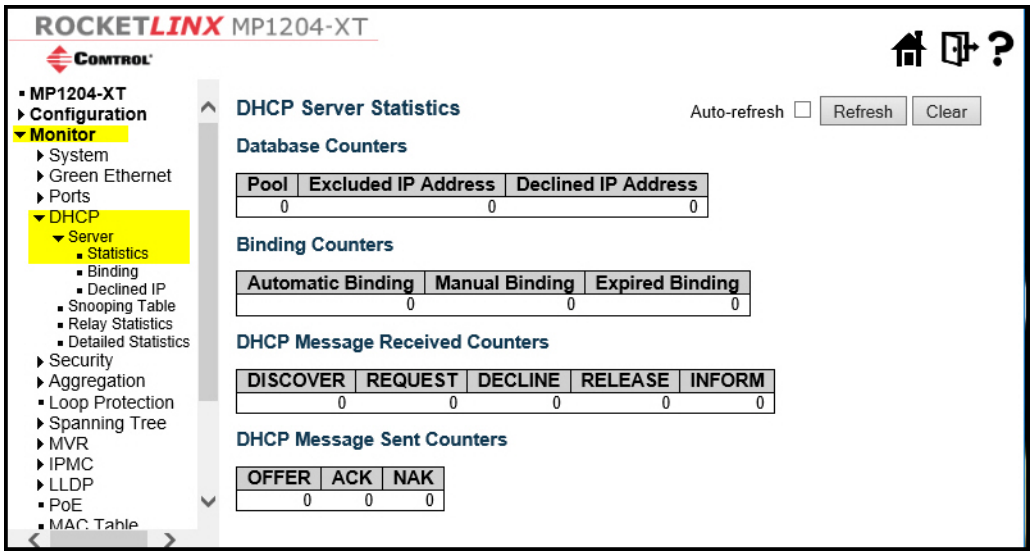
DHCP | Server Sub-Menus

The following pages are under the **DHCP | Server** sub-menu.

- DHCP | Server | Statistics on Page 194
- DHCP | Server | Binding on Page 195
- DHCP | Server | Declined IP on Page 196

DHCP | Server | Statistics

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

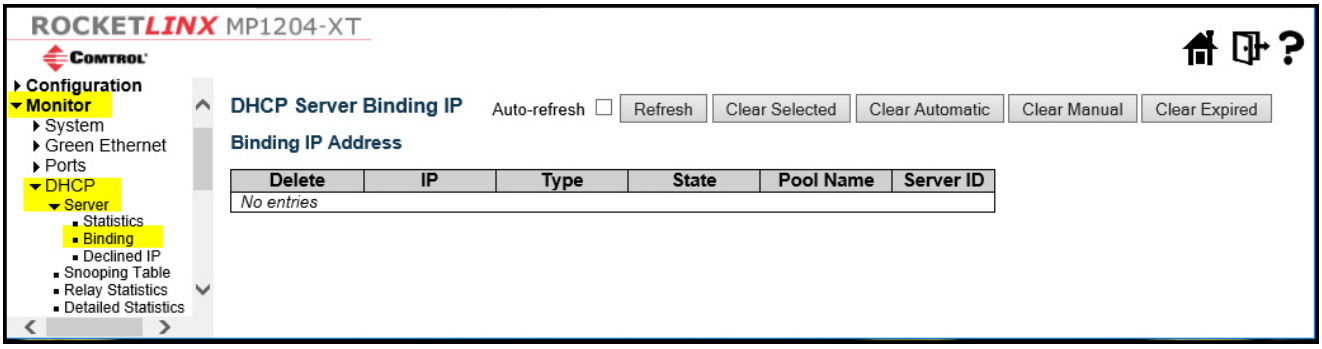


Item	Monitor | DHCP | Server |Statistics
Database Counters	
Pool	Number of pools.
Excluded IP Address	Number of excluded IP address ranges.
Declined IP Address	Number of declined IP addresses.
Binding Counters	
Automatic Binding	Number of bindings with network-type pools.
Manual Binding	Number of bindings 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	
OFFER	Number of DHCP OFFER messages sent.
ACK	Number of DHCP ACK messages sent.

Item	Monitor | DHCP | Server |Statistics (Continued)
NAK	Number of DHCP NAK messages sent.

DHCP | Server | Binding

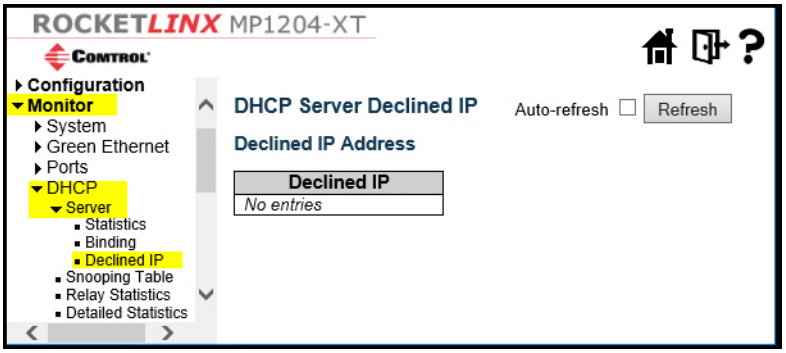
This page displays bindings generated for DHCP clients.



Item	Monitor | DHCP | Server | Binding
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.
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.

DHCP | Server | Declined IP

This page displays declined IP addresses.



Item	Monitor | DHCP | Server | Declined IP
Declined IP	List of IP addresses declined.

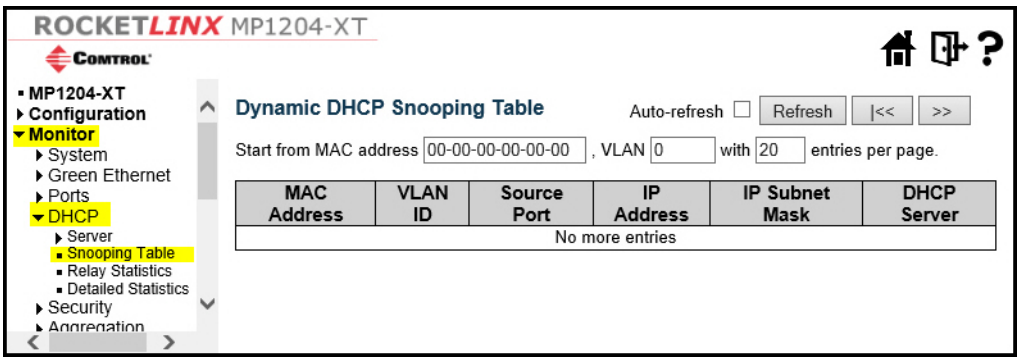
DHCP | Snooping Table

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 page shows the first 20 entries from the beginning of the Dynamic DHCP snooping Table.

The **MAC address** and **VLAN** input fields allows you to select the starting point in the Dynamic DHCP snooping Table. Clicking the **Refresh** button updates 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 >> uses 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.

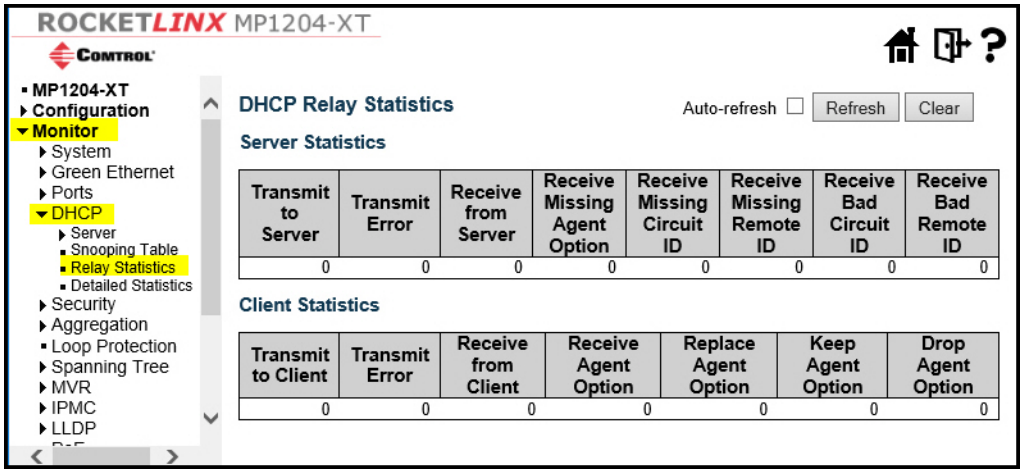


Item	Monitor | DHCP | Snooping Table
MAC Address	User MAC address of the entry.
VLAN ID	VLAN-ID in which the DHCP traffic is permitted.
Source Port	Switch Port Number for which the entries are displayed.
IP Address	User IP address of the entry.

Item	Monitor | DHCP | Snooping Table
IP Subnet Mask	User IP subnet mask of the entry.
DHCP Server Address	DHCP Server address of the entry.

DHCP | Relay Statistics

This page provides statistics for DHCP relay.

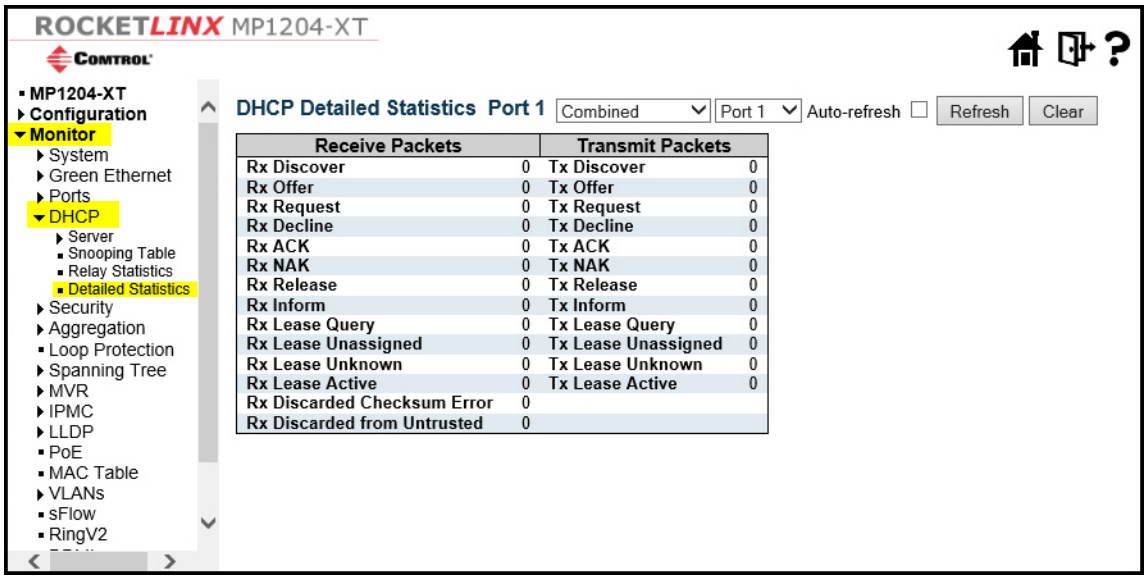


Item	Monitor | DHCP | Relay Statistics
Server Statistics	
Transmit to Server	The number of packets that are relayed from client to server.
Transmit Error	The number of packets that resulted in errors while being sent to clients.
Receive from Server	The number of packets received from server.
Receive 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.

Item	Monitor | DHCP | Relay Statistics (Continued)
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.

DHCP | 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.



Item	Monitor | DHCP | Detailed Statistics
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.

Item	Monitor | DHCP | Detailed Statistics (Continued)
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.

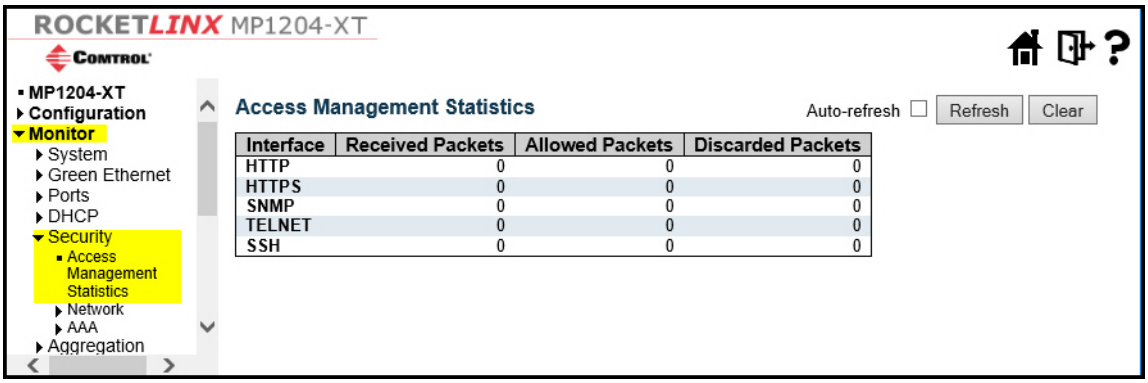
Monitor | Security Menus

The following pages are under the **Monitor | Security** menu:

- Security | Access Management Statistics on Page 200
- Security | Network Sub-Menus on Page 200
- Security | AAA Sub-Menus on Page 213
- Monitor | Security | Switch Menus on Page 215

Security | Access Management Statistics

This page provides statistics for access management.



Item	Security | Access Management
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.

Security | Network Sub-Menus

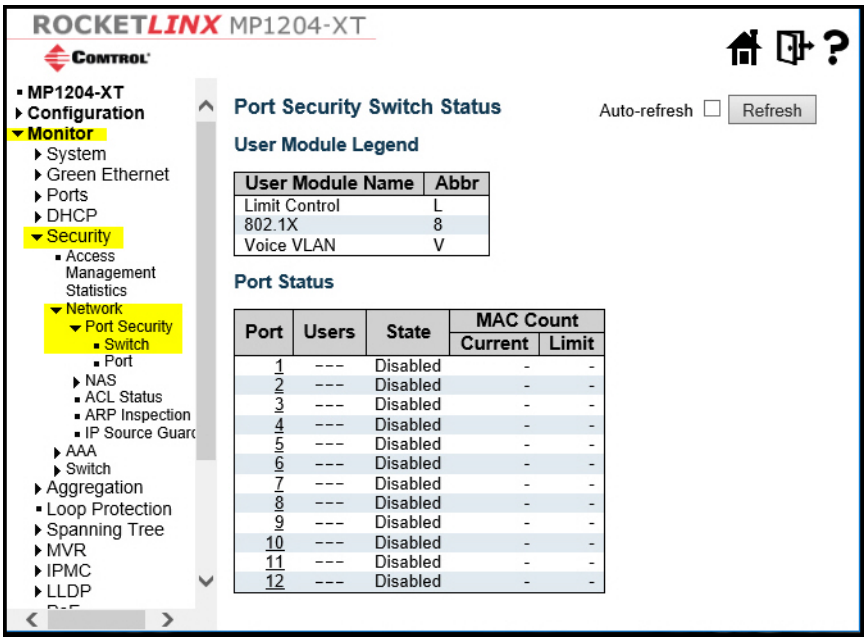
The following pages are under the **Security | Network** menu.

- Security | Network | Port Security | Switch on Page 201
- Security | Network | Port Security | Port on Page 203
- Security | Network | NAS | Switch on Page 204
- Security | Network | NAS | Port on Page 207
- Security | Network | ACL Status on Page 210
- Security | Network | ARP Inspection on Page 211
- Security | Network | IP Source Guard on Page 212

Security | 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 is 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.

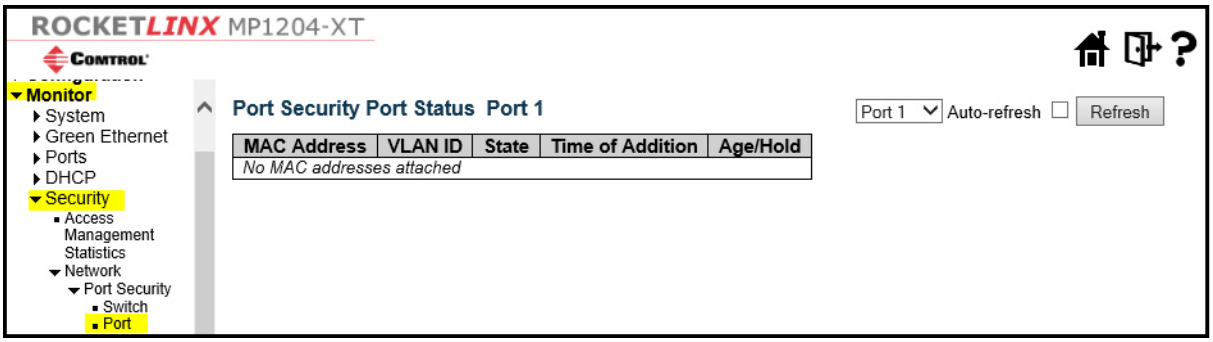


Item	Monitor | Security | Network | Port Security | Switch
User Module Legend	
User Module Name	The full name of a module that may request Port Security services.
Abbr	A one-letter abbreviation of the user module. This is used in the Users column in the port status table.
Port Status	
Port	The port number 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.

Item	Monitor | Security | Network | Port Security | Switch (Continued)
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 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 shows a dash (-). • If the Limit Control user module is not enabled on the port, the Limit column shows a dash (-).

Security | Network | Port Security | Port

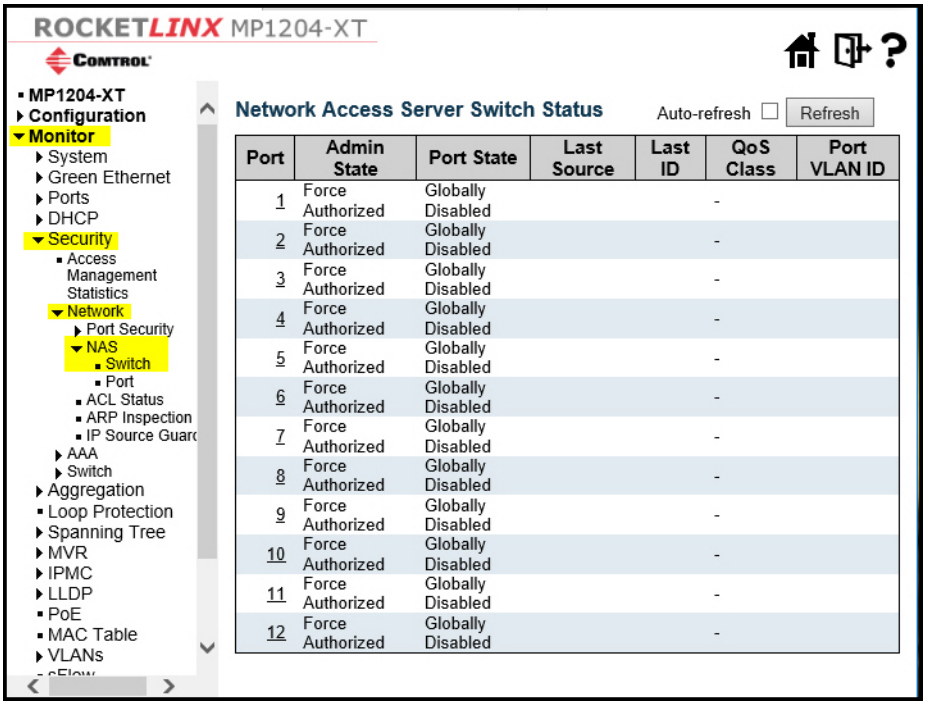
This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. 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 is blocked until that user module decides otherwise.



Item	Monitor | Security | Network | Port Security | Port
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 is not 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 stays 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 periodically checks that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address is removed from the MAC table. Otherwise a new age period begins. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) is shown.

Security | Network | NAS | Switch

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



Item	Monitor | Security | Network | NAS | Switch
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 on Page 205 for a description of possible values.
Port State	The current state of the port. It can undertake one of the following values: • **Globally Disabled**: NAS is globally disabled. • **Link Down**: NAS is globally enabled, but there is no link on the port. • **Authorized**: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. • **Unauthorized**: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. • **X Auth/Y Unauth**: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.
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.

Item	Monitor | Security | Network | NAS | Switch (Continued)
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. Read more about RADIUS-assigned VLANs here. • If the port is moved to the Guest VLAN, (Guest) is appended to the VLAN ID.

NAS Admin State

If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:

- **Force Authorized** - In this mode, the MP1204-XT sends one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.
- **Force Unauthorized -** In this mode, the MP1204-XT sends one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.
- **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.

  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.

  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.*

- **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.

  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.

- **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.

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.

The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

- **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.

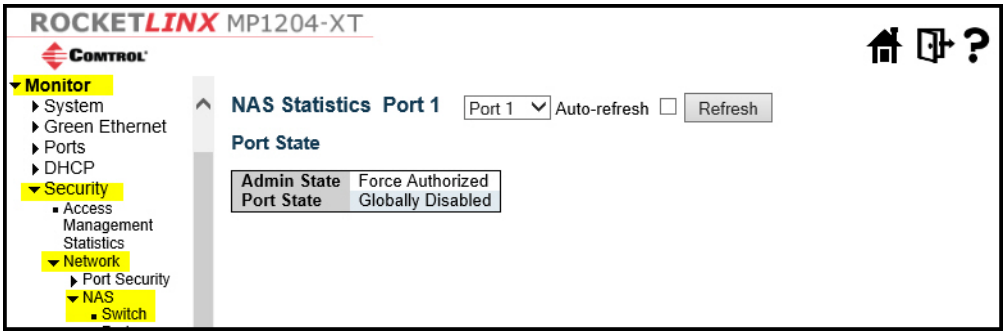
  When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

  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.

Security | Network | NAS | 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.



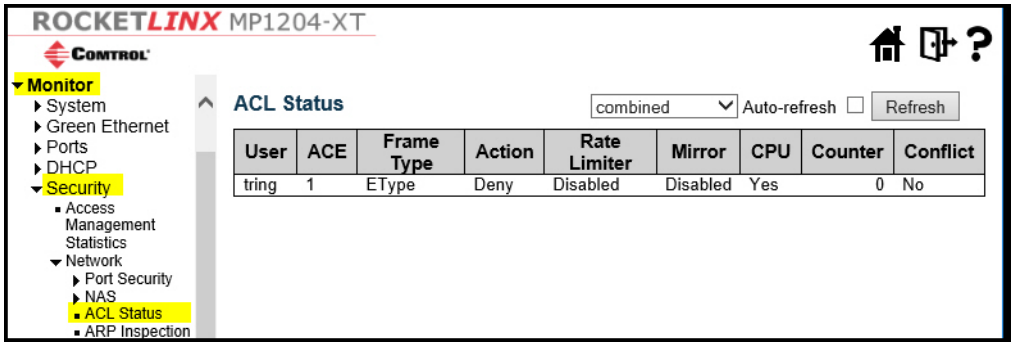
Item	Monitor | Security | Network | NAS | Port
Port State	
Admin State	The port's current administrative state. Refer to NAS Admin State on Page 205 for a description of possible values.
Port State	The current state of the port. • **Globally Disabled**: NAS is globally disabled. • **Link Down**: NAS is globally enabled, but there is no link on the port. • **Authorized**: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. • **Unauthorized**: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. • **X Auth/Y Unauth**: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.
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. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, (Guest) is appended to the VLAN ID. Read more about Guest VLANs here.
Port Counters	
EAPOL Counters	These supplicant frame counters are available for these administrative states: • Force Authorized • Force Unauthorized • Port-based 802.1X • Single 802.1X • Multi 802.1X

Item	Monitor | Security | Network | NAS | Port (Continued)
Backend Server Counters	These backend (RADIUS) frame counters are available for these administrative states: • Port-based 802.1X • Single 802.1X • Multi 802.1X • MAC-based Auth.
Last Supplicant/ Client Info	Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states: • Port-based 802.1X • Single 802.1X • Multi 802.1X • MAC-based Auth.
Selected Counters	
Selected Counters	The Selected Counters table is visible when the port is in one of the following administrative states: • Multi 802.1X • MAC-based Auth. The table is identical to and is placed next to the Port Counters table, and is empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.
Attached MAC Addresses	
Identity	Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached. This column is not available for MAC-based Auth.
MAC Address	For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client. Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.
VLAN ID	This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.

Item	Monitor | Security | Network | NAS | Port (Continued)
State	The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client remains in the unauthenticated state for Hold Time seconds.
Last Authentication	Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Security | Network | 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.



Item	Monitor | Security | ACL Status
User	Indicates the ACL user.
Ingress Port	Indicates the ingress port of the ACE. Possible values are: • **All**: The ACE matches all ingress port. • **Port**: The ACE matches a specific ingress port.
Frame Type	Indicates the frame type of the ACE. Possible values are: • **Any**: The ACE matches any frame type. • **EType**: The ACE matches Ethernet Type frames. Note that an Ethernet Type based ACE does not get matched by IP and ARP frames. • **ARP**: The ACE matches ARP/RARP frames. • **IPv4**: The ACE matches all IPv4 frames. • **IPv4/ICMP**: The ACE matches IPv4 frames with ICMP protocol. • **IPv4/UDP**: The ACE matches IPv4 frames with UDP protocol. • **IPv4/TCP**: The ACE matches IPv4 frames with TCP protocol. • **IPv4/Other**: The ACE matches IPv4 frames, which are not ICMP/UDP/TCP. • **IPv6**: The ACE matches 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.

Item	Monitor | Security | ACL Status (Continued)
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.
CPU Once	Forward first 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.

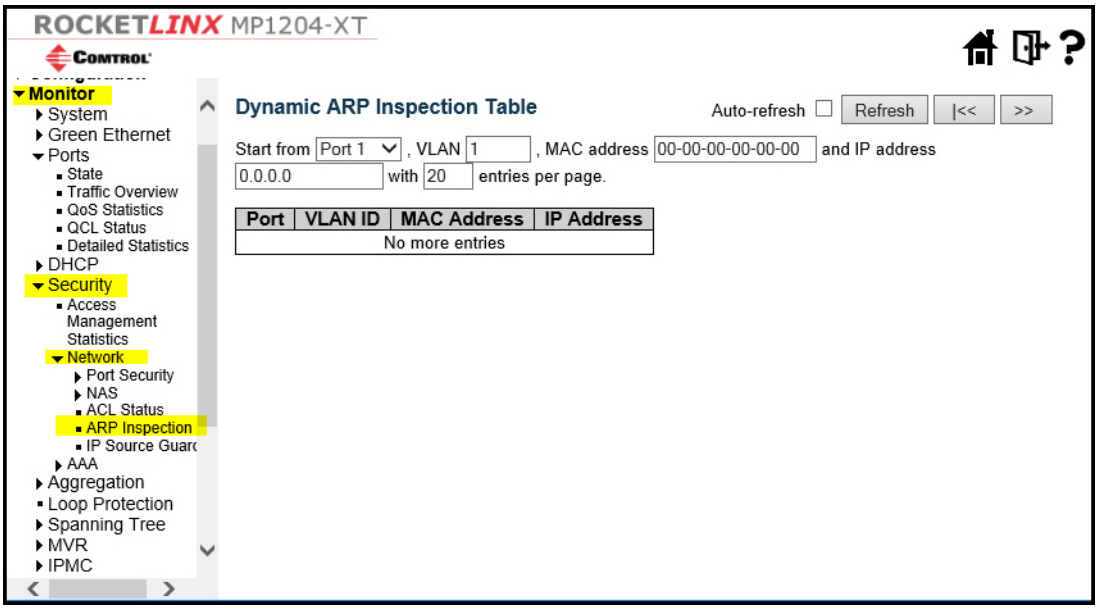
Security | Network | ARP Inspection

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 page shows 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 allows you to select the starting point in the Dynamic ARP Inspection Table. Clicking the **Refresh** button updates 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 >> uses 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.



Item	Monitor | Security | Network | ARP Inspection
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.

Security | Network | 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 page shows 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 allows you to select the starting point in the Dynamic IP Source Guard Table. Clicking the **Refresh** button updates 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 >> uses 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.

Item	Monitor | Security | Network | IP Source Guard
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.

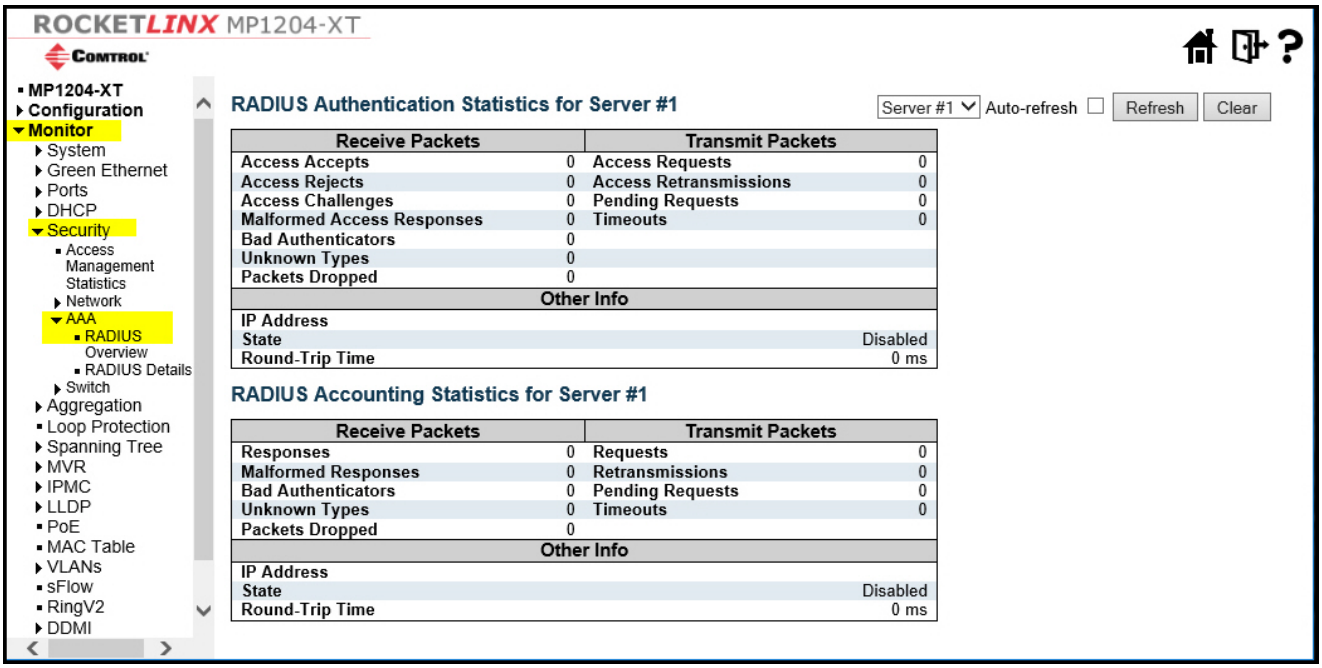
Security | AAA Sub-Menus

The following pages are under the **Security | AAA** menu.

- Security | AAA | RADIUS Overview on Page 213
- Security | AAA | RADIUS Details on Page 214

Security | AAA | RADIUS Overview

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

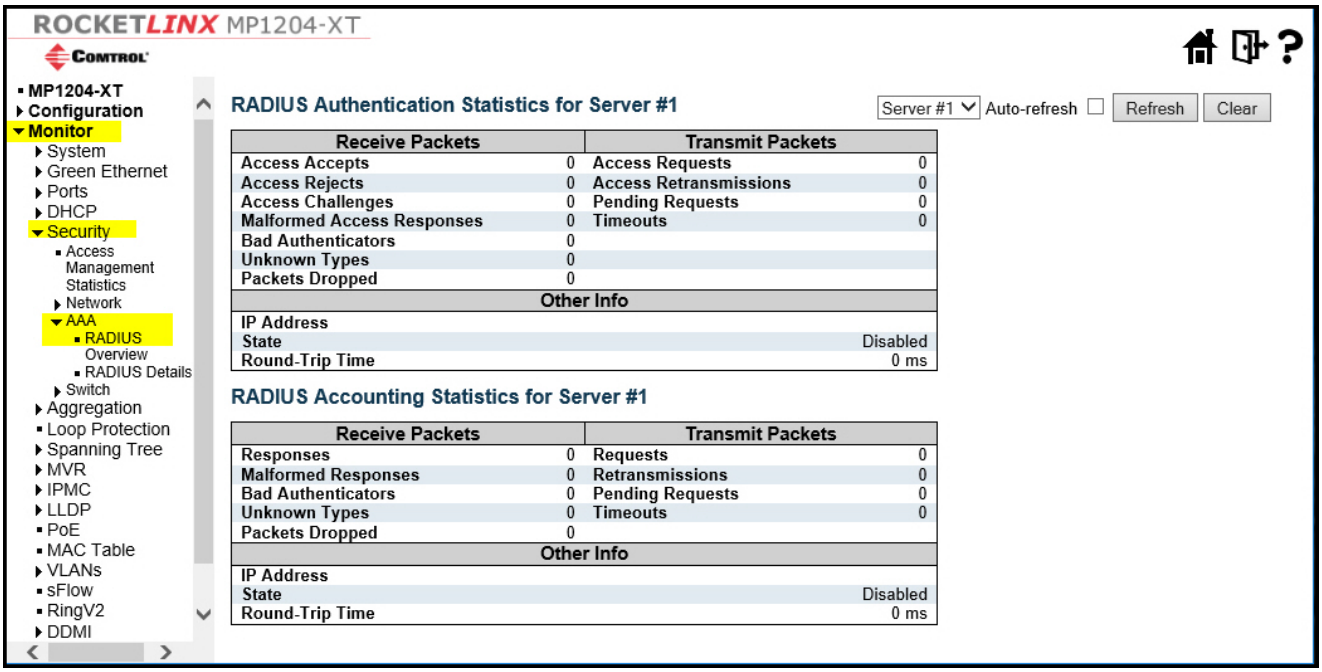


Item	Monitor | Security | AAA | RADIUS Overview
RADIUS Authentication Servers	
#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
Status	The current status of the server. This field takes one of the following values: • **Disabled**: The server is disabled. • **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. • **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 gets 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.
RADIUS Accounting Servers	
#	The RADIUS server number. Click to navigate to detailed statistics for this server.

Item	Monitor | Security | AAA | RADIUS Overview (Continued)
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
Status	• The current status of the server. This field takes one of the following values: • **Disabled**: The server is disabled. • **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. • **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 gets 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.

Security | AAA | RADIUS Details

This page provides detailed statistics for a particular RADIUS server.



Item	Monitor |Security | AAA | RADIUS Details
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.

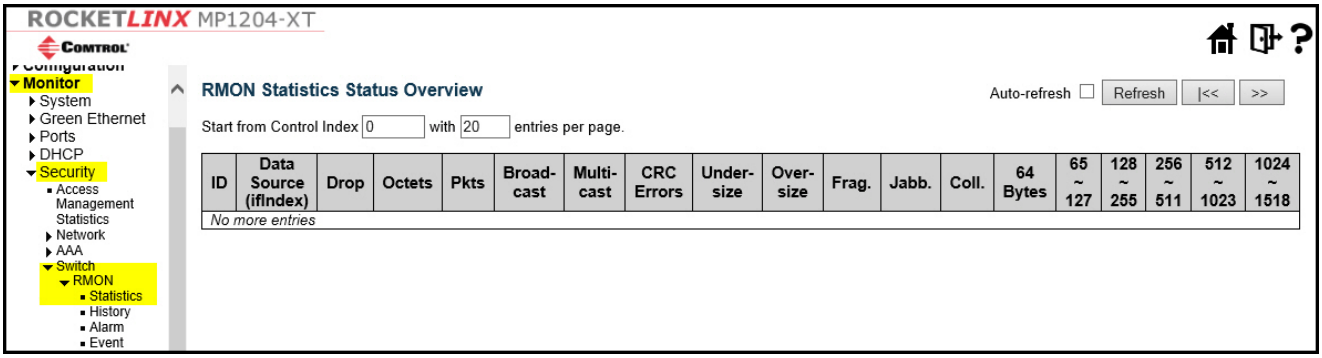
Item	Monitor |Security | AAA | RADIUS Details (Continued)
RADIUS Accounting Statistics	
Packet Counters	RADIUS accounting server packet counter. There are five receive and four transmit counters.
Other Info	This section contains information about the state of the server and the latest round-trip time.

Monitor | Security | Switch Menus

- Security | Switch | RMON | Statistics on Page 215
- Security | Switch | RMON | History on Page 217
- Security | Switch | RMON | Alarm on Page 218
- Security | Switch | RMON | Event on Page 219

Security | 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 page shows the first 20 entries from the beginning of the Statistics table. The first displayed is the one with the lowest ID found in the Statistics table.

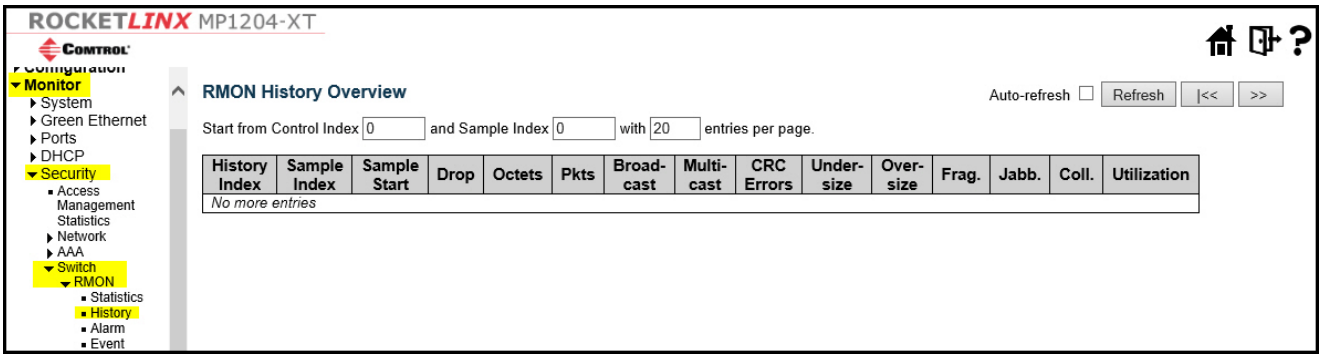


Item	Monitor | Security | Switch | RMON | Statistics
ID	Indicates the index of Statistics entry.
Data Source (ifIndex)	The port ID which wants to be monitored.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
Octets	The total number of octets of data (including those in bad packets) received on the network.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Item	Monitor | Security | Switch | RMON | Statistics (Continued)
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 to 127 octets in length.
128~255	The total number of packets (including bad packets) received that were between 128 to 255 octets in length.
256~511	The total number of packets (including bad packets) received that were between 256 to 511 octets in length.
512~1023	The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.
1024~1588	The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.
|<<	Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.
>>	Updates the table, starting with the entry after the last entry currently displayed.

Security | Switch | RMON | 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 page shows the first 20 entries from the beginning of the History table. The first displayed is the one with the lowest History Index and Sample Index found in the History table.

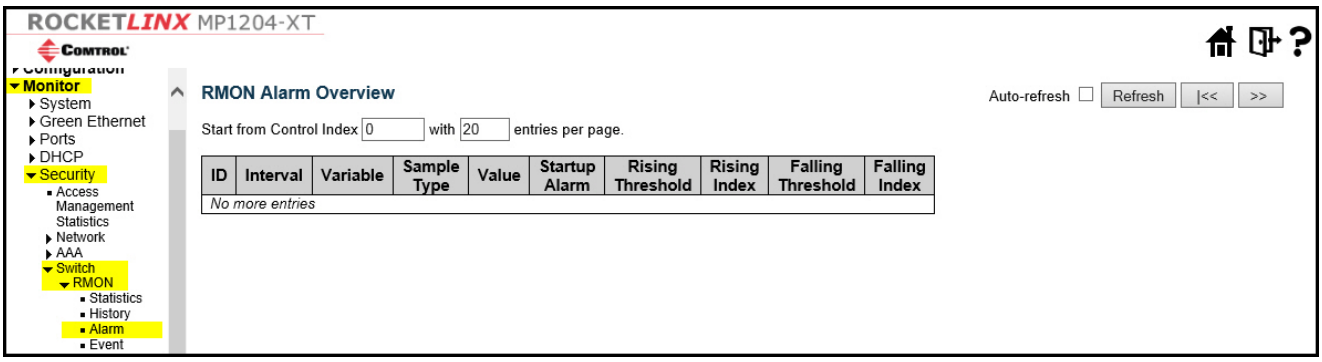


Item	Monitor | Security |Switch | RMON | History
History Index	Indicates the index of History control entry.
Sample Index	Indicates the index of the data entry associated with the control entry.
Sample Start	The value of sysUpTime at the start of the interval over which this sample was measured.
Drop	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.

Item	Monitor | Security |Switch | RMON | History (Continued)
|<<	Updates the table starting from the first entry in the History table, i.e., the entry with the lowest History Index and Sample Index.
>>	Updates the table, starting with the entry after the last entry currently displayed.

Security | Switch | RMON | Alarm

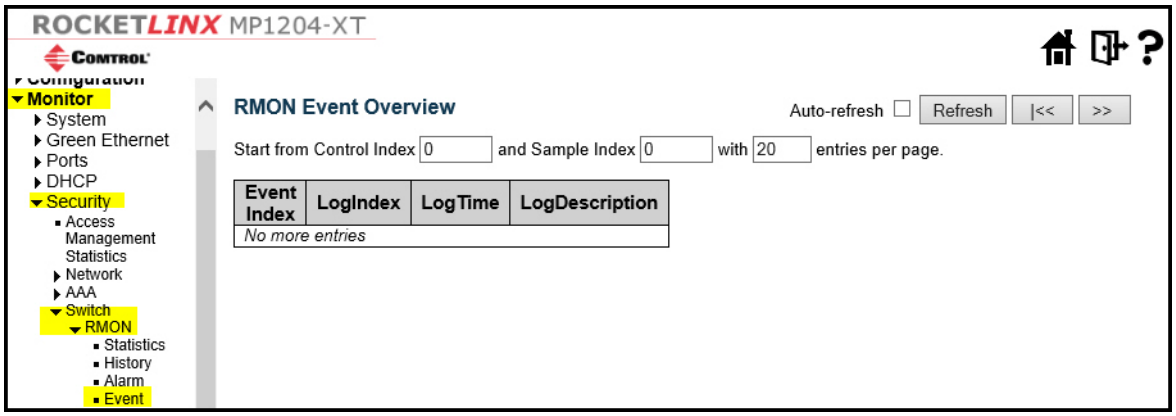
This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the **entries per page** input field. When first visited, the page shows the first 20 entries from the beginning of the Alarm table. The first displayed is the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



Item	Monitor | Security | Switch | RMON |Alarm
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.
|<<	Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.
>>	Updates the table, starting with the entry after the last entry currently displayed.

Security | Switch | RMON | 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 page shows the first 20 entries from the beginning of the Event table. The first displayed is the one with the lowest Event Index and Log Index found in the Event table.



Items	Monitor | Security | Switch |RMON |Event
Event Index	Indicates the index of the event entry.
Log Index	Indicates the index of the log entry.
Log Time	Indicates Event log time.
Log Description	Indicates the Event description.
|<<	Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index.
>>	Updates the table, starting with the entry after the last entry currently displayed.

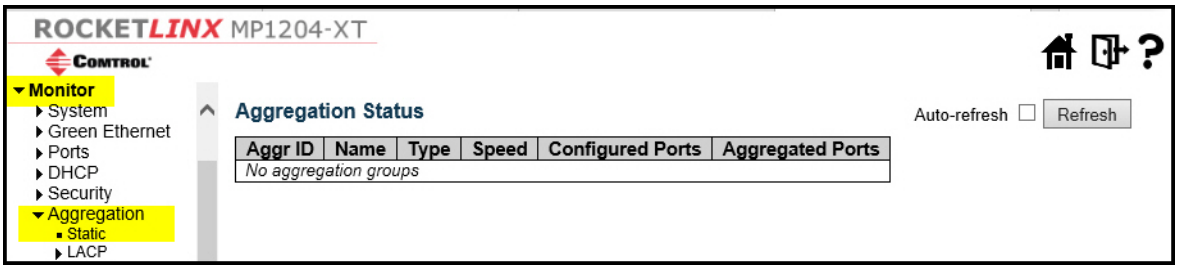
Monitor | Aggregation Menus

The following sub-menus are under the **Aggregation** menu.

- Aggregation | Static on Page 220
- Aggregation | LACP Sub-Menus on Page 220

Aggregation | Static

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



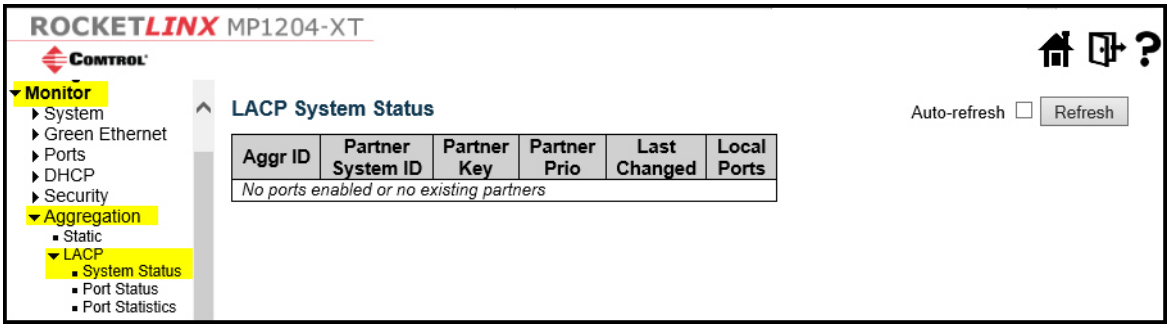
Item	Monitor | Aggregation | Status
Aggr ID	The Aggregation ID associated with this aggregation instance.
Name	Name of the Aggregation group ID.
Type	Type of the Aggregation group(Static or LACP).
Speed	Speed of the Aggregation group.
Configured ports	Configured member ports of the Aggregation group.
Aggregated ports	Aggregated member ports of the Aggregation group.

Aggregation | LACP Sub-Menus

- Aggregation | LACP | System Status on Page 221
- Aggregation | LACP | Port Status on Page 221
- Aggregation | LACP | Port Statistics on Page 222

Aggregation | LACP | System Status

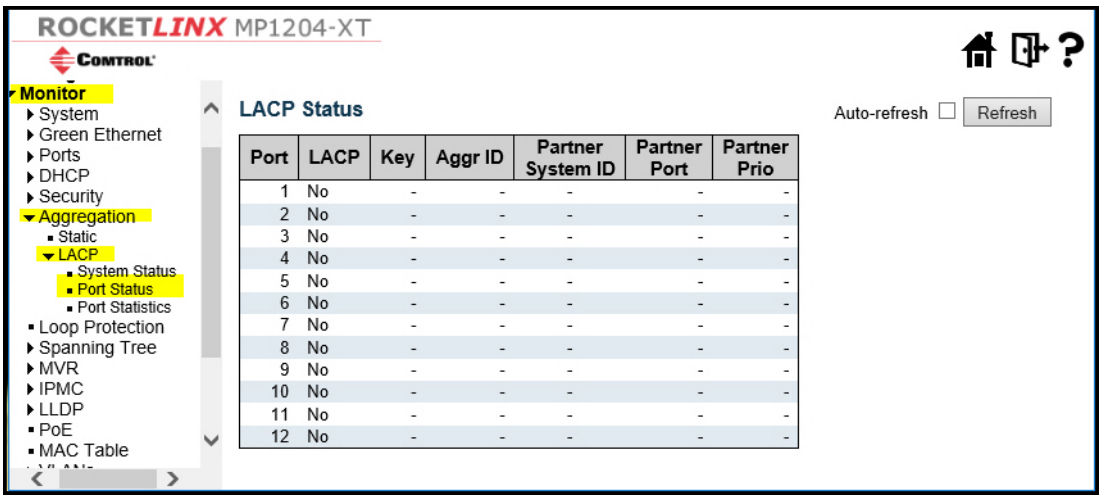
This page provides a status overview for all LACP instances.



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.

Aggregation | LACP | Port Status

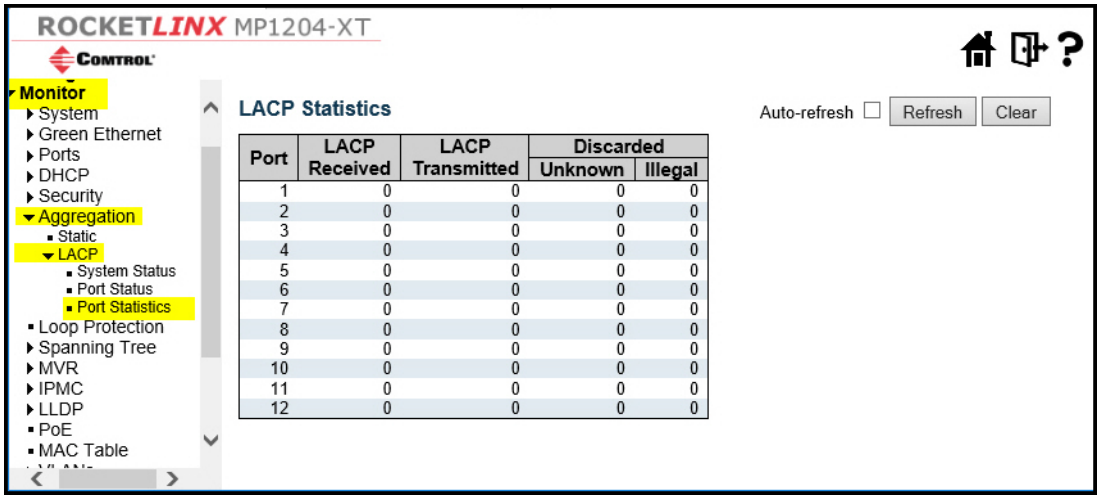
This page provides a status overview for LACP status for all ports.



Item	Monitor | Aggregation | LACP | Port Status
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 joins if other port leaves. Meanwhile it's 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.

Aggregation | LACP | Port Statistics

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

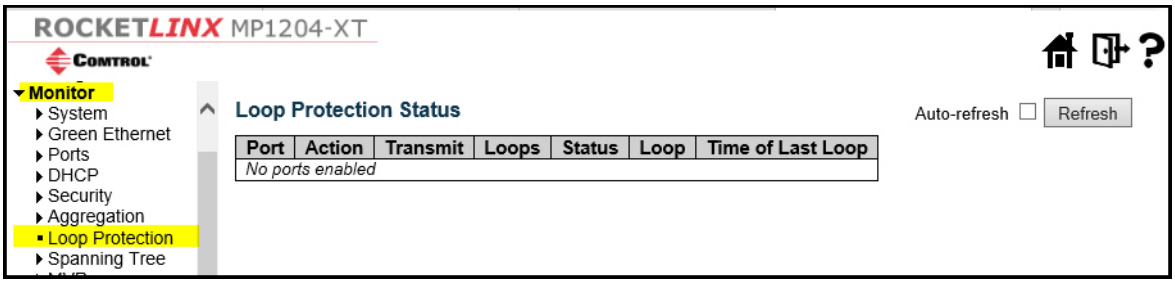


Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0

Item	Monitor | Aggregation | LACP | Port Statistics
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.

Monitor | Loop Protection

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



Item	Monitor | Loop Protection
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.

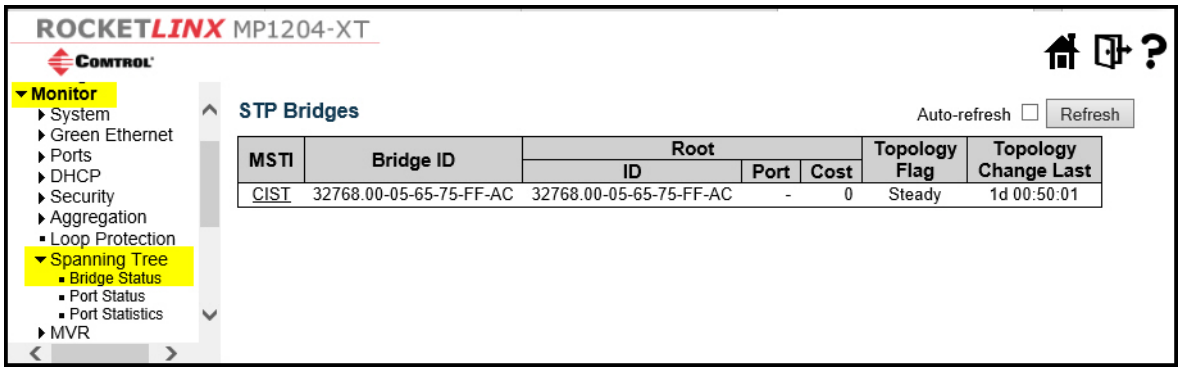
Monitor | Spanning Tree Menu

The following pages are under the Spanning Tree menu.

- Spanning Tree | Bridge Status on Page 224
- Spanning Tree | Port Status on Page 225
- Spanning Tree | Port Statistics on Page 226

Spanning Tree | Bridge Status

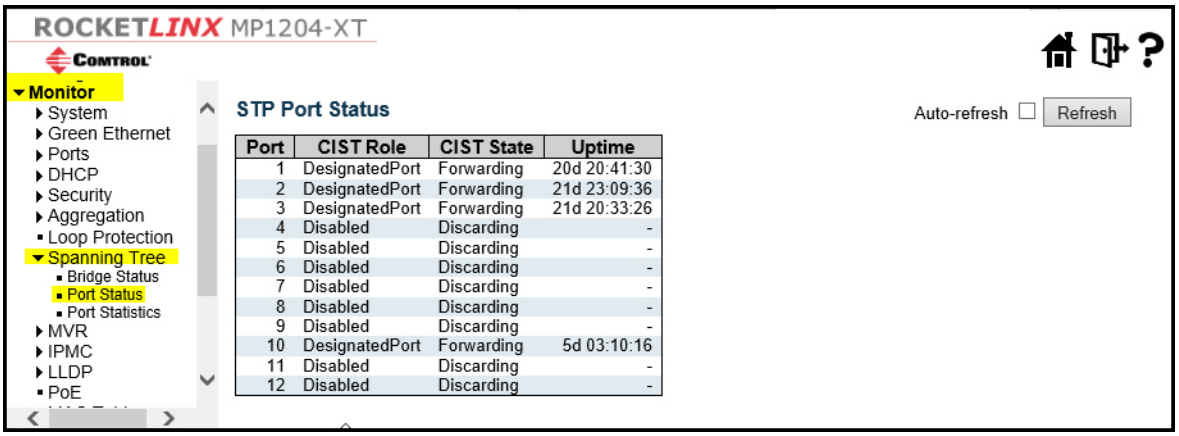
This page provides a status overview of all STP bridge instances.



Item	Monitor | Spanning Tree | Bridge Status
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.

Spanning Tree | Port Status

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

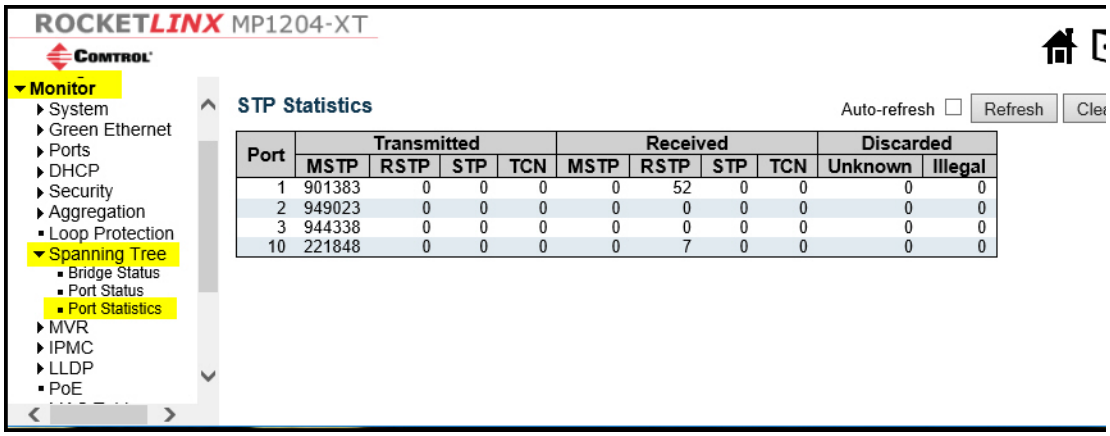


Port	CIST Role	CIST State	Uptime
1	DesignatedPort	Forwarding	20d 20:41:30
2	DesignatedPort	Forwarding	21d 23:09:36
3	DesignatedPort	Forwarding	21d 20:33:26
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	DesignatedPort	Forwarding	5d 03:10:16
11	Disabled	Discarding	-
12	Disabled	Discarding	-

Item	Monitor | Spanning Tree | Port Status
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,**or **Disabled**.
CIST State	The current STP port state of the CIST port. The port state can be one of the following values: **Discarding**, **Learning**, or ***Forwarding***.
Uptime	The time since the bridge port was last initialized.

Spanning Tree | Port Statistics

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



Item	Monitor | Spanning Tree | Port Statistics
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.

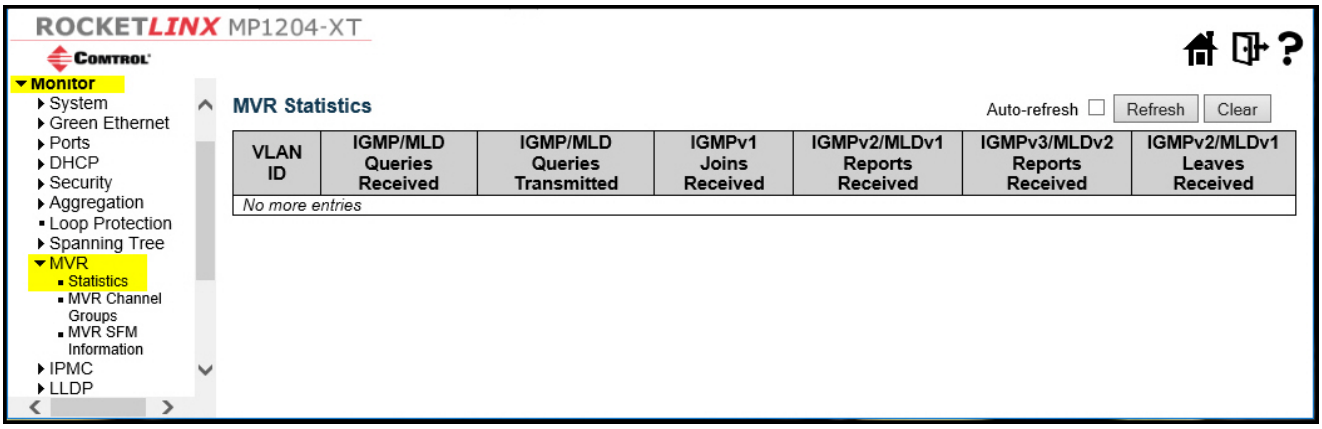
Monitor | MVR Menu

The following pages are under the MVR menu.

- MVR | Statistics on Page 227
- MVR | MVR Channel Groups on Page 228
- MVR | SFM Information on Page 229

MVR | Statistics

This page provides MVR Statistics information.



Item	Monitor | MVR | Statistics
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.

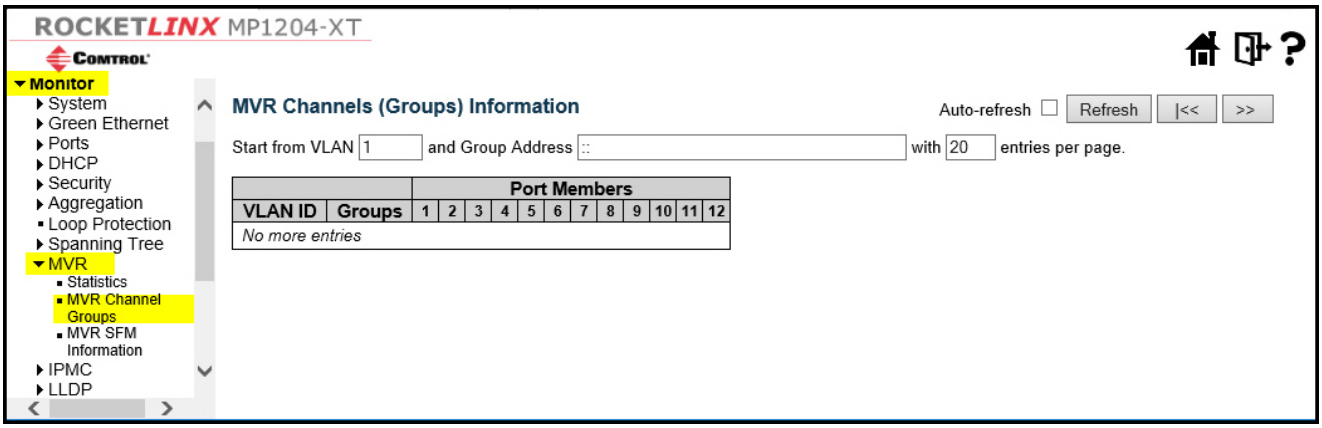
MVR | MVR Channel Groups

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 page shows the first 20 entries from the beginning of the MVR Channels (Groups) Information Table.

The **Start from VLAN**, and **Group Address** input fields allows you to select the starting point in the MVR Channels (Groups) Information Table.

Clicking the **Refresh** button updates 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 [>>] uses 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.



Item	Monitor | MVR | MVR Channel Groups
VLAN ID	VLAN ID of the group.
Groups	Group ID of the group displayed.
Port Members	Ports under this group.

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 page shows the first 20 entries from the beginning of the MVR SFM Information Table.

The **Start from VLAN**, and **Group Address** input fields allows you to select the starting point in the MVR SFM Information Table. Clicking the **Refresh** button updates 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 >> uses 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.

Item	Monitor | MVR | MVR SFM Information
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.

IPMC Menu

The following sub-menus are under the IPMC menu.

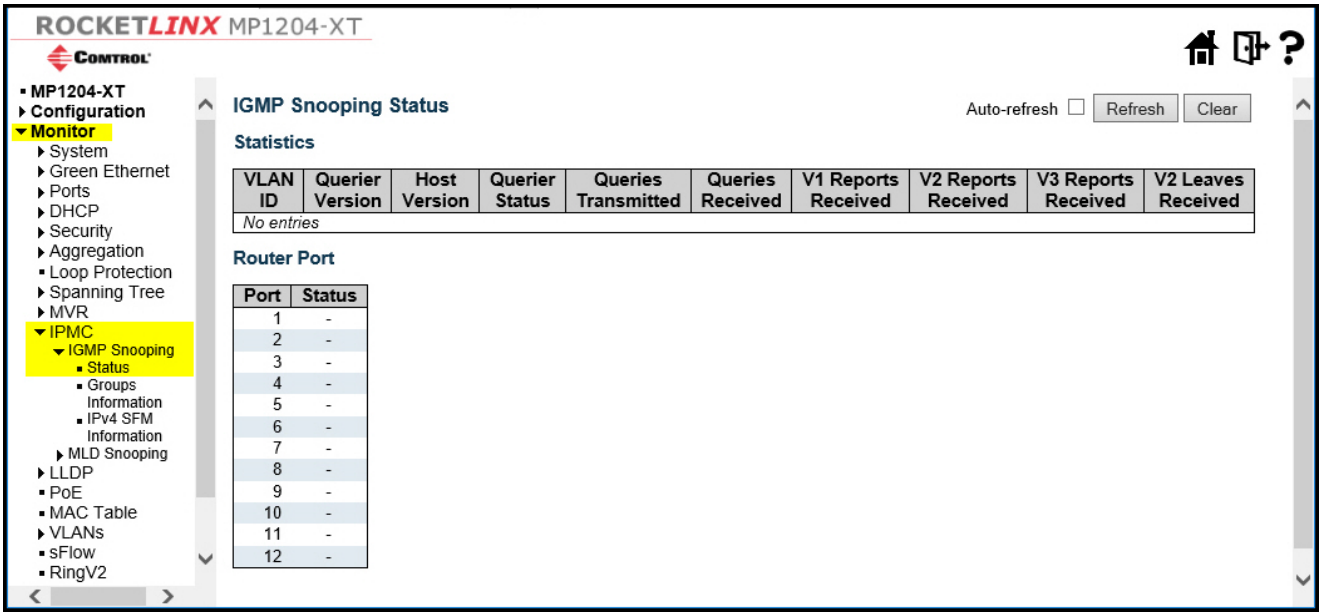
- IPMC | IGMP Snooping Sub-Menus on Page 230
- IPMC | MLD Snooping on Page 232

IPMC | IGMP Snooping Sub-Menus

- IPMC | IGMP Snooping | Status on Page 230
- IPMC | IGMP Snooping | Groups Information on Page 231
- IPMC | IGMP Snooping | IPv4 SFM Information on Page 232

IPMC | IGMP Snooping | Status

This page provides IGMP Snooping status.



Item	Monitoring | IPMC | IGMP Snooping | Status
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.

Item	Monitoring | IPMC | IGMP Snooping | Status
V3 Report Received	The number of Received V3 Reports.
V2 Leaves Received	The number of Received V2 Leaves.
Router Port	Displays 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.

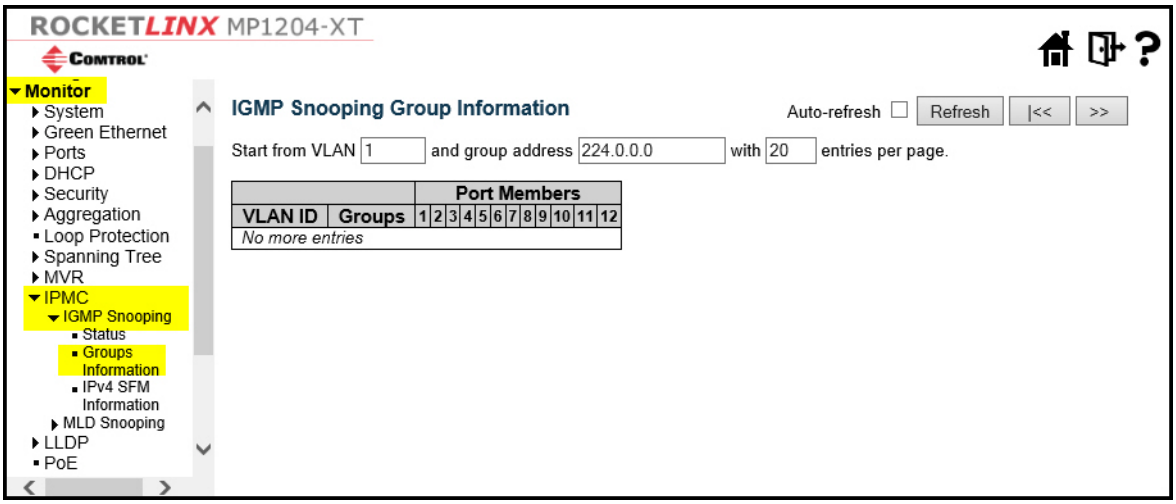
IPMC | IGMP Snooping | Groups Information

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 page shows the first 20 entries from the beginning of the IGMP Group Table.

The **Start from VLAN**, and **group** input fields allows you to select the starting point in the IGMP Group Table. Clicking the **Refresh** button updates 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 >>| uses 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.



Item	Monitor | IPMC | IGMP Snooping | Groups Information
VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group.

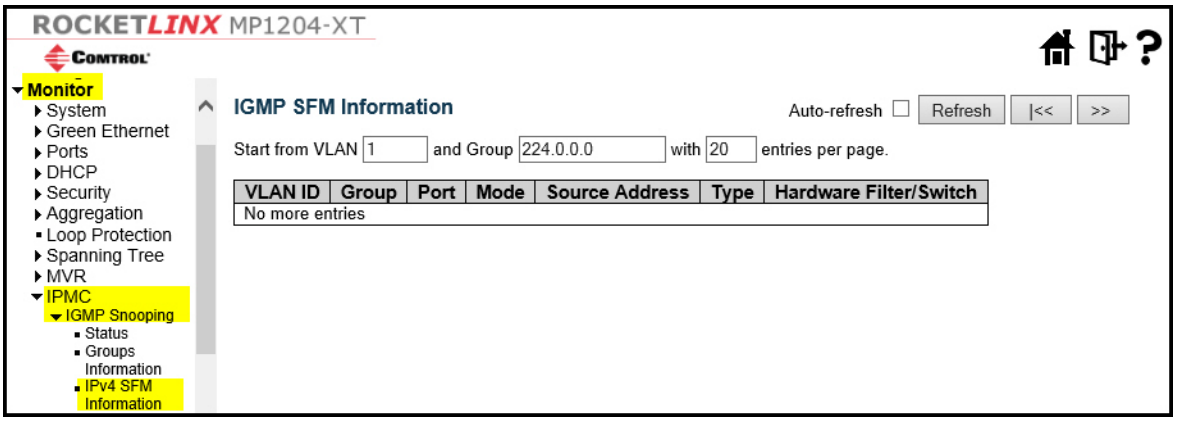
IPMC | IGMP Snooping | IPv4 SFM Information

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 page showsthe first 20 entries from the beginning of the IGMP SFM Information Table.

The **Start from VLAN**, and **group** input fields allows you to select the starting point in the IGMP SFM Information Table. Clicking the **Refresh** button updates 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 [>>] uses 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.



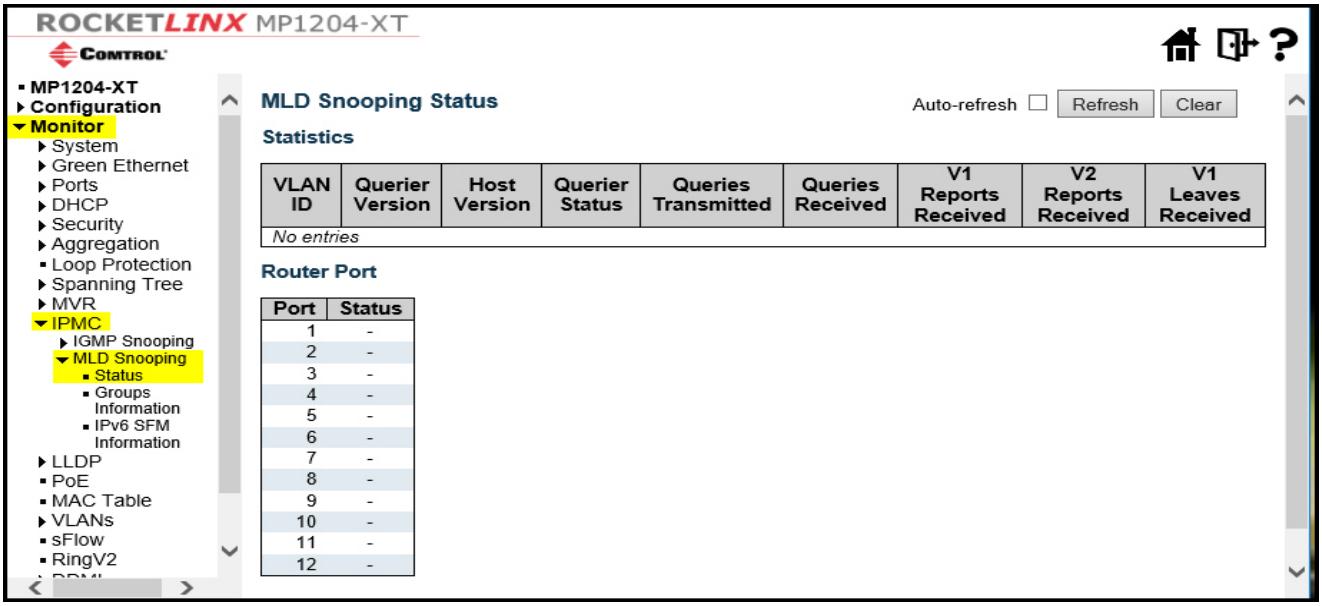
Item	Monitor | IPMC | IGMP Snooping | IPv4 SFM Information
VLAN ID	VLAN ID of the group.
Group	Group address of the group displayed.
Port	Switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either **Include** or **Exclude**.
Source 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.

IPMC | MLD Snooping

- IPMC | MLD Snooping | Status on Page 233
- IPMC | MLD Snooping | Groups Information on Page 234
- IPMC | MLD Snooping | IPv6 SFM Information on Page 235

IPMC | MLD Snooping | Status

This page provides MLD Snooping status.



Item	Monitor | IPMC | MLD Snooping | Status
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** denotes 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.

IPMC | MLD Snooping | Groups Information

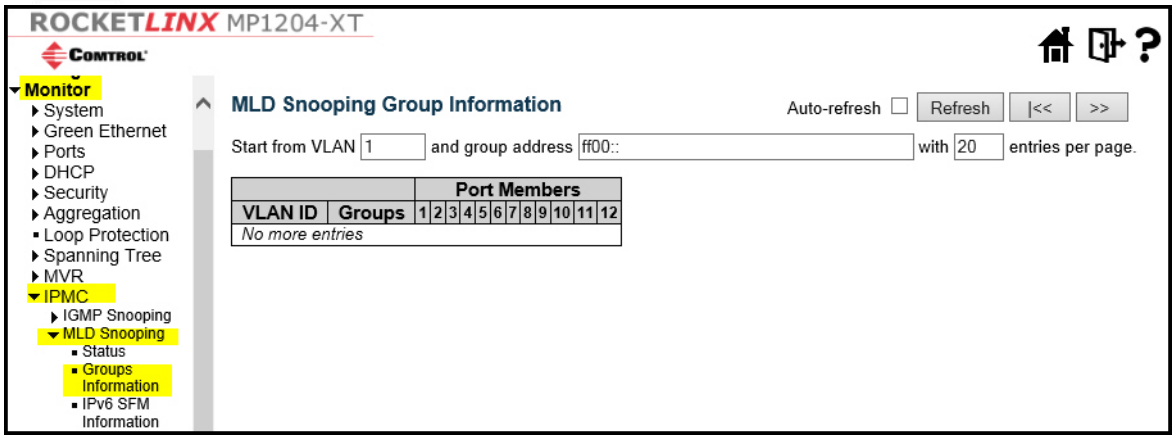
Each page shows up to 99 entries from the MLD Group table, default being 20, selected through the **entries per page** input field. When first visited, the page shows the first 20 entries from the beginning of the MLD Group Table.

The **Start from VLAN**, and **group** input fields allows you to select the starting point in the MLD Group Table. Clicking the **Refresh** button updates 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 >> uses 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.



Item	Monitor | IPMC | MLD Snooping | Groups Information
VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group.

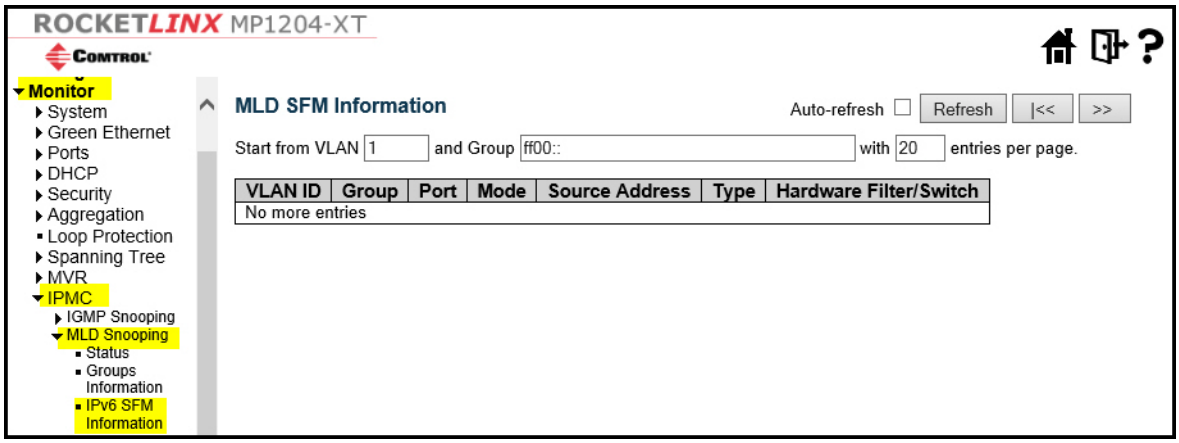
IPMC | MLD Snooping | IPv6 SFM Information

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 page showsthe first 20 entries from the beginning of the MLD SFM Information Table.

The **Start from VLAN**, and **group** input fields allows you to select the starting point in the MLD SFM Information Table. Clicking the **Refresh** button updates 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 >> uses 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.



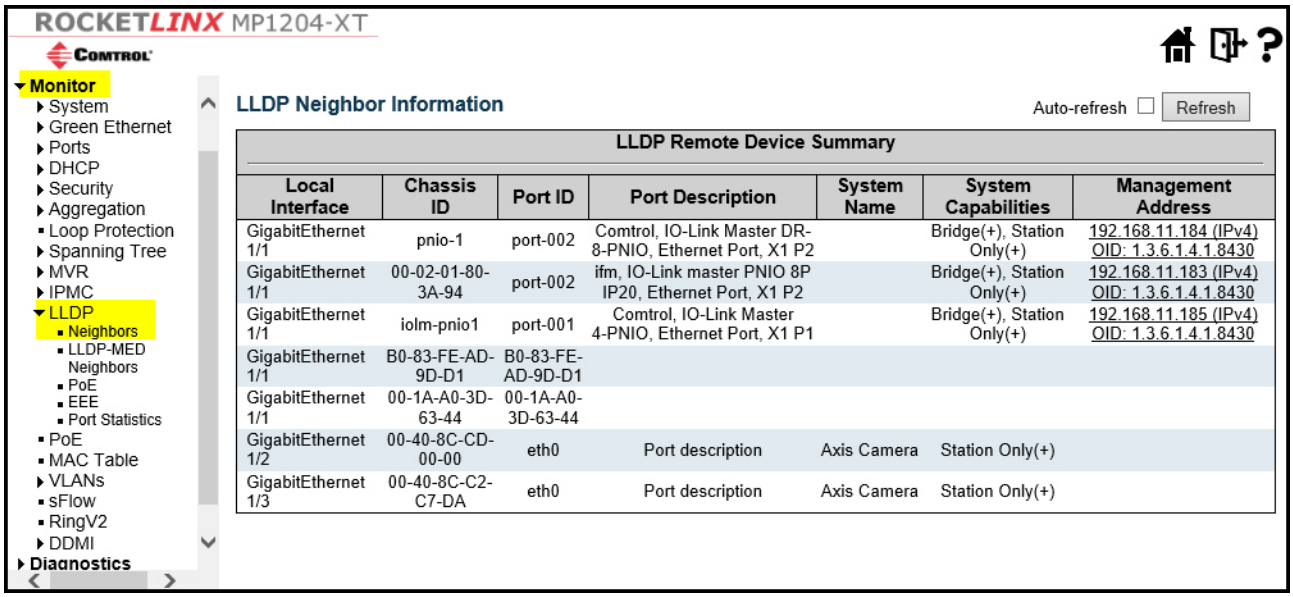
Item	Monitor | IPMC | MLD Snooping | Groups Information
VLAN ID	VLAN ID of the group.
Group	Group address of the group displayed.
Port	Switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either **Include** or **Exclude**.
Source 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.

Monitor | LLDP

The following pages are under the **Monitor | LLDP** menu.

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.

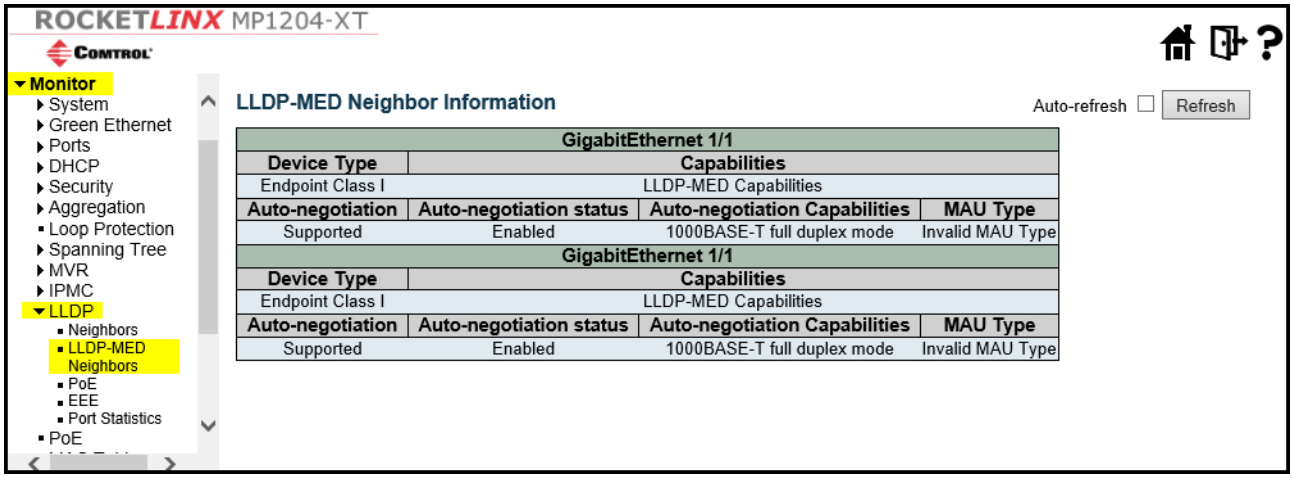


Item	Monitor | LLDP | Neighbors
Local Port	The port on which the LLDP frame was received.
Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames.
Port ID	The Port ID is the identification of the neighbor port.
Port Description	Port Description is the port description advertised by the neighbor unit.
System Name	System Name is the name advertised by the neighbor unit.

Item	Monitor | LLDP | Neighbors (Continued)
System Capabilities	System Capabilities describes the neighbor unit's capabilities. The possible capabilities are: 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.

LLDP | LLDP-MED Neighbors

This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. This function applies to VoIP devices which support LLDP-MED.



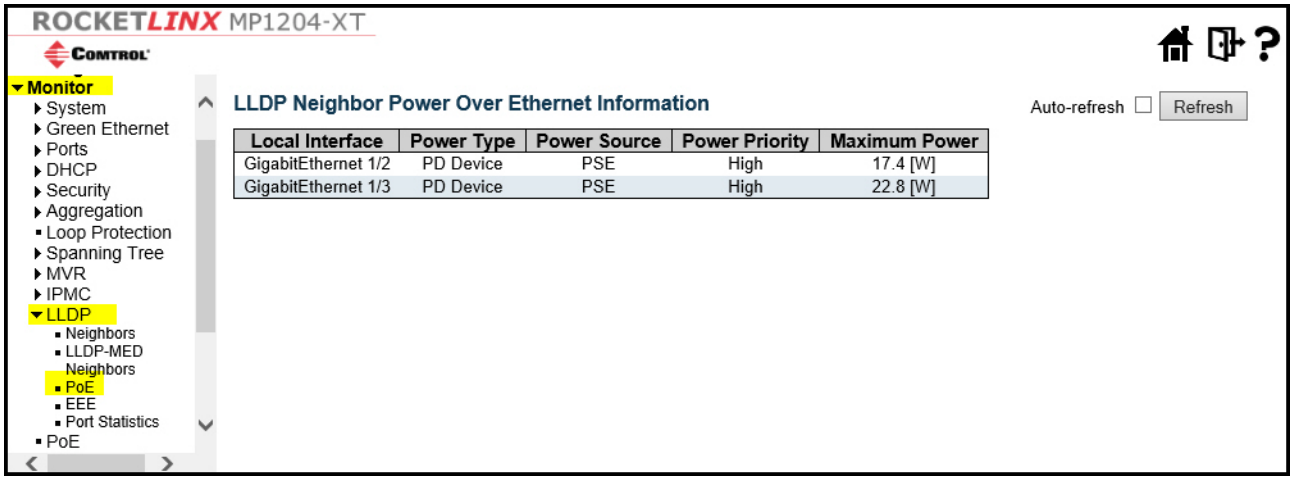
Item	Monitor | LLDP | LLDP-MED Neighbors
Port	The port on which the LLDP frame was received.
Device Type	LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices. **LLDP-MED Network Connectivity Device Definition** LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies: 1. LAN Switch/Router 2. IEEE 802.1 Bridge 3. IEEE 802.3 Repeater (included for historical reasons) 4. IEEE 802.11 Wireless Access Point 5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method. **LLDP-MED Endpoint Device Definition** LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework. Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following. Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For example, any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also supports all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) also supports all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

Item	Monitor | LLDP | LLDP-MED Neighbors (Continued)
Device Type (Continued)	**LLDP-MED Generic Endpoint (Class I)** The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057. Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management. **LLDP-MED Media Endpoint (Class II)** The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar. Discovery services defined in this class include media-type-specific network layer policy discovery. **LLDP-MED Communication Endpoint (Class III)** The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user. Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.
LLDP-MED Capabilities	LLDP-MED Capabilities describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are: 1. LLDP-MED capabilities 2. Network Policy 3. Location Identification 4. Extended Power via MDI - PSE 5. Extended Power via MDI - PD 6. Inventory 7. Reserved
Application Type	Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below. 1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. 2. Voice Signaling - for use in network topologies that require a different policy for the voice signaling than for the voice media. 3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

Item	Monitor | LLDP | LLDP-MED Neighbors (Continued)
Application Type (Continued)	4. Guest Voice Signaling - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. 5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. 6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. 7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. 8. Video Signaling - for use in network topologies that require a separate policy for the video signaling than for the video media.
Policy	Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either **Defined** or **Unknown** • **Unknown**: The network policy for the specified application type is currently unknown. • **Defined**: The network policy is defined.
TAG	TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be **Tagged** or **Untagged**. • **Untagged**: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. • **Tagged**: The device is using the IEEE 802.1Q tagged frame format.
VLAN ID	VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.
Priority	Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).
DSCP	DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).
Auto-negotiation	Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.
Auto-negotiation status	Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode is determined the operational MAU type field value rather than by auto-negotiation.
Auto-negotiation Capabilities	Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

LLDP | 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.

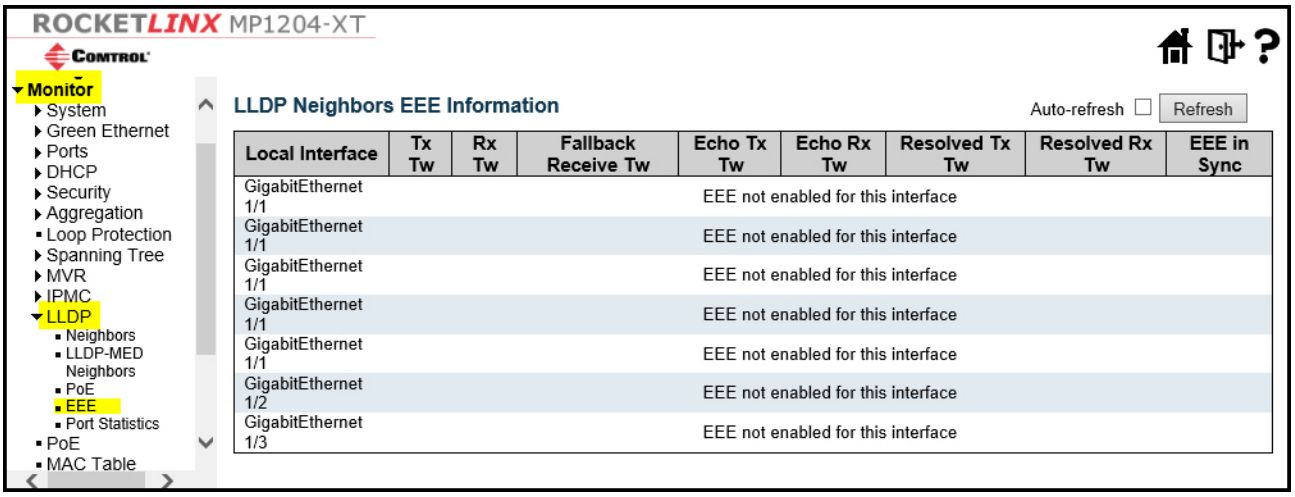


Item	Monitor | LLDP | PoE
Local Interface	The interface for this switch on which the LLDP frame was received. .
Power Type	The **Power Type** represents whether the device is a Power Sourcing Entity (PSE) or Power Device (PD). If the Power Type is unknown it is represented as **Reserved**
Power Source	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 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**.

LLDP | EEE

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called wakeup time. To achieve minimal latency, devices can use LLDP to exchange information about their respective tx and rx wakeup time , as a way to agree upon the minimum wakeup time they need.

This page provides an overview of EEE information exchanged by LLDP.



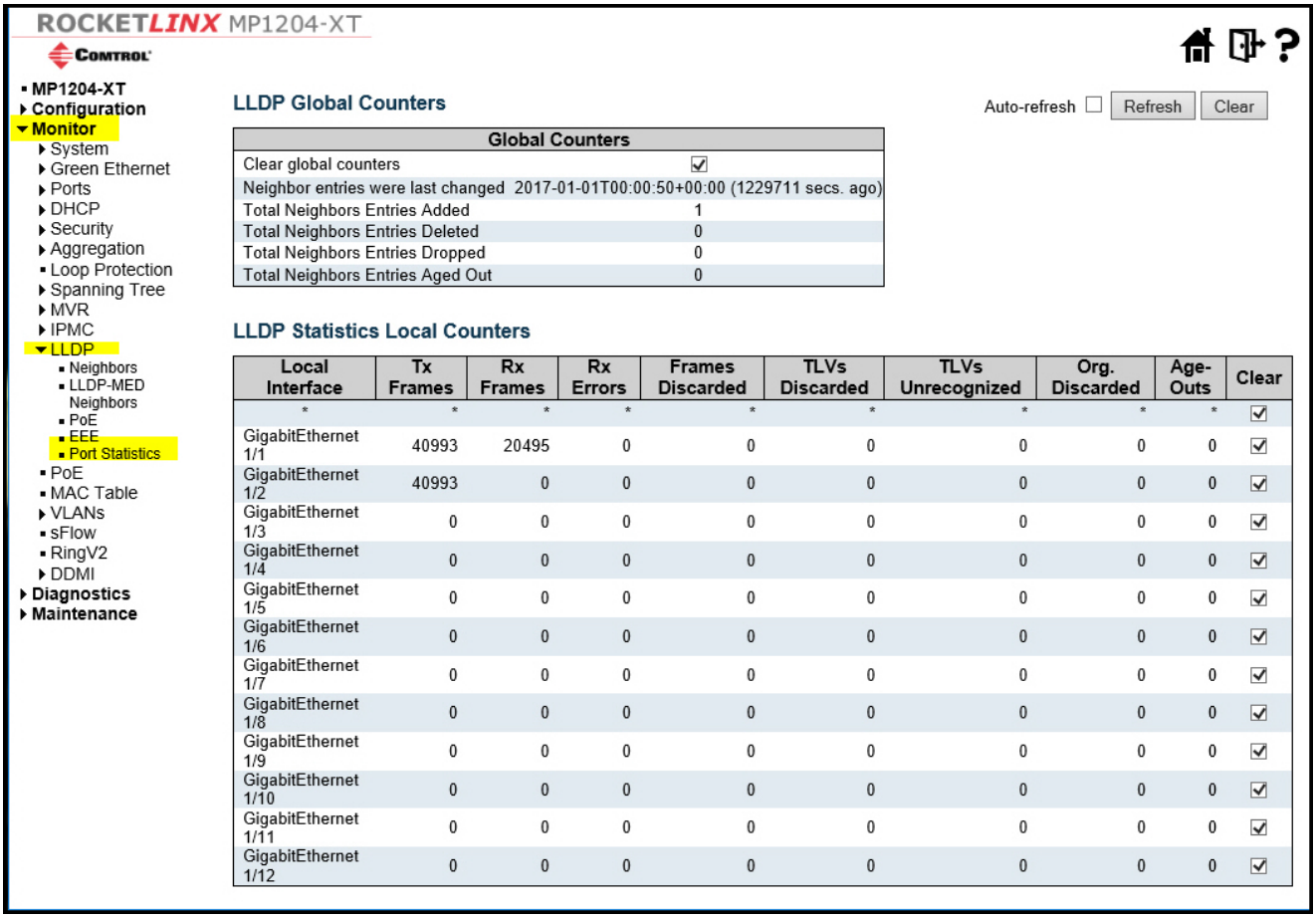
Item	Monitor | LLDP | EEE
Local Port	The port on which LLDP frames are received or transmitted.
Tx Tw	The link partner's maximum time that transmit path can hold-off sending data after deassertion of LPI.
Rx Tw	The link partner's time that receiver would like the transmitter to hold-off to allow time 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**.
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.

Item	Monitor | LLDP | EEE (Continued)
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.

LLDP | 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 port counters for the currently selected switch.

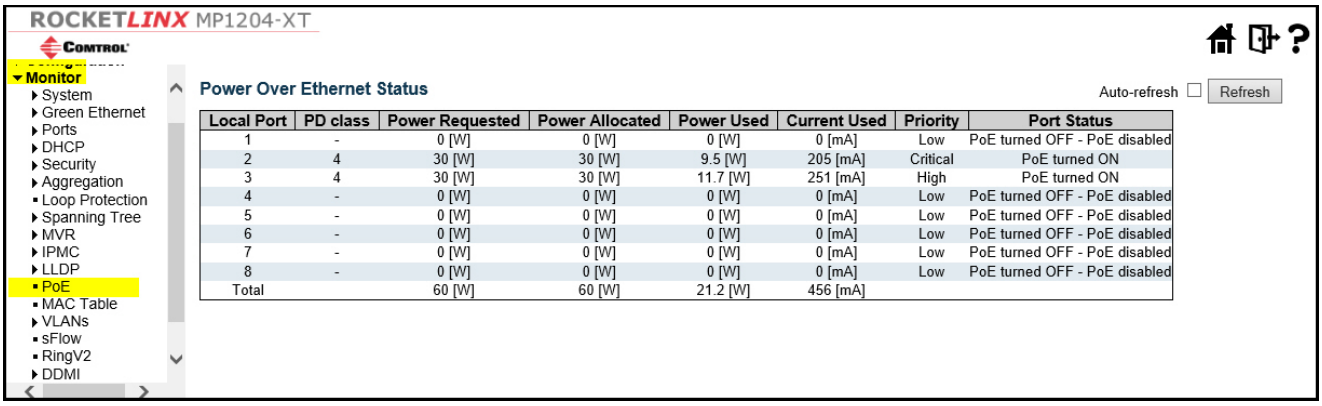


Item	Monitor | LLDP | Port Statistics
Global Counters	
Neighbor entries were last change	Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.
Total Neighbors Entries Added	Shows the number of new entries added since switch reboot.
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.

Item	Monitor | LLDP | Port Statistics (Continued)
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.
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.

Monitor | PoE

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



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	PoE turned OFF - PoE disabled
2	4	30 [W]	30 [W]	9.5 [W]	205 [mA]	Critical	PoE turned ON
3	4	30 [W]	30 [W]	11.7 [W]	251 [mA]	High	PoE turned ON
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
5	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
6	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
7	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
8	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
Total		60 [W]	60 [W]	21.2 [W]	456 [mA]		

Item	Monitor | PoE
PoE Status	
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 uses. 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	This shows the requested amount of power the PD wants to be reserved.
Power Allocated	This shows the amount of power the switch has allocated for the PD.
Power Used	This shows how much power the PD currently is using.
Current Used	This shows how much current the PD currently is using.
Priority	This shows the port's priority configured by the user.

Item	Monitor | PoE (Continued)
Port Status	This 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.

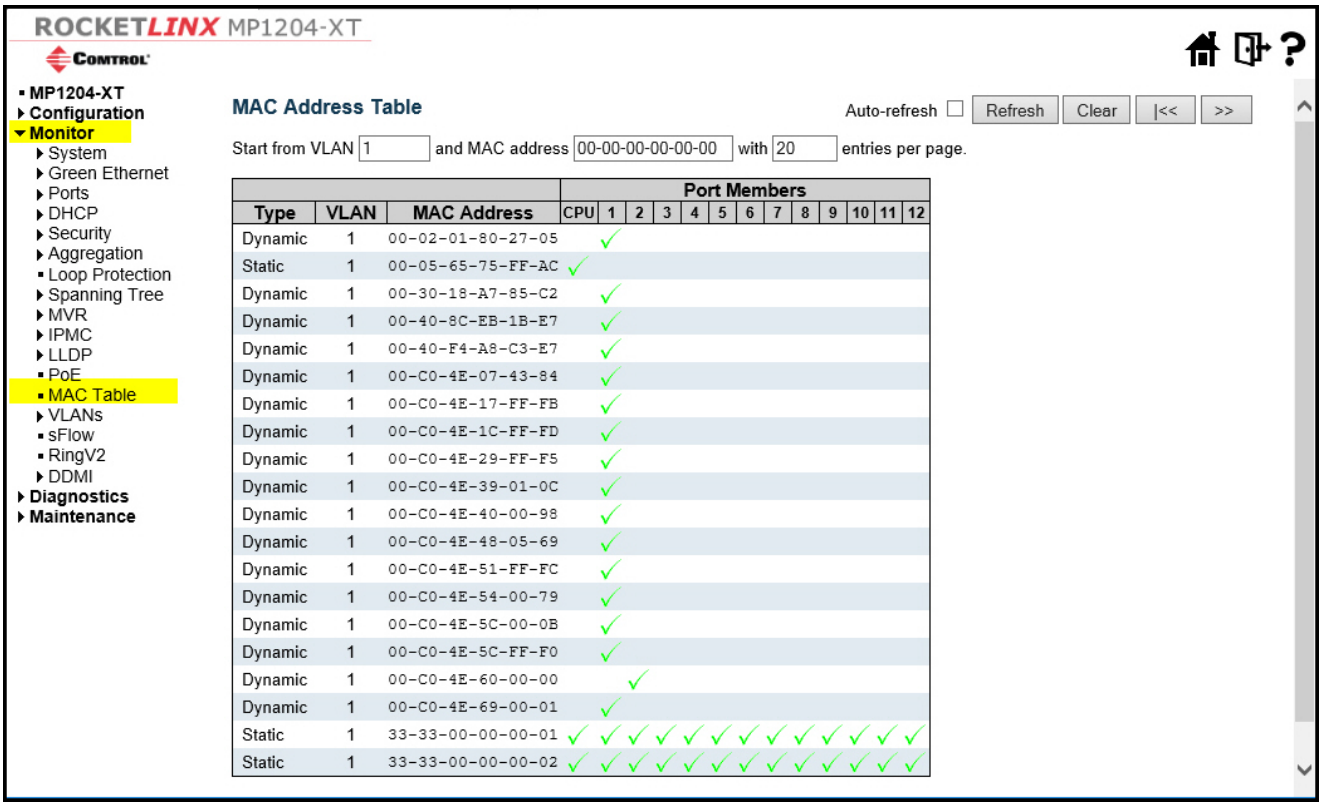
Monitor | MAC Table

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 page shows the first 20 entries from the beginning of the MAC Table. The first displayed is 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 you to select the starting point in the MAC Table. Clicking the **Refresh** button updates 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 [>>] uses 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.



			Port Members												
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12
Dynamic	1	00-02-01-80-27-05		✓											
Static	1	00-05-65-75-FF-AC	✓												
Dynamic	1	00-30-18-A7-85-C2		✓											
Dynamic	1	00-40-8C-EB-1B-E7		✓											
Dynamic	1	00-40-F4-A8-C3-E7		✓											
Dynamic	1	00-C0-4E-07-43-84		✓											
Dynamic	1	00-C0-4E-17-FF-FB		✓											
Dynamic	1	00-C0-4E-1C-FF-FD		✓											
Dynamic	1	00-C0-4E-29-FF-F5		✓											
Dynamic	1	00-C0-4E-39-01-0C		✓											
Dynamic	1	00-C0-4E-40-00-98		✓											
Dynamic	1	00-C0-4E-48-05-69		✓											
Dynamic	1	00-C0-4E-51-FF-FC		✓											
Dynamic	1	00-C0-4E-54-00-79		✓											
Dynamic	1	00-C0-4E-5C-00-0B		✓											
Dynamic	1	00-C0-4E-5C-FF-F0		✓											
Dynamic	1	00-C0-4E-60-00-00			✓										
Dynamic	1	00-C0-4E-69-00-01		✓											
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Item	Monitor | MAC Table
Switch (stack only)	The stack unit where the entry is learned.
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.

Monitor | VLANs

The following pages are under the Monitor | VLANs menu.

- VLANs | Membership on Page 249
- VLANs | Ports on Page 250

VLANs | Membership

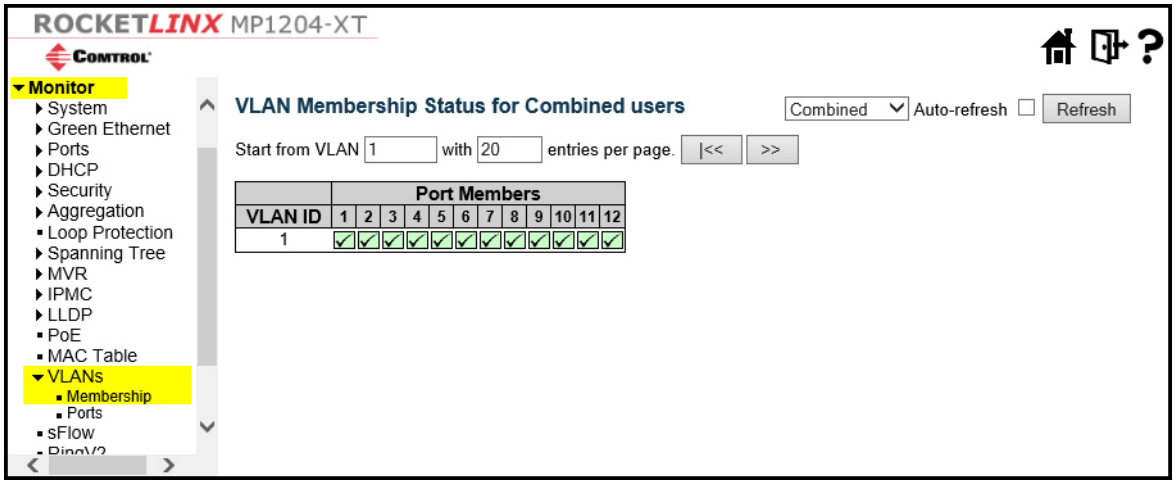
Each page shows up to 99 entries from the VLAN table (default being 20), selected through the **entries per page** input field. When first visited, the page shows the first 20 entries from the beginning of the VLAN Table. The first displayed is the one with the lowest VLAN ID found in the VLAN Table.

The **VLAN** input field allows you to select the starting point in the VLAN Table.

Clicking the **Refresh** button updates the displayed table starting from that or the closest next VLAN Table match.

The >> uses 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.

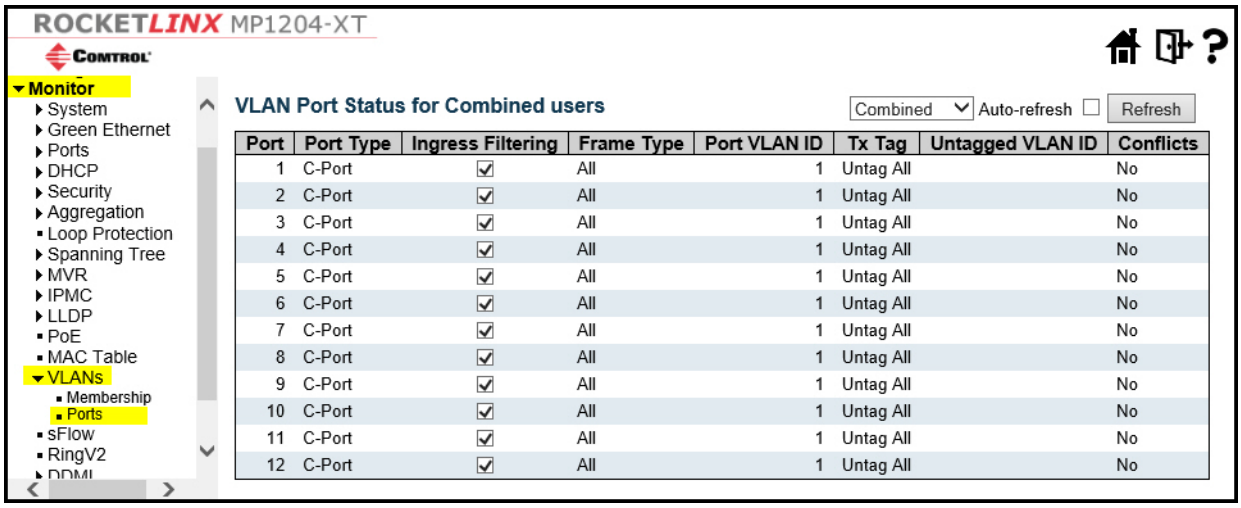


Item	Monitor | VLANs | Membership
VLAN User	Various internal software modules may use VLAN services to configure VLAN memberships on the fly. • The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. • The **Combined** entry shows a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.
VLAN ID	VLAN ID for which the Port members are displayed.

Item	Monitor | VLANs | Membership (Continued)
Port Members	A row of check boxes for each port is displayed for each VLAN ID. • If a port is included in a VLAN, a check mark with a green background is displayed. • If a port is in the forbidden port list, a red X with a pink background is displayed. • If a port is in the forbidden port list and at the same time attempted included in the VLAN, the following image is displayed: . The port is not a member of the VLAN in this case.

VLANs | Ports

This page provides VLAN Port Status.



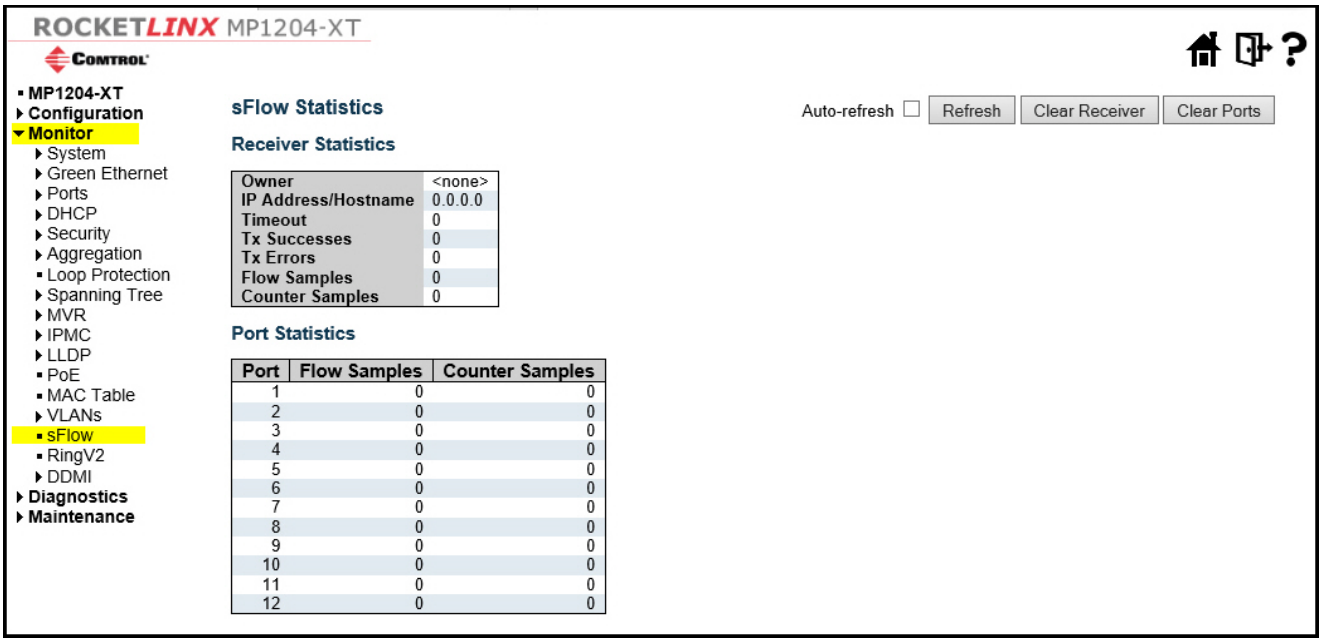
Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	1	Untag All		No
2	C-Port	☑	All	1	Untag All		No
3	C-Port	☑	All	1	Untag All		No
4	C-Port	☑	All	1	Untag All		No
5	C-Port	☑	All	1	Untag All		No
6	C-Port	☑	All	1	Untag All		No
7	C-Port	☑	All	1	Untag All		No
8	C-Port	☑	All	1	Untag All		No
9	C-Port	☑	All	1	Untag All		No
10	C-Port	☑	All	1	Untag All		No
11	C-Port	☑	All	1	Untag All		No
12	C-Port	☑	All	1	Untag All		No

Item	Monitor | VLANs | Ports
VLAN User	Various internal software modules may use VLAN services to configure VLAN port configuration on the fly. • 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 shows a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware. • 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.
Port	The logical port for the settings contained in the same row.
Port Type	Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port.) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.

Item	Monitor | VLANs | Ports
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	Shows the acceptable frame types (All, Taged, Untagged) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.
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	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. The field is empty if not overridden by the selected user.
Untagged VLAN ID	If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field shows the VLAN ID the user wants to tag or untag on egress. The field is empty if not overridden by the selected user.
Conflicts	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. 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. If conflicts exist, it is displayed as **Yes** for the Combined user and the offending software module. The Combined user reflects what is actually configured in hardware.

Monitor - sFlow

This page shows receiver and per-port sFlow statistics.

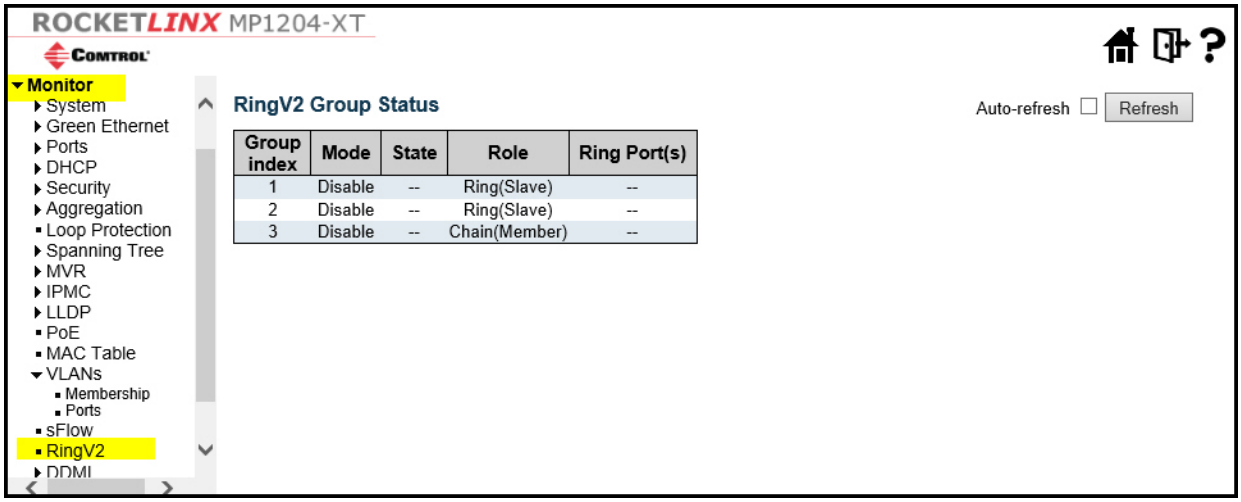


Item	Monitor | sFlow
Receiver Statistics	
Owner	This field shows the current owner of the sFlow configuration. It assumes one of three values as follows: • If sFlow is currently unconfigured/unclaimed, Owner contains **<none>**. • If sFlow is currently configured through Web or CLI, Owner contains **<Configured through local management>**. • If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.
IP Address/ Hostname	The IP address or hostname of the sFlow receiver.
Timeout	The number of seconds remaining before sampling stops and the current sFlow owner is released.
Tx Successes	The number of UDP datagrams successfully sent to the sFlow receiver.
Tx Errors	The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping page (**Diagnostics | Ping/Ping6**).
Flow Samples	The total number of flow samples sent to the sFlow receiver.
Counter Samples	The total number of counter samples sent to the sFlow receiver.

Item	Monitor | sFlow
Port Statistics	
Port	The port number for which the following statistics applies.
Rx and Tx Flow Samples	The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.
Counter Samples	The total number of counter samples sent to the sFlow receiver originating from this port.

Monitor - RingV2

This page provides a status overview for all Ring statuses.



Item	Monitor | RingV2
Group Index	The group index. This parameter is used for easy identifying which ring group.
Mode	It indicates whether the group is enabled.
Role	It indicates group is configured as which role.
State	• When ring is complete, it shows **Normal**. • When ring is incomplete (at least one link is down), it shows **Fail**.
Ring Port(s)	Describes current status of ring port(s).

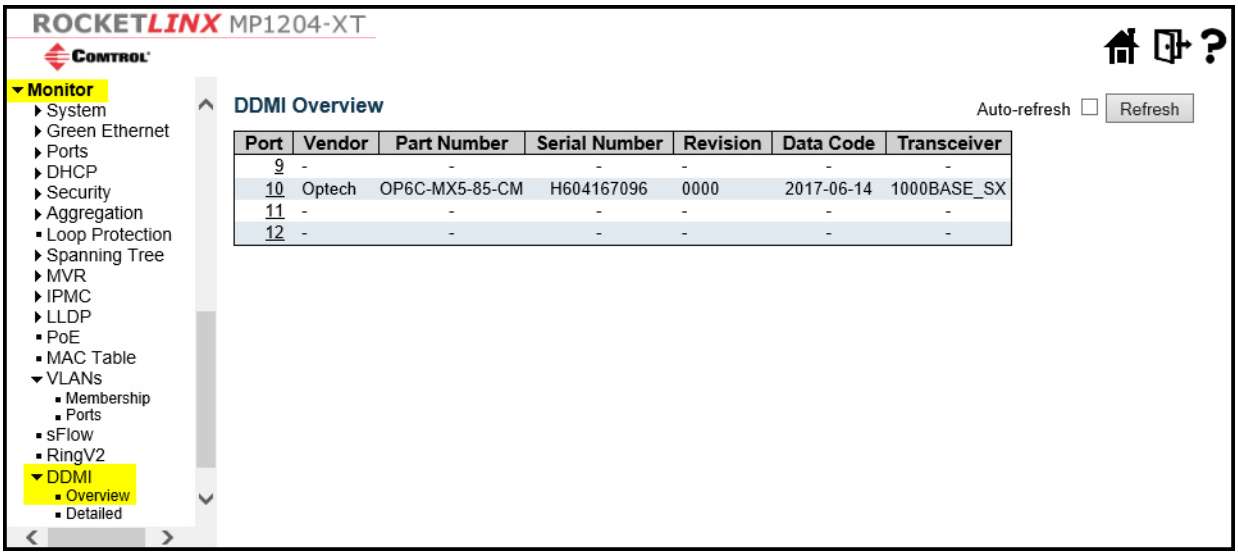
Monitor | DDMI

The following pages are under the DDMI menu.

- DDMI | Overview on Page 254
- DDMI | Detailed on Page 255

DDMI | Overview

Use this page to display DDMI overview information.

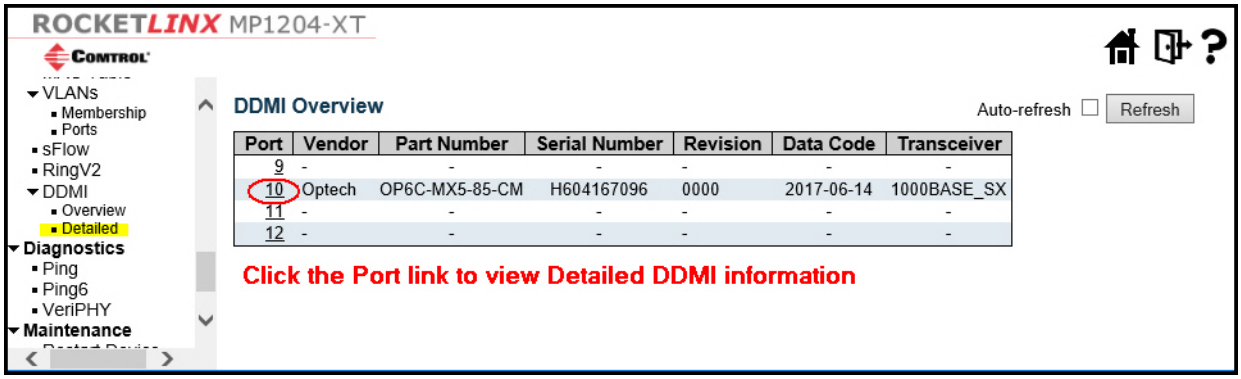


Item	Monitor | DDMI | Overview
Port	DDMI port.
Vendor	Indicates Vendor name SFP vendor name.
Part Number	Indicates Vendor PN Part number provided by SFP vendor.
Serial Number	Indicates Vendor SN Serial number provided by vendor.
Revision	Indicates Vendor rev Revision level for part number provided by vendor.
Date Code	Indicates Date code Vendor's manufacturing date code.
Transceiver	Indicates Transceiver compatibility.

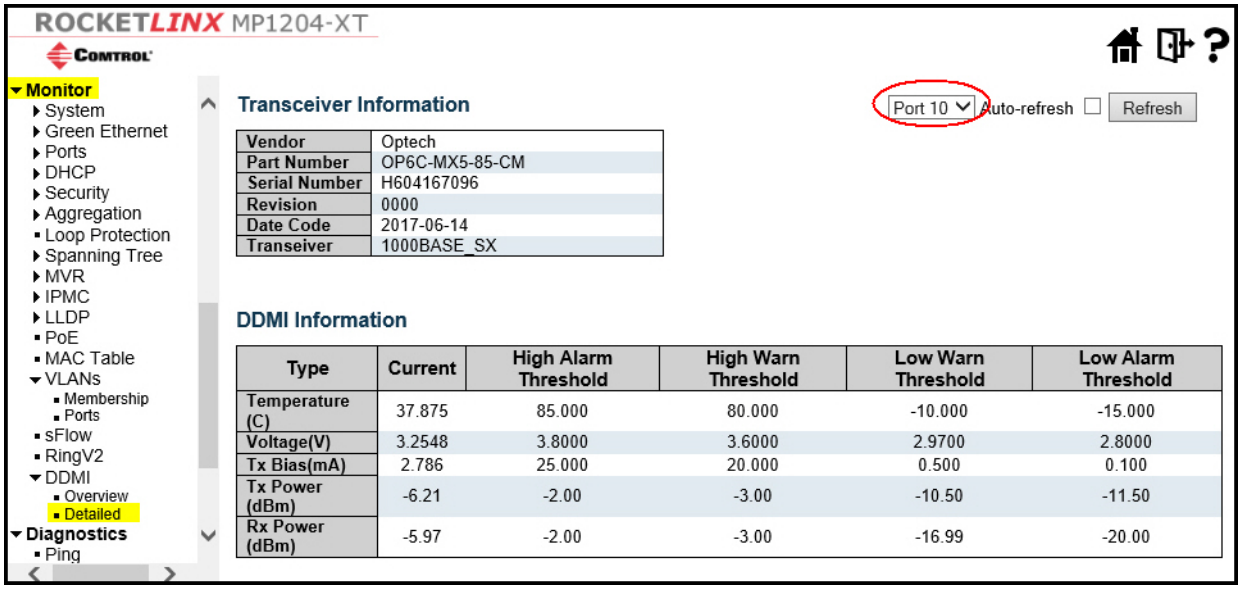
DDMI | Detailed

You can display DDMI detailed information on this page.

You can access the **DDMI | Detailed** page by clicking on the Port link in the **DDMI | Overview** page or by selecting the appropriate port in the drop list.



This illustrates the **Monitor | DDMI | Detailed** page.



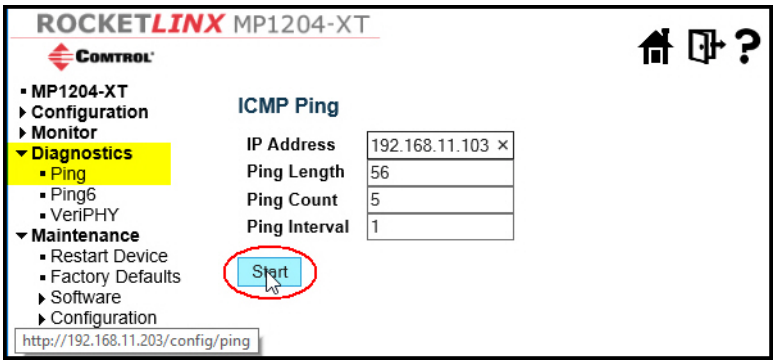
Item	Monitor | DDMI | Detailed
Transceiver Information	
Vendor	Indicates Vendor name SFP vendor name.
Part Number	Indicates Vendor PN Part number provided by SFP vendor.
Serial Number	Indicates Vendor SN Serial number provided by vendor.
Revision	Indicates Vendor rev Revision level for part number provided by vendor.
Date Code	Indicates Date code Vendor's manufacturing date code.
Transceiver	Indicates Transceiver compatibility.

Item	Monitor | DDMI | Detailed
DDMI Information	
Current	The current value of temperature, voltage, TX bias, TX power, and RX power.
High Alarm Threshold	The high alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.
High Warn Threshold	The high warn threshold value of temperature, voltage, TX bias, TX power, and RX power.
Low Warn Threshold	The low warn threshold value of temperature, voltage, TX bias, TX power, and RX power.
Low Alarm Threshold	The low alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.

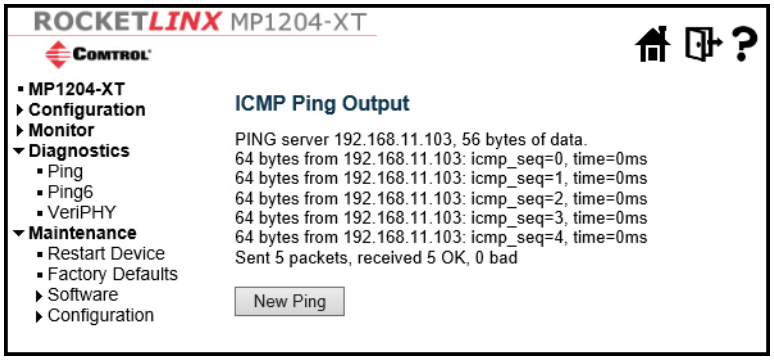
Diagnostics Pages

Ping

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



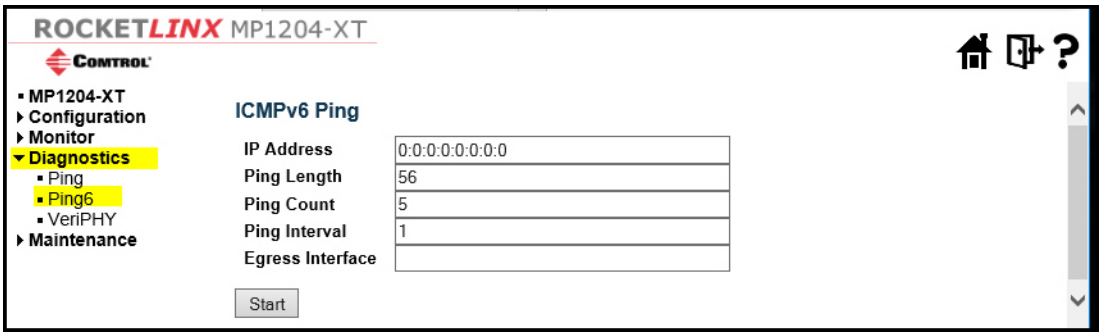
This screen shot shows the Ping response.



Item	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 are 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.

Ping6

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.



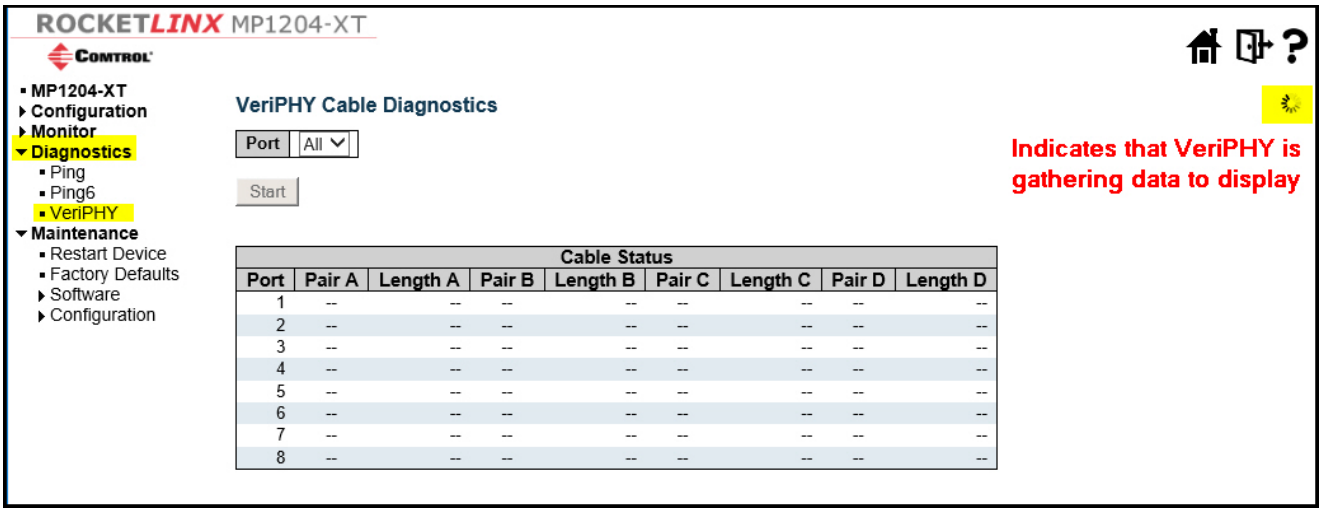
Item	Diagnostics | Ping6
IP Address	The destination IP Address.
Ping Length	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
Ping Count	The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 second 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 are 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.

VeriPhy

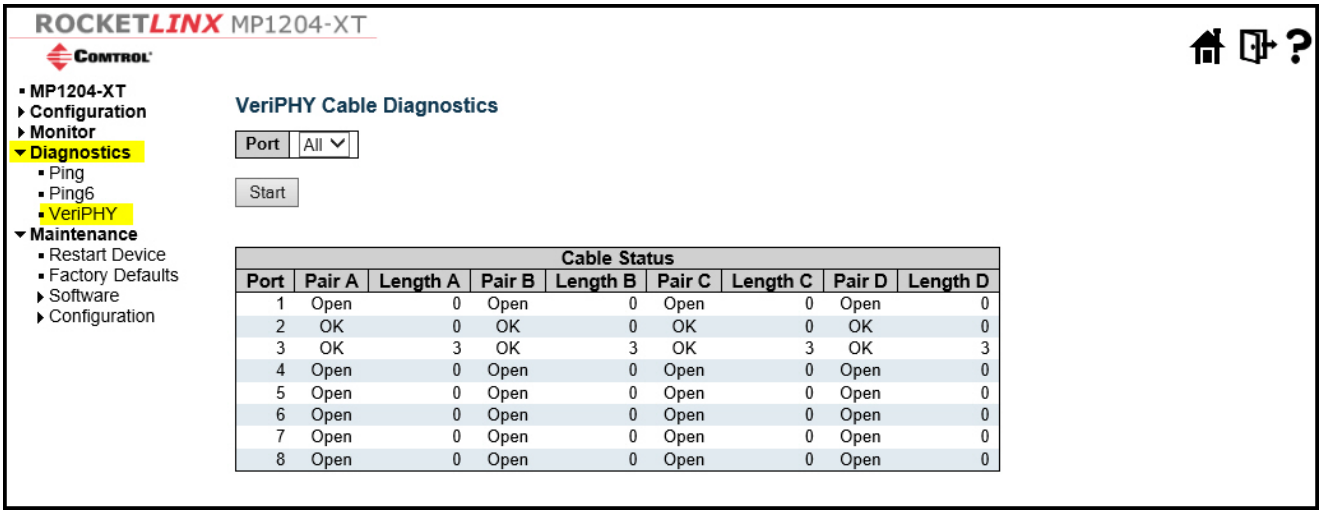
Press the **Start** button to run the diagnostics. This takes approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table.

Note: *VeriPHY is only accurate for cables of length 7 - 140 meters.*

10 and 100 Mbps ports are linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port causes the MP1204-XT to stop responding until VeriPHY is complete.



After pressing the **Start** button, the following table shows up.



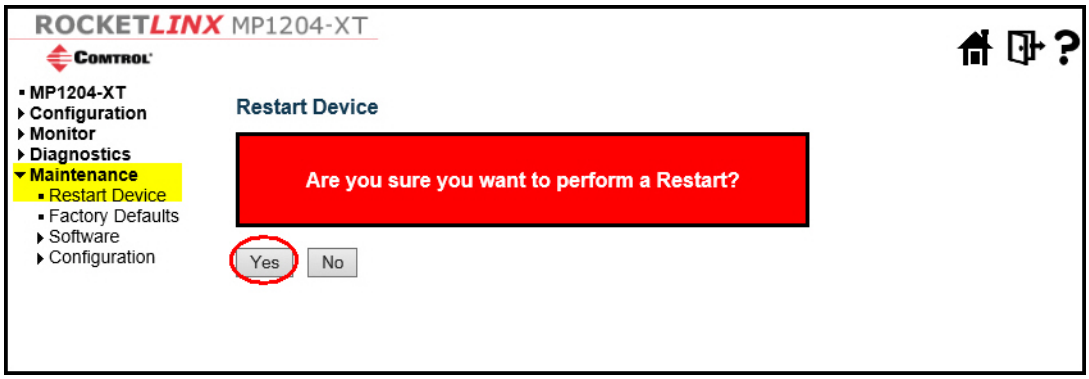
Item	Diagnostics | VeriPHY
Port	The port where you are requesting VeriPHY Cable Diagnostics.

Item	Diagnostics | VeriPHY (Continued)
Cable Status	**Port**: Port number. **Pair**: The status of the cable pair. • OK - Correctly terminated pair • Open - Open 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

Maintenance Pages

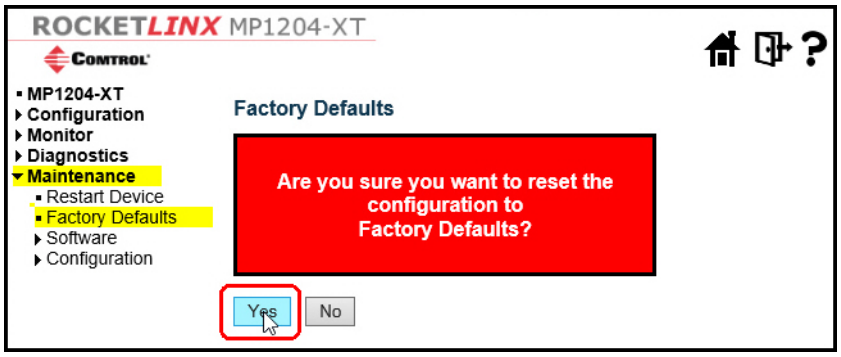
Maintenance | Restart Device

You can restart the MP1204-XT using this page.



Maintenance | Factory Defaults

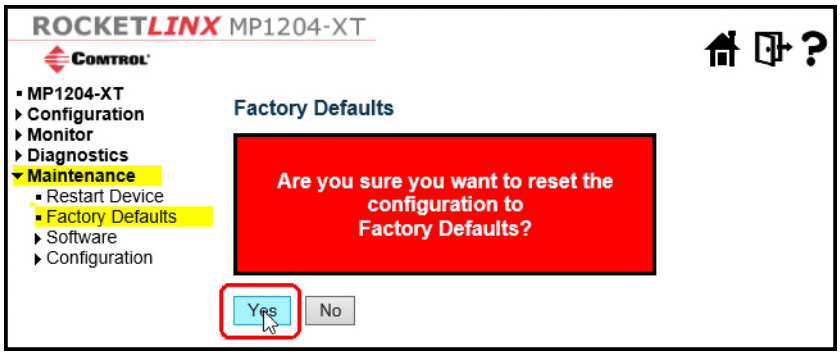
You can reset the configuration of the MP1204-XT on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary.



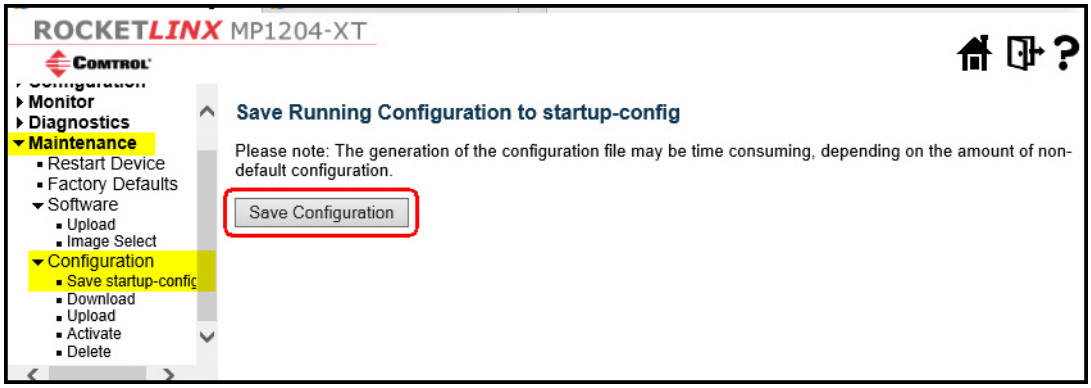
Using the Web Interface to Reset the Default Settings

Use this procedure to reset the configuration to default settings but keep the IP settings.

1. Log into the web interface using the IP address.
2. Click **Maintenance | Factory Defaults** and then click the **Yes** button.

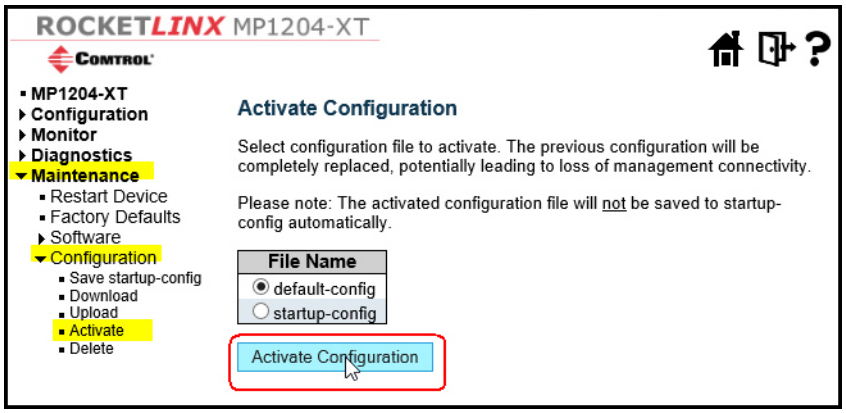


3. Click **Maintenance | Configuration | Save startup-config**.
4. Click the **Save Configuration** button.



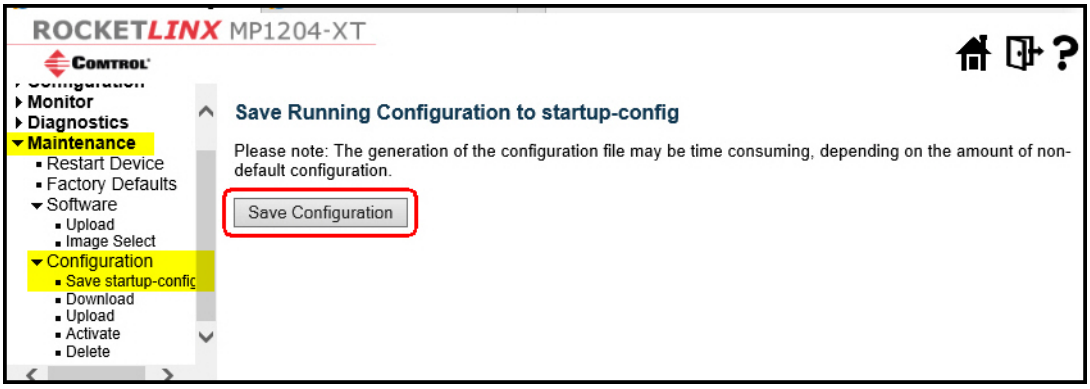
Use this procedure if you want to reset all of the configuration settings including the IP settings.

1. Click **Maintenance | Configuration | Activate**.
2. Select **default-config** and then click the **Activate Configuration** button.



3. Change your system's IP address to the same network segment as 192.168.250.X networks.
4. Log into the MP1204-XT default IP address (192.168.250.250).

5. Click **Maintenance | Configuration | Save startup-config** and then click the **Save Configuration** button.



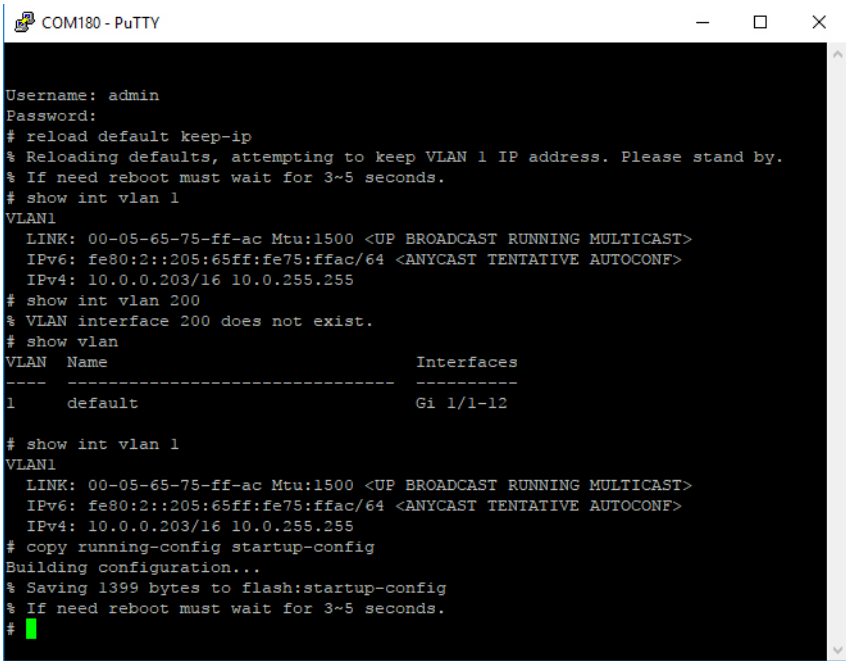
Using the CLI to Reset the Default Settings

You can choose to reset:

- MP1204-XT configuration excluding IP configuration settings
- All of the configuration settings (Page 263)

Use this procedure to reset the configuration to default settings but keep the IP settings.

1. Access the CLI using the console port or telnet.
2. Type **reload defaults keep-ip**
3. Check the interface VLAN and IP address to confirm only management IP setting kept by entering these commands:
   - **show int vlan 1**
   - **show vlan**
   - **show int vlan 1**
4. Save the new settings to the flash by entering: **copy running-config startup-config**



To reset the all configuration to default completely including the IP configuration settings:

1. Access the CLI using the console port or telnet.
2. Enter: **reload defaults**
3. Check the interface VLAN and IP address and confirm that they all changed to default settings.
4. Save the new settings to the flash by entering: **copy running-config startup-config**

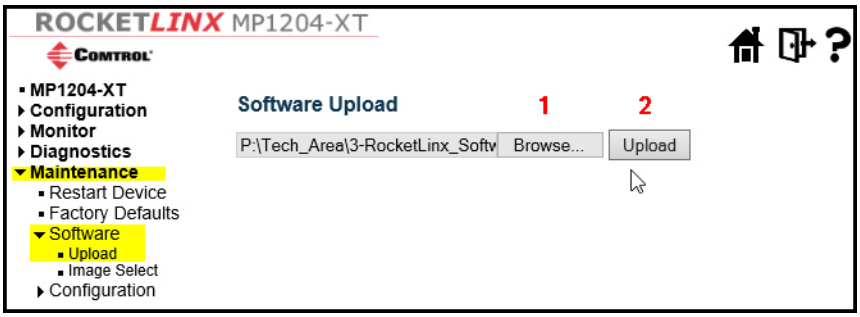
Maintenance | Software

The following pages are under the **Maintenance | Software** menu.

- *Software | Upload* on Page 264
- *Software | Image Select* on Page 265

Software | Upload

This page facilitates an update of the firmware controlling the MP1204-XT.

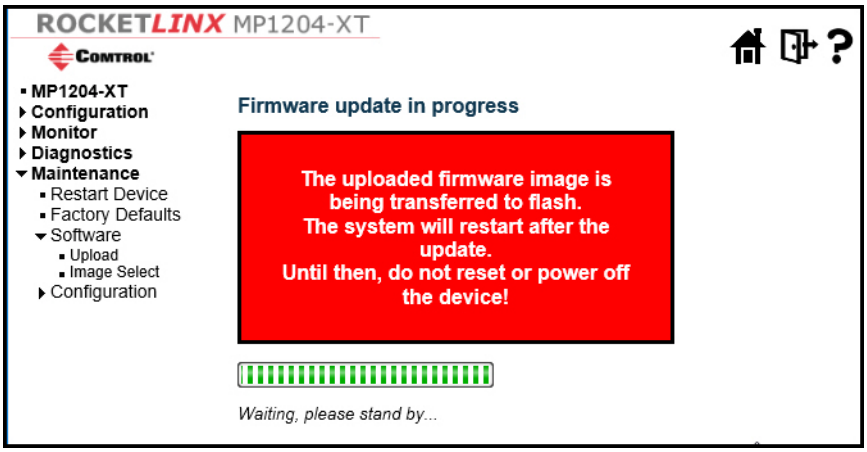


Note: *While the firmware is being updated, Web access appears to not be functioning. The front LED flashes Green / Off with a frequency of 10 Hz while the firmware update is in progress.* ***Do not restart or power off the device at this time or the switch may fail to function afterwards****.*

In the event that you need to upgrade the firmware on the MP1204-XT, you can refer to the following procedure.

1. Open the Web UI using the IP address and go to the **Maintenance | Software | Upload** page.
2. Select the software file, and click **Upload** button.

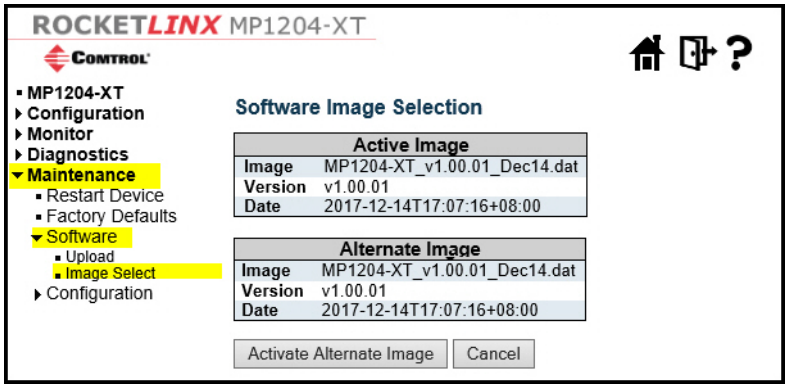
Note: *After starting to upload software to device, do NOT cold / warm start device and wait for it to automatically reboot and then upgrade is finished.*



Software | 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 page displays two tables with information about the active and alternate firmware images.



Notes:

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 automatically uses 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.

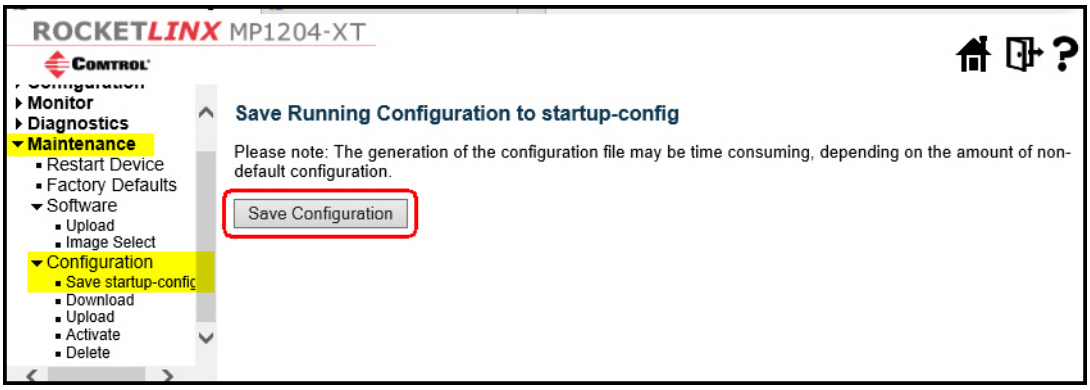
Item	Maintenance | Software |Image Select
Image	The flash index name of the firmware image. The name of primary (preferred) image is image, the alternate image is named **image.bk.**
Version	The version of the firmware image.
Data	The date where the firmware was produced.

Maintenance | Configuration

The following pages are under the Maintenance | Configuration menu.

Configuration | Save startup-config

Copy the **running-config** to the **startup-config**, thereby ensuring that the currently active configuration is used at the next reboot.

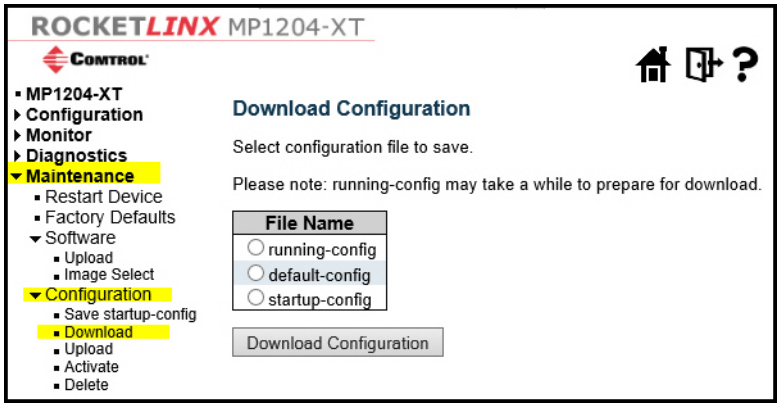


Configuration | Download

It is possible to download any of the files on the switch to the web browser.

Select the file and click the **Download Configuration** button.

Note: *Downloading the running-config may take a little while to complete, as the file must be prepared for download.*



Configuration | Upload

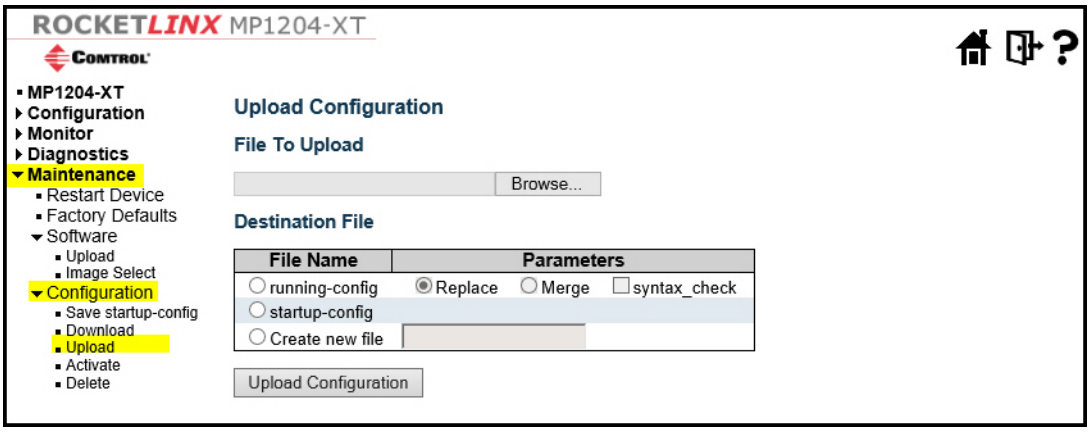
It is possible to upload a file from the web browser to all the files on the switch, except the **default-config** file, which is read-only.

Select the file to upload, select the destination file on the target, then click the **Upload Configuration** button.

If the destination is the **running-config** file, the file is applied to the MP1204-XT 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**.

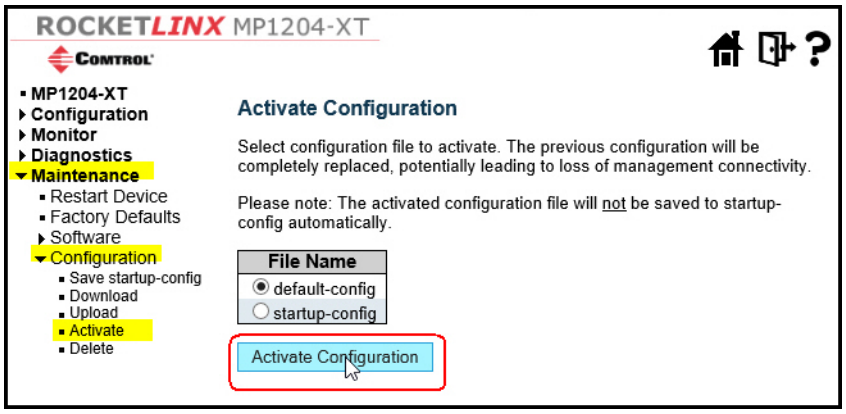
If the file system is full (i.e. contains the three system files mentioned above plus two other files), it is not possible to create new files, but an existing file must be overwritten or another deleted first.



Configuration | Activate

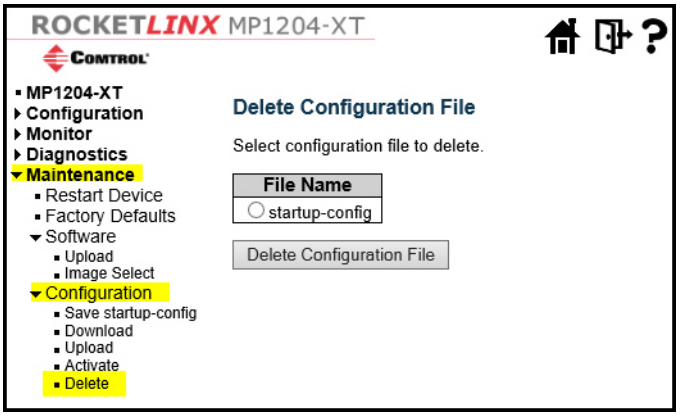
It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.

Select the file to activate and click the **Activate Configuration** button. This initiates the process of completely replacing the existing configuration with that of the selected file.



Configuration | 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.



Command Line Interface (CLI)

Interface Connection

You can refer to *Using the Console Port* on Page 29 for more information.

Interface	Parameter
Console	Baud rate: 115200bps,
Data bit	8
Parity	None
Stop bit	1
Telnet	Port 23
SSH	Port 22 (In Windows, you can run terminal emulator such as PuTTY)

Execution Modes

The CLI contains several execution modes. Users will see different set of commands under different execution modes. The following table lists all the execution modes and their purposes. When users enter a certain execution mode, the corresponding mode prompts are displayed automatically on the screen. The mode prompts of all the execution modes are also listed in the table.

Mode	Access Level	Prompt
Init Mode	Guest	>
Enable Mode	Guest	#
Config Mode	Guest	(conf)#
Alarm Profile Config Mode	Engineer	(alarm-profile-conf)#
Gigabit Interface Config Mode	Engineer	(gigabit-intf-conf)#
ACL Profile Config Mode	Engineer	(acl-profile-conf)#
scheduler Profile Config Mode	Engineer	(sch-profile-conf)#
Vlan Interface Config Mode	Engineer	(vlan-intf-conf)#
IGMP MVR Profile Config Mode	Engineer	(igmp-mvr-profile-conf)#
IGMP ACL Profile Config Mode	Engineer	(igmp-acl-profile-conf)#
RingV2 Group Config Mode	Engineer	(ring)#
Trunk Group Config Mode	Engineer	(trunk-group-conf)#

Getting Help

You can get help by entering a question mark (**?**) at each position in the command. The displayed result depends on the execution mode and previous input.

Terminal Key Function

Following is the list of all the terminal keys and their function.

ENTER CTRL-M	Run a CLI config script
TAB CTRL-I	Tab completion. • If tab is pressed after a non-whitespace character, complete the word before the Tab. • If tab is pressed after a whitespace character, complete the next word.
?	Display available commands • If **?** is pressed after a non-whitespace character, show possible choices for this word. • If **?** is pressed after a whitespace character, show possible choices for the next word.
<Up Arrow> CTRL-P	Up history
<Down Arrow> CTRL-N	Down history
Home CTRL-A	Move the cursor to the beginning of the input line
End CTRL-E	Move the cursor to the end of the input line
<Left Arrow> CTRL-B	Move the cursor backward
<Right Arrow> CTRL-F	Move the cursor forward
BACKSPACE CTRL-H	Erase the character before the cursor

Notation Conventions

The notation conventions for the parameter syntax of each CLI command are as follows:

- Parameters enclosed in **[ ]** are optional.
- Parameter values are separated by a vertical bar (|) only when one of the specified values can be used.
- Parameter values are enclosed in **{ }** when you must use one of the values specified.

Initialize Mode Commands

The commands in this section (except **enable** command) can be executed under all command modes. These commands are global commands.

exit

Description	Exit current mode and quit CLI.
Syntax	exit
Parameter	None

configure terminal

Description	Enter configuration mode.
Syntax	configure terminal
Parameter	None

enable

Description	Enter enable mode.
Syntax	enable
Parameter	None

Show terminal

Description	Show CLI environment variables
Syntax	show terminal
Parameter	None

Show history

Description	Show command history (Note: commands issued in one execution mode only appear in history of that execution mode)
Syntax	show history
Parameter	None

Show clock

Description	Show current time
Syntax	show clock [detail]
Parameter	None

Show clock detail

Description	Show detailed information
Syntax	show clock detail
Parameter	None

Enable Mode Commands

All the **show - -** commands in this section can also be executed under any other command mode except **Initialize Mode**.

configure terminal

Description	Enter configuration mode.
Syntax	configure
Parameter	None

disable

Description	Enter init mode.
Syntax	disable
Parameter	None

show aaa

Description	Show AAA
Syntax	show aaa
Parameter	None

show access management

Description	Access management configuration	
Syntax	show access management [statistics | <access_id_list>]	
Parameter	**Name**	**Description**
	statistics	Statistics data
	access_id_list	ID of access management entry

show access-list

Description	Access list	
Syntax	show access-list [interface [(<port_type> [<v_port_type_list>])]] [rate-limiter [<rate_limiter_list>]] [ace statistics [<ace_list>]] show access-list ace-status [static] [link-oam] [loop-protect] [dhcp] [ptp] [upnp] [arp-inspection] [mep] [ipmc] [ip-source-guard] [ip-mgmt] [conflicts] [switch <switch_list>]	
Parameters	**Name**	**Description**
	interface	Select an interface to configure
	ace-status	The local ACEs status
	port_type	GigabitEthernet,1 Gigabit Ethernet Port
	v_port_type_list	PORT_LIST, Port list in 1/1-14
	rate-limiter	Rate limiter
	rate_limiter_list	<RateLimiterList : 1~16> Rate limiter ID
	ace	Access list entry
	statistics	Traffic statistics
	ace_list	<AceId : 1~256> ACE ID
	static	The ACEs that are configured by users manually
	loop-protect	The ACEs that are configured by Loop Protect module
	ipmc	The ACEs that are configured by IPMC module
	ip-source-guard	The ACEs that are configured by IP Source Guard module
	dhcp	The ACEs that are configured by DHCP module
	conflicts	The ACEs that did not get applied to the hardware due to hardware limitations
	arp-inspection	The ACEs that are configured by ARP Inspection module

show aggregation

Description	Aggregation	
Syntax	show aggregation [mode]	
Parameter	**Name**	**Description**
	mode	Traffic distribution mode

show alarm

Description	Alarm information	
Syntax	show alarm { history | current }	
Parameter	**Name**	**Description**
	current	Show alarm current information
	history	Show alarm history information

show cpu-load

Description	CPU LOAD
Syntax	show cpu-load

show green-ethernet

Description	Green Ethernet	
Syntax	show green-ethernet [interface (<port_type> [<port_list>])] show green-ethernet eee [interface (<port_type> [<port_list>])] show green-ethernet energy-detect [interface (<port_type> [<port_list>])] show green-ethernet short-reach [interface (<port_type> [<port_list>])]	
Parameters	**Name**	**Description**
	eee	Shows green ethernet EEE status for a specific port or ports
	energy-detect	Shows green ethernet energy-detect status for a specific port or ports
	short-reach	Shows green ethernet short-reach status for a specific port or ports
	interface	Shows green ethernet status for a specific port or ports
	port_type	GigabitEthernet, 1 Gigabit Ethernet Port
	port_list	<port_type_list> Port list in 1/1-14

show ip

Description	IP information
Syntax	show ip

	Name	Description
Parameters	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

show ipmc

Description	IPMC information	
Syntax	show ipmc profile [<profile_name>] [detail] show ipmc range [<entry_name>]	
Parameters	**Name**	**Description**
	profile	IPMC profile configuration
	range	A range of IPv4/IPv6 multicast addresses for the profile
	profile_name	<ProfileName : word16> Profile name in 16 char's
	detail	Detail information of a profile
	entry_name	<EntryName : word16> Range entry name in 16 char's

show ipv6

Description	IPv6 information	
Syntax	show ipv6	
Parameters	**Name**	**Description**
	interface	Select an interface to configure
	mld	Multicasat Listener Discovery
	neighbor	IPv6 neighbors
	route	IPv6 routes
	statistics	Traffic statistics

show lacp

Description	LACP information	
Syntax	show lacp { internal | statistics | system-id | neighbour }	
Parameters	**Name**	**Description**
	internal	Internal LACP configuration
	neighbour	Neighbour LACP status
	statistics	Internal LACP statistics
	system-id	LACP system id

show line

Description	Alive line information	
Syntax	show line [alive]	
Parameters	**Name**	**Description**
	alive	Display information about alive lines

show logging

Description	Logging information	
Syntax	show logging <log_id> [switch <switch_list>] show logging [info] [warning] [error] [switch <switch_list>]	
Parameters	**Name**	**Description**
	log_id	<logging_id: 1-4294967295> Logging ID
	error	Error
	info	Infomation
	warning	Warning

show loop-protec

Description	Loop protect information	
Syntax	show loop-protect [interface (<port_type> [<plist>])]	
Parameters	**Name**	**Description**
	interface	Interface status and configuration
	port_type	GigabitEthernet, 1 Gigabit Ethernet Port
	plist	<port_type_list> Port list in 1/1-14

show ntp status

Description	Show SNTP information.
Syntax	show sntp
Parameter	None

show users

Description	Show account list.
Syntax	show account
Parameter	None

show running-cfg

Description	Show running configuration.
Syntax	show running-cfg
Parameter	None

show running-config interface Gigabit

Description	Show port config	
Syntax	show running-config interface (<port_type> [<list>]) [all-defaults]	
Parameters	**Name**	**Description**
	list	<port_type_list> Port list in 1/1-14
	all-defaults	Include most/all default values

show running-config interface vlan

Description	Show default running configuration.
Syntax	show running-config interface vlan <vlan_list> [all-defaults]
Parameter	None

show running-config all-defautls

Description	Show all default setting
Syntax	show running-config [all-defaults]
Parameter	None

show running-config feature

Description	Show running config feature	
Syntax	show running-config feature <feature_name> [all-defaults]	
Parameters	**Name**	**Description**
	feature_name	CWORD Valid words are 'GVRP' 'access' 'access-list' 'aggregation' 'alm_profile' 'arp-inspection' 'auth' 'clock' 'dhcp' 'dhcp-snooping' 'dhcp_server' 'dns' 'dot1x' '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' 'lldp' 'logging' 'loop-protect' 'mac' 'monitor' 'mstp' 'mvr' 'mvr-port' 'ntp' 'phy' 'port' 'port-security' 'pvlan' 'qos' 'rmon' 'snmp' 'source-guard' 'ssh' 'tring_g1' 'tring_g2' 'tring_g3' 'user' 'vlan' 'voice-vlan' 'web-privilege-group-level'
	all-defaults	Include most/all default values

show running-config line

Description	Line information	
Syntax	show running-config line { console | vty } <list> [all-defaults]	
Parameters	**Name**	**Description**
	console	Console
	vty	VTY
	list	<range_list> List of console/VTYs
	all-defaults	Include most/all default values

show running-config vlan

Description	VLAN information	
Syntax	show running-config vlan <list> [all-defaults]	
Parameters	**Name**	**Description**
	list	<vlan_list> List of VLAN numbers
	all-defaults	Include most/all default values

show version

Description	Show firmware hardware and software status update status.
Syntax	show version
Parameter	None

show clock

Description	Show current time.
Syntax	Show clock
Parameter	None

show ddmi

Description	Show DDMI configuration
Syntax	show ddmi
Parameter	None

show version

Description	Show version information.
Syntax	show version
Parameter	None

show system inventory

Description	Show system inventory.
Syntax	show system inventory
Parameter	None

show mac address table aging-time

Description	Show aging time for MAC learning table (system-wide).
Syntax	show aging time
Parameter	None

show mac address table

Description	Show MAC learning table.
Syntax	show mac address-table [conf | static | aging-time | { { learning | count } [interface <port_type> [<port_type_list>]] } | { address <mac_addr> [vlan <vlan_id>] } | vlan <vlan_id> | interface <port_type> [<port_type_list>]]
Parameter	None

show mac address table conf

Description	User added static mac addresses
Syntax	show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>])] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]

show mac address table count

Description	Total number of mac addresse
Syntax	show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>])] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]

show mac address table learning

Description	Learn/disable/secure stat
Syntax	show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>])] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]

show mac address table static

Description	All static mac addresses
Syntax	show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>])] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]

show mac address table interface

Description	Show MAC learning table per port.	
Syntax	show mac address-table [interface <port_type> [<port_type_list>]]	
Parameter	**Name**	**Description**
	<portNo>	Valid values: 1 ~10 Type: Mandatory

show mac address vlan <vlanid>

Description	Show MAC learning table per VLAN index.	
Syntax	show mac address-table { learning | count } vlan <vlan_id>	
Parameter	**Name**	**Description**
	<vlanid>	Valid values: 1~4094 Type: Mandatory

show mvr

Description	MVR information	
Syntax	show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]	
Parameters	**Name**	**Description**
	vlan	Search by VLAN
	v_vlan_list	<vlan_list> MVR multicast VLAN list
	name	Search by MVR name
	mvr_name	<MvrName : word16> MVR multicast VLAN name
	group-database	Multicast group database from MVR
	interface	Search by port
	port_type	GigabitEthernet, 1 Gigabit Ethernet Port
	v_port_type_list	PORT_LIST, Port list in 1/1-14
	sfm-information	Including source filter multicast information from MVR
	detail	Detail information/statistics of MVR group database

show fdb static table

Description	Show static MAC forwarding table.
Syntax	show mac address-table static
Parameter	None

show fdbstatic interface gigabit <portNo>

Description	Show static MAC forwarding table per gigabit port.	
Syntax	Show mac address-table { learning | count } [interface <port_type> [<port_type_list>]]	
Parameters	**Name**	**Description**
	<port_type>	Port type in Fast or Giga ethernet
	<portNo>	Valid values: 1 ~ 10 Type: Mandatory

show fdbstatic vlan <vlanid>

Description	Show static MAC forwarding table per VLAN index.	
Syntax	show mac address-table { learning | count } vlan <vlanid>	
Parameter	**Name**	**Description**
	<vlanid>	Valid values: 1~4094 Type: Mandatory

show interface port < port_type_list >

Description	Show interface information per \port.	
Syntax	show interface <port_type> [<port_type_list>] status	
Parameters	**Name**	**Description**
	<port_type>	Port type in Fast or Giga ethernet
	<portNo>	Valid values: 1 ~ 10 Type: Mandatory

show interface port <portNo> statistics

Description	Show Ethernet counter per gigabit port.	
Syntax	show interface <port_type> [<port_type_list>] statistics	
Parameter	**Name**	**Description**
	<port_type>	Port type in Fast or Giga ethernet
	<portNo>	Valid values: 1 ~ 10 Type: Mandatory
	counter	Show Gigabit Ethernet counter.

show platform phy

Description	PHYs' information
Syntax	show platform phy [interface (<port_type> [<v_port_type_list>])] show platform phy id [interface (<port_type> [<v_port_type_list>])] show platform phy instance show platform phy status [interface (<port_type> [<v_port_type_list>])]

	Name	Description
Parameters	id	ID
	instance	PHY Instance Information
	status	Status
	interface	Interface
	port_type	GigabitEthernet, 1 Gigabit Ethernet Port
	v_port_type_list	PORT_LIST, Port list in 1/1-14

show poe

Description	Show PoE status and information for each port	
Syntax	show poe show poe [interface (<port_type> [<v_port_type_list>])]	
Parameters	**Name**	**Description**
	poe	Power over Ethernet
	port_type	GigabitEthernet, 1 Gigabit Ethernet Port
	v_port_type_list	PORT_LIST, Port list in 1/1-14

show port-security

Description	Port security	
Syntax	show port-security	
Parameters	**Name**	**Description**
	port	Show MAC Addresses learned by Port Security
	switch	Show Port Security status
	interface	Interface
	port_type	GigabitEthernet, 1 Gigabit Ethernet Port
	v_port_type_list	PORT_LIST, Port list in 1/1-14

show profile alarm

Description	Profile alarm
Syntax	show profile alarm
Parameter	None

show sflow

Description	Sflow information	
Syntax	show sflow show sflow statistics { receiver [<rcvr_idx_list>] | samplers [interface [<samplers_list>] (<port_type> [<v_port_type_list>])] }	
Parameters	**Name**	**Description**
	receiver	Show statistics for receiver
	samplers	Show statistics for samplers
	interface	Interface
	port_type	GigabitEthernet, 1 Gigabit Ethernet Port
	v_port_type_list	<port_type_list> Port list in 1/1-14

show snmp

Description	SNMP information	
Syntax	show snmp show snmp access [<group_name> { v1 | v2c | v3 | any } { auth | noauth | priv }] show snmp community v3 [<community>] show snmp host [<conf_name>] [system] [switch] [interface] [aaa] show snmp mib context show snmp mib ifmib ifIndex show snmp security-to-group [{ v1 | v2c | v3 } <security_name>] show snmp user [<username> <engineID>] show snmp view [<view_name> <oid_subtree>]	
Parameters	**Name**	**Description**
	access	access configuration
	group_name	<GroupName : word32> group name
	any	any security model
	v1	v1 security model
	v2c	v2c security model
	v3	v3 security model
	auth	authNoPriv Security Level
	noauth	noAuthNoPriv Security Level
	priv	authPriv Security Level
	community	Community
	community	<Community : word127> Specify community name
	host	Set SNMP host's configurations

Description	SNMP information (continued)	
Parameters (continued)_	conf_name	<ConfName : word32> Name of the host configuration
	aaa	AAA event group
	interface	Interface event group
	switch	Switch event group
	system	System event group
	mib	MIB(Management Information Base)
	context	MIB context
	ifmib	IF-MIB
	ifIndex	The IfIndex that is defined in IF-MIB
	security-to-group	security-to-group configuration
	security_name	<SecurityName : word32> security group name
	user	User
	username	<Username : word32> Security user name
	engineID	<Engiedid : word10-32> Security Engine ID
	view	MIB view configuration
	view_name	<ViewName : word32> MIB view name
	oid_subtree	<OidSubtree : word255> MIB view OID

show spanning-tree

Description	System Wide Spanning Tree Setting/Status.	
Syntax	show spanning-tree [summary | active | { interface (<port_type> [<v_port_type_list>]) } | { detailed [interface (<port_type> [<v_port_type_list_1>])] } | { mst [configuration | { <instance> [interface (<port_type> [<v_port_type_list_2>])] }] }]	
Parameters	**Name**	**Description**
	active	STP active interfaces
	detailed	STP statistics
	interface	Choose port
	mst	Configuration
	summary	STP summary

show switchport forbidden

Description	Lookup VLAN Forbidden port entry	
Syntax	show switchport forbidden [{ vlan <vid> } | { name <name> }]	
Parameters	**Name**	**Description**
	vlan	Show forbidden access for specific VLAN id
	vid	VLAN id
	name	Show forbidden access for specific VLAN name
	name	VLAN name

show tacacs-server

Description	TACACS+ configuration
Syntax	show tacacs-server
Parameter	None

show vlan

Description	Show bridge port memberset/status.
Syntax	show vlan
Parameter	None

show vlan id

Description	Show bridge port member set/status per VLAN index (1~4094).	
Syntax	show vlan id <vlanid>	
Parameter	**Name**	**Description**
	<vlanid>	Valid values: 1~4094 Type: Mandatory.

show vlan name

Description	Show bridge port member set/status per VLAN name (32 words).	
Syntax	show vlan name <vword32>	
Parameter	**Name**	**Description**
	< vword32>	Valid values: 32 words Type: Mandatory.

show vlan brief

Description	VLAN summary information	
Syntax	show vlan [id <vlan_list> | name <name> | brief]	
Parameters	**Name**	**Description**
	id	VLAN status by VLAN id
	vlan_list	<vlan_list> VLAN IDs 1-4095
	name	VLAN status by VLAN name
	name	<vword32> A VLAN name
	brief	VLAN summary information

show vlan ip-subnet

Description	Show VLAN ip-subnet entries	
Syntax	show vlan ip-subnet [id <subnet_id>]	
Parameters	**Name**	**Description**
	id	Show a specific ip-subnet entry
	subnet_id	<1-128> The specific ip-subnet to show

show vlan mac

Description	Show VLAN MAC entries	
Syntax	show vlan mac [address <mac_addr>]	
Parameters	**Name**	**Description**
	address	Show a specific MAC entry
	mac_addr	<mac_ucast> The specific MAC entry to show

show vlan protocol

Description	Protocol-based VLAN status	
Syntax	show vlan protocol [eth2 { <etype> | arp | ip | ipx | at }] [snap { <oui> | rfc-1042 | snap-8021h } <pid>] [llc <dsap> <ssap>]	
Parameters	**Name**	**Description**
	eth2	Ethernet protocol based VLAN status
	etype	0x600-0xffff> Ether Type(Range: 0x600 - 0xFFFF)
	arp	Ether Type is ARP
	ip	Ether Type is IP
	ipx	Ether Type is IPX
	at	Ether Type is AppleTalk
	llc	LLC-based VLAN status
	dsap	<0x0-0xff> DSAP (Range: 0x00 - 0xFF)
	ssap	<0x0-0xff> SSAP (Range: 0x00 - 0xFF)
	snap	SNAP-based VLAN status
	oui	<0x0-0xffffff> SNAP OUI (Range 0x000000 - 0XFFFFFF)
	rfc-1042	SNAP OUI is rfc-1042
	snap-8021h	SNAP OUI is 8021h

show vlan status

Description	Show the VLANs configured for each interface	
Syntax	show vlan status [interface (<port_type> [<plist>])] [combined | admin | nas | mvr | voice-vlan | mstp | erps | vcl | evc | gvrp | all | conflicts]	
Parameters	**Name**	**Description**
	admin	Show the VLANs configured by administrator
	all	Show all VLANs configured
	combined	Show the VLANs configured by a combination
	conflicts	Show VLANs configurations that has conflicts
	gvrp	Show the VLANs configured by GVRP
	interface	Show the VLANs configured for a specific interface(s)
	mstp	Show the VLANs configured by MSTP.
	mvr	Show the VLANs configured by MVR
	nas	Show the VLANs configured by NAS
	vcl	Show the VLANs configured by VCL
	voice-vlan	Show the VLANs configured by Voice VLAN

show qos-queue-mapping

Description	Show CoS queue mapping table.
Syntax	show qos maps
Parameter	None

show interface ports <portNo> priority

Description	Show QoS per gigabit port.	
Syntax	show interface <port_type> [<port_type_list>] statistics { priority [<0~7>] }	
Parameter	**Name**	**Description**
	priority [<0~7>]	Valid values:0 ~7 Type: Mandatory
	<port_type>	Port type in Fast or Giga ethernet
	<portNo>	Valid values:0 ~ 10 Type: Mandatory

show qos

Description	Show scheduler profile table.
Syntax	show queue-scheduler profile
Parameter	None

show queue-shaper

Description	Show queue shaper information.
Syntax	show queue-shaper
Parameter	None

show port-shaper

Description	Show port shaper information.
Syntax	show port-shaper
Parameter	None

show pvlan [<pvlan_list>]

Description	PVLAN ID	
Syntax	show pvlan [<pvlan_list>]	
Parameter	**Name**	**Description**
	pvlan_list	PVLAN ID to show configuration for

show pvlan isolation [interface <port_type> [<port_type_list>]]

Description	Show all port isolation information.	
Syntax	show pvlan isolation [interface <port_type> [<port_type_list>]]	
Parameters	**Name**	**Description**
	<port_type>	Port type in Fast or Giga ethernet
	<portNo>	Valid values: 1 ~ 10 Type: Mandatory

show interface gigabit <portNo> port-isolation

Description	Show isolation information per gigabit port.	
Syntax	show pvlan isolation [interface <port_type> [<port_type_list>]]	
Parameter	**Name**	**Description**
	<portNo>	Valid values: 1 ~ 10 Type: Mandatory

show interface gigabit <portNo> storm-control

Description	Show storm control information per gigabit port.	
Syntax	show interface gigabit <portNo> storm-control	
Parameters	**Name**	**Description**
	<port_type>	Port type in Fast or Giga ethernet
	<portNo>	Valid values: 1~10 Type: Mandatory

show interface gigabit <portNo> transceiver

Description	Show interface transceiver	
Syntax	show interface GigabitEthernet interface <port_type_list> transceiver	
Parameter	**Name**	**Description**
	<portNo>	Valid values: 11 ~ 14 (for 14 port model) Type: Mandatory

show qos interface

Description	QoS interface information	
Syntax	show qos [{ interface [(<port_type> [<port>])] }	
Parameters	**Name**	**Description**
	interface	Interface
	port_type	GigabitEthernet, 1 Gigabit Ethernet Port
	port	PORT_LIST, Port list in 1/1-14

show qos maps

Description	MAPS	
Syntax	show qos maps { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] }	
Parameters	**Name**	**Description**
	cos-dscp	Map for cos to dscp
	dscp-classify	Map for dscp classify enable
	dscp-cos	Map for dscp to cos
	dscp-egress-translation	Map for dscp egress translation
	dscp-ingress-translation	Map for dscp ingress translation

show qos qce

Description	QCE	
Syntax	show qos { qce [<qce>] }	
Parameter	**Name**	**Description**
	qce	<Id : 1-256> QCE ID

show qos storm {unknown-uc|unknown-mc|broadcast}

Description	Show storm control information by VLAN.	
Syntax	show vlan unknown-uc show vlan unknown-mc show vlan broadcast	
Parameters	**Name**	**Description**
	unknown-uc	Show unknown unicast storm control information by VLAN. Type: Mandatory
	unknown-mc	Show unknown multicast storm control information by VLAN. Type: Mandatory
	broadcast	Show broadcast storm control information by VLAN. Type: Mandatory

show port-mirror

Description	Show port mirror information.
Syntax	show port-mirror
Parameter	None

show ringv2

Description	Show ring protect information
Syntax	show ring
Parameter	None

show rmon

Description	show rmon information	
Syntax	show rmon alarm [<id_list>] show rmon event [<id_list>] show rmon history [<id_list>] show rmon statistics [<id_list>]	
Parameters	**Name**	**Description**
	alarm	Display the RMON alarm table
	event	Display the RMON event table
	history	Display the RMON history table
	statistics	Display the RMON statistics table
	id_list	<1~65535>, Statistics entry list

show interface gigabit <portNo>

Description	Show interface gigaport information	
Syntax	show interface gigabit <portNo>	
Parameter	**Name**	**Description**
	<portNo>	Gigabit port. Valid values: 1 ~ 10 Type: Mandatory

show ext-tpid

Description	Show TPID for the VLAN Tag
Syntax	show ext-tpid
Parameter	None

show interface vlan

Description	Show VLAN interface information of all VLANs.
Syntax	show interface vlan
Parameter	None

show interface vlan <vlanid>

Description	Show VLAN interface information of specify VLAN.	
Syntax	show interface vlan <vlanid>	
Parameter	**Name**	**Description**
	<vlanid>	VLAN ID. Valid values: 1 ~ 4094 Type: Mandatory

show protocol-vlan

Description	Show protocol based VLAN information for all entries.
Syntax	show protocol-vlan
Parameter	None

show interface gigabit <portNo> vlan

Description	Show vlan information per port	
Syntax	show interface gigabit <portNo> vlan	
Parameter	**Name**	**Description**
	<portNo>	Gigabit port. Valid values: 1 ~ 10 Type: Mandatory

show vlan-trans

Description	Show VLAN translation table for all
Syntax	show vlan-trans
Parameter	None

show multicast-fdb

Description	Show IGMP group membership table
Syntax	show multicast-fdb
Parameter	None

show dot1x

Description	Show dot1x information.
Syntax	show dot1x
Parameter	None

show dot1x status

Description	Show dot1x stats.
Syntax	show dot1x status [interface <port_type> [<port_type_list>]] [brief]
Parameter	None

show dot1x statistics

Description	Show dot1x statistics	
Syntax	show dot1x statistics { eapol | radius | all } [interface (<port_type> [<v_port_type_list>])]	
Parameters	**Name**	**Description**
	all	Show all dot1x statistics
	eapol	Show EAPOL statistics
	radius	Show Backend Server statistics
	interface	Interface
	port_type	GigabitEthernet, 1 Gigabit Ethernet Port
	v_port_type_list	PORT_LIST, Port list in 1/1-14

show radius-server [statistics]

Description	show radius-server statistics	
Syntax	show radius-server [statistics]	
Parameter	**Name**	**Description**
	[statistics]	Count radius packet statistics

show rfc2544 profile [<word32>]

Description	show rfc2544 profile name	
Syntax	show rfc2544 profile [<word32>]	
Parameter	**Name**	**Description**
	<word32>	rfc2544 profile name

show voice

Description	Vlan for voice traffic	
Syntax	show voice vlan [oui <oui> | interface (<port_type> [<port_list>])]	
Parameters	**Name**	**Description**
	vlan	Vlan for voice traffic
	oui	OUI configuration
	oui	OUI value
	interface	Select an interface to configure
	port_type	GigabitEthernet, 1 Gigabit Ethernet Port
	port_list	<port_type_list> Port list in 1/1-14

show web

Description	Web privilege	
Syntax	show web privilege group [<group_name>] level	
Parameters	**Name**	**Description**
	privilege	Web privilege
	group	Web privilege grou
	group_name	CWORD Valid words are 'Aggregation' 'DHCP' 'Debug' 'Dhcp_Client' 'Diagnostics' 'EEE' 'Green_Ethernet' 'IP2' 'IPMC_Snooping' 'LACP' 'LLDP' 'Loop_Protect' 'MAC_Table' 'MVR' 'Maintenance' 'Mirroring' 'NTP' 'Ports' 'Private_VLANs' 'QoS' 'RPC' 'Security' 'Spanning_Tree' 'System' 'Timer' 'VCL' 'VLANs' 'Voice_VLAN' 'XXRP' 'sFlow'
	level	Web privilege group level

Configure Mode Commands

Commands that can be executed under **Configure** mode.

interface gigabit <portNo>

Description	Gigabit Ethernet interface. (enter gigabit interface mode)	
Syntax	interface gigabit <portNo>	
Parameter	**Name**	**Description**
	<portNo>	Valid values: 1 ~ 10 Type: Mandatory

interface vlan <vlanid>

Description	Vlan Ethernet interface (enter mode of interface vlan)	
Syntax	interface vlan <vlanid>	
Parameter	**Name**	**Description**
	<vlanid>	Valid values: 1 ~ 4094 Type: Mandatory

aaa

Description	Authentication	
Syntax	aaa authentication	
Parameter	**Name**	**Description**
	authentication	Authentication

access

Description	Management configuration	
Syntax	access management	
Parameter	**Name**	**Description**
	management	Access management configuration

access-list

Description	Enter Acl Profile Config Mode	
Syntax	profile acl	
Parameter	**Name**	**Description**
	<vlanid>	Valid values: 1 ~ 4094 Type: Mandatory

aggregation mode

Description	Traffic distribution mode	
Syntax	aggregation mode { dmac | ip | port | smac }	
Parameter	**Name**	**Description**
	dmac	Destination MAC affects the distribution
	ip	IP address affects the distribution
	port	IP port affects the distribution
	smac	Source MAC affects the distribution

alarm history clear

Description	Clear alarm history
Syntax	alarm history clear
Parameter	None

banner

Description	Banner control	
Syntax	banner { LINE | exec | login | motd }	
Parameter	**Name**	**Description**
	LINE	c banner-text c, where 'c' is a delimiting character
	exec	Set EXEC process creation banner
	login	Set login banner
	motd	Set Message of the Day banner

ddmi

Description	Enable DDMI function
Syntax	ddmi
Parameter	None

default access-list rate-limiter

Description	Rate limiter	
Syntax	default access-list rate-limiter [<rate_limiter_list>]	
Parameter	**Name**	**Description**
	RateLimiterId : 1-16	Rate limiter ID

profile sch

Description	Enter Scheduling Profile Config Mode
Syntax	profile sch
Parameter	None

ntp server <1-5> ip-address <ip>

Description	Set NTP server address.	
Syntax	ntp server <1-5> ip-address { <ipv4_ucast> | <ipv6_ucast> | <hostname> }	
Parameters	**Name**	**Description**
	<1-5>	index number
	<ipv4> <ipv6>	Type: Mandatory
	<hostname>	Server name

clock timezone

Description	Set time zone.	
Syntax	clock timezone <word16> <-23-23> [<0-59>]	
Parameters	**Name**	**Description**
	< word16>	Valid values: please see 'list timezone' Type: Mandatory
	default	Set time zone to default (GMT/UTC). Type: Mandatory

clock summer-time set [start-time] [end-time]

Description	Set date/time.	
Syntax	clock summer-time <word16> date [<1-12> <1-31> <2000-2097> <hhmm> <1-12> <1-31> <2000-2097> <hhmm> [<1-1440>]]	
Parameters	**Name**	**Description**
	< word16>	Valid values: please see 'list timezone' Type: Mandatory
	<day>	Valid values: 1 ~ 31 Type: Mandatory
	<month>	Valid values: 1 ~ 12 Type: Mandatory
	<year>	Valid values: 2000-2097 Type: Mandatory
	<minute>	Valid values: 0 ~ 59 Type: Mandatory
	<second>	Valid values: 0 ~ 59 Type: Optional

account add <username>

Description	Add an account.	
Syntax	username <word31> privilege <0-15> password encrypted <word4-44>	
Parameters	**Name**	**Description**
	< word31>	Valid values: 1 ~ 31 characters Type: Mandatory
	<0-15>	Valid values: 0 ~ 15 Type: Mandatory
	< word4-44>	Valid values: 4-44 characters Type: Mandatory

account delete <username>

Description	Delete an account.	
Syntax	no username <word31>	
Parameter	**Name**	**Description**
	< word31>	Valid values: 1 ~ 31 characters Type: Mandatory

syslog {enable|disable}

Description	Disable or enable syslog service.
Syntax	logging on no logging on
Parameter	None

configuration save and replace

Description	Save and install configuration	
Syntax	copy { startup-config | running-config | <Filename> } { startup-config | running-config | < Filename > } [syntax-check]	
Parameter	**Name**	**Description**
	running-config	Currently running configuration
	startup-config	Startup configuration
	syntax-check	Perform syntax check on source configuration
	Filename	File in FLASH or on TFTP server

clear ip igmp snooping statistics

Description	clear ipigmpsnoopingstatisti	
Syntax	clear ip igmp snooping [vlan<vlan_list>] statistics	
Parameter	**Name**	**Description**
	vlan_list	VLAN list.

clear logging

Description	clear logging	
Syntax	clear logging [info] [warning] [error] [switch <switch_list>]	
Parameters	**Name**	**Description**
	info	Information
	warning	Warning
	error	Error
	Switch list	List of switch ID, ex, 1,3-5,6

clear mac address-table

Description	clear mac address-table
Syntax	clear mac address-table
Parameter	None

debug

Description	Set prompt for testing	
Syntax	debug prompt	
Parameter	**Name**	**Description**
	<word>	Word for prompt in 32 char's

delete

Description	Delete one file in flash: file system	
Syntax	delete <word>	
Parameter	**Name**	**Description**
	<word>	Name of file to delete

dir

Description	Directory of all files in flash: file system
Syntax	dir
Parameter	None

do

Description	To run exec commands in config mode	
Syntax	do <line>	
Parameter	**Name**	**Description**
	<line>	Exec Command

duplex

Description	Set duplex mode	
Syntax	duplex { half | full | auto [half | full] }	
Parameters	**Name**	**Description**
	half	Forced half duplex.
	full	Forced full duplex.
	auto	Auto negotiation of duplex mode.
	[half | full]	Advertise half /full duplex.

editing

Description	Enable command line editing
Syntax	editing
Parameter	None

firmware

Description	Firmware swap and upgrade	
Syntax	firmware { swap | upgrade }	
Parameters	**Name**	**Description**
	swap	Swap between Active and Alternate firmware image
	upgrade	Firmware upgrade

flowcontrol

Description	Enable/Disable flow control.	
Syntax	flowcontrol { on | off }	
Parameters	**Name**	**Description**
	on	Enable flow control.
	off	Disable flow control.

frame-sizes

Description	Select the frame sizes that the enabled tests will loop through	
Syntax	frame-sizes { [64] [128] [256] [512] [1024] [1280] [1518] [2000] [9600] }	
Parameters	**Name**	**Description**
	64	Enable testing with 64-byte TST PDUs
	128	Enable testing with 128-byte TST PDUs
	256	Enable testing with 256-byte TST PDUs
	512	Enable testing with 512-byte TST PDUs
	1024	Enable testing with 1024-byte TST PDUs
	1280	Enable testing with 1280-byte TST PDUs
	1518	Enable testing with 1518-byte TST PDUs
	2000	Enable testing with 2000-byte TST PDUs
	9600	Enable testing with 9600-byte TST PDUs

green-etherneteee

Description	Powering down of PHYs when there is no traffic.
Syntax	green-etherneteee
Parameter	None

green-etherneteee optimize-for-power

Description	Set if EEE shall be optimized for least power consumption (else optimized for least traffic latency).
Syntax	green-etherneteee optimize-for-power
Parameter	None

green-etherneteee urgent-queues

Description	Enables EEE urgent queue. An urgent queue means that latency is kept to a minimum for traffic goin to that queue. Note: EEE power savings will be reduced.	
Syntax	green-etherneteee urgent-queues [<range_list>]	
Parameter	**Name**	**Description**
	range_list	EEE Interface.

help

Description	Description of the interactive help system
Syntax	help
Parameter	None

iparp inspection

Description	iparp inspection
Syntax	iparp inspection
Parameter	None

ip arp inspection translate

Description	IP ARP inspection entry interface configuration	
Syntax	ip arp inspection translate [interface <port_type><port_type_id><vlan_id><mac_ucast><ipv4_ucast>]	
Parameters	**Name**	**Description**
	port_type	Port type in Fast or Gigaethernet
	port_type_id	Port ID in the format of switch-no/port-no
	vlan_id	Select a VLAN id to configure
	mac_ucast	Select a MAC address to configure
	ipv4_ucast	Select an IP Address to configure

ip arp inspection entry

Description	arp inspection entry interface config	
Syntax	ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>	
Parameters	**Name**	**Description**
	port_type	Port type in Fast or Giga ethernet
	in_port_type_id	Port ID in the format of switch-no/port-no
	vlan_var	Select a VLAN id to configure
	mac_var	Select a MAC address to configure
	ipv4_var	Select an IP Address to configure

ip arp inspection vlan

Description	IP ARP inspection vlan setting	
Syntax	ip arp inspection vlan<vlan_list>	
Parameter	**Name**	**Description**
	vlan_list	arp inspection vlan list

ip dns proxy

Description	IP DNS proxy service
Syntax	ipdns proxy
Parameter	None

ip http secure-redirect

Description	IP http secure-redirect
Syntax	ip http secure-redirect
Parameter	None

ip http secure-server

Description	IP Secure HTTP web server
Syntax	ip http secure-server
Parameter	None

ip source binding interface

Description	IP source binding entry interface configuration	
Syntax	Ip source binding interface <port_type> <port_type_id> <vlan_id> <ipv4_ucast> <mac_ucast>	
Parameters	**Name**	**Description**
	port_type	Port type in Fast or Giga ethernet
	port_type_id	Port ID in the format of switch-no/port-no
	vlan_id	Select a VLAN id to configure
	ipv4_ucast	Select an IP Address to configure
	mac_ucast	Select a MAC address to configure

ip ssh

Description	IP Secure Shell
Syntax	ipssh
Parameter	None

ip name-server

Description	IP name server	
Syntax	ip name-server { <v_ipv4_ucast> | dhcp [interface vlan <v_vlan_id>] }	
Parameters	**Name**	**Description**
	v_ipv4_ucast	A valid IPv4 unicast address
	dhcp	Dynamic Host Configuration Protocol
	v_vlan_id	VLAN identifier(s): VID

ip route

Description	IP Route	
Syntax	ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>	
Parameters	**Name**	**Description**
	v_ipv4_addr	Network
	v_ipv4_netmask	Netmask
	v_ipv4_gw	Gateway

ip routing

Description	IP routing
Syntax	ip routing
Parameter	None

ip verify

Description	IP verify	
Syntax	ip verify [source] [translate]	
Parameters	**Name**	**Description**
	source	verify source
	translate	ip verify source translate all entries

ipmc profile

Description	IPMC profile configuration
Syntax	ipmc profile
Parameter	None

ipmc range

Description	A range of IPv4/IPv6 multicast addresses for the profile	
Syntax	ipmc range <word16> { <ipv4_mcast> [<ipv4_mcast>] | <ipv6_mcast> [<ipv6_mcast>] }	
Parameters	**Name**	**Description**
	word16	Range entry name in 16 char's
	ipv4_mcast	Valid IPv4 multicast address
	ipv4_mcast	Valid IPv4 multicast address that is not less than start address
	ipv6_mcast	Valid IPv6 multicast address
	ipv6_mcast	Valid IPv6 multicast address that is not less than start address

lacp

Description	LACP system priority	
Syntax	lacp system-priority <v_1_to_65535>	
Parameters	**Name**	**Description**
	system-priority	System priority
	<v_1_to_65535>	Priority value, lower means higher priority

line

Description	Console terminal control	
Syntax	line { <0~16> | console 0 | vty <0~15> }	
Parameters	**Name**	**Description**
	<0~16>	List of line numbers
	console	Console terminal line
	vty	Virtual terminal

login host

Description	Domain name and IP address	
Syntax	logging host { <v_ipv4_ucast> | <v_word45> }	
Parameters	**Name**	**Description**
	hostname	Donain name of the log server
	ipv4_ucast	IP address of the log server

login level

Description	Log level	
Syntax	logging level { info | warning | error }	
Parameters	**Name**	**Description**
	error	Error
	info	Information
	warning	Warning

login on

Description	Log on
Syntax	logging on
Parameter	None

logout

Description	System logout
Syntax	logout
Parameter	None

mac address-table aging-time

Description	MAC table entries/configuration	
Syntax	mac address-table aging-time <v_0_10_to_1000000>	
Parameter	**Name**	**Description**
	<v_0_10_to_1000000>	Aging time in seconds, 0 disables aging

mac address-table static

Description	MAC table entries/configuration	
Syntax	mac address-table static <v_mac_addr> vlan <v_vlan_id> interface (<port_type> [<v_port_type_list>])	
Parameters	**Name**	**Description**
	<v_mac_addr	48 bit MAC address
	v_vlan_id	VLAN IDs 1-4095
	port_type	Select an interface to configure
	v_port_type_list	Port list

more

Description	File in FLASH or on TFTP server
Syntax	more <Path>
Parameter	None

no

Description	Function disable	
Syntax	no { debug | port-securit | terminal }	
Parameters	**Name**	**Description**
	debug	Debugging functions
	port-securit	Port security (psec limit)
	terminal	Set terminal line parameters

ping

Description	The ping function	
Syntax	ping { ip | ipv6 }	
Parameters	**Name**	**Description**
	ip	IP (ICMP) echo
	ipv6	IPv6 (ICMPv6) echo

port-security

Description	Port security	
Syntax	port-security [aging] [time <v_10_to_10000000>]	
Parameters	**Name**	**Description**
	aging	Enable/disable port security aging
	time	Time in seconds between check for activity on learned MAC addresses
	v_10_to_10000000	<10-10000000> seconds

privilege

Description	User privileges	
Syntax	privilege { exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-profile } level <privilege> <cmd>	
Parameters	**Name**	**Description**
	config-vlan	VLAN Configuration Mode
	configure	Global configuration mod
	dhcp-pool	DHCP Pool Configuration Mode
	exec	Exec mode
	if-vlan	VLAN Interface Mode
	interface	Port List Interface Mode
	ipmc-profile	IPMC Profile Mode
	line	Line configuration mode
	rfc2544-profile	RFC2544 Profile Mode
	snmps-host	SNMP Server Host Mode
	stp-aggr	STP Aggregation Mode

reload

Description	System or configuration reset	
Syntax	reload { cold | default }	
Parameters	**Name**	**Description**
	cold	Reload cold
	defaults	Reload defaults without rebooting

rmon

Description	RMON	
Syntax	rmon {alarm | event}	
Parameters	**Name**	**Description**
	alarm	Configure an RMON alarm
	event	Configure an RMON event

rmon alarm

Description	RMON Alarm	
Syntax	rmon alarm <id> <oid_str> <interval> { absolute | delta } rising-threshold <rising_threshold> [<rising_event_id>] falling-threshold <falling_threshold> [<falling_event_id>] { [rising | falling | both] }	
Parameters	**Name**	**Description**
	id	Alarm entry ID
	ifInDiscards	The number of inbound packets that are discarded even the packets are normal
	fInErrors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol
	ifInNUcastPkts	The number of broad-cast and multi-cast packets delivered to a higher-layer protocol
	ifInOctets	The total number of octets received on the interface, including framing characters
	ifInUcastPkts	The number of uni-cast packets delivered to a higher-layer protocol
	ifInUnknownProtos	The number of the inbound packets that were discarded because of the unknown or un-support protocol
	ifOutDiscards	The number of outbound packets that are discarded event the packets is normal
	ifOutErrors	The The number of outbound packets that could not be transmitted because of errors
	ifOutNUcastPkts	The number of broad-cast and multi-cast packets that request to transmit
	ifOutOctets	The number of octets transmitted out of the interface, including framing characters
	ifOutUcastPkts	The number of uni-cast packets that request to transmit
	interval	Sample interval
	absolute	Test each sample directly
	delta	Test delta between samples
	rising_threshold	<-2147483648-2147483647> rising threshold value
	rising_event_id	<0-65535> Event to fire on rising threshold crossing
	falling_threshold	<-2147483648-2147483647> falling threshold value
	falling_event_id	<0-65535> Event to fire on falling threshold crossing
	both	Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default)
	falling	rigger alarm when the first value is less than the falling threshold
	rising	Trigger alarm when the first value is larger than the rising threshold

rmon alarm

Description	RMON Event	
Syntax	rmon event <id> [log] [trap <community>] { [description <description>] }	
Parameters	**Name**	**Description**
	description	Specify a description of the event
	log	Generate RMON log when the event fires
	trap	Generate SNMP trap when the event fires

terminal

Description	Terminal control	
Syntax	terminal { editing | exec-timeout | help | history | length | width }	
Parameters	**Name**	**Description**
	editing	Enable command line editing
	exec-timeout	Set the EXEC timeout
	help	Description of the interactive help system
	history	Control the command history function
	length	Set number of lines on a screen
	width	Set width of the display terminal

vlan <vlanid>

Description	Configure VLAN.	
Syntax	vlan <vlanid>	
Parameter	**Name**	**Description**
	<vlanid>	Create an empty VLAN index. Valid values: 1 ~ 4094 Type: Mandatory

vlan <vlanid> <name>

Description	Configure VLAN's name.	
Syntax	vlan <vlanid> <name>	
Parameters	**Name**	**Description**
	<vlanid>	Create an empty VLAN index. Valid values: 1 ~ 4094 Type: Mandatory
	<name>	VLAN Name (0~31) String Size:0~31 Type: Mandatory

lan disable <vlanid>

Description	Delete VLAN memberset/setting.	
Syntax	vlan disable <vlanid>	
Parameter	**Name**	**Description**
	<vlanid>	Valid values: 1 ~ 4094 Type: Mandatory

mac address-table aging-time <time>

Description	Configure aging time for a bridge port.	
Syntax	mac address-table aging-time <time>	
Parameter	**Name**	**Description**
	<time>	Valid values: 10 ~ 1000000 (seconds), 0: disable aging Type: Mandatory

mtu <value>

Description	MTU size.	
Syntax	mtu <value>	
Parameter	**Name**	**Description**
	<value>	Range. Valid values: 1536~9000 (bytes) Type: Mandatory

media-type

Description	Configure media-type	
Syntax	media-type { rj45 | sfp | dual }	
Parameters	**Name**	**Description**
	rj45	rj45 interface (copper interface).
	sfp	sfp interface (fiber interface).
	dual	Dual media interface (cu & fiber interface).

monitor destination interface

Description	The destination port. That is the port that traffic should be mirrored to.	
Syntax	monitor destination interface <port_type> <port_type_id>	
Parameters	**Name**	**Description**
	<port_type	Port type
	<port_type_id>	Port Number

monitor source interface

Description	Mirror Interface traffic	
Syntax	monitor source { { interface (<port_type> [<v_port_type_list>]) }	
Parameters	**Name**	**Description**
	port_type	1 Gigabit Ethernet Port
	v_port_type_lis	Port list

monitor source cpu

Description	Mirror Interface traffic	
Syntax	monitor source { cpu [<cpu_switch_range>] } } { both | rx | tx }	
Parameters	**Name**	**Description**
	both	Setting source port to both will mirror both ingress and egress traffic
	rx	Setting source port to rx will mirror ingress traffic
	tx	Setting source port to tx will mirror egress traffic

speed

Description	Configures interface speed. If you use 10, 100, or 1000 keywords with the auto keyword the port will only advertise the specified speeds.	
Syntax	speed { 10g | 2500 | 1000 | 100 | 10 | auto { [10] [100] [1000] } }	
Parameters	Name	Description
	1000	1Gbps
	100	100Mbps
	10	10Mbps
	auto	Auto negotiation
	[10]	10Mbps
	[10 0]	100Mbps
	[1000]	1Gbps

tacacs-server host

Description	Configure TACACS+ server	
Syntax	tacacs-server host <word1-255> [port <0-65535>] [timeout <1-1000>] [key <line1-63>]	
Parameters	**Name**	**Description**
	word1-255	Hostname or IP address
	0-65535	TCP port number
	1-1000	Wait time in seconds
	line1-63	The shared key

tacacs-server key

Description	Configure TACACS+ encryption key	
Syntax	tacacs-server key <line1-63>	
Parameter	**Name**	**Description**
	line1-63	

tacacs-server timeout

Description	Time to wait for a TACACS+ server to reply	
Syntax	tacacs-server timeout <1-1000>	
Parameter	**Name**	**Description**
	1-1000	Wait time in seconds

traps

Description	trap event configuration	
Syntax	traps [aaa authentication] [system [coldstart] [warmstart]] [switch [stp] [rmon]]	
Parameters	**Name**	**Description**
	aaa authentication	AAA authentication fail event
	coldstart	Cold start event
	warmstart	Warm start event
	stp	STP event
	rmon	RMON event

upnp

Description	Set UPnP's configurations
Syntax	upnp
Parameter	None

upnp advertising-duration

Description	Set UPnP's advertising duration	
Syntax	upnp advertising-duration <100-86400>	
Parameter	**Name**	**Description**
	100-86400	advertising duration

upnp ttl

Description	Set UPnP's TTL value	
Syntax	upnp ttl <1-255>	
Parameter	**Name**	**Description**
	1-255	TTL value

username

Description	User account	
Syntax	username <username> privilege <priv> password encrypted <encry_password> username <username> privilege <priv> password none username <username> privilege <priv> password unencrypted <password>	
Parameters	**Name**	**Description**
	username	<Username : word31> User name allows letters, numbers and underscores
	privilege	Set user privilege level
	priv	User privilege level
	password	Specify the password for the user
	encrypted	Specifies an ENCRYPTED password will follow
	none	NULL password
	unencrypted	Specifies an UNENCRYPTED password will follow

web

Description	Web privileges	
Syntax	web privilege group <group_name> level { [cro <cro>] [crw <crw>] [sro <sro>] [srw <srw>] }*1	
Parameters	**Name**	**Description**
	privilege	Web privilege
	group	Web privilege group
	group_name	Valid words are 'Aggregation' 'DHCP' 'Debug' 'Dhcp_Client' 'Diagnostics' 'EEE' 'Green_Ethernet' 'IP2' 'IPMC_Snooping' 'LACP' 'LLDP' 'Loop_Protect' 'MAC_Table' 'MVR' 'Maintenance' 'Mirroring' 'NTP' 'Ports' 'Private_VLANs' 'QoS' 'RPC' 'Security' 'Spanning_Tree' 'System' 'Timer' 'VCL' 'VLANs' 'Voice_VLAN' 'XXRP' 'sFlow'
	level	Web privilege group level
	cro	Configuration Read-only level
	crw	Configuration Read-write level
	sro	Status/Statistics Read-only level
	srw	Status/Statistics Read-write level
	cro	<Cro : 0-15>
	crw	<Crw : 0-15>
	sro	<Sro : 0-15>
	srw	<Srw : 0-15>

flow-control {enable|disble}

Description	Enable/Disable flow-control.	
Syntax	flow-control {enable|disable}	
Parameters	**Name**	**Description**
	enable	Enable flow-control.
	disable	Disable flow-control.

speed

Description	Configure gigabit Ethernet speed and Copper/SFP for gigabit port 7~8. (port1~6 Only support copper, no SFP) (port 9, 10 only support auto)	
Syntax	speed {auto | full-l000mbps | full-100mbps | full-10mbps | half-100mbps | half-10mbps}	
Parameters	**Name**	**Description**
	auto	Auto negotiation.
	full-l000mbps	Set 1000Mbps full duplexing.
	full-100mbps	Set 100Mbps full duplexing.
	full-10mbps	Set 10Mbps full duplexing.
	half-100mbps	Set 100Mbps half duplexing.
	half-10mbps	Set 10Mbps half duplexing.

port {enable/disable}

Description	Set interface gigabit port enable or disable.	
Syntax	port {enable/disable}	
Parameters	**Name**	**Description**
	disable	Turn off gigabit port.
	enable	Turn off gigabit port.

Date/Time

Description	Set device date and time	
Syntax	clock datetime <2000-2037> <1-12> <1-31> <0-23> <0-59> <0-59>	
Parameters	**Name**	**Description**
	<2000-2037>	year
	<1-12>	month
	<1-31>	Date
	<0-23>	Hour
	<0-59>	minute
	<0-59>	Second

VLAN Commands

This subsection provides the VLAN commands.

vlan

Description	VLAN commands	
Syntax	vlan <vlan_list>	
Parameter	**Name**	**Description**
	vlan_lis	ISL VLAN IDs 1~4095

vlan ethertype s-custom-port

Description	Vlan Ether type for custom S-ports configuration	
Syntax	vlan ethertype s-custom-port <0x0600-0xffff>	
Parameter	**Name**	**Description**
	0x0600-0xffff	Ethertype (Range: 0x0600-0xffff)

vlan protocol

Description	VLAN protocol	
Syntax	vlan protocol { { eth2 { <0x600-0xffff> | arp | ip | ipx | at } } | { snap { <0x0-0xffffff> | rfc_1042 | snap_8021h } <0x0-0xffff> } | { llc <0x0-0xff> <0x0-0xff> } } group <word16>	
Parameters	**Name**	**Description**
	0x600-0xffff	Ether Type(Range: 0x600 - 0xFFFF)
	arp	Ether Type is ARP
	ip	Ether Type is IP
	ipx	Ether Type is IPX
	at	Ether Type is AppleTalk
	0x0-0xffffff	SNAP OUI (Range 0x000000 - 0XFFFFFF)
	rfc_1042	SNAP OUI is rfc_1042
	snap_8021h	SNAP OUI is 8021h
	0x0-0xffff	PID (Range: 0x0 - 0xFFFF)
	0x0-0xff	DSAP (Range: 0x00 - 0xFF)
	0x0-0xff	SSAP (Range: 0x00 - 0xFF)
	word16	Group Name (Range: 1 - 16 characters)

vlan-trunking

Description	Change whether trunking of unknown VLANs is enabled
Syntax	vlan-trunking
Parameter	None

switchport access vlan

Description	Set switch access mode of the interface	
Syntax	switchport access vlan <vlan_id>	
Parameter	**Name**	**Description**
	vlan_id	VLAN ID of the VLAN when this port is in access mode

switchport forbidden vlan

Description	Adds or removes forbidden VLANs from the current list of forbidden VLANs	
Syntax	switchport forbidden vlan { add | remove } <vlan_list>	
Parameters	**Name**	**Description**
	add	Add to existing list.
	remove	Remove from existing list.
	vlan_list	VLAN IDs

switchport hybrid acceptable-frame-type

Description	Set acceptable frame type on a port	
Syntax	switchport hybrid acceptable-frame-type { all | tagged | untagged }	
Parameters	**Name**	**Description**
	all	Allow all frames
	tagged	Allow only tagged frames
	untagged	Allow only untagged frames

switchport hybrid allowed vlan

Description	Set allowed VLAN characteristics when interface is in hybrid mode	
Syntax	switchport hybrid allowed vlan { all | none | [add | remove | except] <vlan_list> }	
Parameters	**Name**	**Description**
	all	All VLANs
	none	No VLANs
	add	Add VLANs to the current list
	remove	Remove VLANs from the current list
	except	All VLANs except the following
	vlan_list	VLAN IDs of the allowed VLANs when this port is in hybrid mode

switchport hybrid egress-tag

Description	Egress VLAN tagging configuration	
Syntax	switchport hybrid egress-tag { none | all [except-native] }	
Parameters	**Name**	**Description**
	none	No egress tagging
	all	Tag all frames
	except-native	Tag all frames except frames classified to native VLAN of the hybrid port

switchport hybrid ingress-filtering

Description	VLAN Ingress filter configuration
Syntax	switchport hybrid ingress-filtering
Parameter	None

switchport mode

Description	Set switching mode	
Syntax	switchport mode { access | trunk | hybrid }	
Parameters	**Name**	**Description**
	access	Set mode to ACCESS unconditionally
	trunk	Set mode to TRUNK unconditionally
	hybrid	Set mode to HYBRID unconditionally

switchport trunk allowed vlan

Description	Set allowed VLAN characteristics when interface is in trunk mode	
Syntax	switchport trunk allowed vlan { all | none | [add | remove | except] <vlan_list> }	
Parameters	**Name**	**Description**
	all	All VLANs
	none	No VLANs
	add	Add VLANs to the current list
	remove	Remove VLANs from the current list
	except	All VLANs except the following
	vlan_list	VLAN IDs of the allowed VLANs when this port is in trunk mode

switchport vlan protocol group

Description	Protocol-based VLAN group commands	
Syntax	switchport vlan protocol group <word16> vlan <vlan_id>	
Parameters	**Name**	**Description**
	word16	Group Name (Range: 1 - 16 characters)
	vlan_id	VLAN ID required for the group to VLAN mapping (Range: 1-4095)

Interface VLAN Mode Commands

This subsection contains the Interface VLAN mode commands.

interface

Description	Interface configuration	
Syntax	interface <port_type> [<port_type_list>]	
Parameters	**Name**	**Description**
	port_type	Port type in Fast or Giga
	port_type_list	List of Port ID, ex, 1/1,3-5;2/2-4,6

interface vlan

Description	VLAN interface configurations	
Syntax	interface vlan<vlan_list>	
Parameter	**Name**	**Description**
	vlan_list	List of VLAN interface numbers, 1~4095

ip address

Description	IPv4 address configurations	
Syntax	ip address { { <ipv4_addr><ipv4_netmask> } | { dhcp [fallback <ipv4_addr><ipv4_netmask> [timeout <uint>]] } }	
Parameters	**Name**	**Description**
	ipv4_addr	IP address
	ipv4_netmask	IP netmask
	dhcp	Enable DHCP
	fallback	DHCP fallback settings
	ipv4_addr	DHCP fallback address
	ipv4_netmask	DHCP fallback netmask
	timeout	DHCP fallback timeout
	uint	DHCP fallback timeout in seconds

ip name-server

Description	Interface Internet Protocol config commands Domain Name System	
Syntax	ip name-server { <ipv4_ucast> | dhcp [interface vlan<vlan_id>] }	
Parameters	**Name**	**Description**
	ipv4_ucast	A valid IPv4 unicast address
	vlan_id	VLAN identifier(s): VID

ip dhcp excluded-address

Description	Prevent DHCP from assigning certain addresses	
Syntax	ip dhcp excluded-address <low_ip> [<high_ip>]	
Parameters	**Name**	**Description**
	low_ip	Low IP address
	high_ip	High IP addres

ip dhcp pool

Description	Pool name in 32 characters
Syntax	ip dhcp pool <pool_name>
Parameter	None

ip dhcp server

Description	DHCP Server
Syntax	ip dhcp server
Parameter	None

ip dhcp relay

Description	DHCP relay agent configuration
Syntax	ipdhcp relay
Parameter	None

ip dhcp relay information option

Description	IP DHCP relay information option (Option 82)
Syntax	ipdhcp relay information option
Parameter	None

ip dhcp retry interface vlan

Description	Restart the DHCP query process	
Syntax	ipdhcp retry interface vlan<vlan_id>	
Parameter	**Name**	**Description**
	vlan_id	Vlan ID

ip dhcp snooping

Description	IP DHCP snooping
Syntax	ipdhcp snooping
Parameter	None

ip helper-address

Description	DHCP relay server	
Syntax	ip helper-address <v_ipv4_ucast>	
Parameter	**Name**	**Description**
	Ip : ipv4_ucast	IP address of the DHCP relay server

ipv6 address

Description	Configure the IPv6 address of an interface	
Syntax	ipv6 address <ipv6_subnet>	
Parameter	**Name**	**Description**
	ipv6_subnet	IPv6 prefix x:x::y/z

ipv6mtu

Description	IPv6 Maximum transmission unit	
Syntax	ipv6 mtu<1280-1500>	
Parameter	**Name**	**Description**
	1280-1500	MTU value in bytes

RingV2 Group Mode Commands

This subsection contains RingV2 Group mode commands.

ringv2 protect

Description	To configure ring protection.	
Syntax	ring protect	
Parameters	**Name**	**Description**
	group1	Configure ring protection v2 group1 (Ring)
	group2	Configure ring protection v2 group2 (Ring)
	group3	Configure ring protection v2 group3 (Chain)

guard-time

Description	Set guard time	
Syntax	guard-time { <ringGuardTimerDef> }	
Parameter	**Name**	**Description**
	ringGuardTimerDef	<10-3600>, unit: second. Default is 10 seconds

mode

Description	Enable/Disable ring group	
Syntax	mode { disable | enable }	
Parameters	**Name**	**Description**
	disable	Set the specified Ring group to Disabled
	enable	Set the specified Ring group to Enabled

node1 interface GigabitEthernet <portNo>}

Description	Set interface of ring protection node	
Syntax	node1 interface GigabitEthernet <portNo>	
Parameter	**Name**	**Description**
	<portNo>	Valid values: 1~max port index.

node2 interface GigabitEthernet <portNo>}

Description	Set interface of ring protection node	
Syntax	Node2 interface GigabitEthernet <portNo>	
Parameter	**Name**	**Description**
	<portNo>	Valid values: 1~max port index.

role

Description	Set role for group	
Syntax	role { ring-master | ring-slave | coupling-primary | coupling-backup | dual-homing | chain-head | chain-tail | chain-member | b-chain-terminal-1 | b-chain-terminal-2 | b-chain-central-block | b-chain-member}	
Parameters	**Name**	**Description**
	ring-master	Set role to ring master
	ring-slave	Set role to ring slave
	coupling-primary	Set role to coupling primary
	coupling-backup	Set role to coupling backup
	dual-homing	Set role to dual homing
	chain-head	Set role to chain head
	chain-member	Set role to chain member
	chain-tail	Set role to chain tail
	b-chain-central-block	Set role to balancing chain central block
	b-chain-member	Set role to balancing chain member
	b-chain-terminal-1	Set role to balancing chain terminal 1
	b-chain-terminal-2	Set role to balancing chain terminal 2

Spanning Tree

This subsection contains the Spanning Tree commands.

spanning-tree

Description	Enable/disable STP on this interface
Syntax	spanning-tree
Parameter	None

spanning-tree aggregation

Description	Spanning Tree protocol
Syntax	spanning-tree aggregation
Parameter	None

spanning-tree auto-edge

Description	Auto detect edge status
Syntax	spanning-tree auto-edge
Parameter	None

spanning-tree bpdu-guard

Description	Enable/disable BPDU guard
Syntax	spanning-tree bpdu-guard
Parameter	None

spanning-tree edge

Description	Edge port spanning-tree STP Bridge
Syntax	spanning-tree edge
Parameter	None

spanning-tree edge bpdu-filter

Description	Enable BPDU filter (stop BPDU tx/rx)
Syntax	spanning-tree edge bpdu-filter
Parameter	None

spanning-tree mode

Description	mode STP protocol mode stp 802.1D Spanning Tree rstp Rabid Spanning Tree (802.1w) mstp Multiple Spanning Tree (802.1s)	
Syntax	spanning-tree mode { stp | rstp | mstp }	
Parameters	**Name**	**Description**
	stp	802.1D Spanning Tree
	rstp	Rabid Spanning Tree (802.1w)
	mstp	Multiple Spanning Tree (802.1s)

spanning-tree mst cost

Description	STP bridge instance STP Cost of this port	
Syntax	spanning-tree mst <0-7> cost { <1-200000000> | auto }	
Parameters	**Name**	**Description**
	<0-7>	instance 0-7 (CIST=0, MST2=1...)
	<1-200000000>	STP Cost of this port

spanning-tree mst port-priority

Description	port-priority	
Syntax	spanning-tree mst <0-7> port-priority <0-240>	
Parameters	**Name**	**Description**
	<0-7>	instance 0-7 (CIST=0, MST2=1...)
	<0-240>	STP priority of this port

spanning-tree mst priority

Description	Priority of the instance Range in seconds	
Syntax	spanning-tree mst <0-7> priority <0-61440>	
Parameters	**Name**	**Description**
	<0-7>	instance 0-7 (CIST=0, MST2=1...)
	<0-61440>	Priority of the instance

spanning-tree mst vlan

Description	VLAN keyword	
Syntax	spanning-tree mst <0-7> vlan <vlan_list>	
Parameters	**Name**	**Description**
	<0-7>	instance 0-7 (CIST=0, MST2=1...)
	<vlan_list>	Range of VLANs

spanning-tree mst forward-time

Description	forward-time Delay between port states	
Syntax	spanning-tree mst forward-time <4-30>	
Parameter	**Name**	**Description**
	<4-30>	Delay between port states

spanning-tree mst max-age

Description	Max bridge age before timeout.	
Syntax	spanning-tree mst max-age <6-40> [forward-time <4-30>]	
Parameters	**Name**	**Description**
	<6-40>	Max bridge age before timeout
	<4-30>	forward-time

spanning-tree mst max-hops

Description	MSTP bridge max hop count	
Syntax	spanning-tree mst max-hops <6-40>	
Parameter	**Name**	**Description**
	<6-40>	MSTP bridge max hop count

spanning-tree mst name

Description	Name of the bridge Revision Revision keyword	
Syntax	spanning-tree mst name <word32> revision <0-65535>	
Parameters	**Name**	**Description**
	<word32>	Name of the bridge
	<0-65535>	Revision keyword

spanning-tree mst <instance>

Description	instance 0-7 (CIST=0, MST2=1...)	
Syntax	spanning-tree mst <instance> priority <prio> spanning-tree mst <instance> vlan <v_vlan_list>	
Parameters	**Name**	**Description**
	instance	<Instance : 0-7> instance 0-7 (CIST=0, MST2=1...)
	priority	Priority of the instance
	vlan	VLAN keyword
	prio	<Prio : 0-61440> Range in seconds
	v_vlan_list	<vlan_list> Range of VLANs

spanning-tree recovery

Description	Recovery	
Syntax	spanning-tree recovery interval <interval>	
Parameters	**Name**	**Description**
	interval	The interval
	interva	Interval : 30-86400> Range in seconds

spanning-tree transmit

Description	Transmit	
Syntax	spanning-tree transmit hold-count <holdcount>	
Parameters	**Name**	**Description**
	hold-count	Max number of transmit BPDUs per sec
	holdcount	<Holdcount : 1-10> 1-10 per sec, 6 is default

sFlow Configure Commands

This subsection contains sFlow Configure commands.

sflow

Description	Enables/disables flow sampling on this port.	
Syntax	sflow [<range_list>]	
Parameter	**Name**	**Description**
	< range_list >	Sampler instance

sflow agent-ip

Description	The agent IP address used as agent-address in UDP datagrams. Defaults to IPv4 loopback address.	
Syntax	sflow agent-ip { ipv4 <ipv4_addr> | ipv6 <ipv6_addr> }	
Parameters	**Name**	**Description**
	< ipv4_addr >	Ipv4 address
	< ipv6_addr>	ipv6 address

sflow collector-address

Description	Sflow runtime, see sflow_icli_functions	
Syntax	sflow collector-address [receiver <range_list>] [<word>]	
Parameter	**Name**	**Description**
	< range_list >	Sampler instance

sflow max-datagram-size

Description	Statistics flow Maximum datagram size.	
Syntax	sflow max-datagram-size [receiver <range_list>] <200-1468>	
Parameters	**Name**	**Description**
	<range_list>	receiver list
	<200-1468>	packet byte

sflow max-sampling-size

Description	Specifies the maximum number of bytes to transmit per flow sample.	
Syntax	sflow max-sampling-size [sampler <range_list>] [<14-200>]	
Parameters	**Name**	**Description**
	< range_list >	Sampler instance
	<200-1468>	packet byte

sflow collector-port

Description	Collector UDP port	
Syntax	sflow collector-port [receiver <rcvr_idx_list>] <collector_port>	
Parameter	**Name**	**Description**
	collector_port	<Collector Port : 1-65535> Port number

sflow sampling-rate

Description	Specifies the statistical sampling rate. The sample rate is specified as N to sample 1/Nth of the packets n the monitored flows. There are no restrictions on the value, but the switch will adjust it to the closest possible sampling rate.	
Syntax	sflow sampling-rate [sampler <range_list>] [<1-4294967295>]	
Parameters	**Name**	**Description**
	< range_list >	Sampler instance
	<1-4294967295>	Sampling rate

sflow timeout

Description	Receiver timeout measured in seconds. The switch decrements the timeout once per second, and as long as it is non-zero, the receiver receives samples. Once the timeout reaches 0, the receiver and all its configuration is reset to defaults.	
Syntax	sflow timeout [receiver <range_list>] <0-2147483647>	
Parameters	**Name**	**Description**
	< range_list >	Sampler instance
	<0-2147483647>	Number of seconds.

SNMP Configure Commands

This subsection contains SNMP Configure commands.

snmp-server

Description	Enable SNMP server
Syntax	snmp-server
Parameter	None

snmp-server access

Description	snmp-server access configuration	
Syntax	snmp-server access < group name > model { v1 | v2c | v3 | any } level { auth | noauth | priv } [read <word255>] [write <word255>]	
Parameters	**Name**	**Description**
	< group name >	32 words
	< v1 | v2c | v3 | any >	V1~v3 security model
	< level >	security level
	{ auth | noauth | priv }	authNoPriv Security Level
		noAuthNoPriv Security Level
		authPriv Security Level
	read	specify a read view for the group
	<word255>	read view name

snmp-server community v2c

Description	Set the SNMP v2c community	
Syntax	snmp-server community v2c <word127> [ro | rw]	
Parameters	**Name**	**Description**
	< word127 >	Community word
	< ro >	Read only
	<rw>	Read write

snmp-server community v3

Description	S Set the SNMP v3 community	
Syntax	snmp-server community v3 <word127> [<ipv4_addr> <ipv4_netmask>]	
Parameters	**Name**	**Description**
	< word127 >	Community word
	< ipv4_addr >	IPv4 address
	<ipv4_netmask>	IPv4 netmask

snmp-server host

Description	Set SNMP server's configurations	
Syntax	snmp-server host <word32>	
Parameter	**Name**	**Description**
	< word32 >	Name of the host configuration

snmp-server host traps

Description	Set SNMP host's configurations	
Syntax	snmp-server host < Name of the host configuration > traps [linkup] [linkdown] [lldp]	
Parameters	**Name**	**Description**
	< Name of the host configuration >	Name of the host configuration
	<200-1468>	packet byte
	[linkup]	Link up event
	[linkdown]	Link down event
	[lldp]	LLDP event

snmp-server trap

Description	Set SNMP server's configurations
Syntax	snmp-server trap
Parameter	None

snmp-server user

Description	Set the SNMPv3 user's configurations	
Syntax	snmp-server user <Username> engine-id <Engine ID octet string> [{ md5 <word8-32> | sha <word8-40> } [priv { des | aes } <word8-32>]]	
Parameters	**Name**	**Description**
	<Username >	32 words
	<Engine ID octet string>	word10-32
	MD5	Set MD5 protocol
	sha	Set SHA protocol
	<word8-40>	SHA password
	priv	Set Privacy
	{ des | aes }	Set DES/AES protocol
	<word8-32>	Set privacy password

snmp-server version

Description	Set the SNMP server's version	
Syntax	snmp-server version { v1 | v2c | v3 }	
Parameter	**Name**	**Description**
	{ v1 | v2c | v3 }	SNMP v1,v2c,v3

snmp-server view

Description	Snmp MIB view configuration	
Syntax	snmp-server view <word32> <word255> { include | exclude }	
Parameters	**Name**	**Description**
	< word32 >	MIB view name
	< word255>	MIB view OID
	{ include | exclude }	Included/Excluded type from the view

SNMP trap receive ipv6 host

Description	host configuration	
Syntax	host <ipv6_ucast> [<1-65535>] [traps | informs]	
Parameters	**Name**	**Description**
	ipv6_ucast	IP address of SNMP trap host
	1-65535	UDP port of the trap messges
	traps	Send Trap messages to this host
	informs	Send Inform messages to this host

snmp-server contact

Description	SNMP server contact	
Syntax	snmp-server contact <v_line255>	
Parameter	**Name**	**Description**
	v_line255	<line255> contact string

snmp-server engine-id

Description	SNMP server engine ID	
Syntax	snmp-server engine-id local <engineID>	
Parameters	**Name**	**Description**
	local	Set SNMP local engine ID
	engineID	<Engineid : word10-32> local engine ID

snmp-server location

Description	SNMP server loation	
Syntax	snmp-server location <v_line255>	
Parameter	**Name**	**Description**
	v_line255	<line255> location string

snmp-server security-to-group

Description	SNMP server security	
Syntax	snmp-server security-to-group model { v1 | v2c | v3 } name <security_name> group <group_name>	
Parameters	**Name**	**Description**
	model	security model
	v1	v1 security model
	v2c	v2c security model
	v3	v3 security model
	name	security user
	security_name	<SecurityName : word32> security user name
	group	security group
	group_name	<GroupName : word32> security group name

SNMP trap receive ipv4 host

Description	host configuration	
Syntax	host { <ipv4_ucast> | <hostname> } [<1-65535>] [traps | informs]	
Parameters	**Name**	**Description**
	Ipv4_ucast	IP address of SNMP trap host
	hostname	hostname of SNMP trap host
	1-65535	UDP port of the trap messges
	traps	Send Trap messages to this host
	informs	Send Inform messages to this host

QoS Function Commands

This subsection contains QoS Function commands.

qos qce

Description	QCE setting	
Syntax	qos qce { <Id : 1-256> | refresh | update }	
Parameters	**Name**	**Description**
	<Id : 1-256>	QCE ID
	refresh	Refresh QCE tables in hardware
	update	Update an existing QCE

qos storm

Description	QoS storm	
Syntax	qos storm { unicast | multicast | broadcast } { { <rate> [kfps] } | { 1024 kfps } }	
Parameters	**Name**	**Description**
	broadcast	Police broadcast frames
	multicast	Police multicast frames
	unicast	Police unicast frames
	<rate>	1024, Rate is 1024 kfps <Rate : 1,2,4,8,16,32,64,128,256,512> Policer rate (default fps)

qos cos

Description	Class of service configuration	
Syntax	qos cos <0-7>	
Parameter	**Name**	**Description**
	<0-7>	Specific class of service

qos dscp-classify

Description	Set qos dscp-classify.
Syntax	qos dscp-classify { zero | selected | any }
Parameter	None

qos dscp-remark

Description	Set qos dscp-remark
Syntax	qos dscp-remark { rewrite | remap | remap-dp }
Parameter	None

qos dscp-translate

Description	Enable qos dscp-translate mode
Syntax	qos dscp-translate
Parameter	None

qos map cos-dscp

Description	Configure cos mapping to dscptable	
Syntax	qos map cos-dscp <0~7> dpl <0~1> dscp { <0-63> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }	
Parameters	**Name**	**Description**
	<0~7>	Cos level
	<0~1>	Specific drop precedence level
	<0-63>	Dscp level
	be	Default PHB(DSCP 0) for best effort traffic
	af11~13	Assured Forwarding PHB 11~13(DSCP 10,12,14)
	af22~23	Assured Forwarding PHB 22~23(DSCP 20,22)
	af31~33	Assured Forwarding PHB 31~33(DSCP 26,28,30)
	Af41~43	Assured Forwarding PHB 41~43(DSCP 34,36,38)
	cs1~7	Class Selector PHB CS1~7 precedence 1~7(DSCP 8*(cs value))
	ef	Expedited Forwarding PHB(DSCP 46)
	va	Voice Admit PHB(DSCP 44)

qos map cos-dscp

Description	Configure dscp mapping to cos table	
Syntax	qos map dscp-cos { <0~63> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } cos <0-7> dpl <dpl>	
Parameters	**Name**	**Description**
	<0~7>	Cos level
	<0-63>	Dscp level
	be	Default PHB(DSCP 0) for best effort traffic
	af11~13	Assured Forwarding PHB 11~13(DSCP 10,12,14)
	af22~23	Assured Forwarding PHB 22~23(DSCP 20,22)
	af31~33	Assured Forwarding PHB 31~33(DSCP 26,28,30)
	Af41~43	Assured Forwarding PHB 41~43(DSCP 34,36,38)
	cs1~7	Class Selector PHB CS1~7 precedence 1~7(DSCP 8*(cs value))
	ef	Expedited Forwarding PHB(DSCP 46)
	va	Voice Admit PHB(DSCP 44)
	<0~1>	Specific drop precedence level

qos map dscp-egress-translation

Description	Configure dscp egress-translation	
Syntax	qos map dscp-egress-translation { <0~63> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } <0~1> to { <0-63> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }	
Parameters	**Name**	**Description**
	<0~7>	Cos level
	<0-63>	Dscp level
	be	Default PHB(DSCP 0) for best effort traffic
	af11~13	Assured Forwarding PHB 11~13(DSCP 10,12,14)
	af22~23	Assured Forwarding PHB 22~23(DSCP 20,22)
	af31~33	Assured Forwarding PHB 31~33(DSCP 26,28,30)
	Af41~43	Assured Forwarding PHB 41~43(DSCP 34,36,38)
	cs1~7	Class Selector PHB CS1~7 precedence 1~7(DSCP 8*(cs value))
	ef	Expedited Forwarding PHB(DSCP 46)
	va	Voice Admit PHB(DSCP 44)
	<0~1>	Specific drop precedence level

qos map dscp-ingress-translation

Description	Configure dscp ingress-translation	
Syntax	qos map dscp-ingress-translation { <0~63> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } to { <0-63> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }	
Parameters	**Name**	**Description**
	<0~7>	Cos level
	<0-63>	Dscp level
	be	Default PHB(DSCP 0) for best effort traffic
	af11~13	Assured Forwarding PHB 11~13(DSCP 10,12,14)
	af22~23	Assured Forwarding PHB 22~23(DSCP 20,22)
	af31~33	Assured Forwarding PHB 31~33(DSCP 26,28,30)
	Af41~43	Assured Forwarding PHB 41~43(DSCP 34,36,38)
	cs1~7	Class Selector PHB CS1~7 precedence 1~7(DSCP 8*(cs value))
	ef	Expedited Forwarding PHB(DSCP 46)
	va	Voice Admit PHB(DSCP 44)
	<0~1>	Specific drop precedence level

qos policer

Description	Configure qos policer	
Syntax	qos policer <unit> [fps] [flowcontrol]	
Parameters	**Name**	**Description**
	< unit >	Traffic meter
	< fps >	Frame rate
	[flowcontrol]	Enable flowcontrol mode

qos wrr

Description	Specifies qos wrr mode	
Syntax	qos wrr <1-100> <1-100> <1-100> <1-100> <1-100> <1-100>	
Parameter	**Name**	**Description**
	<1-100>	every level proportion

qos queue-shaper

Description	Configure queue-shaper command	
Syntax	qos queue-shaper queue <0~7> <uint> [excess]	
Parameters	**Name**	**Description**
	<1-100>	every level proportion
	<unit>	Traffic meter
	[excess]	Agree the shaper could be excess or not

qos queue-policer

Description	Configure queue-policer command	
Syntax	qos queue-policer queue <0~7> <uint>	
Parameters	**Name**	**Description**
	<0~7>	Queue number
	<uint>	Traffic meter

qos shaper <unit>

Description	Configure qos shaper command	
Syntax	qos shaper <uint>	
Parameters	**Name**	**Description**
	<1-100>	every level proportion
	<unit>	Traffic meter

IGMP Functional Commands

This subsection contains IGMP Functional commands.

ip igmp host-proxy [leave-proxy]

Description	IGMP proxy for leave configuration	
Syntax	ip igmp host-proxy [leave-proxy]	
Parameter	**Name**	**Description**
	leave-proxy	IGMP proxy for leave

ip igmp snooping

Description	Snooping igmp
Syntax	ip igmp snooping
Parameter	None

ip igmp snooping immediate-leave

Description	IP IGMP snooping immediate leave configuration
Syntax	Ip igmp snooping immediate-leave
Parameter	None

ip igmp snooping last-member-query-interval

Description	IP IGMP snooping Last Member Query Interval in tenths of seconds	
Syntax	ip igmp snooping last-member-query-interval <0-31744>	
Parameter	**Name**	**Description**
	0-31744	0 - 31744 tenths of seconds

ip igmp snooping max-groups

Description	IGMP group throttling configuration	
Syntax	ip igmp snooping max-groups <1-10>	
Parameter	**Name**	**Description**
	1-10	Maximun number of IGMP group registration

ip igmp snooping mrouter

Description	IP IGMP snooping Multicast router port configuration
Syntax	Ip igmp snooping mrouter
Parameter	None

ip igmp snooping querier

Description	IP IGMP querier configuration	
Syntax	ip igmp snooping querier { election | address <ipv4_ucast> }	
Parameters	**Name**	**Description**
	election	Act as an IGMP Querier to join Querier-Election
	address	IGMP Querier address configuration
	ipv4_ucast	A valid IPv4 unicast address

ip igmp snooping query-interval

Description	IP IGMP snooping Query-Intervalin seconds	
Syntax	ip igmp snooping query-interval <1-31744>	
Parameter	**Name**	**Description**
	1-317	1 - 31744 seconds

ip igmp snooping vlan

Description	ipigmp snooping vlan IDs	
Syntax	ip igmp snooping vlan<vlan_list>	
Parameter	**Name**	**Description**
	vlan_list	VLAN identifier(s): VID

ip igmp ssm-range

Description	SSM range	
Syntax	ip igmp ssm-range <v_ipv4_mcast> <ipv4_prefix_length>	
Parameters	**Name**	**Description**
	v_ipv4_mcast	Valid IPv4 multicast address
	ipv4_prefix_length	Length

ip igmp unknown-flooding

Description	IP IGMP flooding unregistered IPv4 multicast traffic
Syntax	ip igmp unknown-flooding
Parameter	None

clear ip igmp snooping statistics

Description	clear ip igmp snooping statisti	
Syntax	clear ip igmp snooping [vlan<vlan_list>] statistics	
Parameters	**Name**	**Description**
	vlan_list	VLAN list.

MVR Functional Commands

This subsection contains MVR Functional commands.

mvr

Description	Multicast VLAN Registration configuration
Syntax	mvr
Parameter	None

mvr immediate-leave

Description	mvr immediate leave configuration
Syntax	mvr immediate-leave
Parameter	None

mvr name channel

Description	Multicast VLAN name and channel configuration	
Syntax	mvr name <word16> channel <word16>	
Parameters	**Name**	**Description**
	name <word16>	MVR multicast VLAN name
	channel <word16>	Profile name in 16 char's

mvr frame priority

Description	Multicast VLAN interface CoS priority	
Syntax	mvr name <word16> frame priority <0-7>	
Parameters	**Name**	**Description**
	name <word16>	MVR multicast VLAN name
	priority <0-7>	CoS priority ranges from 0 to 7

mvr name <word16> frame tagged

Description	MVR control frame in TX, Tagged IGMP/MLD frames will be sent	
Syntax	mvr name <word16> frame tagged	
Parameter	**Name**	**Description**
	name <word16>	MVR multicast VLAN name

mvr name <word16> igmp-address <ipv4_ucast>

Description	MVR address configuration used in IGMP	
Syntax	mvr name <word16> igmp-address <ipv4_ucast>	
Parameters	**Name**	**Description**
	name <word16>	MVR multicast VLAN name
	<ipv4_ucast>	A valid IPv4 unicast address

mvr name <word16> last-member-query-interval <0-31744>

Description	Configure last Member Query Interval in tenths of seconds	
Syntax	mvr name <word16> last-member-query-interval <0-31744>	
Parameters	**Name**	**Description**
	name <word16>	MVR multicast VLAN name
	<0-31744>	0 - 31744 tenths of seconds

mvr name <word16> mode

Description	Dynamic MVR operation mode	
Syntax	mvr name <word16> mode { dynamic | compatible }	
Parameters	**Name**	**Description**
	dynamic	Dynamic MVR operation mode
	compatible	Compatible MVR operation mode

mvr name <word16> type

Description	MVR port role configuration	
Syntax	mvr name <word16> type { source | receiver }	
Parameters	**Name**	**Description**
	source	MVR source port
	receiver	MVR receiver port

mvr vlan

Description	Multicast VLAN Registration configuration	
Syntax	mvr vlan <vlan_list> [name <word16>]	
Parameters	**Name**	**Description**
	< vlan_list >	MVR multicast VLAN list
	name <word16>	MVR multicast VLAN name in 16 char's

mvr vlan <vlan_list> channel

Description	MVR channel configuration	
Syntax	mvr vlan <vlan_list> channel <word16>	
Parameters	**Name**	**Description**
	< vlan_list >	MVR multicast VLAN list
	channel <word16>	MVR multicast channel name in 16 char's

mvr vlan <vlan_list> frame priority

Description	Interface CoS priority	
Syntax	mvr vlan <vlan_list> frame priority <0-7>	
Parameters	**Name**	**Description**
	< vlan_list >	MVR multicast VLAN list
	<0-7>	CoS priority ranges from 0 to 7

mvr vlan <vlan_list> frame tagged

Description	Set tagged IGMP/MLD frames will be sent	
Syntax	mvr vlan <vlan_list> frame tagged	
Parameter	**Name**	**Description**
	< vlan_list >	MVR multicast VLAN list

mvr vlan <vlan_list> igmp-address

Description	Set tagged IGMP/MLD frames will be sent	
Syntax	mvr vlan <vlan_list> igmp-address <ipv4_ucast>	
Parameters	Name	Description
	< vlan_list >	MVR multicast VLAN list
	<ipv4_ucast>	A valid IPv4 unicast address for IGMP

mvr vlan <vlan_list> mode

Description	Dynamic MVR vlan operation mode	
Syntax	mvr vlan <vlan_list> mode { dynamic | compatible }	
Parameters	**Name**	**Description**
	< vlan_list >	MVR multicast VLAN list
	dynamic	Dynamic MVR operation mode
	compatible	Compatible MVR operation mode

mvr vlan <vlan_list> type

Description	MVR vlan role configuration	
Syntax	mvr vlan <vlan_list> type { source | receiver }	
Parameters	**Name**	**Description**
	< vlan_list >	MVR multicast VLAN list
	source	MVR source port
	receiver	MVR receiver port

MLD Functional Commands

This subsection contains MLD Functional commands.

ipv6 mld host-proxy

Description	IPv6 MLD proxy configuration	
Syntax	ipv6 mld host-proxy [leave-proxy]	
Parameter	**Name**	**Description**
	leave-proxy	MLD proxy for leave configuration

ipv6 mld snooping

Description	ipv6 mld snooping
Syntax	ipv6 mld snooping
Parameter	None

ipv6 mld snooping compatibility

Description	IPv6 MLD snooping compatibility configuration	
Syntax	ipv6 mld snooping compatibility { auto | v1 | v2 }	
Parameters	**Name**	**Description**
	auto	Compatible with MLDv1/MLDv2
	v1	Forced MLDv1
	v2	Forced MLDv2

ipv6 mld snooping immediate-leave

Description	IPv6 MLD snooping immediate-leave configuration
Syntax	ipv6 mld snooping immediate-leave
Parameter	None

ipv6 mld snooping last-member-query-interval

Description	ipv6 mld snooping last member query interval in tenths of seconds	
Syntax	ipv6 mld snooping last-member-query-interval <0-31744>	
Parameter	**Name**	**Description**
	0-31744	0 - 31744 tenths of seconds

ipv6 mld snooping max-groups

Description	IPv6 MLD group throttling configuration	
Syntax	ipv6 mld snooping max-groups <1-10>	
Parameter	**Name**	**Description**
	1-10	Maximum number of MLD group registration

ipv6 mld snooping mrouter

Description	ipv6 mld snooping multicast router port configuration
Syntax	ipv6 mld snooping mrouter
Parameter	None

ipv6 mld snooping query-interval

Description	IPv6 MLD snooping query interval in seconds	
Syntax	ipv6 mld snooping query-interval <1-31744>	
Parameter	**Name**	**Description**
	1-31744	1 - 31744 seconds

ipv6 mld snooping query-max-response-time

Description	IPv6 MLD snooping querymaxresponse interval in tenths of seconds	
Syntax	ipv6 mld snooping query-max-response-time <0-31744>	
Parameter	**Name**	**Description**
	0-31744	0 - 31744 tenths of seconds

ipv6 mld snooping vlan

Description	ipv6 mld snooping vlan	
Syntax	ipv6 mld snooping vlan<vlan_list>	
Parameter	Name	Description
	vlan_list	VLAN identifier(s): VID

ipv6 mld ssm-range

Description	SSM range	
Syntax	ipv6 mld ssm-range <v_ipv6_mcast> <ipv6_prefix_length>	
Parameters	**Name**	**Description**
	v_ipv6_mcast	Valid IPv6 multicast address
	ipv6_prefix_length	length

ipv6 mld unknown-flooding

Description	Flooding unregistered IPv6 multicast traffic
Syntax	ipv6 mld unknown-flooding
Parameter	None

ipv6 route

Description	IPv6 Route	
Syntax	ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> }	
Parameters	**Name**	**Description**
	v_ipv6_subnet	IPv6 prefix x:x::y/z
	v_ipv6_ucast	IP address of the DHCP relay server
	v_vlan_id	VLAN ID
	v_ipv6_addr	IP address

Authenticate Mode Commands

This subsection contains Authenticate mode commands.

radius-server attribute 32

Description	Configure radius-server attribute	
Syntax	radius-server attribute 32 <id>	
Parameter	**Name**	**Description**
	id	Id : line1-253

radius-server attribute 4

Description	Configure radius-server attribute	
Syntax	radius-server attribute 4 <ipv4_ucast>	
Parameter	**Name**	**Description**
	<ipv4_ucast>	ipv4_ucast address

radius-server attribute 95

Description	Configure radius-server attribute	
Syntax	radius-server attribute 95 <ipv6_ucast>	
Parameter	**Name**	**Description**
	<ipv6_ucast>	Ipv6_ucast address

radius-server deadtime

Description	Configure radius-server deadtime	
Syntax	radius-server deadtime <1-1440>	
Parameter	**Name**	**Description**
	<1-1440>	Time in minutes

radius-server host [auth-port] [acct-port] [timeout] [retransmit] [key]

Description	Configure radius-server host behavior	
Syntax	radius-server host <word1-255> [auth-port <0-65535>] [acct-port <0-65535>] [timeout <1-1000>] [retransmit <1-1000>] [key <line1-63>]	
Parameters	**Name**	**Description**
	<word1-255>	Hostname or IP address
	auth-port <0-65535>	UDP port number for RADIUS authentication server
	acct-port <0-65535>	UDP port number for RADIUS accounting server
	timeout <1-1000>	Wait time in seconds for this RADIUS server to reply (overrides default)
	retransmit <1-1000>	

radius -server key

Description	radius-server key	
Syntax	radius-server key <key>	
Parameter	**Name**	**Description**
	key	<Key : line1-63> The shared key

radius-server retransmit

Description	radius-server retransmit	
Syntax	radius-server retransmit <retries>	
Parameter	**Name**	**Description**
	retries	<Retries : 1-1000> Number of retries for a transaction

radius-server timeout

Description	radius-server timeout	
Syntax	radius-server timeout <seconds>	
Parameter	**Name**	**Description**
	seconds	<Seconds : 1-1000> Wait time in second

tacacs-server deadtime <1-1440>

Description	Time to stop using a TACACS+ server that doesn't respond	
Syntax	tacacs-server deadtime <1-1440>	
Parameter	**Name**	**Description**
	< <1-1440>	Time in minutes

tacacs-server host [auth-port] [timeout] [key]

Description	Configure tacacs-server host behavior	
Syntax	tacacs-server host <word1-255> [port <0-65535>] [timeout <1-1000>] [key <line1-63>]	
Parameter	**Name**	**Description**
	< <1-1440>	TCP port number

tacacs-server deadtime <1-1440>

Description	Time to stop using a TACACS+ server that doesn't respond	
Syntax	tacacs-server deadtime <1-1440>	
Parameter	**Name**	**Description**
	< <1-1440>	Time in minutes

tacacs-server deadtime <1-1440>

Description	Time to stop using a TACACS+ server that doesn't respond	
Syntax	tacacs-server deadtime <1-1440>	
Parameter	**Name**	**Description**
	< <1-1440>	Time in minutes

dot1x feature

Description	Globally enables/disables a dot1x feature functionality	
Syntax	dot1x feature { [guest-vlan] [radius-qos] [radius-vlan] }	
Parameter	**Name**	**Description**
	guest-vlan	Globally enables/disables state of guest-vlan
	radius-qos	Globally enables/disables state of RADIUS-assigned QoS.
	radius-vlan	Globally enables/disables state of RADIUS-assigned VLAN.

dot1x authentication timer

Description	dot1x authentication timer	
Syntax	dot1x authentication timer { inactivity <v_10_to_100000> } | { re-authenticate <v_1_to_3600>}	
Parameters	**Name**	**Description**
	inactivity	Time in seconds between check for activity on successfully authenticated MAC addresses
	re-authenticate	The period between re-authentication attempts in seconds

dot1x max-reauth-req

Description	Max value of authentication request	
Syntax	dot1x max-reauth-req <1-255>	
Parameter	**Name**	**Description**
	<1-255>	number of times

dot1x re-authentication

Description	re-authentication
Syntax	dot1x re-authentication
Parameter	None

dot1x system-auth-controln

Description	System authentication control
Syntax	dot1x system-auth-control
Parameter	None

dot1x timeout

Description	Timeout control	
Syntax	dot1x timeout { quiet-period <v_10_to_1000000>} | { tx-period <v_1_to_65535}	
Parameters	**Name**	**Description**
	quiet-period	Time in seconds before a MAC-address that failed authentication gets a new authentication chance
	tx-period	the time between EAPOL retransmissions

dot1x guest-vlan

Description	G Enables/disables Guest VLAN globally or on one or more ports	
Syntax	dot1x guest-vlan dot1x guest-vlan<1-4095>	
Parameter	**Name**	**Description**
	<1-4095>	Guest VLAN ID used when entering the Guest VLAN.

dot1x initialize

Description	Forces a reinitialization of the clients on the port and thereby a reauthentication immediately.	
Syntax	dot1x initialize [interface <port_type> [<port_type_list>]]	
Parameters	**Name**	**Description**
	<port_type>	Port type in Fast or Giga
	<port_type_list>	List of Port ID, ex, 1/1,3-5;2/2-4,6

dot1x port-control

Description	Sets the port security state.	
Syntax	dot1x port-control { force-authorized | force-unauthorized | auto | single | multi | mac-based }	
Parameters	**Name**	**Description**
	force-authorized	Port access is allowed
	force-unauthorized	Port access is not allowed
	auto	Port-based 802.1X Authentication
	single	Single Host 802.1X Authentication
	multi	Multiple Host 802.1X Authentication
	mac-based	Switch authenticates on behalf of the client

dot1x radius-vlan

Description	Enables/disables per-port state of RADIUS-assigned VLAN.
Syntax	dot1x radius-vlan
Parameter	None

show radius-server [statistics]

Description	show radius-server statistics	
Syntax	show radius-server [statistics]	
Parameter	**Name**	**Description**
	[statistics]	Count radius packet statistics

enable

Description	Privilege level control	
Syntax	Enable { password [level <priv>] <password>} | { secret { 0 | 5 } [level <priv>] <password>}	
Parameters	**Name**	**Description**
	password	Assign the privileged level clear password
	secret	Assign the privileged level secret

end

Description	Level exit
Syntax	end
Parameter	None

exit

Description	Level exit
Syntax	end
Parameter	None

hostname

Description	This system's network name
Syntax	hostname <hostname>
Parameter	None

Loop-Protection Configure Commands

This subsection contains Loop-protection Configure commands.

loop-protect

Description	Loop protection configuration on port
Syntax	loop-protect
Parameter	None

loop-protect action

Description	Loop protection configuration on port	
Syntax	loop-protect action { [shutdown] [log]	
Parameters	**Name**	**Description**
	shutdown	Shutdown port
	log	Generate log

loop-protect shutdown-time

Description	Loop protection shutdown time interval	
Syntax	loop-protect shutdown-time <0-604800>	
Parameter	**Name**	**Description**
	0-604800	Shutdown time in second

loop-protect transmit-time

Description	Loop protection transmit time interval	
Syntax	loop-protect transmit-time <1-10>	
Parameter	**Name**	**Description**
	1-10	Transmit time in second

loop-protect tx-mode

Description	Loop protection actively generate PDUs
Syntax	loop-protect tx-mode
Parameter	None

LLDP Configure Commands

This subsection contains LLDP Configure commands.

lldp holdtime

Description	Sets LLDP hold time (The neighbor switch will discarded the LLDP information after \"hold time\" multiplied with \"timer\" seconds).	
Syntax	lldp holdtime <2-10>	
Parameter	**Name**	**Description**
	<2-10>	Holdtime 2-10 seconds

lldp med

Description	LLDP MED	
Syntax	LLDP MED	
Parameter	**Name**	**Description**
	datum	Datum (geodetic system) type • nad83-mllw: Mean lower low water datum 1983 • nad83-navd88: North American vertical datum 1983 • wgs84: World Geodetic System 1984
	fast	Number of times to repeat LLDP frame transmission at fast start <v_1_to_10> : <1-10>
	location-tlv	LLDP-MED Location Type Length Value parameter • altitude: Altitude parameter • civic-addr: Civic address information and postal information • elin-addr: Emergency Location Identification Number, (for example, E911 and others), such as defined by TIA or NENA. • latitude: Latitude parameter • longitude: Longitude parameter
	media-vlan-policy	Use the media-vlan-policy to create a policy, which can be assigned to an interface <Index : 0-31> : Policy id for the policy which is created

lldp receive

Description	Enable/Disable decoding of received LLDP frames.
Syntax	lldp receive
Parameters	None

lldp reinit <1-10>

Description	LLDP tx reinitialization delay in seconds.	
Syntax	lldp reinit <1-10>	
Parameter	**Name**	**Description**
	<1-10>	Reinitialization delay time

lldp timer <5-32768>

Description	Sets LLDP TX interval (The time between each LLDP frame transmitted in seconds).	
Syntax	lldp timer <5-32768>	
Parameter	**Name**	**Description**
	<5-32768>	5-32768 seconds.

lldp tlv-select

Description	Which optional TLVs to transmit.	
Syntax	lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name }	
Parameters	**Name**	**Description**
	management-address	Enable/Disable transmission of management address
	port-description	Enable/Disable transmission of port description
	system-capabilities	Enable/Disable transmission of system capabilities
	system-description	Enable/Disable transmission of system description
	system-name	Enable/Disable transmission of system name.

lldp transmission-delay

Description	Sets LLDP transmission-delay (the amount of time that the transmission of LLDP frames will delayed after LLDP configuration has changed) in seconds.)	
Syntax	lldp transmission-delay <1-8192>	
Parameter	**Name**	Description
	<1-8192>	transmission-delay seconds

lldp transmit

Description	Enable/Disabled transmision of LLDP frames.
Syntax	lldp transmit
Parameter	None

RFC2544 Testing Configure Commands

This subsection contains RFC2544 Testing Configure commands.

rfc2544 profile <word32>

Description	RFC2544 profile configuration	
Syntax	rfc2544 profile <word32>	
Parameter	**Name**	**Description**
	<word32>	Profile name up to 32 characters long

rfc2544 rename profile

Description	Rename an existing profile	
Syntax	rfc2544 rename profile <word32> <word32>	
Parameters	**Name**	**Description**
	profile <word32>	Old profile name
	<word32>	New profile name

rfc2544 save <word32> <word>

Description	Save a report to a file on a TFTP server	
Syntax	rfc2544 save <word32> <word>	
Parameter	**Name**	**Description**
	<word32>	Name of existing report to save
	<word>	TFTP server URL on the form tftp://server[:port]/path-to-file

rfc2544 start <word32> profile <word32> [desc <line128>]

Description	Start execution of a pre-configured profile	
Syntax	rfc2544 start <word32> profile <word32> [desc <line128>]	
Parameters	**Name**	**Description**
	start <word32>	Unique name of resulting report
	profile <word32>	Name of existing profile to execute
	desc <line128>	Description that will appear in the report

rfc2544 stop <word32>

Description	Stop execution of an ongoing test	
Syntax	rfc2544 stop <word32>	
Parameter	**Name**	**Description**
	<word32>	Report name to stop execution of

show rfc2544 profile [<word32>]

Description	show rfc2544 profile name	
Syntax	show rfc2544 profile [<word32>]	
Parameter	**Name**	**Description**
	<word32>	rfc2544 profile name

GVRP Configure Commands

This subsection contains GVRP Configure commands.

gvrp

Description	Enable GVRP on port(s)
Syntax	gvrp
Parameter	None

gvrpjoin request vlan

Description	Emit a Join-Request for test purpose	
Syntax	gvrp join-request vlan<vlan_list>	
Parameter	**Name**	**Description**
	vlan_list	List of VLANs

gvrpleave request vlan

Description	Emit a leave-Request for test purpose	
Syntax	gvrp leave-request vlan<vlan_list>	
Parameter	**Name**	**Description**
	vlan_list	List of VLANs

gvrp max-vlans

Description	gvrpmaximum number of VLANs	
Syntax	gvrp max-vlans<1-4095>	
Parameter	**Name**	**Description**
	<1-4095>	A valid range is from 1-4095.

gvrp time { [join-time <1-20>] [leave-time <60-300>] [leave-all-time <1000-50>]

Description	Set gvrp time	
Syntax	gvrp time { [join-time <1-20>] [leave-time <60-300>] [leave-all-time <1000-5000>] }	
Parameter	**Name**	**Description**
	1-20	join timer, available from 1 to 20
	60-300	leave timer, available from 60 to 300
	1000-5000	leaveall timer, available from 1000 to 5000

Voice VLAN Configure Commands

This subsection contains Voice VLAN Configure commands.

voice vlan

Description	Vlan for Voice appliance attributes
Syntax	voice vlan
Parameter	None

voice vlan aging-time

Description	Set secure learning aging time for voice traffic	
Syntax	voice vlan aging-time <10-10000000>	
Parameter	**Name**	**Description**
	10-10000000	Aging time, 10-10000000 seconds

voice vlan class

Description	Set voice traffic class	
Syntax	voice vlan class { <0-7> | low | normal | medium | high }	
Parameters	**Name**	**Description**
	0-7	Traffic class value
	low	Traffic class low (0)
	normal	Traffic class normal (1)
	medium	Traffic class medium (2)
	high	Traffic class high (3)

voice vlan oui

Description	Set voice traffic OUI configuration	
Syntax	voice vlan oui <oui> [description <line32>]	
Parameters	**Name**	**Description**
	oui	OUI value
	description	Set description for the OUI
	line32	Description line

voice vlan vid

Description	Set voice VLAN ID	
Syntax	voice vlan vid <vlan_id>	
Parameter	**Name**	**Description**
	<vlan_id>	VLAN ID, 1-4095

Profile Alarm Commands

This subsection contains Profile Alarm commands.

profile alarm

Description	Profile alarm
Syntax	profile alarm
Parameter	None

alarm

Description	Set alarm content	
Syntax	alarm <alarmId> { mask | unmask | major | minor }	
Parameters	101~114: GE-1~14 Port link down (for 14 port model)	
	Name	**Description**
	alarmId	151: set Power alarm
	mask	Set alarm as mask, it means event will not be send notify
	unmask	Set alarm as un-mask, it means event will be send notify
	major	Set alarm level as major
	minor	Set alarm level as minor

PoE Commands

This subsection contains PoE commands.

poe management mode

Description	Use management mode to configure PoE power management method.	
Syntax	poe management mode <mode>	
Parameters	**Name**	**Description**
	allocation-consumption	Max. port power determined by allocated, and power is managed according to power consumption.
	allocation-reserved-power	Max. port power determined by allocated, and power is managed according to reserved power.
	class-consumption	Max. port power determined by class, and power is managed according to power consumption.
	class-reserved-power	Max. port power determined by class, and power is managed according to reserved power.
	lldp-consumption	Max. port power determined by LLDP Media protocol, and power is managed according to power consumption.
	lldp-reserved-power	Max. port power determined by LLDP Media protocol, and power is managed according to reserved power.

poe supply

Description	Use poe supply to specify the maximum power the power supply can deliver.	
Syntax	poe supply <power>	
Parameter	**Name**	**Description**
	<power>	Value: 1-240 Maximum power the power supply can deliver.

poe mode

Description	Set PoE mode.	
Syntax	poe mode <mode>	
Parameters	**Name**	**Description**
	disable	Set poe to disable
	enable	Set poe to enable always
	schedule	Set poe to enable by scheduling

poe operation

Description	Set PoE operation mode.	
Syntax	poe operation <af/at>	
Parameters	**Name**	**Description**
	af	Set operation mode to 802.3af(Maximum power 15.4W)
	at	Set operation mode to 802.3at(Maximum power 30.0 W)

poe power

Description	Set maximum power for port in allocation mode.	
Syntax	poe power limit <power>	
Parameter	**Name**	**Description**
	<power>	Maximum power for the interface (0-15.4 Watt for PoE standard mode, 0-30.0 Watt for PoE plus mode)

poe priority

Description	Set PoE port priority	
Syntax	poe priority <priority>	
Parameters	**Name**	**Description**
	critical	Set priority to critical.
	high	Set priority to high.
	low	Set priority to low.

poe reset

Description	Set PoE power reset time.	
Syntax	poe reset <Hour> <Minute> <range_list>	
Parameters	**Name**	**Description**
	<0-23>	Hour
	<0-59>	Minute
	<range_list>	Day(s).(1:Sunday, 2:Monday, 3:Tuesday, 4:Wednesday, 5:Thuesday, 6:Friday, 7:Saturday)

poe schedule

Description	Set PoE power scheduling during the week.	
Syntax	poe schedule <Day> <range_list>	
Parameters	**Name**	**Description**
	fri mon sat sun thu tue wed	Day
	<range_list>	There are 48 time interval one day. Each interval has 30 minutes. ([1]<00:00-00:29> [2]<00:30-00:59>[3]<01:00-01:29> ... [47]<23:00-23:29> [48]<23:30-23:59>).

Glossary

A

ACE

ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for an individual application.

ACL

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are three web pages associated with the manual ACL configuration:

- **ACL|Access Control List**: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the **Ports** page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.
- **ACL|Ports**: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the **Access Control List** - page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property.
- **ACL|Rate Limiters**: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under **Ports** and **Access Control List** pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES

AES is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

AMS

AMS is an acronym for Auto Media Select. AMS is used for dual media ports (ports supporting both copper (cu) and fiber (SFP) cables. AMS automatically determines if a SFP or a CU cable is inserted and switches to the corresponding media. If both SFP and cu cables are inserted, the port will select the preferred media.

APS

APS is an acronym for Automatic Protection Switching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability. (Also Port Aggregation, Link Aggregation).

ARP

ARP is an acronym for Address Resolution Protocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by *poisoning* the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CC

CC is an acronym for Continuity Check. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM

CCM is an acronym for Continuity Check Message. It is a OAM frame transmitted from a MEP to it's peer MEP and used to implement CC functionality.

CDP

CDP is an acronym for Cisco Discovery Protocol.

D

DDMI

DDMI is an acronym for Digital Diagnostics Monitoring Interface. It provides an enhanced digital diagnostic monitoring interface for optical transceivers which allows real time access to device operating parameters.

DEI

DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is **vlan_id, module_id, port_no**. The parameter of **vlan_id** is the first two bytes represent the VLAN ID. The parameter of **module_id** is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of **port_no** is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Server

DHCP Server is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP client.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

DoS is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, on-line accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.

An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

Drop Precedence Level

Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level. A DP level of 0 (zero) corresponds to 'Committed' (Green) frames and a DP level of 1 corresponds to **Discard Eligible** (Yellow) frames.

DSA

The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993. Four revisions to the initial specification have been released: FIPS 186-1 in 1996, FIPS 186-2 in 2000, FIPS 186-3 in 2009, and FIPS 186-4 in 2013.

DSCP

DSCP is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

E

ECE

ECE is EVC Control Entry. These rules are ordered in a list to control the preferred classification.

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

ERPS

ERPS is an abbreviation for Ethernet Ring Protection Switching defined in ITU/T G.8032. It provides fast protection and recovery switching for Ethernet traffic in a ring topology while also ensuring that the Ethernet layer remains loop-free.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

EVC

EVC is an acronym for Ethernet Virtual Connection. MEF standards describe services provided to customers at User Network Interfaces (UNIs). Inside provider networks, nodes are connected using Internal Network-to-Network Interfaces (I-NNIs). Connections between service providers are done using External Network-to-Network Interfaces (E-NNIs). An Ethernet Virtual Connection is an association of two or more UNIs.

F

FTP

FTP is an acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

Fast Leave

Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

G

GARP

GARP is an acronym for Generic Attribute Registration Protocol. It is a generic protocol for registering attribute with other participants, and is specified in IEEE 802.1D-2004, clause 12.

GVRP

GVRP is an acronym for GARP VLAN Registration Protocol. It is a protocol for dynamically registering VLANs on ports, and is specified in IEEE 802.1Q-2005, clause 11. GVRP is an example of the use of GARP, hence the G in GVRP.

H

HQoS

HQoS is an acronym for Hierarchical Quality of Service. It is a method of QoS that can be configured on a service level.

HTTP

HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provides authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate log-ons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for on-line video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier. There will be only one IGMP Querier that wins Querier election on a particular link.

IMAP

IMAP is an acronym for Internet Message Access Protocol. It is a protocol for email clients to retrieve email messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network.

IP is a **best effort** system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing

for in excess of four billion unique addresses. This number is reduced drastically by the practice of web masters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeros after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for IP MultiCast.

IPMC supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.

IPMC Profile

IPMC Profile is an acronym for IP MultiCast Profile.

IPMC Profile is used to deploy the access control on IP multicast streams.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

IVL

In Independent VLAN Learning, every VLAN uses its own logical source address table as opposed to SVL where two or more VLANs share the same part of the MAC address table.

J

JSON

JSON (Java Script Object Notation) is a lightweight data-interchange format. As an alternative to XML, it can be used to transmit dynamic data between web server and application. It uses human-readable text and consist with one or more attribute–value pairs.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.

LLC

The IEEE 802.2 Logical Link Control (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multi-point network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

LLDP

LLDP is an IEEE 802.1ab standard protocol.

The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LLQI

LLQI (Last Listener Query Interval) is the maximum response time used to calculate the Maximum Response Code inserted into Specific Queries. It is used to detect the departure of the last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval).

LOC

LOC is an acronym for Loss Of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

MEP

MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5

MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm. Mirroring. For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MLD Querier

A router sends MLD Query messages onto a particular link. This router is called the Querier. There will be only one MLD Querier that wins Querier election on a particular link.

MPLS

The Multi-Protocol Label Switching (MPLS). It is a mechanism for speeding up the network traffic transmission. The protocol use the Layer 2(Switching) label to forward packets. Instead of the Layer 3(Routing) level, it can avoid the complex destination lookups in routing table. MPLS uses a variety of protocols to establish the network path, which are called Label Switched Paths (LSPs) then forward the packet via the network paths. The packet will be labeled at the edge of the service provider's network and service providers can use the label information to decide the best way for traffic flow forwarding.

The MPLS-TP (Multi-Protocol Label Switching Transport Profile) extensions to MPLS being designed by the IETF based on requirements provided by service providers. It will be designed for use as a network layer technology in transport networks. MPLS-TP provides service providers with a reliable packet-based technology that is based upon circuit-based transport networking, and thus is expected to align with current organizational processes and large-scale work procedures similar to other packet transport technologies.

MPLS-TP is expected to be a low cost L2 technology (if the limited profile to be specified is implemented in isolation) that will provide QoS, end-to-end OAM and protection switching.

MSTP

In 2002, the IEEE introduced an evolution of RSTP: the Multiple Spanning Tree Protocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by IEEE 802.1s, but was later incorporated in IEEE 802.1D-2005.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).

N

NAS

NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS

NetBIOS is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

OAM

OAM is an acronym for Operation Administration and Maintenance.

It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on this

Optional TLVs.

A LLDP frame contains multiple TLVs

For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

P

PCP

PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD

PD is an acronym for Powered Device. In a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).

PING

ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

PoE

PoE is an acronym for Power Over Ethernet.

Power Over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3

POP3 is an acronym for Post Office Protocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a **store-and-forward** service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then

the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

PPPoE

PPPoE is an acronym for Point-to-Point Protocol over Ethernet.

It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks (Wikipedia).

POST

POST is an acronym for Post On Self Telf.

It is run automatically on various components at power on. The power on self test (POST) is used to test the basic hardware. It includes ready-made tests (e.g. BIST) embedded in hardware or ASICs such as memory tests, serdes tests, internal loopback test etc.

Private VLAN

In a private VLAN, PVLANs provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

PTP

PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

Q

QCE

QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: **Ethernet Type**, **VLAN**, **UDP/TCP Port**, **DSCP, TOS**, and **Tag Priority**.

Frames can be classified by one of 4 different QoS classes: **Low**, **Normal**, **Medium**, and **High** for individual application.

QCL

QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL in SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

QoS class

Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

Querier Election

Querier election is used to dedicate the Querier, the only one router sends Query messages, on a particular link. Querier election rule defines that IGMP Querier or MLD Querier with the lowest IPv4/IPv6 address wins the election.

R

RARP

RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI

RDI is an acronym for Remote Defect Indication. It is a OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP

RFC2544

RFC2544 describes a number of tests that may be run to assess the performance characteristics of a network interconnecting devices. In this context, it is specialized towards determining whether a network section conforms to a service level agreement (SLA) and is usually run during service activation.

Router Port

A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSA

RSA is one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician, had developed an equivalent system in 1973, but it wasn't declassified until 1997.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SAMBA

Samba is a program running under UNIX-like operating systems that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.

Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2.

Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows **Neighborhood Network**.

sFlows

Flow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector.

Additional information can be found at http://sflow.org.

SHA

SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SSID

Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH

SSH is an acronym for Secure SHell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

SVL

Shared VLAN Learning allows for frames initially classified to a particular VLAN (based on Port VLAN ID or VLAN tag information) be bridged on a shared VLAN. In SVL two or more VLANs are grouped to share common source address information in the MAC table. The common entry in the MAC table is identified by a Filter ID (FID). SVL is useful for configuration of more complex, asymmetrical cross-VLAN traffic patterns, like E-TREE (Rooted-Multi-point) and Multi-netted Server.

The alternative VLAN learning mode is IVL. The default VLAN learning mode is IVL and not all switches support SVL.

Switch ID

Switch IDs (1-1) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+

TACACS+ is an acronym for Terminal Access Controller Access Control System Plus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for TELetype NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

ToS

ToS is an acronym for Type of Service. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV is an acronym for Type Length Value. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

TKIP

TKIP is an acronym for Temporal Key Integrity Protocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

TT-LOOP

TT-LOOP is an acronym for Traffic Test Loop, a firmware module that provides methods to perform tests that are defined in RFC 2544 (Benchmarking Methodology for Network Interconnect Devices) and Y.1564 (remote end).

U

UDLD

UDLD is an acronym for Uni Directional Link Detection. UDLD protocol monitors the physical configuration of the links between devices and ports that support UDLD. It detects the existence of unidirectional links.Its functionality is to provide mechanisms useful for detecting one way connections before they create a loop or other protocol malfunction. RFC 5171 specifies a way at data link layer to detect Uni directional link.

UDP

UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP

UPnP is an acronym for Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components User PriorityUser Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

V

VLAN

Virtual LAN. A method to restrict communication between switch ports. At layer 2, the network is partioned into multiple, distinct, mutually isolated broadcast domains.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

W

WEP

WEP is an acronym for Wired Equivalent Privacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio, so are more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network (Wikipedia).

WiFi

WiFi is an acronym for Wireless Fidelity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA

WPA is an acronym for Wi-Fi Protected Access. It was created in response to several serious weaknesses researchers had found in the previous system , Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).

WPA-PSK

WPA-PSK is an acronym for Wi-Fi Protected Access - Pre Shared Key. WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPA-Radius

WPA-Radius is an acronym for Wi-Fi Protected Access - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable **pre-shared key** (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPS

WPS is an acronym for Wi-Fi Protected Setup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network (Wikipedia).

WRED

WRED is an acronym for Weighted Random Early Detection. It is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level is used as input to WRED. A higher DP level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

WTR

WTR is an acronym for Wait To Restore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.

Y

Y.1564

Y.1564 is an Ethernet service activation test methodology (SAM), which is an ITU-T standard for turning up, installing and troubleshooting Ethernet-based services. It is the only standard test methodology that allows for complete validation of Ethernet service-level agreements (SLAs) in a single test. ITU-T Y.1564 is designed around three key objectives:

1. To serve as a network service level agreement (SLA) validation tool, ensuring that a service meets its guaranteed performance settings in a controlled test time.
2. To ensure that all services carried by the network meet their SLA objectives at their maximum committed rate, proving that under maximum load network devices and paths can support all the traffic as designed.
3. To perform medium- and long-term service testing, confirming that network elements can properly carry all services while under stress during a soaking period.

ITU-T Y.1564 defines an out-of-service test methodology to assess the proper configuration and performance of an Ethernet service prior to customer notification and delivery. (Wikipedia).