MILTECH™-912

Miniature Managed 12 Port Gigabit Ethernet Switch

User Guide

June 2014

Version: 1.00

Contents

Document Title: Gigabit Ethernet Switch MILTECH-912 – User Manual				
Description	**Rev**	**Description of Change**	**ECO**	**Update Date**
UM_001	1.00	Initial Version		02/04/2014

	Name	**Signature**	**Date**
Author	Chaviva Kaufman		02/04/2014
Initiator	Ehud Palgi		07/04/2014
Approved	Ehud Palgi		29/06/2014

1 Overview

The MILTECH-912 is Gigabit Ethernet Switch designed and produced by Techaya Inc., for use in harsh military environments.

The MILTECH-912 is a fully managed switch with 12 triple speed (10/100/1000) BaseT Ethernet ports and one RS-232 serial management port. Its rugged monolithic design is intended to operate in severe environments without the need for forced air cooling.

This document is intended to provide the information required to interface with the Techaya Gigabit Ethernet Switch (MILTECH-912) hardware.

The Part Number of the Techaya 12-Port Gigabit Ethernet Switch is MILTECH-912.

2 Product Details

This section provides an overview of key product details:

- Electrical Connections: see section 2.1 below
- Interface Port Details: see section 2.2 on page 15
- Hardware Mounting: see section 2.3 on page 17
- Indicators: see section 2.4 on page 17

2.1 Electrical Connections

The MILTECH-912 has 2 LAN connectors and 1 Power connector.

2.1.1 Power Connector

The Power connector Part number is D38999-24WB35PN (shall size 11).

The Power connector contains the following electrical interfaces:

- Input Power (nominal 28 VDC per MIL-STD-704A and MIL-STD-1275B)
- Mating cable connector for Power is Part Number D38999-26WB35SN

The following table gives the pinout connections for the (PWR) power connector.

Table 1 - Power Connector Pinouts

Pin #	Description
1	N.C
2	N.C
3	28VDC RTN input
4	28VDC RTN input
5	N.C
6	28V DC input
7	28V DC input
8	N.C
9	N.C
10	N.C
11	N.C
12	N.C
13	N.C

The input power requirements are as specified in MIL-STD-704A and MIL-STD-1275B:

- Aircraft, 28 VDC, Category B (curves 2 and 3)
- Ground Mobile, 28VDC

During normal operations the maximum power draw of the MILTECH-912 is 7 watts typical.

2.1.2 2 LAN Connectors - 12 Ports

The LAN Connectors are identical. Connector Part Number is D38999-24WF35PN (shall size 19).

There is a mating cable connector for LAN connectors, Part Number is D38999-26WF35SN.

The following table gives the pinout connections for the 2 LAN connectors.

Table 2 - LAN Connectors Pinouts

LAN Connector - J2				LAN Connector - J3			
Pin #	Description	Pin #	Description	Pin #	Description	Pin #	Description
1	CH 8 D -	34	CH 4 B +	1	NC	34	CH 12 B +
2	CH 8 C -	35	CH 4 B -	2	NC	35	CH 12 B -
3	CH 6 D +	36	CH 2 A -	3	NC	36	CH 10 A -
4	CH 7 A -	37	CH 2 A +	4	NC	37	CH 10 A +
5	CH 7 A +	38	N.U	5	NC	38	NC
6	CH 8 D +	39	CH 2 D -	6	NC	39	CH 10 D -
7	CH 8 C +	40	CH 3 C +	7	UART Transmit – (RS232-Tx) output	40	CH 11 C +
8	CH 6 D -	41	CH 1 C -	8	UART Receive + (RS232-Rx) input	41	CH 9 C -
9	CH 6 C -	42	CH 1 C +	9	Signal GND for RS232	42	CH 9 C +
10	CH 7 B -	43	CH 4 A -	10	NC	43	CH 12 A -
11	CH 7 B +	44	CH 4 A +	11	NC	44	CH 12 A +
12	CH 5 B +	45	CH 2 B +	12	NC	45	CH 10 B +
13	CH 5 B -	46	CH 2 B -	13	NC	46	CH 10 B -
14	CH 8 B +	47	CH 2 D +	14	NC	47	CH 10 D +
15	CH 8 B -	48	CH 3 C -	15	GND for reset	48	CH 11 C -
16	CH 6 C +	49	CH 1 A +	16	Reset input	49	CH 9 A +
17	CH 7 C -	50	CH 1 A -	17	O/G input PWR rail	50	CH 9 A -
18	CH 7 C +	51	CH 4 D +	18	O/G input	51	CH 12 D +
19	CH 5 C -	52	CH 4 D -	19	NC	52	CH 12 D -
20	CH 5 C +	53	CH 2 C -	20	NC	53	CH 10 C -
21	CH 5 A -	54	CH 2 C +	21	NC	54	CH 10 C +
22	CH 8 A -	55	CH 3 D +	22	NC	55	CH 11 D +
23	CH 6 B +	56	CH 3 D -	23	NC	56	CH 11 D -
24	CH 6 B -	57	CH 1 D +	24	NC	57	CH 9 D +
25	CH 7 D-	58	CH 4 C -	25	NC	58	CH 12 C -
26	CH 7 D +	59	CH 4 C +	26	NC	59	CH 12 C +
27	CH 5 D +	60	CH 3 B +	27	NC	60	CH 11 B +
28	CH 5 D -	61	CH 3 A +	28	NC	61	CH 11 A +
29	N.U	62	CH 1 B -	29	NC	62	CH 9 B -
30	CH 5 A +	63	CH 1 D -	30	NC	63	CH 9 D -
31	CH 8 A +	64	CH 3 B -	31	O/G output	64	CH 11 B -
32	CH 6 A -	65	CH 3 A -	32	O/G output common	65	CH 11 A -
33	CH 6 A +	66	CH 1 B +	33	NC	66	CH 9 B +

2.2 Interface Port Details

This section gives the specifications for the Ethernet and Serial ports.

2.2.1 Ethernet Ports

The MILTECH-912 Ethernet switches can be connected using Medium Dependent Interface (MDI) or Medium Dependent Interface Crossover (MDIX) schemes.

> **Note:**
> - MDI is the preferred connection choice.
> - MDIX is not advised.

The following table gives wiring connections for the MILTECH-912 Gigabit Ethernet ports relative to the available link speeds.

Table 3 - Ethernet Port Connections

MILTECH-912 PIN	RJ-45 Pinout P/N	MDI			MDI-X		
		1000 Base-T	100 Base-T	10 Base-T	1000 Base-T	100 Base-T	10 Base-T
Port X - A(+/-)	1/2	BI_DA+-	TX+-	TX+-	BI_DA+-	RX+-	RX+-
Port X - B(+/-)	3/6	BI_DB+-	RX+-	RX+-	BI_DB+-	TX+-	TX+-
Port X - C(+/-)	4/5	BI_DC+-	Unused	Unused	BI_DC+-	Unused	Unused
Port X - D(+/-)	7/8	BI_DD+-	Unused	Unused	BI_DD+-	Unused	Unused

2.2.2 Serial Ports

Port J3 is a shared port for both serial and LAN.

With a dedicated cable the user can access the CLI mode via Port J3. To manage the switch via the Web interface, use any of the LAN connectors.

The following table gives wiring connections for the serial port.

Table 4 - Serial Port Connections

Signal	Direction	Type	Connects	Notes
TX (PIN-7)	Output	RS-232	DB9 PIN 2	
RX (PIN-8)	Input	RS-232	DB9 PIN 3	
GND (PIN-9)	Reference	Ground	DB9 PIN 5	

There is one serial port that is associated with the Management Processor; Port J3. This port is RS-232 compatible and can operate at:

- 115,200 baud rate

- 1 Stop Bits
- No Parity
- No Flow Control

The Management port supports out-of-band configuration of the MILTECH-912. For in-band Ethernet management configuration use any one of the 12 ports.

2.3 Hardware Mounting

The MILTECH-912 weighs 1.050kg and can be mounted via four 4-40 UNC threads (located on the back of the unit) to any flat surface.

The overall external dimensions of the MILTECH-912 are 178(L) x 136(W) x 44.4(H) millimeters.

2.4 Indicators

The MILTECH-912 unit has 25 LEDs indication, 1 PWR LED and 24 LAN LEDs.

The PWR LED is illuminated when input power is applied to the MILTECH-912.

Each of the 12 LAN ports of the unit has two LEDs indication, Link/Act and Speed (10/100/1000).

Table 5 - LED Indicators

LED	Marking	Description
Speed	Port number	10 or 100 OFF
		1000 Green
Link/Activity	Port number	ON – Link is OK
		Flashing – Transmitting or Receiving Data
		OFF – No link and No Data

3 Command Line Interface

The MILTECH-912 Command Line Interface (CLI) is used for out-of-band control of the MILTECH-912. It provides the ability to customize configurations and status monitoring.

3.1 Command Line Overview

Some of the commands have optional parameters.

If a required parameter is missing the terminal will display the following message:

```
% Incomplete command
```

3.1.1 Context-Sensitive Help

To receive context-sensitive help directly from the command line:

Key	Help Description
?	Show next possible input and a description
Ctrl Q	Show syntax of possible commands
Tab	Show next possible input without a description or complete a word if it is unambiguous

3.1.2 Command Line Syntax

Each command is described by its syntax using the following delimiters:

[…] square brackets indicate an optional construct

{ } curly brackets indicate a grouping

"|" a straight line indicates a choice between two or more options

It is possible to have sequences of optional parameters. For example:

{ [a] [b] [c] }*1 the "*1" indicates that at least one of the optional parameters must be present

[a] {[b]} [c] curly brackets in a sequence of optional parameters indicates one or more of the parameters has a fixed position

See the following examples:

Example 1:

Request help with the show access-list command (3 options):

Input (enter the command and then a question mark):

```
M912# show access-list?
```

Output:

```
access-list    Access list
<cr>
```

Input (enter the command and then a question mark a second time):

```
    M912# show access-list?
```

Output:

```
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> ]
```

Input (enter the command a space and then a question mark):

```
    M912# show access-list ?
```

Output:

```
        |             Output modifiers
        ace           Access list entry
        ace-status    The local ACEs status
        interface     Select an interface to configure
        rate-limiter  Rate limiter
        <cr>
```

Example 2

Use the show command with no parameters:

Input:

```
    M912# show access-list
```

Since none of the optional parameters were used to limit the display, all entries in the access list are shown.

Output (partial view):

```
    Switch access-list ace number: 0

    Switch access-list rate limiter ID 1 is 1 pps
    Switch access-list rate limiter ID 2 is 1 pps
    Switch access-list rate limiter ID 3 is 1 pps
    Switch access-list rate limiter ID 4 is 1 pps
    Switch access-list rate limiter ID 5 is 1 pps
    Switch access-list rate limiter ID 6 is 1 pps
    Switch access-list rate limiter ID 7 is 1 pps
    Switch access-list rate limiter ID 8 is 1 pps
    Switch access-list rate limiter ID 9 is 1 pps
    Switch access-list rate limiter ID 10 is 1 pps
    Switch access-list rate limiter ID 11 is 1 pps
    Switch access-list rate limiter ID 12 is 1 pps
    Switch access-list rate limiter ID 13 is 1 pps
    Switch access-list rate limiter ID 14 is 1 pps
    Switch access-list rate limiter ID 15 is 1 pps
    Switch access-list rate limiter ID 16 is 1 pps
```

……..

```
    GigabitEthernet 1/2 :
    ---------------------
    GigabitEthernet 1/2 access-list action is permit
    GigabitEthernet 1/2 access-list policy ID is 0
    GigabitEthernet 1/2 access-list rate limiter ID is disabled
    GigabitEthernet 1/2 access-list redirect is disabled
    GigabitEthernet 1/2 access-list mirror is disabled
    GigabitEthernet 1/2 access-list logging is disabled
    GigabitEthernet 1/2 access-list shutdown is disabled
    GigabitEthernet 1/2 access-list port-state is enabled
    GigabitEthernet 1/2 access-list counter is 0
```

Example 3

Use show access-list for port 6 on switch 1 only (1/6 only):

Input:

```
    M912# show access-list interface gigabitethernet 1/6
```

Output:

```
    GigabitEthernet 1/6 :
    ---------------------
    GigabitEthernet 1/6 access-list action is permit
    GigabitEthernet 1/6 access-list policy ID is 0
    GigabitEthernet 1/6 access-list rate limiter ID is disabled
    GigabitEthernet 1/6 access-list redirect is disabled
    GigabitEthernet 1/6 access-list mirror is disabled
    GigabitEthernet 1/6 access-list logging is disabled
    GigabitEthernet 1/6 access-list shutdown is disabled
    GigabitEthernet 1/6 access-list port-state is enabled
    GigabitEthernet 1/6 access-list counter is 0
    M912#
```

3.1.3 Output Modifiers

It is possible to filter the output of display commands with output modifiers:

Modifier	Description
begin	begin with the line that matches
exclude	exclude lines that match
include	include lines that match
LINE	String to match output lines

The following example shows the proper syntax for an output modifier:

Input:

```
M912# show access-list | include policy
```

Output:

```
GigabitEthernet 1/1 access-list policy ID is 0
GigabitEthernet 1/2 access-list policy ID is 0
GigabitEthernet 1/3 access-list policy ID is 0
GigabitEthernet 1/4 access-list policy ID is 0
GigabitEthernet 1/5 access-list policy ID is 0
GigabitEthernet 1/6 access-list policy ID is 0
GigabitEthernet 1/7 access-list policy ID is 0
GigabitEthernet 1/8 access-list policy ID is 0
```

3.1.4 Ethernet Interface Reference

In the MILTECH-912, the Ethernet interface (“port”) is referenced in the following manner:

*	means all ports of all types on all switches

GigabitEthernet: defines the Ethernet type (1 Gigabit Ethernet Port), which requires a follow-up parameter (< port_type_list> in the sample below) that specifies the switch and the port number(s) on the switch (for example: 1/8 indicates port 8 on switch 1 or 3/1,3,5-7 indicates ports 1, 3, 5, 6, and 7 on switch 3)

Sample Syntax:

```
clear dot1x statistics [ interface ( <port_type> [ < port_type_list> ]
) ]
```

3.1.5 CLI Command Description

The following sections will describe each command as follows:

- List the individual command
- Give a brief description of the action triggered by the command
- Show the syntax of the command, and list the legal values and meanings of the parameters

3.2 Clear Commands

Use the clear commands to reset functions. The following functions can be reset (cleared):

Access	Access management
Access-list	Access list
Dot1x	IEEE Standard for port-based Network Access Control
IP	Interface Internet Protocol config commands
LACP	Clear LACP statistics
LLDP	Clears LLDP statistics.
Logging	Syslog
MAC	MAC Address Table

Spanning-Tree	STP Bridge
Statistics	Clear statistics for one or more given interfaces

3.2.1 Clear Access

Clear Access Management statistics.

Syntax:

```
clear access management statistics
```

3.2.2 Clear Access-List

Clear Access-List Entry (ACE) traffic statistics.

Syntax:

```
clear access-list ace statistics
```

3.2.3 Clear Dot1x

Clears the statistics counters for IEEE Standard for port-based Network Access Control.

Syntax:

```
clear dot1x statistics [ interface ( <port_type> [ <v_port_type_list>
] ) ]
clear dot1x statistics
```

interface:

<port_type>: values are:

*	All switches or all ports
GigabitEthernet:	set specific Gigabit Ethernet Port number
[<v_port_type_list>:	port list in 1/1-8

3.2.4 Clear IP

interface Internet Protocol config commands.

IP ARP

Clear ARP cache.

Syntax:

```
clear ip arp
```

IP IGMP

Clear running IGMP snooping counters.

Syntax:

```
clear ip igmp snooping [ vlan <v_vlan_list> ] statistics
```

[vlan <v_vlan_list>]: VLAN identifier(s): VID)

IP Statistics

Clear IP statistic.

Syntax:

```
clear ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp
] [ icmp-msg <type> ]
```

[system]: IPv4 system traffic

[interface vlan <v_vlan_list>]:
VLAN identifier(s): VID)

[icmp]: IPv4 ICMP traffic

[icmp-msg <type>]:
IPv4 ICMP traffic for designated message type (<type : 0~255> ICMP message type ranges from 0 to 255)

Examples:

```
clear ip statistics
clear ip statistics icmp-msg 2
clear ip statistics interface vlan 2
clear ip statistics system
```

3.2.5 Clear LACP

Clear all LACP statistics.

Syntax:

```
clear lacp statistics
```

3.2.6 Clear LLDP

Clears LLDP statistics.

Syntax:

```
clear lldp statistics
```

3.2.7 Clear Logging

Clear System logs.

Syntax:

```
clear logging [ info ] [ warning ] [ error ] [ switch <switch_list> ]
```

logging options are: info
warning
error

3.2.8 Clear MAC

Clear the MAC Address Table.

Syntax:

```
clear mac address-table
```

3.2.9 Clear Spanning-Tree

Clear the STP Bridge. It is possible to clear the whole bridge or a specific interface. (detected-protocols – Set the STP migration check)

Syntax:

```
clear spanning-tree { { statistics [ interface ( <port_type> [
<v_port_type_list> ] ) ] } | { detected-protocols [ interface (
<port_type> [ <v_port_type_list_1> ] ) ] } }
```

3.2.10 Clear Statistics

Clear the statistics for one or more interfaces.

Syntax:

```
clear statistics [ interface ] ( <port_type> [ <v_port_type_list> ] )
```

interface:

<port_type>, values are:

*	All switches or all ports
GigabitEthernet:	set specific Gigabit Ethernet Port number
[<v_port_type_list>:	port list in 1/1-8

Example:

```
clear statistics interface gigabitethernet 1/8
```

3.3 Configuration Commands

The CLI – Configuration section of this manual describes how to configure the MILTECH-912™ Gigabit Ethernet Switch, using the MILTECH-912™ Command Line interface. Many parameters may be configured from the Web User interface described later in this manual (4 Web Interface – Introduction on page 80).

Input:

```
    M912# config
```

Ouput (prompt changes):

```
    M912(config)#
```

3.3.1 AAA

Set the Authentication, Authorization, and Accounting parameters for the authentication login.

Syntax:

```
aaa authentication login { console | http } { { local | radius } [ {
local | radius } [ { local | radius } ] ] }
```

console:	Configure Console
http:	Configure HTTP
local:	Use local database for authentication
radius:	Use RADIUS for authentication

3.3.2 Access

Set the Access Management configuration.

```
access management <access_id> <access_vid> <start_addr> [ to
<end_addr> ] { [ web ] [ snmp ] | all }
```

<access_id>: ID of access management entry, values are 1-16

<access_vid>: The VLAN ID for the access management entry, values are 1-4095

<start_addr>: Start IPv4 address

<end_addr>: End IPv4 address

3.3.3 Access-List ACE

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

Syntax:

```
access-list ace <ace_id> [update] <parameter-name>< parameter-value>
```

<ace_id>: ID of ace entry, value can be 1-256

[update]: Update an existing ACE

3.3.3.1 Access-List ACE Action

Configure the ACE action to be taken.

Syntax:

```
access-list ace <ace_id> action <deny | filter | permit>
```

Example:

Input:

```
M912(config)# access-list ace 1 action deny
```

<ace_id>: ID of ace entry, value can be 1-256

action values:

deny

filter

permit

3.3.3.2 Access-List ACE Dmac-Type

Set the type of destination MAC address for the ACL.

Syntax:

```
access-list ace <ace_id> dmac-type < any | broadcast | multicast |
uniicast >
```

<ace_id>: ID of ace entry, value can be 1-256

dmac-type:

any:	Don't-care the type of destination MAC address
broadcast:	Broadcast destination MAC address
multicast:	Multicast destination MAC address
unicast:	Unicast destination MAC address)

3.3.3.3 Access-List ACE Frametype

Set the frame type for the ACL.

Syntax:

```
access-list ace <ace_id> frametype < any | arp | etype | ipv4 | ipv4-
icmp | ipv4-tcp | ipv4-udp | ipv6 | ipv6-icmp| ipv6-tcp | ipv6-udp >
```

<ace_id>: ID of ace entry, value can be 1-256

frametype:

any:	Don't-care the frame type
arp:	Frame type of ARP
etype:	Frame type of etype
ipv4:	Frame type of IPv4
ipv4-icmp:	Frame type of IPv4 ICMP
ipv4-tcp:	Frame type of IPv4 TCP
ipv4-udp:	Frame type of IPv4 TCP
ipv6:	Frame type of IPv6
ipv6-icmp:	Frame type of IPv6 ICMP
ipv6-tcp:	Frame type of IPv6 TCP
ipv6-udp:	Frame type of IPv6 UDP

3.3.3.4 Access-List ACE Ingress

Set the ingress configuration for the ACL.

Syntax:

```
access-list ace <ace_id> ingress
{ any | interface {* | gigabitethernet <port-list>} }
```

<ace_id>: ID of ace entry, value can be 1-256

ingress options:

any: do not care which ingress interface

interface:

<port_type>, values are:

*	All switches or all ports
GigabitEthernet:	set specific Gigabit Ethernet Port number
<port-list>	port list in 1/1-8

3.3.3.5 Access-List ACE Logging

Set the ACL logging configuration.

Syntax:

```
access-list ace <ace_id> logging
```

<ace_id>: ID of ace entry, value can be 1-256

> **Note:** The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.

3.3.3.6 Access-List ACE Mirror

Mirror frame to destination mirror port according to the ACL.

Syntax:

```
access-list ace <ace_id> mirror
```

<ace_id>: ID of ace entry, value can be 1-256

3.3.3.7 Access-List ACE Next

Insert the current ACE before the next ACE ID, values are:

Syntax:

```
access-list ace <ace_id> next { <ace_id_next> | last}
```

<ace_id>:	ID of ace entry, value can be 1-256
<ace_id_next >:	the next ID, values can be: 1-256
last:	place the current ACE to the end of access list

3.3.3.8 Access-List ACE Policy

Set the ACE Policy ID.

Syntax:

```
access-list ace <ace_id> policy <policy_id>
```

<ace_id>:	ID of ace entry, value can be 1-256
<policy_id>:	value can be 0-255

3.3.3.9 Access-List ACE Rate Limiter

Set the rate limiter ID or disable rate limiter for specific ACL.

Syntax:

```
access-list ace <ace_id> rate-liimiter {<rate_limiter_id> | disable}
```

<ace_id>:	ID of ace entry, value can be 1-256
<rate_limiter_id>:	rate limiter ID (values are: 1-16)
Disable:	disable rate-limiter)

3.3.3.10 Access-List ACE Redirect

Redirect frame to specific port according to ACL.

Syntax:

```
access-list ace <ace_id> redirect
{ disable | interface {* | gigabitethernet <port-list>} }
```

<ace_id>: ID of ace entry, value can be 1-256

redirect options:

disable: disable redirect

interface:

<port_type>, values are:

*	All switches or all ports
GigabitEthernet:	set specific Gigabit Ethernet Port number
<port-list>	port list in 1/1-8

3.3.3.11 Access-List ACE Shutdown

Shutdown Shutdown incoming traffic according to specific ACL. The shutdown feature only works when the packet length is less than 1,518 (without VLAN tags).

Syntax:

```
access-list ace <ace_id> shutdown
```

<ace_id>: ID of ace entry, value can be 1-256

3.3.3.12 Access-List ACE Tag

Set an ACE according to packet's Tag status.

Syntax:

```
access-list ace <ace_id> tag <any | tagged | untagged>
```

<ace_id>: ID of ace entry, value can be 1-256

any: don't-care tagged or untagged

tagged: tagged

untagged: untagged

3.3.3.13 Access-List ACE Tag-Priority

Set the ACE according to packet's tag priority.

Syntax:

```
access-list ace <ace_id> tag-priority <tag_priority_value >
```

<ace_id>: ID of ace entry, value can be 1-256

`<tag_priority_value>:`

0-1: the range of tag priority

0-3: the range of tag priority

2-3: the range of tag priority

4-5: the range of tag priority

4-7: the range of tag priority

6-7: the range of tag priority

0-7: the value of tag priority,
value may be any single number from 1 thru 7

any: don not-care the value of tag priority field

3.3.3.14 Access-List ACE VID

Set the ACE according to packet's VLAN ID.

Syntax:

```
access-list ace <ace_id> vid {<vid> | any}
```

<vid>: the value(s) of VID field, values are: 1-4095

any: do not-care the value of VID field

3.3.4 Access-List Rate-Limiter

Set the Access (Control) List Rate Limiter.

Syntax:

```
access-list rate-limiter [ <rate_limiter_list> ] { pps <pps_rate> |
100pps <pps100_rate> | kpps <kpps_rate> | 100kbps <kpbs100_rate> }
```

[<rate_limiter_list>]: rate limiter id, values are 1-16

pps:	packets per second
kpps:	thousands of packets per second
100kbps:	100k bits per second

3.3.5 Aggregation

Set Link Aggregation (LAG) parameters.

Syntax:

```
aggregation mode { [ smac ] [ dmac ] [ ip ] [ port ] }
```

mode: Traffic distribution mode

[smac]:	source MAC affects the distribution
[dmac]:	destination MAC affects the distribution
[ip]:	IP address affects the distribution
[port]:	IP port affects the distribution

3.3.6 Banner

Define a log in banner. There are three types of banners:

exec:	set EXEC process creation banner
login:	set login banner
motd:	set Message of the Day banner

Syntax:

```
banner [ motd ] <banner>
banner exec <banner>
banner login <banner>
```

The banner text is delimited by a user defined character:

c banner-text c, where ‘c’ is a delimiting character and “banner-text” is the banner.

Example:

Input:

```
    M912(config)# banner  x This is the banner. x<CR>
```

(the delimiter is “x”)

3.3.7 Default

Set a command to its defaults.

Syntax:

```
default access-list rate-limiter [ <rate_limiter_list> ]
```

<rate_limiter_list>: rate limiter ID, value can be 1-16>

3.3.8 Do

To run exec commands in config mode (while working in a sub-menu)

Syntax:

```
do <command>
```

3.3.9 Dot1x

IEEE Standard protocol for port-based Network Access Control

```
M912(config)# dot1x??
```

dot1x authentication timer inactivity

Time in seconds between check for activity on successfully authenticated MAC addresses.

Syntax:

```
dot1x authentication timer inactivity <v_10_to_100000>
```

<v_10_to_100000>: value can be 10-1,000,000 seconds

dot1x authentication timer re-authenticate

The period between re-authentication attempts in seconds.

Syntax:

```
dot1x authentication timer re-authenticate <v_1_to_3600>
```

<v_1_to_3600>: value can be 1-3,600 seconds

dot1x feature

Globally enables/disables a dot1x feature functionality.

Syntax:

```
dot1x feature { [ guest-vlan ] [ radius-qos ] [ radius-vlan ] }*1
```

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 re-authentication

Set Re-authentication state.

Syntax:

```
dot1x re-authentication
```

dot1x system-auth-control

Set the global dot1x state.

Syntax:

```
dot1x system-auth-control
```

dot1x timeout quiet-period

Time in seconds before a MAC-address that failed authentication gets a new authentication chance.

Syntax:

```
dot1x timeout quiet-period <v_10_to_1000000>
```

<v_10_to_1000000>: value can be 10-1,000,000 seconds

dot1x timeout tx-period

The time between EAPOL retransmissions.

Syntax:

```
dot1x timeout tx-period <v_1_to_65535>
```

<v_1_to_65535>: value can be 1-65,535 seconds

3.3.10 Enable

Modify enable password parameters.

Enable Password

Assign the privileged level clear password.

Syntax:

```
enable password [ level <priv> ] <password>
```

[level <priv>]: Set exec level password. Level number values can be from 1-15

<password>: The UNENCRYPTED (cleartext) password

Syntax:

```
enable password [ level <priv> ] <password>
```

Example:

Input:

```
    M912(config)# enable password level 1 miltech912pswrd
```

Enable Secret

Assign the privileged level password encryption.

Syntax:

```
enable secret { 0 | 5 } [ level <priv> ] <password>
```

0: Specifies an UNENCRYPTED password will follow

5: Specifies an ENCRYPTED secret will follow

[level <priv>]: Set exec level password. Level number values can be from 1-15

<password>: Password

Example:

Input:

```
M912(config)# enable secret 0 level 1 miltech912pswrd
```

3.3.11 End

Go back to EXEC mode.

Syntax:

```
end
```

3.3.12 Exit

Exit from current mode.

Syntax:

```
exit
```

3.3.13 Green-Ethernet

Green Ethernet, reduces power consumption. The following Green Ethernet options are available:

eee: Energy Efficient Ethernet, power down of PHYs when there is no traffic

led: LED power reduction, reduce LED intensity

3.3.13.1 green-ethernet eee optimize-for-power

Set if EEE shall be optimized for least power consumption (else optimized for least traffic latency).

Syntax:

```
green-ethernet eee optimize-for-power
```

3.3.13.2 green-ethernet led interval

Set the interval in whole hours at which to configure the LED intensity.

Syntax:

```
green-ethernet led interval <v_0_to_24> intensity <v_0_to_100>
```

<v_0_to_24> : interval from 00.00 to 24.00 hours
(00 is used to start at midnight,
24 is used to stop at midnight).

<v_0_to_100>: LED intensity from 0 to 100

3.3.13.3 green-ethernet led on-event

Specifies when to turn LEDs on at 100% intensity.

Syntax:

```
green-ethernet led on-event { [ link-change <v_0_to_65535> ]
[ error ] }*1
```

link-change: specifies how long to turn LEDs intensity to 100%,
when a link changes state

<v_0_to_65535>: number of seconds to set LEDs intensity to 100%
at link change, values 0 to 65,535

[error]: set LEDs intensity to 100% if an error occurs

3.3.14 Help

Description of the interactive help system

Syntax:

```
help
```

3.3.15 Hostname

Set system's network name.

Syntax:

```
hostname <hostname>
```

3.3.16 Interface - Port Type

Select an interface to configure.

Syntax:

```
interface ( <port_type> [ <plist> ] )
```

interface:

<port_type>, values are:

*	All switches or all ports
GigabitEthernet:	set specific Gigabit Ethernet Port number
<plist>	port list in 1/1-8

Input:

```
    M912(config)# interface *
```

Or Input:

```
    M912(config)# interface gigabitethernet 1/8
```

Output (prompt change to interface mode – port type):

```
    M912(config-if)#
```

3.3.16.1 (Interface - Port Type) Access-List

The following access-list options are available:

Access-List Action

Set the access-list action.

Syntax:

```
access-list action <deny | permit>
```

Access-List Logging

Logging frame information.

> **Note:** The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.

Access-List Mirror

Mirror frame to destination mirror port.

Syntax:

```
access-list mirror
```

Access-List Policy

Set specific policy to access list.

Syntax:

```
access-list policy <policy_id>
```

<policy_id>: value can be 0-255

Access-List Port-State

Re-enable shutdown port that was shut down by access-list module.

Syntax:

```
access-list port-state
```

Access-List Rate-Limiter

Set Rate Limiter to an ACL.

Syntax:

```
access-list rate-limiter <rate_limiter_id>
```

<rate_limiter_id>: rate limiter ID (values are: 1-16)

Access-List Redirect

Re-direct port traffic to another port by access-list module.

Syntax:

```
access-list redirect interface { <port_type> <port_type_id> | ( 
<port_type> [ <port_type_list> ] ) }
```

interface: <port_type>, values are:

*	all switches or all ports
GigabitEthernet:	set specific Gigabit Ethernet Port number
<port-list>:	port list in 1/1-8

Access-List Shutdown

Shut down incoming port. The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).

Syntax:

```
access-list shutdown
```

> **Note:** To re-enable a port that was shut down, use the Access-List Port-State command described above.

3.3.16.2 (Interface - Port Type) Aggregation

Create an aggregation group.

Syntax:

```
aggregation group <v_uint>
```

Example:

```
aggregation group 1
```

3.3.16.3 (Interface - Port Type) Do

Use the do command to run exec commands in config mode.

Syntax:

```
do <command>
```

3.3.16.4 (Interface - Port Type) dot1x

Dot1x is the IEEE Standard for port-based Network Access Control. This command sets dot1x per port.

Dot1x Port Control

Set the port security state, values are:

force-authorized:	port access is allowed
force-unauthorized:	port access is not allowed
auto:	port-based 802.1X authentication
mac-based:	switch authenticates on behalf of the client

Syntax:

```
dot1x port-control { force-authorized | force-unauthorized | auto |
mac-based }
```

Dot1x Re-authenticate

Refresh (restart) 802.1X authentication process.

Syntax:

```
dot1x re-authenticate
```

3.3.16.5 (Interface - Port Type) Duplex

Set the interface duplexity. Values are:

half: forced half duplex

full: forced full duplex

auto: auto negotiation of duplex mode, with an optional specification:

- full: advertise full duplex
- half: advertise half duplex

Syntax:

```
duplex { half | full | auto [ half | full ] }
```

3.3.16.6 (Interface - Port Type) End

Go back to EXEC mode.

Syntax:

```
end
```

3.3.16.7 (Interface - Port Type) Excessive-Restart

Restart back off algorithm after 16 collisions. (No excessive-restart means discard frame after 16 collisions.)

Syntax:

```
excessive-restart
```

3.3.16.8 (Interface - Port Type) Exit

Exit from current mode.

Syntax:

```
exit
```

3.3.16.9 (Interface - Port Type) Flowcontrol

Set traffic flow control, values are:

off: disable flow control

on: enable flow control

Syntax:

```
flowcontrol { on | off }
```

3.3.16.10 (Interface - Port Type) Green-Ethernet

Green Ethernet is used to reduce power consumption. The following options are available:

Green-Ethernet EEE

Enable powering down of PHYs when there is no traffic.

Syntax:

```
green-ethernet eee
```

Green-Ethernet Urgent-Queues

Enable EEE urgent queue. When urgent queue is enabled latency is kept to a minimum for traffic going to that queue.

> **Note:** EEE power savings will be reduced

It has the following optional parameter:

[< urgent_queue_range_list >]: EEE interface

Syntax:

```
green-ethernet eee urgent-queues [ <urgent_queue_range_list> ]
```

Green-Ethernet Energy-Detect

Enable power saving for ports with no link partner.

Syntax:

```
green-ethernet energy-detect
```

Green-Ethernet Short Reach

Enable power saving for ports connected to link partner with short cable.

Syntax:

```
green-ethernet short-reach
```

3.3.16.11 (Interface - Port Type) Help

The Help command displays a description of the interactive help system.

Syntax:

```
help
```

3.3.16.12 (Interface - Port Type) IP

Set the interface IGMP Snooping state. The following options are available:

igmp:	Internet Group Management Protocol	
	immediate-leave:	immediate leave configuration
	mrouter:	multicast router port configuration

Syntax:

```
ip igmp snooping immediate-leave
ip igmp snooping mrouter
```

3.3.16.13 (Interface - Port Type) LACP

Enable LACP on this interface.

Syntax:

```
lacp
```

LACP Key

Set the key of the LACP aggregation. Values are:

1-65,535:	key value
auto:	choose a key based on port speed

Syntax:

```
lacp key { <v_1_to_65535> | auto }
```

LACP Port-Priority

Set the LACP priority of the port. Values are:

1-65,535:	priority value, lower means higher priority

Syntax:

```
lacp port-priority <v_1_to_65535>
```

LACP Role

Set the LACP active / passive role. Values are:

active:	transmit LACP BPDUs continuously
passive:	wait for neighbor LACP BPDUs before transmitting

Syntax:

```
lacp role { active | passive }
```

LACP Timeout

Set the period between BPDU transmissions. Values are:

fast:	transmit BPDU each second (fast timeout)
slow:	transmit BPDU each 30th second (slow timeout)

Syntax:

```
lacp timeout { fast | slow }
```

3.3.16.14 (Interface - Port Type) LLDP

Set LLDP configurations. The following options are available:

receive: enable/disable decoding of received LLDP frames

tlv-select: which optional TLVs to transmit, the values are:

- 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

transmit: enable/disable transmission of LLDP frames

Syntax:

```
lldp receive
lldp tlv-select { management-address | port-description | system-
capabilities | system-description | system-name }
lldp transmit
```

3.3.16.15 (Interface - Port Type) Loop-Protect

Set the loop protection configuration on the port.

loop-protect: enable loop protection configuration on this port

loop-protect action: action to take if loop detected, values are:

- shutdown: shutdown port
- log: generate log

loop-protect tx-mode: actively generate PDUs

Syntax:

```
loop-protect
loop-protect action { [ shutdown ] [ log ] }*1
loop-protect tx-mode
```

3.3.16.16 (Interface - Port Type) MAC

Set the MAC security mode.

address-table: MAC table configuration

- learning: port learning mode
- [secure]: port secure mode

Syntax:

```
mac address-table learning [ secure ]
```

3.3.16.17 (Interface - Port Type) Media-Type

Set the media type, values are:

- dual: dual media interface (copper and fiber interface)
- rj45: rj45 interface (copper interface only)

sfp: sfp interface (fiber interface)

Syntax:

```
media-type { rj45 | sfp | dual }
```

3.3.16.18 (Interface - Port Type) MTU

Set the maximum transmission unit. The following is a required parameter:

<max_length>: maximum frame size in bytes (values are: 1,518-9,600)

Syntax:

```
mtu <max_length>
```

3.3.16.19 (Interface - Port Type) No

Negate a command or set its defaults. The following is a list of no commands available from interface Port Mode:

Interface Mode - No Commands (access-list)

```
no access-list logging
no access-list mirror
no access-list policy
no access-list port-state
no access-list rate-limiter
no access-list shutdown
no access-list { redirect | port-copy }
no aggregation group
```

Interface Mode - No Commands (d-i)

```
no dot1x port-control
no duplex
no excessive-restart
no flowcontrol
no green-ethernet eee
no green-ethernet eee urgent-queues [ <urgent_queue_range_list>
           ]
no green-ethernet energy-detect
no green-ethernet short-reach
no ip igmp snooping immediate-leave
no ip igmp snooping mrouter
```

Interface Mode - No Commands (l)

```
no lacp
no lacp key { <v_1_to_65535> | auto }
no lacp port-priority <v_1_to_65535>
no lacp role { active | passive }
no lacp timeout { fast | slow }
no lldp receive
no lldp tlv-select { management-address | port-description |
           system-capabilities | system-description | system-
           name }
```

```
no lldp transmit
no loop-protect
no loop-protect action
no loop-protect tx-mode
```

Interface Mode - No Commands (m-q)

```
no mac address-table learning [ secure ]
no media-type
no mtu
no pvlan <pvlan_list>
no pvlan isolation
no qos cos
no qos dei
no qos dpl
no qos pcp
no qos policer
no qos qce { [ addr ] [ key ] }*1
no qos queue-shaper queue <queue>
no qos shaper
no qos wrr
```

Interface Mode - No Commands (s-t)

```
no shutdown
no snmp-server host <conf_name> traps
no spanning-tree
no spanning-tree auto-edge
no spanning-tree bpdu-guard
no spanning-tree edge
no spanning-tree link-type
no spanning-tree restricted-role
no spanning-tree restricted-tcn
no speed
no switchport access vlan
no switchport forbidden vlan
no switchport hybrid acceptable-frame-type
no switchport hybrid allowed vlan
no switchport hybrid egress-tag
no switchport hybrid ingress-filtering
no switchport hybrid native vlan
no switchport hybrid port-type
no switchport mode
no switchport trunk allowed vlan
no switchport trunk native vlan
no switchport trunk vlan tag native
no thermal-protect port-prio
```

3.3.16.20 (Interface - Port Type) PVLAN

Set the private VLAN options. There are two private VLAN options:

<pvlan_list >:	list of PVLANs, range is from 1 to the number of ports
isolation:	port isolation

Syntax:

```
pvlan <pvlan_list>
pvlan isolation
```

3.3.16.21 (Interface - Port Type) QoS

Set the Quality of Service (QoS) parameters. The following QoS options are available:

QoS COS

Set the class of service configuration. The parameter is:

<cos>: Specific class of service, values are 0-7

Syntax:

```
qos cos <cos>
```

QoS DEI

Set Drop Eligible Indicator configuration. The parameter is:

<dei>: Specific Drop Eligible Indicator, values are 0-1

Syntax:

```
qos dei <dei>
```

QoS DPL

Set Drop Precedence Level configuration. The parameter is:

<dpl>: specific Drop Precedence Level

Syntax:

```
qos dpl <dpl>
```

QoS PCP

Set the Priority Code Point configuration. The parameter is:.

<pcp>: specific Priority Code Point, values are 0-7

Syntax:

```
qos pcp <pcp>
```

QoS Policer

Set the rate limitation policer configuration. The parameters are:

<rate>:	policer rate (default kbps), values are 100-3,300,000
[fps]:	rate is fps
[flowcontrol]:	enable flow control

Syntax:

```
qos policer <rate> [ fps ] [ flowcontrol ]
```

QoS QCE

Set the QoS Control Entry according to Source or Destination MAC address. The parameters are:

addr: setup address match mode

source: Match SMAC and SIP (default)

destination: Match DMAC and DIP

Syntax:

```
qos qce { [ addr { source | destination } ] }*1
```

QoS Queue-Shaper Queue

Set the queue-shaper configuration. The parameters are:

<queue>: specify queue or range, values are 1-7

<rate>: shaper rate in kbps, values are 100-3,300,000

[excess]: allow use of excess bandwidth

Syntax:

```
qos queue-shaper queue <queue> <rate> [ excess ]
```

QoS Shaper

Set the QoS shaper configuration. The parameters are:

<rate>: Shaper rate in kbps, values are 100-3,300,000

Syntax:

```
qos shaper <rate>
```

QoS WRR

Set the Weighted Round Robin configuration. The parameters are:

<w0> <w1> <w2> <w3> <w4> <w5>:

weight for queue n, values can be from 1 to 100

Syntax:

```
qos wrr <w0> <w1> <w2> <w3> <w4> <w5>
```

3.3.16.22 (Interface - Port Type) Shutdown

Use the shutdown command to shut down the interface.

Syntax:

```
shutdown
```

3.3.16.23 (Interface - Port Type) SNMP-Server Host

Set SNMP host's configurations.

<conf_name>:	name of the host configuration
traps:	enable traps
[linkdown]:	link down event
[linkup]:	link up event
[lldp]:	LLDP event

Syntax:

```
snmp-server host <conf_name> traps [ linkup ] [ linkdown ] [ lldp ]
```

3.3.16.24 (Interface - Port Type) Spanning-Tree

Set the spanning tree protocol mode per interface.

auto-edge:	auto detect edge status
bpdu-guard:	enable/disable BPDU guard
edge:	edge port
link-type:	port link-type
auto:	auto detect
point-to-point:	forced to point-to-point
shared:	forced to shared
restricted-role:	port role is restricted (never root port)
restricted-tcn:	restrict topology change notifications

Syntax:

```
spanning-tree
spanning-tree auto-edge
spanning-tree bpdu-guard
spanning-tree edge
spanning-tree link-type { point-to-point | shared | auto }
spanning-tree restricted-role
spanning-tree restricted-tcn
```

3.3.16.25 (Interface - Port Type) Speed

Configures interface speed. If you use 10, 100, or 1000 keywords with the auto keyword the port will only advertise the specified speeds. Values are:

10:	10Mbps
100:	100Mbps
1000:	1Gbps
Auto:	auto negotiation

Syntax:

```
speed { 10g | 2500 | 1000 | 100 | 10 | auto { [ 10 ] [ 100 ] [ 1000 ]
} }
```

3.3.16.26 (Interface - Port Type) Switchport

Set VLAN characteristics.

Switchport Access VLAN

Set VLAN access mode characteristics of the interface. Requires the following parameter:

vlan: Set VLAN when interface is in access mode, enter the pvid:

<pvid>: VLAN ID of the VLAN when this port is in access mode

Syntax:

```
switchport access vlan <pvid>
```

Switchport Forbidden VLAN

Add or remove forbidden VLANs from the current list of forbidden VLANs.

The parameters are:

<vlan_list>: VLAN IDs

add/remove: add to or remove from the existing list

Syntax:

```
switchport forbidden vlan { add | remove } <vlan_list>
```

Switchport Hybrid Acceptable-Frame-Type

Set acceptable frame type on a port. Values are:

all: allow all frames

tagged: allow only tagged frames

untagged: allow only untagged frames

Syntax:

```
switchport hybrid acceptable-frame-type { all | tagged | untagged }
```

Switchport Hybrid Allowed VLAN

Set allowed VLAN characteristics when interface is in hybrid mode. Values are:

<vlan_list> VLAN IDs of the allowed VLANs when this port is in hybrid mode

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

Syntax:

```
switchport hybrid allowed vlan { all | none | [ add | remove | except
] <vlan_list> }
```

Switchport Hybrid Egress-Tag

Set egress VLAN tagging configuration. Values are:

none:	no egress tagging
all:	tag all frames
except-native:	tag all frames except frames classified to native VLAN of the hybrid port

Syntax:

```
switchport hybrid egress-tag { none | all [ except-native ] }
```

Switchport Hybrid Ingress-Filtering

VLAN ingress filter configuration (enable ingress filtering).

Syntax:

```
switchport hybrid ingress-filtering
```

Switchport Hybrid Native VLAN

Set native VLAN. Values are:

<pvid>: VLAN ID of the native VLAN when this port is in hybrid mode

Syntax:

```
switchport hybrid native vlan <pvid>
```

Switchport Hybrid Port-Type

Set the port type. Values are:

c-port:	customer port
s-custom-port:	custom provider port
s-port:	provider port
unaware:	port in not aware of VLAN tags

Syntax:

```
switchport hybrid port-type { unaware | c-port | s-port | s-custom-
port }
```

Switchport Mode

Set mode of the interface.

access:	set mode to ACCESS unconditionally
hybrid:	set mode to HYBRID unconditionally
trunk:	set mode to TRUNK unconditionally

Syntax:

```
switchport mode { access | trunk | hybrid }
```

Switchport Trunk Allowed VLAN

Set allowed VLAN characteristics when interface is in trunk mode. Set the following additional parameters:

<vlan_list>:	VLAN IDs of the allowed VLANs when this port is in trunk mode
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

Syntax:

```
switchport trunk allowed vlan { all | none | [ add | remove | except ]
<vlan_list> }
```

Switchport Trunk Native VLAN

Set native VLAN when interface is in trunk mode. Set the following parameter:

<vlan_id>: VLAN ID of the native VLAN when this port is in trunk mode

Syntax:

```
switchport trunk native vlan <pvid>
```

Switchport Trunk VLAN Tag Native

Tag Native VLAN.

Syntax:

```
switchport trunk vlan tag native
```

3.3.16.27 (Interface - Port Type) Thermal-Protect Port-Prio

Set the thermal priority for the interface. Set the priority values:

<prio>: priority values can be from 0-3

Syntax:

```
thermal-protect port-prio <prio>
```

3.3.17 Interface - VLAN

Set the VLAN interface configuration parameters.

Syntax:

```
interface vlan <vlist>
```

vlan: VLAN interface configurations

<vlist>: List of VLAN interface numbers, 1~4095

Input:

```
    M912(config)# interface vlan 1
```

Output (prompt change to interface mode – vlan):

```
    M912(config-if-vlan)#
```

The following commands are available in interface mode – vlan:

3.3.17.1 (Interface - VLAN) Do

Run exec commands in config mode.

Syntax:

```
do <command>
```

3.3.17.2 (Interface - VLAN) End

Go back to EXEC mode

Syntax:

```
end
```

3.3.17.3 (Interface - VLAN) Exit

Exit from current mode.

Syntax:

```
exit
```

3.3.17.4 (Interface - VLAN) Help

Display description of the interactive help system.

Syntax:

```
help
```

3.3.17.5 (Interface - VLAN) IP

Set IPv4 Address configuration.

IP Address

Set the IP address configuration.

<address>: IP (IPv4) address

dhcp: enable Dynamic Host Configuration Protocol (DHCP)

fallback: dhcp fallback settings

<fallback_address> dhcp fallback address (send traffic to this ip address if the DHCP server goes offline)

<fallback_netmask> dhcp fallback netmask

[timeout <fallback_timeout>] dhcp fallback timeout, length of time in seconds that the DHCP server can be unresponsive, before traffic will be sent to the fallback address

Syntax:

```
ip address { { <address> <netmask> } | { dhcp
[ fallback <fallback_address> <fallback_netmask>
[ timeout <fallback_timeout> ] ] } }
```

IP IGMP Snooping

Enable IGMP snooping.

Syntax:

```
ip igmp snooping
```

IP IGMP Snooping Querier

Set the IGMP Querier configuration.

Election: act as an IGMP Querier to join Querier-Election

Address: IGMP Querier address configuration

<ipv4_ucast> a valid IPv4 unicast address

Syntax:

```
ip igmp snooping querier { election | address <v_ipv4_ucast> }
```

3.3.17.6 (Interface - VLAN) No

Negate a command or set its defaults.

Syntax of available no commands (for interface VLAN):

```
no ip address
no ip igmp snooping
no ip igmp snooping querier { election | address }
```

3.3.18 IP

Interface Internet Protocol config commands for the following protocols:

http:	Hypertext Transfer Protocol
igmp:	Internet Group Management Protocol
route:	Add IP route

3.3.18.1 IP HTTP Secure-Redirect

Secure HTTP web redirection.

Syntax:

```
ip http secure-redirect
```

3.3.18.2 IP HTTP Secure -Server

Secure HTTP web server.

Syntax:

```
ip http secure-server
```

3.3.18.3 IP IGMP Snooping

Snooping IGMP.

Syntax:

```
ip igmp snooping
```

3.3.18.4 IP IGMP Snooping VLAN

IGMP VLAN.

Syntax:

```
ip igmp snooping vlan <v_vlan_list>
```

<v_vlan_list>: VLAN identifier(s): VID

3.3.18.5 IP IGMP Unknown-Flooding

Flooding unregistered IPv4 multicast traffic.

Syntax:

```
ip igmp unknown-flooding
```

3.3.18.6 IP Route

Add IP route.

Syntax:

```
ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>
```

<v_ipv4_addr>:	Network
<v_ipv4_netmask>:	Netmask

<v_ipv4_gw>: Gateway

3.3.19 Lacp

Set the LACP settings.

lacp system-priority

Syntax:

```
lacp system-priority <v_1_to_65535>
```

<v_1_to_65535>: Priority value, lower means higher priority, values are: 1 to 65,535

3.3.20 Line

Configure a terminal line.

Syntax:

```
line { <0~16> | console 0 | vty <0~15> }
```

<0~16>:	list of line numbers
console 0:	console line number
vty:	virtual terminal, list of vty numbers, values 0-15

3.3.21 Lldp

LLDP configurations.

lldp holdtime

Sets LLDP hold time (The neighbor switch will discarded the LLDP information after “hold time” multiplied with “timer” seconds.).

Syntax:

```
lldp holdtime <val>
```

<val> 2-10 seconds.

LLDP Reinit

LLDP tx reinitialization delay in seconds.

Syntax:

```
lldp reinit <val>
```

<val>	1-10 seconds.

LLDP Timer

Sets LLDP TX interval (The time -in seconds- between each LLDP frame transmitted).

Syntax:

```
lldp timer <val>
```

<val>	5-32,768 seconds

LLDP Transmission-delay

Sets LLDP transmision-delay in seconds. (The amount of time that the transmission of LLDP frames will be delayed after LLDP configuration has changed.)

Syntax:

```
lldp transmission-delay <val>
```

<val>	1-8,192 seconds

3.3.22 Logging

Set syslog parameters.

Logging Host

Select the host to be logged.

Syntax:

```
logging host { <v_ipv4_ucast> | <v_word45> }
```

<ipv4_ucast>	IP address of the log server	
<v_word45>	<hostname>	Donain name of the log server

Logging Level

Set the level of logging.

Syntax:

```
logging level { info | warning | error }
```

error	error
info	information
warning	warning

Logging On

Enable syslog server

Syntax:

```
logging on
```

3.3.23 Loop-Protect

Loop protection configuration.

Syntax:

```
loop-protect
```

Loop Protection Shutdown-Time

Loop protection shutdown time interval.

Syntax:

```
loop-protect shutdown-time <t>
```

<t> shutdown time in seconds, values are 0-604,800

Loop Protection Transmit-Time

Loop protection transmit time interval.

Syntax:

```
loop-protect transmit-time <t>
```

<t> transmit time in seconds, values are 1-10

3.3.24 Mac

Set MAC table entries and configuration.

Mac Address-Table Ageing Time

Set MAC address ageing time.

Syntax:

```
mac address-table aging-time <v_0_10_to_1000000>
```

aging-time Mac address aging time

<v_0_10_to_1000000> aging time in seconds, values are
0 - disables aging
10 to 1,000,000

Mac Address-Table Static

Set static MAC address.

Syntax:

```
mac address-table static <v_mac_addr> vlan <v_vlan_id>
interface ( <port_type> [ <v_port_type_list> ] )
```

<v_mac_addr> 48 bit MAC address: xx:xx:xx:xx:xx:xx

<v_vlan_id>: Vlan ID

interface

<port_type>, values are:

*	All switches or all ports
GigabitEthernet:	set specific Gigabit Ethernet Port number
<v_port_type_list>:	port list in 1/1-8 (monitor source)

3.3.25 Monitor

Set monitor configuration for port mirroring.

The destination port is the port that traffic should be mirrored to.

The source port(s) is the port(s) to be mirrored. (It will be mirrored to the destination port.)

Syntax:

```
monitor destination interface <port_type> <in_port_type>
monitor source { { interface ( <port_type> [ <v_port_type_list> ] ) }
| { cpu [ <cpu_switch_range> ] } } { both | rx | tx }
```

interface

<port_type>, values are:

*	All switches or all ports
GigabitEthernet:	set specific Gigabit Ethernet Port number
<in_port_type>:	port list in 1/1-8 (monitor destination)
<v_port_type_list>:	port list in 1/1-8 (monitor source)

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

3.3.26 No

Negate a command or set its defaults.

No Commands (a-b)

```
no aaa authentication login { console | ssh | http }
no access management
no access management <access_id_list>
no access-list ace <ace_list>
no aggregation mode
no banner [ motd ]
no banner exec
no banner login
```

No Commands (dot1x)

```
no dot1x authentication timer inactivity
no dot1x authentication timer re-authenticate
no dot1x feature { [ guest-vlan ] [ radius-qos ] [ radius-vlan ] }*1
no dot1x re-authentication
no dot1x system-auth-control
no dot1x timeout quiet-period
no dot1x timeout tx-period
```

No Commands (enable)

```
no enable password [ level <priv> ]
no enable secret { [ 0 | 5 ] } [ level <priv> ]
```

No Commands (Green-Ethernet)

```
no green-ethernet eee optimize-for-power
no green-ethernet led interval <0~24>
no green-ethernet led on-event [ link-change ] [ error ]
```

No Commands (h-i)

```
no hostname
no interface vlan <vlist>
```

No Commands (ip)

```
no ip http secure-redirect
no ip http secure-server
no ip igmp snooping
no ip igmp snooping vlan [ <v_vlan_list> ]
no ip igmp unknown-flooding
no ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>
```

No Commands (l-m)

```
no lacp system-priority <v_1_to_65535>
no lldp holdtime
no lldp reinit
no lldp timer
no lldp transmission-delay
no logging host
no logging on
no loop-protect
no loop-protect shutdown-time
no loop-protect transmit-time
no mac address-table aging-time
no mac address-table aging-time <v_0_10_to_1000000>
no mac address-table static <v_mac_addr> vlan <v_vlan_id> interface ( <port_type> [ <v_port_type_list> ] )
no monitor destination
no monitor source { { interface ( <port_type> [ <v_port_type_list> ] ) } | { cpu [ <cpu_switch_range> ] } }
```

No Commands (p-q)

```
no privilege { exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-profile } level <0-15> <cmd>
no qos qce <qce_id_range>
no qos storm { unicast | multicast | broadcast }
```

No Commands (radius)

```
no radius-server attribute 32
no radius-server attribute 4
no radius-server deadtime
no radius-server host <host_name> [ auth-port <auth_port> ] [ acct-port <acct_port> ]
no radius-server key
no radius-server retransmit
no radius-server timeout
```

No Commands (snmp)

```
no snmp-server
no snmp-server access <group_name> model { v1 | v2c | v3 | any } level
{ auth | noauth | priv }
no snmp-server community v2c
no snmp-server community v3 <community>
no snmp-server contact
no snmp-server engined-id local
no snmp-server host <conf_name>
no snmp-server location
no snmp-server security-to-group model { v1 | v2c | v3 } name
<security_name>
no snmp-server trap
no snmp-server user <username> engine-id <engineID>
no snmp-server version
no snmp-server view <view_name> <oid_subtree>
no sntp
```

No Commands (sntp-v)

```
no sntp server
no spanning-tree edge bpdu-filter
no spanning-tree mode
no spanning-tree recovery interval
no spanning-tree transmit hold-count
no thermal-protect prio <prio_list>
no vlan { { ethertype s-custom-port } | <vlan_list> }
```

3.3.27 Password

Specify the password for the administrator

Password Encrypted

Set the ENCRYPTED (hidden) user password.

Syntax:

```
password encrypted <encry_password>
```

<encry_password>: The encrypted (hidden) user password, values are 4 -44 characters

> **Note:** The encrypted (hidden) user password will be decoded by the system internally. You cannot directly use it as plain text and it is not normally humanly-readable text.

Password None

Set the password to null.

Syntax:

```
password none
```

Password Unencrypted

Syntax:

Set an UNENCRYPTED user password.

Syntax:

```
password unencrypted <password>
```

<password>: The unencrypted (plain text) user password. Any printable character including space is accepted.

> **Note:** That you have no opportunity to change the plain text password after this command. The system will always display the ENCRYPTED password.

3.3.28 Privilege

Set the command privilege parameters, to allow or deny access to specific parameters.

Syntax:

```
privilege { exec | configure | config-vlan | line | interface |
if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-
profile } level <privilege> <cmd>
```

exec:	exec mode
configure:	global configuration mode
config-vlan:	VLAN Configuration Mode
line:	line configuration mode
interface:	port list interface Mode
if-vlan:	VLAN interface Mode
ipmc-profile:	IPMC Profile Mode
snmps-host:	SNMP Server Host Mode
stp-aggr:	STP Aggregation Mode
dhcp-pool:	Dynamic Host Configuration Protocol (DHCP) Pool Configuration Mode
rfc2544-profile:	RFC2544 Profile Mode
level:	set privilege level of command
<privilege>:	privilege level, values are 0-15
<cmd>:	initial valid words and literals of the command to modify, in 128 characters

3.3.29 QoS

Quality of Service.

QosS QCE Refresh

Refresh a QoS Control Entry (QCE) tables in hardware.

Syntax:

```
qos qce refresh
```

QosS QCE Update

Update an existing QCE (QoS Control Entry).

Syntax:

```
qos qce { [ update ] } <qce_id>
    [ { next <qce_id_next> } | last ]
    [ interface ( <port_type> [ <port_list> ] ) ]
    [ smac { <smac> | <smac_24> | any } ]
    [ dmac { <dmac> | unicast | multicast | broadcast | any } ]
    [ tag { [ type { untagged | tagged | c-tagged | s-tagged |
             any } ]
            [ vid { <ot_vid> | any } ] [ pcp { <ot_pcp> | any }
             ]
            [ dei { <ot_dei> | any } ] }*1 ]
    [ inner-tag { [ type { untagged | tagged | c-tagged | s-
             tagged | any } ]
            [ vid { <it_vid> | any } ] [ pcp { <it_pcp> | any }
             ]
            [ dei { <it_dei> | any } ] }*1 ]
    [ frame-type
            { any | { etype [ { <etype_type> | any } ] } |
              { llc [ dsap { <llc_dsap> | any } ]
                  [ ssap { <llc_ssap> | any } ]
                  [ control { <llc_control> | any } ] } |
              { snap [ { <snap_data> | any } ] } |
              { ipv4 [ proto { <pr4> | tcp | udp | any } ]
                  [ sip { <sip4> | any } ]
                  [ dip { <dip4> | any } ]
                  [ dscp { <dscp4> | { be | af11 | af12 | af13 |
             af21
                  | af22 | af23 | af31 | af32 | af33 | af41 |
             af42
                  | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 |
             cs7
                  | ef | va } | any } ]
                  [ fragment { yes | no | any } ]
                  [ sport { <sp4> | any } ]
                  [ dport { <dp4> | any } ]
              } |
              { ipv6 [ proto { <pr6> | tcp | udp | any } ]
                  [ sip { <sip6> | any } ]
                  [ dip { <dip6> | any } ]
                  [ dscp { <dscp6> | { be | af11 | af12 | af13 |
             af21
```

```
         | af22 | af23 | af31 | af32 | af33 | af41
         | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 |
      cs6
         | cs7 | ef | va } | any } ]
         [ sport { <sp6> | any } ]
         [ dport { <dp6> | any } ]
      }
     }
  ]
  [ action { [ cos { <action_cos> | default } ]
      [ dpl { <action_dpl> | default } ]
      [ pcp-dei { <action_pcp> <action_dei> | default } ]
      [ dscp { <action_dscp_dscp> | { be | af11 | af12 |
      af13
      | af21 | af22 | af23 | af31 | af32 | af33 | af41 |
      af42
      | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 |
      ef
      | va } | default } ]
      [ policy { <action_policy> | default } ] }*1 ]
```

[update] }   update an existing QCE

<qce_id>   QCE ID, values are 1-256

QoS Storm

Set the QoS storm policer configuration.

Syntax:

```
qos storm { unicast | multicast | broadcast } { { <rate> [ kfps ] } |
{ 1024 kfps } }
```

unicast: police unicast frames

multicast: police multicast frames

broadcast: police broadcast frames

<rate>:   1024 kfps (Policer rate is < 1,2,4,8,16,32,64,128,256,512> (default fps))

[kfps]:   rate is kfps

3.3.30 Radius-Server

Configure RADIUS. The radius-server has the following options:

Radius-Server Attribute

Set the attributes to be used in the RADIUS Access-Request packets.

Syntax:

```
radius-server attribute 32 <id>
radius-server attribute 4 <ipv4>
```

<ipv4>:   <ipv4 address>

<id>: < an NAS identifier from 1 to 253 characters>

Radius-Server Deadtime

Set the time to stop using a RADIUS server that does not respond.

Syntax:

```
radius-server deadtime <minutes>
```

<minutes>: Time in minutes, value from 1-1,440

Radius-Server Host

Specify a RADIUS server.

Syntax:

```
radius-server host <host_name> [ auth-port <auth_port> ]
[ acct-port <acct_port> ] [ timeout <seconds> ]
[ retransmit <retries> ] [ key <key> ]
```

<host_name>: host name or IP address, from 1 to 255 characters

[auth-port <auth_port>]: UDP port for RADIUS authentication server

<auth_port>: value of UDP port number can be 0-65,535

[acct-port <acct_port>]: UDP port for RADIUS accounting server

<acct_port>: value of UDP port number can be 0-65,535

[timeout <seconds>]: Time to wait for this RADIUS server to reply

<seconds>: wait time in seconds, value can be 1-1,000 (overrides default)

[retransmit <retries>]: Specify the number of retries to active server

<retries>: number of retries for a transaction, value can be 1-1,000 (overrides default)

[key <key>]: Server specific key (overrides default)

<key>: the shared key, value can be 1-63 characters

Radius-Server Key

Set RADIUS encryption key

Syntax:

```
radius-server key <key>
```

<key>: the shared key, value can be 1-63 characters

Radius-Server Retransmit

Specify the number of retries to active server

Syntax:

```
radius-server retransmit <retries>
```

<retries> number of retries for a transaction, value can be 1-1,000

Radius-Server timeout

Time to wait for a RADIUS server to reply

Syntax:

```
radius-server timeout <seconds>
```

<seconds>: wait time in seconds, value can be 1-1,000

3.3.31 SNMP-Server

Set SNMP server's configurations (enable the SNMP server).

Syntax:

```
snmp-server
```

3.3.31.1 SNMP-Server SNMP Access

Set SNMP access configuration.

Syntax:

```
snmp-server access <group_name> model { v1 | v2c | v3 | any }
level { auth | noauth | priv } [ read <view_name> ] [ write
<write_name> ]
```

<group_name>: group name, value can be 1 to 32 characters

model: set the security model, values are:

any:	any security model
v1:	v1 security model
v2c:	v2c security model
v3:	v3 security model

level: set the level, values are:

auth:	authNoPriv Security Level
noauth:	noAuthNoPriv Security Level
priv:	authPriv Security Level

<view_name>: view name, value can be 1 to 255 characters (read)

<write_name>: write name, value can be 1 to 255 characters (write)

3.3.31.2 SNMP-Server Community SNMP v2c

Set the SNMP community (SNMPv2c) configuration.

Syntax:

```
snmp-server community v2c <comm> [ ro | rw ]
```

<comm>: community name, value can be 1 to 32 characters

ro:	read only
rw:	read write

3.3.31.3 SNMP-Server Community SNMP v3

Set the SNMP community (SNMPv3) configuration.

Syntax:

```
snmp-server community v3 <v3_comm> [ <v_ipv4_addr> <v_ipv4_netmask> ]
```

<v3_comm> : community name, value can be 1 to 127 characters

<v_ipv4_addr>: IPv4 address

3.3.31.4 SNMP-Server Contact

Set the SNMP server's contact string.

```
snmp-server contact <v_line255>
```

<v_line255>: contact string, value can be from 1 to 255 characters

3.3.31.5 SNMP-Server Engine-Id Local

Set SNMP local engine ID.

Syntax:

```
snmp-server engine-id local <engineID>
```

<engineID>: local engine-id, value can be from 10 to 32 characters

3.3.31.6 SNMP-Server Host

Set SNMP host's configurations.

Syntax:

```
snmp-server host <conf_name>
```

<conf_name> name of the host configuration, value can be from 1 to 32 characters

Example:

Input:

```
M912(config)# snmp-server host miltech_host
```

Output:

```
M912(config-snmps-host)#
```

The following option are available from the SNMP host:

do:	to run exec commands in config mode
end:	go back to EXEC mode
exit:	exit from current mode
help:	description of the interactive help system
host:	host configuration
informs:	send Inform messages to this host
no:	negate a command or set its defaults
shutdown:	disable the trap configuration
traps:	trap event configuration
version:	set SNMP trap version

> **Note:** General commands are described elsewhere in this document (see section 3.3.17 Interface – VLAN on page 49).
> Commands specific to SNMP-Server are described below.

3.3.31.7 SNMP-Server Host Commands

(SNMP-Server Host) Informs

Send Inform messages to this host.

Syntax:

```
informs retries <retries> timeout <timeout>
```

<retries>: number of times to retry sending inform message, value can be from 0 to 255

<timeout>: timeout interval, value can be from 0 to 2,147 seconds

(SNMP-Server Host) Traps

Set the trap event configuration.

Syntax:

```
traps [ aaa authentication ] [ system [ coldstart ] [ warmstart ] ]
[ switch [ stp ] [ rmon ] ]
```

aaa: AAA event group

system: system event group

coldstart: cold start event

warmstart: warm start event

switch: switch event group

rmon: RMON event

stp: STP event

system: System event group

(SNMP-Server Host) Version

Set SNMP trap version.

Syntax:

```
version { v1 [ <v1_comm> ] | v2 [ <v2_comm> ] |
v3 [ probe | engineID <v_word10_to_32> ] [ <securtyname> ] }
```

v1: SNMP trap version 1

[<v1_comm>]: community name, value can be 1 to 127 characters

v2: SNMP trap version 2

[<v2_comm>]: community name, value can be 1 to 127 characters

v3: SNMP trap version 3

engineID: configure trap server's engine ID

probe: probe trap server's engine ID

3.3.31.8 SNMP-Server Location

Set the SNMP server's location string.

Syntax:

```
snmp-server location <v_line255>
```

<v_line255>: location string, value can be 1 to 255 characters

3.3.31.9 SNMP-Server Security-to-group

Set security-to-group configuration.

Syntax:

```
snmp-server security-to-group model { v1 | v2c | v3 } name
<security_name> group <group_name>
```

model: set the security model, values are:

any:	any security model
v1:	v1 security model
v2c:	v2c security model
v3:	v3 security model

<security_name>: security group, value can be 1 to 32 characters

<group_name>: group name, value can be 1 to 32 characters

3.3.31.10 SNMP-Server Trap

Set trap’s configurations (enable the SNMP server traps).

Syntax:

```
snmp-server trap
```

3.3.31.11 SNMP-Server User

Set the SNMPv3 user's configurations.

Syntax:

```
snmp-server user <username> engine-id <engineID> [ { md5 <md5_passwd>
| sha <sha_passwd> } [ priv { des | aes } <priv_passwd> ] ]
```

<username>: user name, value can be 1 to 32 characters

<engineID>: engine identifier, value can be 10 to 32 characters

md5: set MD5 protocol

<md5_passwd> md5 protocol password, value can be 8 to 32 characters

sha: set SHA protocol

<sha_passwd> sha protocol password, value can be 8 to 40 characters

[priv { des | aes } <priv_passwd>:

priv: set Privacy

aes: Set AES protocol

des: Set DES protocol

<priv_passwd>: set privacy password, value can be 8 to 32 characters

3.3.31.12 SNMP-Server Version

Set the SNMP server's version.

Syntax:

```
snmp-server version { v1 | v2c | v3 }
```

v1: SNMPv1

v2c: SNMPv2c

v3: SNMPv3

3.3.31.13 SNMP-Server View

MIB view configuration

Syntax:

```
snmp-server view <view_name> <oid_subtree> { include | exclude }
```

<view_name>: MIB view name, value can be up to 32 characters

<oid_subtree>: MIB view OID, value can be up to 255 characters

exclude: excluded type from the view

include: included type from the view

3.3.32 SNTP

SNTP

Configure SNTP – Simple Network Time Protocol.

Syntax:

```
sntp
```

SNTP Server

Configure SNTP server.

Syntax:

```
sntp server ip-address { <ipv4_var> }
```

<ipv4_var>: ipv4 address

3.3.33 Spanning-Tree

Configure Spanning Tree protocol.

3.3.33.1 Spanning-Tree Aggregation

Aggregation mode

Syntax:

```
spanning-tree aggregation
```

Output (STP Aggregation Prompt):

```
    M912(config-stp-aggr)#
```

Options:

do:	To run exec commands in config mode
end:	Go back to EXEC mode
exit:	Exit from current mode
help:	Description of the interactive help system
no:	Negate a command or set its defaults

```
no spanning-tree
no spanning-tree auto-edge
no spanning-tree bpdu-guard
no spanning-tree edge
no spanning-tree link-type
no spanning-tree restricted-role
no spanning-tree restricted-tcn
```

3.3.33.2 Spanning-Tree Edge bpdu-Filter

Enable BPDU filter (stop BPDU tx/rx).

Syntax:

```
spanning-tree edge bpdu-filter
```

3.3.33.3 Spanning-Tree Edge bpdu-Guard

Enable BPDU guard.

Syntax:

```
spanning-tree edge bpdu-guard
```

3.3.33.4 Spanning-Tree Mode

Set the STP (Spanning Tree Protocol) protocol mode.

Syntax:

```
spanning-tree mode { stp | rstp | mstp }
```

rstp: Rabid Spanning Tree (802.1w)

stp: 802.1D Spanning Tree

mstp: Multiple Spanning Tree (802.1s)

3.3.33.5 Spanning-Tree Recovery Interval

Set the error recovery timeout.

Syntax:

```
spanning-tree recovery interval <interval>
```

<interval>: the interval in seconds, value can be 30 to 86,400 seconds

3.3.33.6 Spanning-Tree transmit Hold-Count

Set the number of BPDUs to transmit.

Syntax:

```
spanning-tree transmit hold-count <holdcount>
```

<holdcount>: the maximum number of transmit BPDUs per sec, value can be from 1 to 10 per second, the default is 6 per second

3.3.34 Thermal-Protect

Set the thermal protection configurations.

Thermal-Protect Prio

Assign a temperature limit to the priority. Ports will shut off when they reach the temperature limit assigned to their priority.

Syntax:

```
thermal-protect prio <prio_list> temperature <new_temp>
```

<prio_list>: prioity or priorities, value can be from 0 to 3

<new_temp>: temperature at which to turn off a port (with the corresponding priority)

3.3.35 Vlan

VLAN commands.

Vlan_List

Syntax:

```
vlan <vlist>
```

Example:

Input:

```
M912(config)# vlan 1
```

Output (change to VLAN Prompt)

```
M912(config-vlan)#
```

do: to run exec commands in config mode

end: go back to EXEC mode

exit: exit from current mode

help: description of the interactive help system

name: ASCII name of the VLAN, value can be up to 32 characters

Syntax:

```
name <vlan_name>
```

no: clear the VLAN name

Syntax:

```
no name
```

Vlan Ethertype

Set the ether type for Custom S-ports.

Syntax:

```
vlan ethertype s-custom-port <etype>
```

<etype>: ethertype (Range: 0x0600-0xffff)

3.4 Copy

Copy one of the following source file types to a specified destination:

running-config: currently running configuration

startup-config: startup configuration

<source_path>/<destination_path>:

flash:filename: file in FLASH or on TFTP server

[syntax-check]: Perform syntax check on source configuration

Syntax:

```
copy { startup-config | running-config | <source_path> } { startup-
config | running-config | <destination_path> } [ syntax-check ]
```

3.5 Debug

3.5.1 Prompt

Set prompt for testing.

Syntax:

```
debug prompt <debug_prompt>
```

<debug_prompt>: word for debug prompt in 32 characters

Example:

Input:

```
debug prompt m912-debug
```

Output (changes prompt):

```
m912-debug#
```

> **Note:** To exit debug mode use the No command described below.

3.5.2 No

Negate a command or set its defaults.

Syntax:

```
no debug prompt (to clear prompt and exit debug mode)
no terminal editing
no terminal exec-timeout
no terminal history size
no terminal length
no terminal width
```

3.6 Delete

Delete one file in flash: file system.

Syntax:

```
delete <path>
```

<path>: path and name of file to delete

3.7 Dir

Directory of all files in flash: file system.

Syntax:

```
Dir | Output modifiers
```

Output Modifiers

begin: begin with the line that matches

exclude: exclude lines that match

include:	include lines that match
LINE:	string to match output lines

3.8 Disable

Turn off privileged commands.

Syntax:

```
disable [ <new_priv> ]
```

Values:

[<new_priv>]: values are <0-15>

3.9 Do

Perform an Exec Command while located in a sub-folder.

Syntax:

```
do <command>
```

3.10 Dot1x

Configure IEEE Standard for port-based Network Access Control.

Syntax:

```
dot1x initialize [ interface ( <port_type> [ <plist> ] ) ]
```

Dot1x Initialize

Force re-authentication immediately.

interface: <port_type>, values are:

*	all switches or all ports
GigabitEthernet:	set specific Gigabit Ethernet Port number
<plist>	port list in 1/1-8

3.11 Enable

Turn on privileged commands.

Syntax:

```
enable [ <new_priv> ]
```

[<new_priv>]: Privileged level, values are <0-15>

3.12 Exit

Exit from EXEC mode.

Syntax:

```
Exit
```

3.13 Firmware

Perform a firmware upgrade or swap.

Firmware Swap

Swap between Active and Alternate firmware image.

Syntax:

```
firmware swap
```

Firmware Upgrade

Upgrade Firmware software with specified file.

Syntax:

```
firmware upgrade <tftpserver_path_file>
```

<tftpserver_path_file>: TFTP Server IP address, path and file name for the server containing the new image.

3.14 Help

Description of the interactive help system

Syntax:

```
help
```

3.15 IP

Set IPv4 commands.

Syntax:

```
ip dhcp retry interface vlan <vlan_id>
```

dhcp:	Dynamic Host Configuration Protocol (DHCP) commands
retry:	restart the DHCP query process
interface:	interface
vlan:	Vlan interface

<vlan_id>: Vlan ID

3.16 Logout

Exit from EXEC mode.

Syntax:

```
logout
```

3.17 More

Display a file in FLASH or on TFTP server.

Syntax:

```
more <path>
```

<Path>: Path to file in FLASH or on TFTP server

3.18 No

Negate a command or set its defaults.

No Debug

To clear prompt and exit debug mode.

Syntax:

```
no debug prompt
```

No Terminal Commands

Clear terminal line parameters. (See section 3.23 Terminal on page 77.)

Syntax:

```
no terminal editing
no terminal exec-timeout
no terminal history size
no terminal length
no terminal width
```

3.19 Ping

Send ICMP echo messages (to troubleshoot IP connectivity issues.).

Syntax:

```
ping ip <v_ip_addr> [ repeat <count> ] [ size <size> ] [ interval
<seconds> ]
```

<v_ip_addr>:

[repeat <count>]: number of times to send ping message

[size <size>]: size of the ICMP PING packet to send

[interval <seconds>]: time, in seconds, to wait before sending additional Ping packet

3.20 Reload

Reload system.

Syntax:

```
reload { { cold } | { defaults [ keep-ip ] } }
```

reload options:

cold:	reload cold
defaults:	reload defaults without rebooting

3.21 Send

Send a message to other tty lines.

Syntax:

```
send { * | <session_list> | console 0 | vty <vty_list> } <message>
```

*	All tty lines
<0~16>:	send a message to multiple lines
console:	primary terminal line
vty:	virtual terminal

The message text is delimited by a user defined character:

c message-text c, where ‘c’ is a delimiting character and “message-text” is the message.

Example:

Input:

```
M912(config)# send  x Hello. x<CR>
```
(the delimiter is “x”)

3.22 Show

Show running system information.

Show Commands (a-c)

```
show aaa
show access management [ statistics | <access_id_list> ]
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> ]
show aggregation [ mode ]
show clock
```

Show Dot1x Commands

```
show dot1x statistics { eapol | radius | all } [ interface (
<port_type> [ <v_port_type_list> ] ) ]
show dot1x status [ interface ( <port_type> [ <v_port_type_list> ] ) ]
[ brief ]
```

Show Green-Ethernet Commands

```
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> ] ) ]
show history
```

Show Interface Commands

```
show interface ( <port_type> [ <in_port_list> ] ) switchport [ access
| trunk | hybrid ]
show interface ( <port_type> [ <v_port_type_list> ] ) capabilities
show interface ( <port_type> [ <v_port_type_list> ] ) statistics [ {
packets | bytes | errors | discards | filtered | { priority [
<priority_v_0_to_7> ] } } ] [ { up | down } ]
show interface ( <port_type> [ <v_port_type_list> ] ) status
show interface ( <port_type> [ <v_port_type_list> ] ) veriphy
show interface vlan [ <vlist> ]
```

Show IP Commands

```
show ip arp
show ip http server secure status
show ip igmp snooping [ vlan <v_vlan_list> ] [ group-database [
interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ]
] [ detail ]
show ip igmp snooping mrouter [ detail ]
show ip interface brief
show ip route
show ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp
] [ icmp-msg <type> ]
```

Show Commands (l-mac)

```
show lacp { internal | statistics | system-id | neighbour }
show line [ alive ]
show lldp neighbors [ interface ( <port_type> [ <v_port_type_list> ] )
]
show lldp statistics [ interface ( <port_type> [ <v_port_type_list> ]
) ]
show logging <log_id> [ switch <switch_list> ]
show logging [ info ] [ warning ] [ error ] [ switch <switch_list> ]
show loop-protect [ interface ( <port_type> [ <plist> ] ) ]
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 Platform Commands

```
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> ] ) ]
```

Show Commands (p-r)

```
show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show port-security switch [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show privilege
show pvlan [ <pvlan_list> ]
show pvlan isolation [ interface ( <port_type> [ <plist> ] ) ]
show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
show radius-server [ statistics ]
```

Show Running-Config Commands

```
show running-config [ all-defaults ]
show running-config feature <feature_name> [ all-defaults ]
show running-config interface ( <port_type> [ <list> ] ) [ all-defaults ]
show running-config interface vlan <list> [ all-defaults ]
show running-config line { console | vty } <list> [ all-defaults ]
show running-config vlan <list> [ all-defaults ]
```

Show SNMP Commands

```
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> ]
```

Show Commands (sntp-vlan)

```
show sntp status
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> ] ) ] } ] } ]
show switchport forbidden [ { vlan <vid> } | { name <name> } ]
show terminal
show thermal-protect [ interface ( <port_type> [ <port_list> ] ) ]
show users [ myself ]
show version
show vlan [ id <vlan_list> | name <name> | brief ]
show vlan status [ interface ( <port_type> [ <plist> ] ) ] [ combined
| admin | nas | mvr | voice-vlan | mstp | erps | vcl | evc | gvrp |
all | conflicts ]
```

3.23 Terminal

Editing

Enable command line editing.

Syntax:

```
terminal editing
```

Exec-timeout

Set the EXEC timeout.

Syntax:

```
terminal exec-timeout <min> [ <sec> ]
```

<min>: timeout in minutes, values are <0-1440>

Help

Display a description of the interactive help system.

Syntax:

```
help
```

History

Control the command history function.

Syntax:

```
terminal history size <history_size>
```

<history_size>: set history buffer size

Length

Set the number of lines on a screen.

Syntax:

```
terminal length <lines>
```

<lines>: number of lines on screen (0 for no pausing), values are: 0 or 3-512

Width

Set the width of the display terminal.

Syntax:

```
terminal width <width>
```

<width>: Number of characters on a screen line (0 for unlimited width), values are: 0 or 40-512

3.24 Factory Default Configuration

The factory default configuration is a VLAN unaware L2 switch with automatic learning/ageing and auto negotiation enabled on all ports:

- **System:** The system name string is M912.
- **Console:** The password string is empty and inactivity timeout is disabled. The prompt is “>“.
- **Port:** All ports are enabled for auto negotiation and flow control is disabled. Max frame size is 1518.
- **MAC Table:**
  - The table is empty
  - Auto learning and ageing are enabled
  - The ageing timer is 300 seconds
- **VLAN:**
  - Only VLAN 1 is present in the table and includes all ports
  - All ports are VLAN unaware with Port VLAN ID 1
  - All ports accept all frame types
- **Aggregation:** No ports are aggregated, but aggregation mode is set to XOR.
- **LACP:** No ports have LACP enabled.
- **RSTP:** No ports and no aggregations have RSTP enabled
- **User Groups:** User group 1 exists and includes all ports.
- **QoS:**
  - IP ToS Precedence priority is enabled and all Precedence values are given high priority
  - VLAN tag priorities will be set according to 802.1p
  - The UDP/TCP port list is empty
  - Default priority is high
  - Default user priority is 0
  - L4 default priority and match priority are low
  - All shaper and policers are disabled
- **Mirror:** Mirroring is disabled.
- **IP:**
  - IP address is 192.168.1.111
  - Mask: 255.255.255.0
  - Gateway:
  - Web interface is enabled.

  - DHCP mode is disabled.
- **SNMP:** SNMP is enabled. Traps are disabled.
- **Dot1X:** 802.1X is disabled. All ports set to “Force Authorized”
- **IGMP Snooping:** Disabled in each defined VLAN

4 Web Interface - Introduction

From the MILTECH-912 Web Interface the user can manage the following aspects of the switch:

- Customize configurations and status monitoring
- Perform diagnostics and maintenance procedures

4.1 Web Interface – Configuration

Below is a list of some of the configurations that may be done using the Web interface:

- IP interfaces and routes
- SNTP mode and server address
- Log mode, address, and level
- Green Ethernet configurations for power savings
- Thermal Protection
- Port Configurations
- Security settings
- Aggregation settings
- Loop Protection settings
- Spanning Tree Protocol (STP) settings
- IPMC (Intelligent Platform Management Controller) snooping configurations
- LLDP () configurations
- MAC table configurations
- VLAN configurations
- QoS (Quality of Service) configurations
- Mirror Configurations

4.2 Web Interface – Monitoring

Below is a list of some of the monitoring that may be done using the Web interface:

- System information
- CPU load
- IP status
- System Logs
- Green Ethernet power savings

- Thermal Protection status
- Ports
  - State
  - Traffic
  - QoS Statistics
  - Detailed Statistics
- Security
- LACP system and port status and port statistics
- Loop Protection
- Spanning Tree Protocol
- IPMC – IGMP snooping
- LLDP
- VLAN

4.3 Web Interface – Diagnostics

Below is a list of some of the diagnostics that may be done using the Web interface:

- Ping to troubleshoot connectivity
- VeriPHY to perform cable diagnostics

4.4 Web Interface – Maintenance

Below is a list of some of the maintenance that may be done using the Web interface:

- Restart the device
- Reset the device to factory defaults
- Upload software
- Save and download configuration files

4.5 Web Interface – Getting Started

All operations are password protected. The password must be entered at login. It is the password as the one used in the command line interface.

The Web interface is enabled in the factory before delivery.

- Default IP address: 192.168.1.111
- Default Subnet Mask: 255.255.255.0

- Default User Name: admin
- Default Password: <empty>

You may restart the Dynamic Host Configuration Protocol (DHCP) query process, if your environment includes a DHCP server. See section 3.15 IP on page 72 for setting IP parameters via the command line interface.

Example input:

```
M912# ip dhcp retry interface vlan 1
```

Open the Web Interface

To open the Web Interface:

1. Open a Web browser
2. Enter the IP address in the browser address bar (default is 192.168.1.111)
3. Press enter

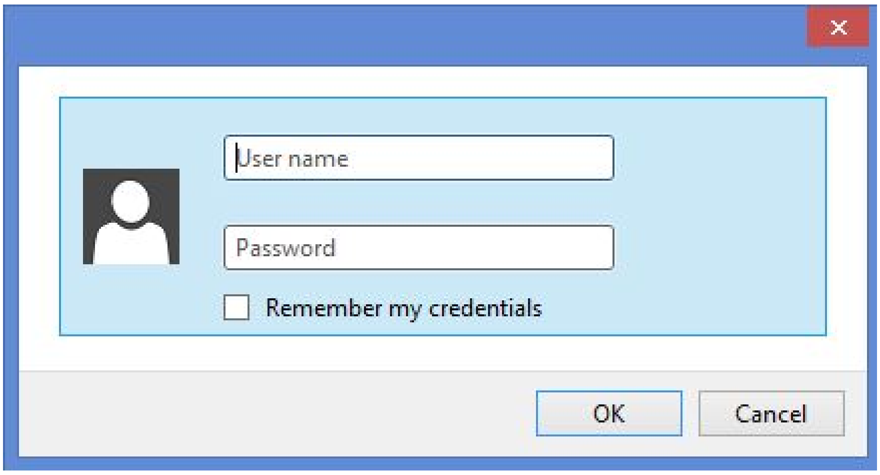
The login window pops up.

4.6 Web Interface – Login Window

Enter the User name* and Password**, and then click **OK** to login.

* The user name string is “admin” by default.

** The password string is empty by default.



The Web Interface opens with the available menu options on the left side of the screen.

5 Web Interface - Configuration

The Web Interface – Configuration section of this manual describes how to configure the MILTECH-912™ Gigabit Ethernet Switch, using the MILTECH-912™ User Interface. Not all configurations are supported via the WEB interface; some configurations may be done strictly from the CLI.

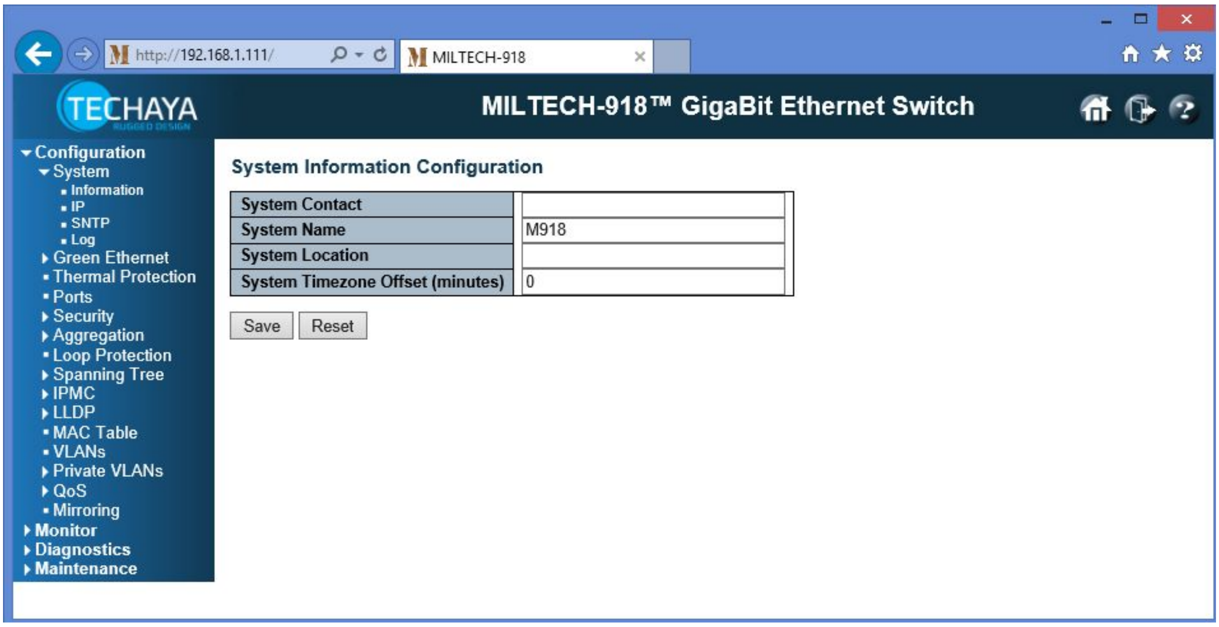
5.1 System Information Configuration

The System Information Configuration page displays and allows updates to the following system details:

- System Contact
- System Name
- System Location
- System Time zone Offset

Click **Save** to save all changes.

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



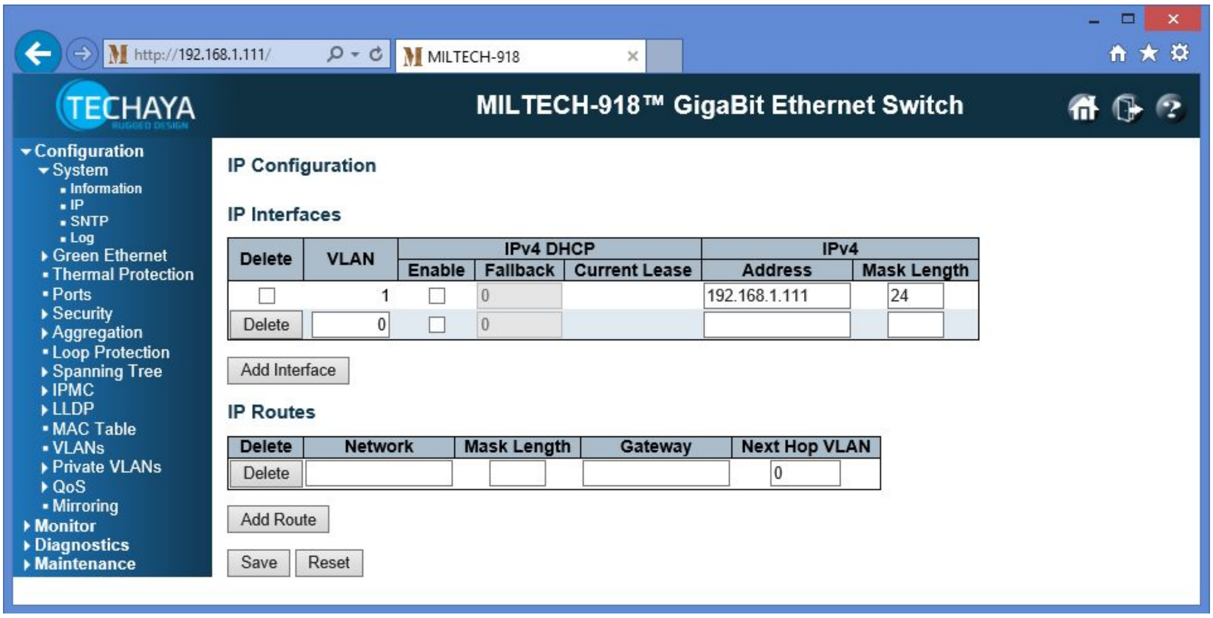
System Information Configuration

System Contact	
System Name	M918
System Location	
System Timezone Offset (minutes)	0

5.2 System – IP

IP Configuration

The IP Configuration page allows the user to configure IP Interfaces and IP Routes. When the page opens, it displays the current configurations.



IP Configuration

IP Interfaces

Delete	VLAN	IPv4 DHCP			IPv4	
		Enable	Fallback	Current Lease	Address	Mask Length
□	1	□	0		192.168.1.111	24
Delete	0	□	0			

Add Interface

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
Delete				0

Add Route

Save Reset

5.2.1 IP Interfaces

Each IP Interface has the following configurable parameters:

Delete

Select this option to delete an existing IP interface.

VLAN

The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.

IPv4 DHCP - Enable

☑ Enable the DHCP client

☐ Disable (default: Disable)

If this option is enabled, the system will configure the IPv4 address and mask of the interface using the Dynamic Host Configuration Protocol (DHCP) protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

IPv4 DHCP - Fallback

The Fallback is the time limit in seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.

IPv4 DHCP - Current Lease

For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.

IPv4 - Address

Set or show 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 Length

Set or show the IPv4 network mask, in number of bits (*prefix length*). Valid values are between 0 and 30 bits for an IPv4 address.

If DHCP is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

5.2.2 IP Routes

Each IP Route has the following configurable parameters:

Delete

Select this option to delete an existing IP route.

Network

Set or show the destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0 or IPv6 notation.

Mask Length

Set or show the destination IP network or host mask, in number of bits (*prefix length*). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).

Gateway

Set or show 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 will be effective only when the corresponding IPv6 interface is valid.
If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway.
If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.

5.2.3 IP Configuration Buttons

Add Interface: Click to add a new IP Interface. A new row opens in the IP Interfaces table. The maximum number of interfaces supported is 8.

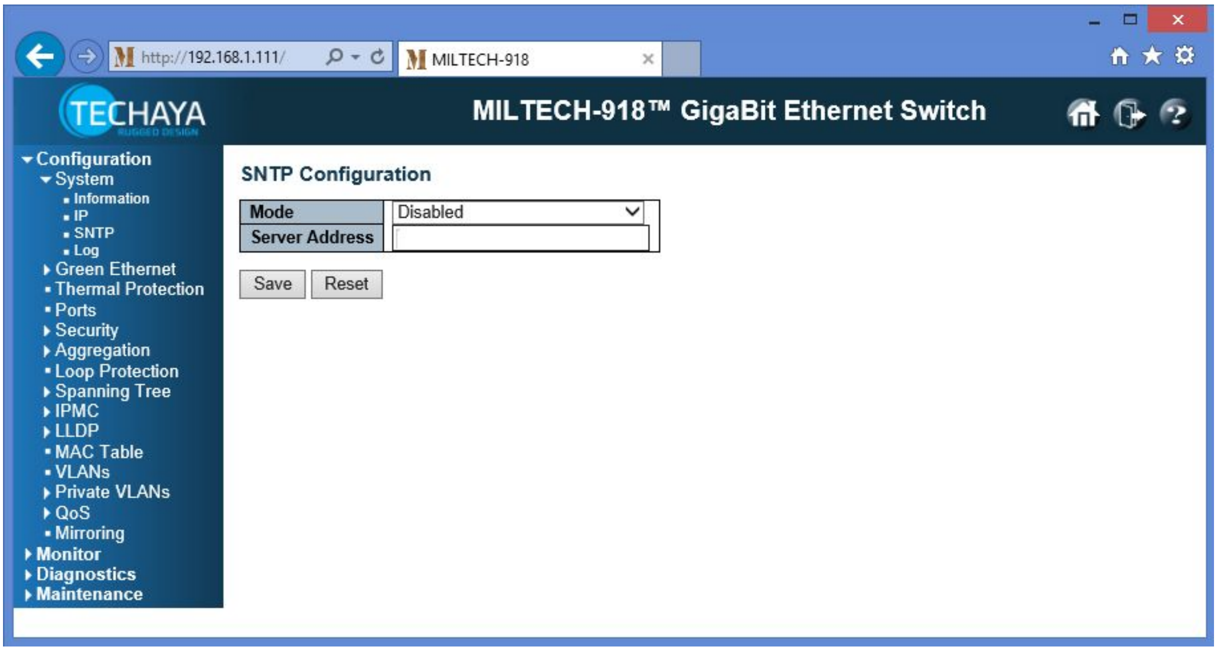
Add Route: Click to add a new IP Route. A new row opens in the IP Routes table. The maximum number of routes is 32.

Save: Click to save all changes.

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

5.3 System - SNTP

Use the SNTP page to configure SNTP.



SNTP Configuration

Mode	Disabled
Server Address	

5.3.1 SNTP Configuration

Mode

Indicates the SNTP mode operation:

Enabled: Enable SNTP client mode operation.

Disabled: Disable SNTP client mode operation.

Server Address

Set or show the IPv4 or IPv6 address of a SNTP 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’.

5.3.2 SNTP Buttons

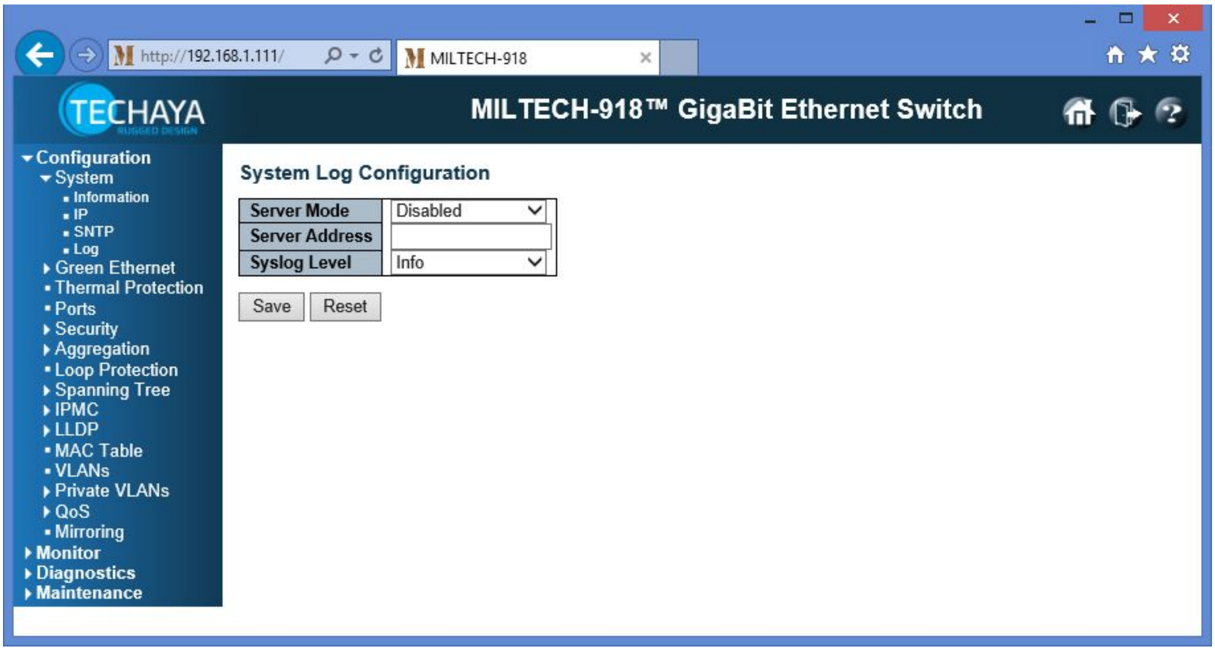
Save: Click to save all changes

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

5.4 System - Log

System Log Configuration

Use the System Log Configuration page to configure System Log.



System Log Configuration

Server Mode	Disabled
Server Address	
Syslog Level	Info

5.4.1 System Log Configuration

Server Mode

Indicates the server mode operation:

Enabled: Enable server mode operation

Disabled: Disable server mode operation

When the server mode is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and is received on UDP port 514. The syslog server will not send acknowledgments back to sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist.

Server Address

Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a host name.

Syslog Level

Indicates the message type to send to syslog server:

Info: Send information, warnings, and errors

Warning: Send warnings and errors

Error: Send errors

5.4.2 System Log Buttons

Save: Click to save all changes

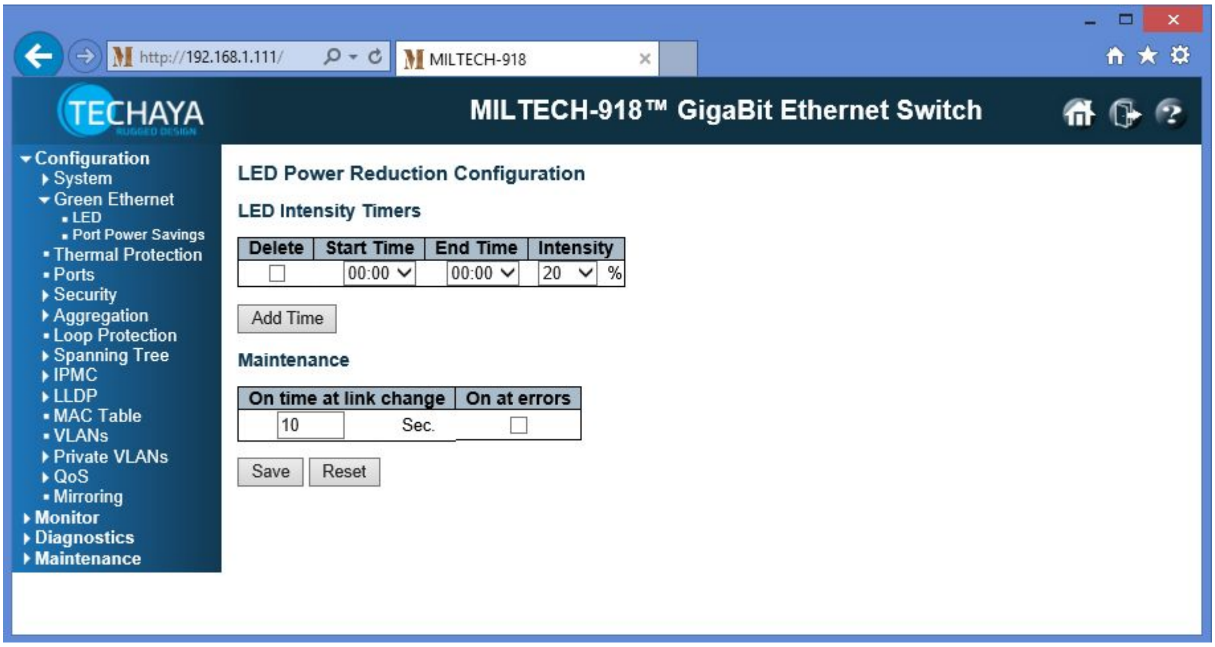
Reset: Click to undo any changes made locally and revert to previously saved values

5.5 Green Ethernet – LED

Power Reduction Configuration

The system status LED shows whether the system is running. The LED is green when system is running and no errors are detected. If errors has been detected the status LED will indicate this by blinking red.

The LEDs power consumption can be reduced by lowering the LEDs intensity.



LED Power Reduction Configuration

LED Intensity Timers

Delete	Start Time	End Time	Intensity
☐	00:00	00:00	20 %

Add Time

Maintenance

On time at link change	On at errors
10 Sec.	☐

Save Reset

5.5.1 Led Intensity Timers

LEDs intensity can be varied throughout the day. For example LED intensity can be lowered during night time, or turned off completely. It is possible to configure a different LED intensity for each of the 24 hours of the day. (Each one would occupy a unique time slot.)

The LED intensity timer has the following configurable parameters:

Delete

☑ Select this option to delete a LED configuration time slot

☐ Default (Do not delete the configuration time slot.)

Start Time

Set or show the time at which the LED's intensity shall be set to the corresponding intensity.

End Time

Set or show the time at which the LED's intensity shall be set to a new intensity. If no intensity is specified for the next hour, the intensity is set to the default intensity.

Intensity

Set or show the LEDs intensity (100% = Full power, 0% = LED off, Default = 100%)

5.5.2 Maintenance

During maintenance of the switch (e.g. adding or moving users), a network administrator might want to have full LED intensity. Therefore, it is possible to specify that the LEDs shall use full intensity at specific period of time. Maintenance Time is the number of seconds that the LEDs will have full intensity after either a port has changed link state, or the LED pushbutton has been pushed.

On Time at Link Change

Set or show the number of seconds for LEDs to be at full intensity during link status change.

On at Errors

☑ Set the LEDs to full intensity on errors

□ LEDs intensity not affected by errors (Default: this is the default)

5.5.3 IP Configuration Buttons

Add Time: Click to add a new time slot

Save: Click to save all changes

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

5.6 Green Ethernet - Port Power Savings

Energy Efficient Ethernet (EEE) is a power savings option that reduces the power usage when there is low or no traffic utilization.

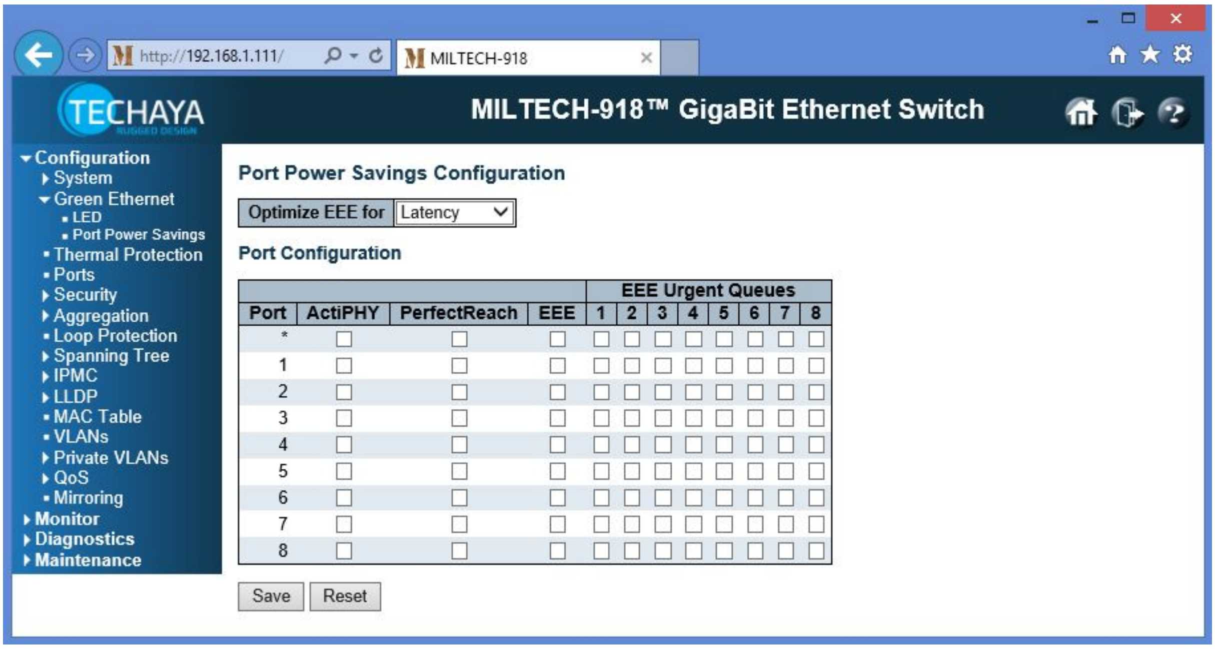
EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP protocol.

EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode.

For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable for EEE.

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

When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there are some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic.



Port Power Savings Configuration

Optimize EEE for: Latency

Port Configuration

				EEE Urgent Queues							
Port	ActiPHY	PerfectReach	EEE	1	2	3	4	5	6	7	8
*	□	□	□	□	□	□	□	□	□	□	□
1	□	□	□	□	□	□	□	□	□	□	□
2	□	□	□	□	□	□	□	□	□	□	□
3	□	□	□	□	□	□	□	□	□	□	□
4	□	□	□	□	□	□	□	□	□	□	□
5	□	□	□	□	□	□	□	□	□	□	□
6	□	□	□	□	□	□	□	□	□	□	□
7	□	□	□	□	□	□	□	□	□	□	□
8	□	□	□	□	□	□	□	□	□	□	□

5.6.1 Port Power Savings Configuration

There are two port power savings options for Energy Efficient Ethernet:

Optimize EEE for

Power: Optimize EEE for the best power savings

Latency: Optimize EEE for the least traffic latency

5.6.2 Port Configuration

The Port Power Savings has the following configurable parameters for each port:

Port

This column shows the switch port number of the logical port.

ActiPHY

ActiPHY works by lowering the power for a port when there is no link. To avoid the link being asleep when no data is sent, it activates the circuitry periodically.

☑ Link down power savings enabled

□ Link down power savings disabled (default: Disable)

PerfectReach

PerfectReach works by determining the cable length and lowering the power for ports with short cables.

☑ Cable length power savings enabled

□ Cable length power savings disabled (default: Disable)

EEE

In order to maximize power savings, the circuit is not started as soon as transmit data is ready for a port. The data is queued until a burst of data is ready to be transmitted. This will give some traffic latency.

☑ EEE is enabled for this switch port

□ EEE is disabled for this switch port (default: Disable)

EEE Urgent Queues

If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up immediately and the latency will be reduced to the wakeup time.

☑ Queue set as urgent - will activate transmission of frames as soon as data is available

□ Queue in regular mode - will postpone transmission until a burst of frames can be transmitted (default: Queue in regular mode)

5.6.3 Port Power Savings Buttons

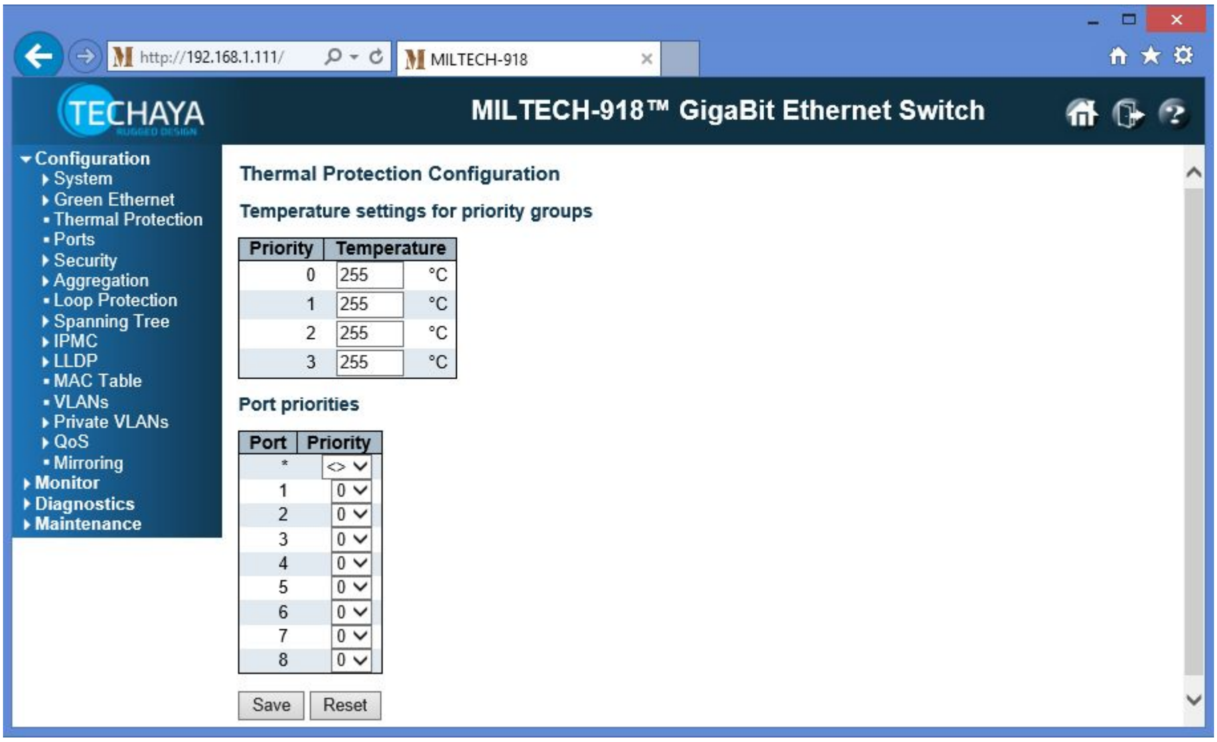
Save: Click to save all changes

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

5.7 Thermal Protection Configuration

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

When the temperature exceeds the configured thermal protection temperature, ports will be turned off in order to decrease the power consumption. Each port is assigned a priority. Each priority is assigned a temperature at which the corresponding ports shall be turned off.



Thermal Protection Configuration

Temperature settings for priority groups

Priority	Temperature	
0	255	°C
1	255	°C
2	255	°C
3	255	°C

Port priorities

Port	Priority
*	<>
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0

5.7.1 Temperature Settings for Priority Groups

Set or show the temperature at which the ports with the corresponding priority will be turned off. Temperatures between 0°C and 255°C are supported.

5.7.2 Port Priorities

The priority the port belongs to. 4 priorities are supported.
(The default priority is 0)

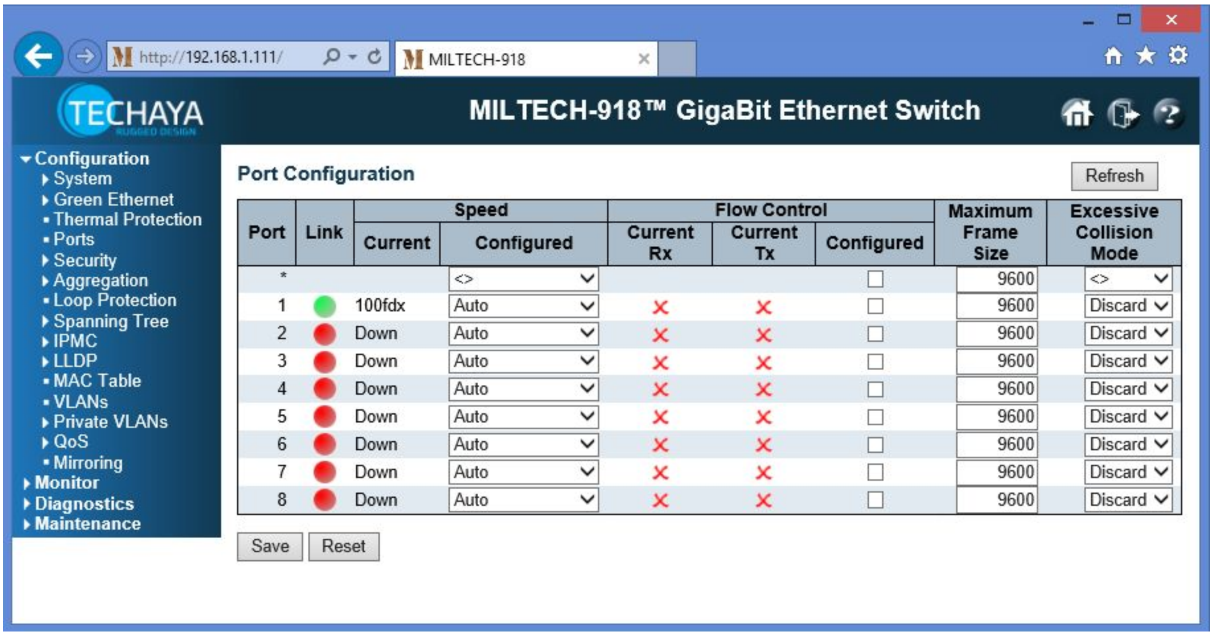
5.7.3 Thermal Protection Configuration Buttons

Save: Click to save all changes

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

5.8 Ports

This page displays the current port configurations.



Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode
		Current	Configured	Current Rx	Current Tx	Configured		
*			<>			☐	9600	<>
1	🟢	100fdx	Auto	✗	✗	☐	9600	Discard
2	🔴	Down	Auto	✗	✗	☐	9600	Discard
3	🔴	Down	Auto	✗	✗	☐	9600	Discard
4	🔴	Down	Auto	✗	✗	☐	9600	Discard
5	🔴	Down	Auto	✗	✗	☐	9600	Discard
6	🔴	Down	Auto	✗	✗	☐	9600	Discard
7	🔴	Down	Auto	✗	✗	☐	9600	Discard
8	🔴	Down	Auto	✗	✗	☐	9600	Discard

5.8.1 Port Configuration

The user can configure the following port parameters:

Port

This column displays the logical port number for this row.

Link

The current link state is displayed graphically. Green indicates the link is up and red that it is down.

Speed - Current

This column displays the current link speed of the port.

Speed - Configured

The user can select any available link speed for the given switch port. Only speeds supported by the specific port are shown. Possible speeds are:

Disabled - Disables the switch port operation.

Auto - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.

10Mbps HDX - Forces the cu port in 10Mbps half duplex mode.

10Mbps FDX - Forces the cu port in 10Mbps full duplex mode.

100Mbps HDX - Forces the cu port in 100Mbps half duplex mode.

100Mbps FDX - Forces the cu port in 100Mbps full duplex mode.

1Gbps FDX - Forces the port in 1Gbps full duplex

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 Rx and Tx settings are determined by the result of the last Auto-Negotiation.

Current Rx

The Current Rx column indicates whether pause frames on the port are obeyed**.**

Current Tx

The Current Tx column indicates whether pause frames on the port are transmitted

Configured

When flow control is configured, the network element can control the flow of data transmission, to prevent the network from becoming overwhelmed.

☑ Flow control is configured for this port. This setting is related to the setting for Configured Link Speed.

□ Flow control is **not** configured for this port. (This is the default.)

Maximum Frame Size

Increasing frame size reduces the effort necessary to transfer large amounts of data. It reduces the number of frames that need processing, thereby reducing the total overhead byte count of all the frames sent.

(Minimum frame size: 64 bytes, Maximum frame size: 9,600 bytes)

Enter the maximum frame size allowed for the switch port, including FCS.

Excessive Collision Mode

Configure port transmit collision behavior:

Discard: Discard frame after 16 collisions (default)

Restart: Restart backoff algorithm after 16 collisions

5.8.2 Port Configuration Buttons

Refresh: Click to refresh the page. Any changes made locally will be undone

Save: Click to save all changes

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

5.9 Security – Switch - Password

System Password

This page allows the user to set the system password required to access the web pages or to log in to the CLI.

Old Password

Enter the current system password. If this is incorrect, the new password will not be set.

New Password

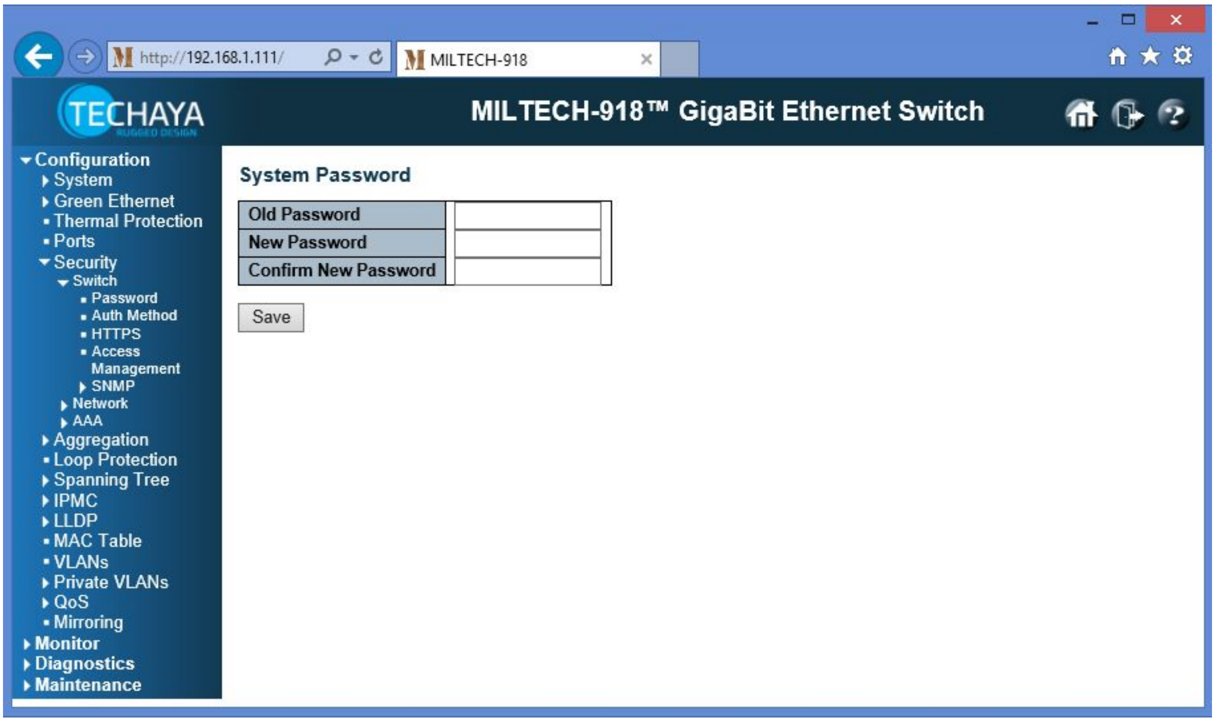
Enter a new system password. The string length can be from 0 to 31 characters, and the allowed content is the ASCII characters from 32 to 126.

Confirm New Password

The new password must be entered twice to catch typing errors.

Save Changes

Click **Save** to save all changes.



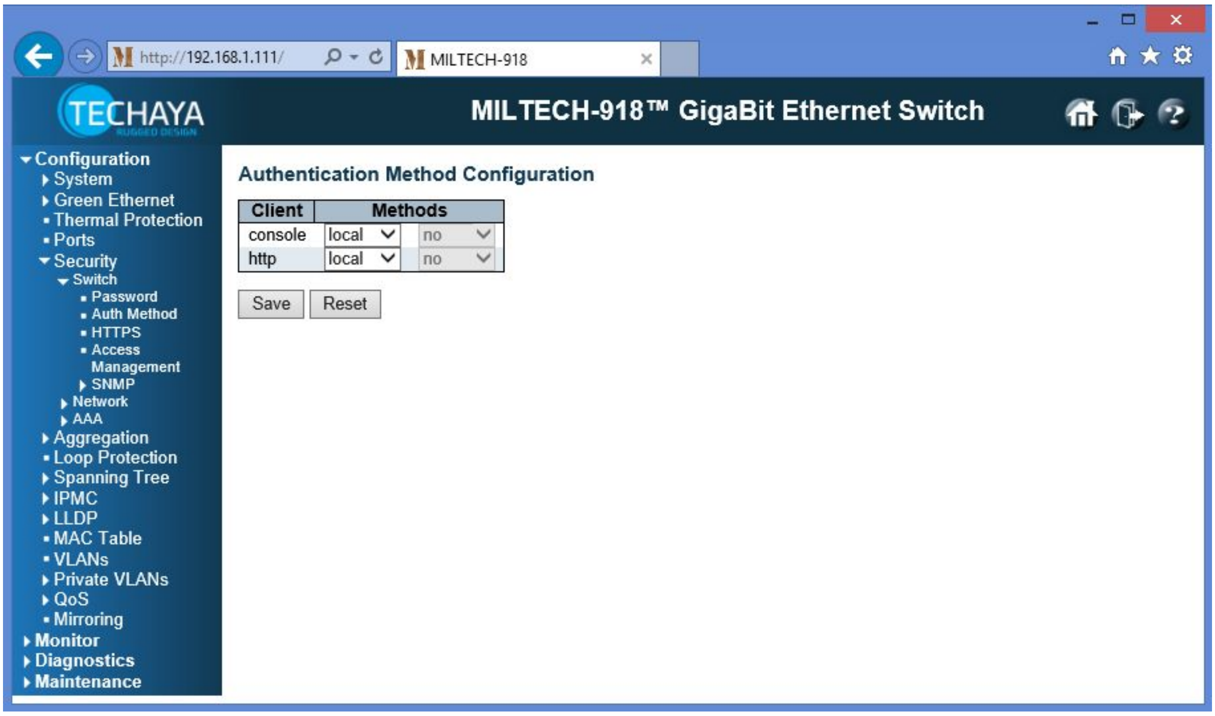
System Password

Old Password	
New Password	
Confirm New Password	

Save

5.10 Security – Switch – Auth Method

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



Authentication Method Configuration

Client	Methods	
console	local	no
http	local	no

5.10.1 Authentication Method Configuration

The authentication method configuration has the following parameters:

Client

The management client for which the configuration applies:

- Console
- Http

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 stack for authentication.

radius: Use remote radius server(s) for authentication.

Methods that involve remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.

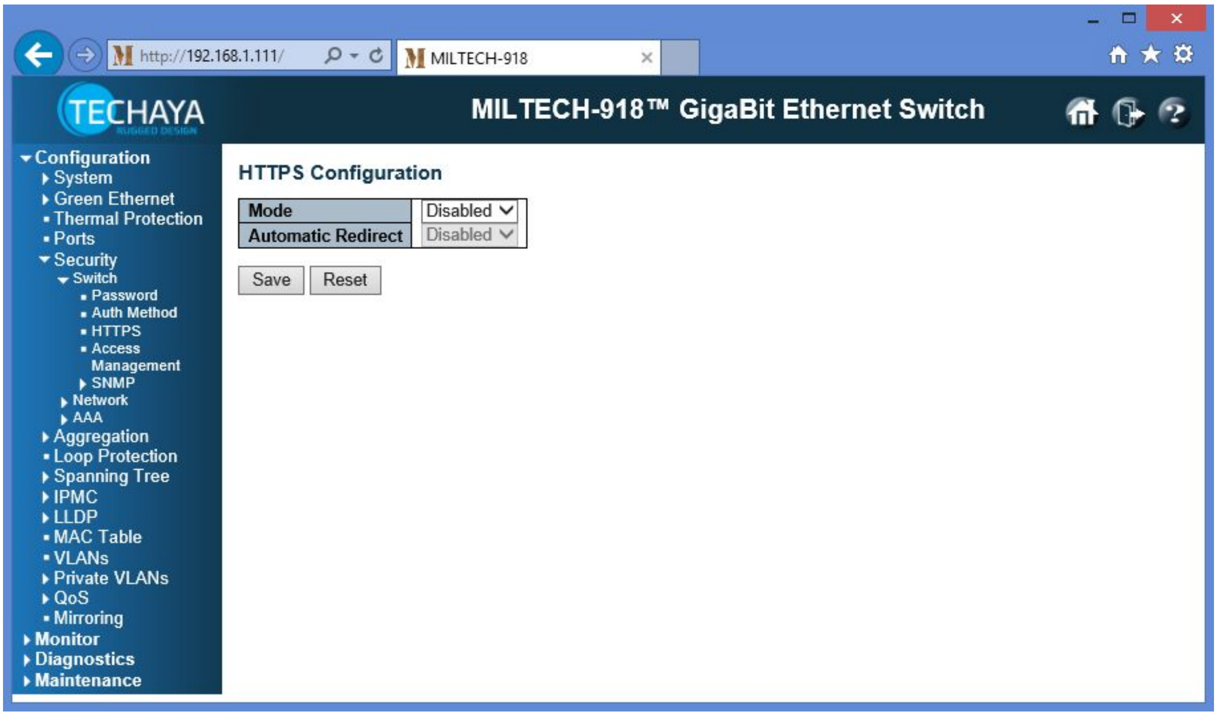
5.10.2 Authentication Method Buttons

Save: Click to save all changes

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

5.11 Security – Switch – HTTPS

The user can configure HTTPS from this page.



HTTPS Configuration

Mode	Disabled
Automatic Redirect	Disabled

5.11.1 HTTPS Configuration

The HTTPS configuration has the following parameters:

Mode

Set or show the HTTPS operation mode.

This mode allows the user to disable HTTPS even when the current connection is HTTPS. Possible modes are:

Enabled: Enable HTTPS mode operation.

Disabled: Disable HTTPS mode operation - operation will automatically redirect the web browser to an HTTP connection. (This is the default mode.)

Automatic Redirect

Set or show the HTTPS redirect operation mode. Automatic Redirect is only available when HTTPS mode is enabled.

Enabled: Enable HTTPS redirect mode operation, to automatically redirect web browser to an HTTPS

Disabled: Disable HTTPS redirect mode operation (This is the default.)

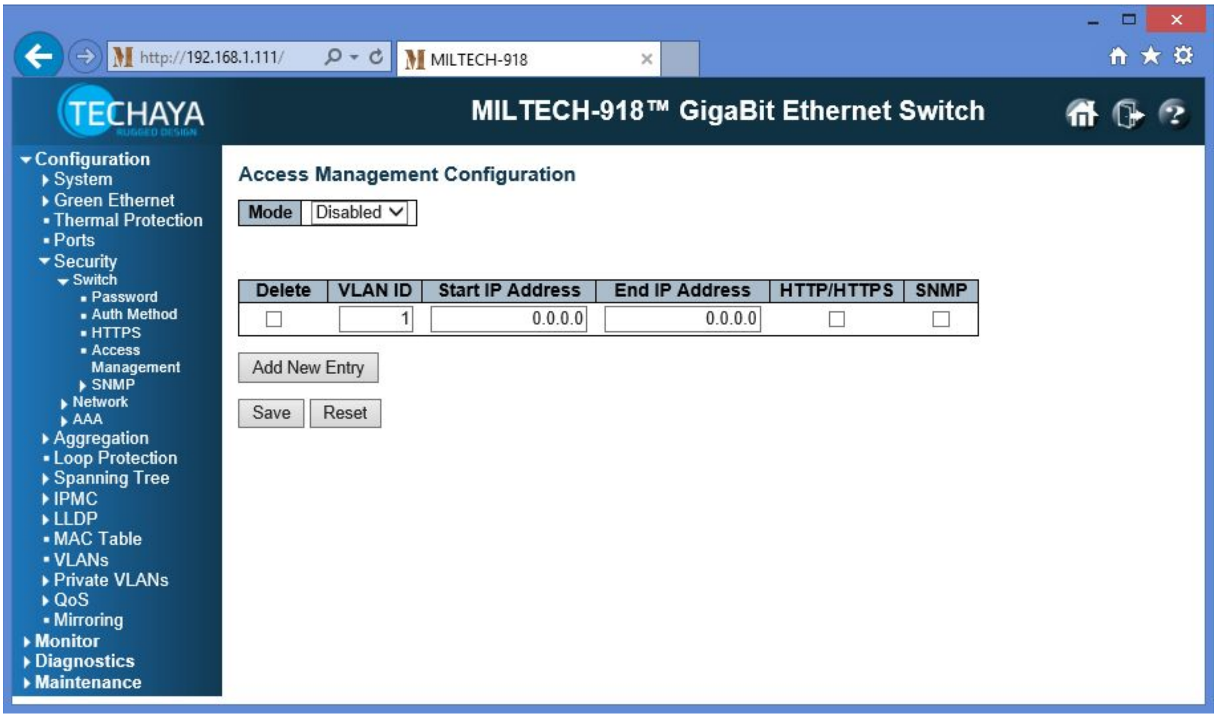
5.11.2 HTTPS Buttons

Save: Click to save all changes

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

5.12 Security – Switch – Access Management

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



Access Management Configuration

Mode: Disabled

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP
□	1	0.0.0.0	0.0.0.0	□	□

Add New Entry

Save Reset

5.12.1 Access Management Configuration

The access management configuration has the following parameters:

Mode

Set or show the access management mode operation.

Enabled: Enable access management mode operation

Disabled: Disable access management mode operation (This is the default mode.)

Delete

☑ Check to delete the entry. It will be deleted during the next save.

□ Do not delete the entry. (This is the default.)

VLAN ID

Set or show the VLAN ID for the access management entry.

Start IP Address

Set or show the start IP address for the access management entry.

End IP Address

Set or show the end IP address for the access management entry.

HTTP/HTTPS

Set or show HTTP/HTTPS interface status.

☑ Enabled - when the host IP address matches the IP address range provided in the entry, the host can access the switch from HTTP/HTTPS interface

□ Disabled (This is the default.)

SNMP

Set or show SNMP interface status.

☑ Enabled - when the host IP address matches the IP address range provided in the entry, the host can access the switch from SNMP interface

□ Disabled (This is the default.)

5.12.2 Access Management Buttons

Add New Entry:
Click to add a new access management entry

Save: Click to save all changes

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

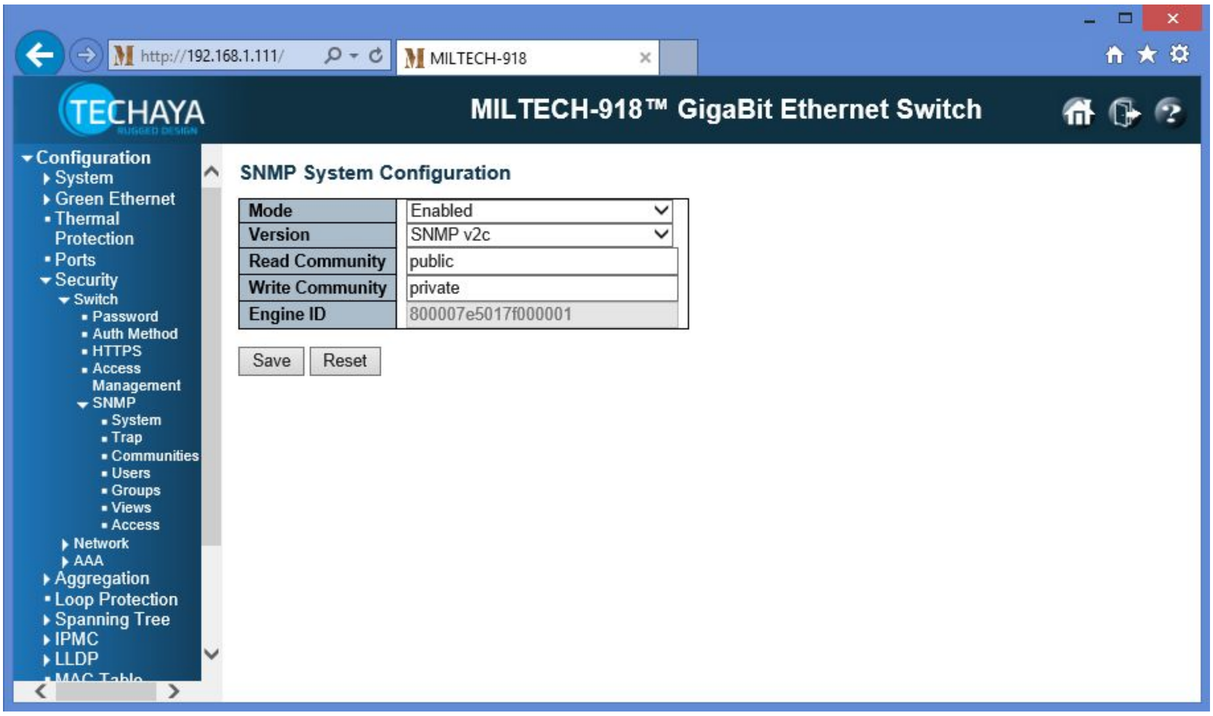
5.13 Security – Switch – SNMP– System

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 allows diverse network objects to participate in network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

5.13.1 System

SNMP System Configuration

The user can configure SNMP from this page.



SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

Mode

Set or show the SNMP mode operation.

Enabled: Enable SNMP mode operation (This is the default mode.)

Disabled: Disable SNMP mode operation

Version

Set or show 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

Set or show 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.

Applicable Only to SNMP versions: SNMPv1 or SNMPv2c

If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Write Community

Set or show 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.

Applicable Only to SNMP versions: SNMPv1 or SNMPv2c

If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Engine ID

Set or show the SNMPv3 engine ID. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

Applicable Only to SNMP version: SNMPv3

5.13.2 SNMP System Configuration Buttons

Save: Click to save all changes

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

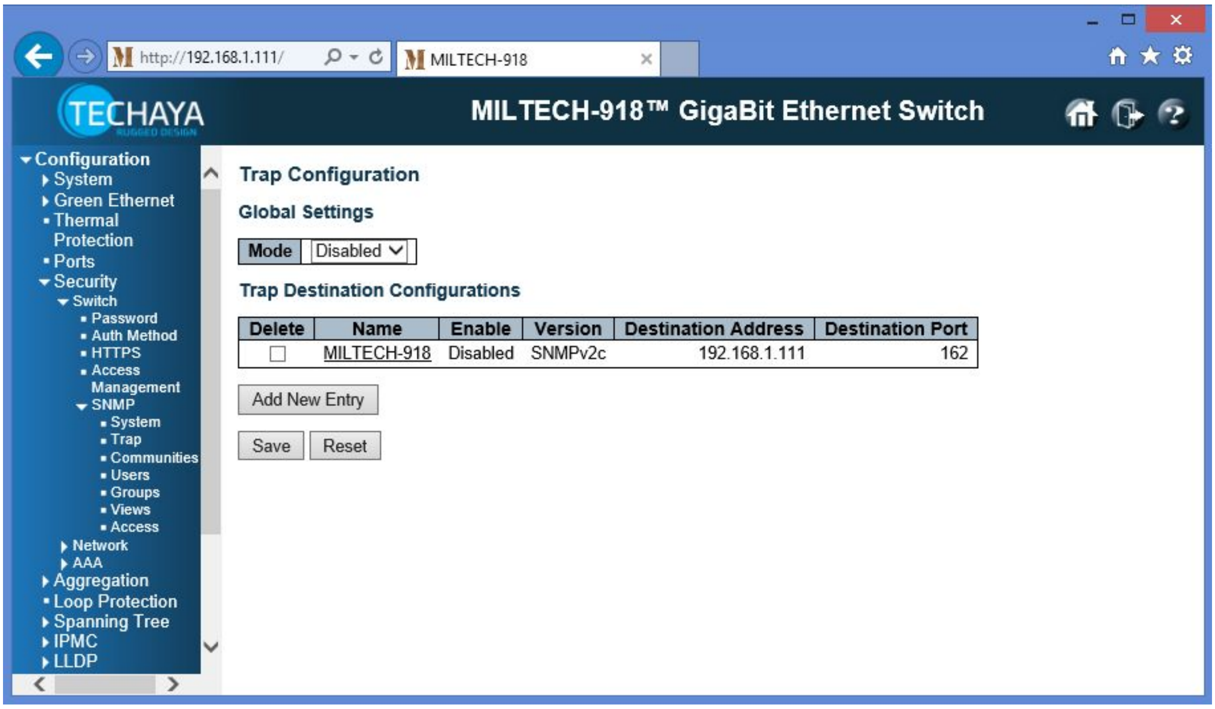
5.14 Security – Switch – SNMP – Trap

The user can enable, disable, and delete SNMP Traps from this page.

Trap Configuration

To create a new trap, click the **Add New Entry** button to open the SNMP Trap Configuration Page.

To edit an existing trap, click on the trap name to open the SNMP Trap Configuration Page for that trap.



Trap Configuration

Global Settings

Mode: Disabled

Trap Destination Configurations

Delete	Name	Enable	Version	Destination Address	Destination Port
□	MILTECH-918	Disabled	SNMPv2c	192.168.1.111	162

5.14.1 Global Settings

Set or show the SNMP trap mode operation.

Mode

Enabled: Enable SNMP trap mode operation

Disabled: Disable SNMP trap mode operation (This is the default mode.)

5.14.2 Trap Destination Configurations

Except for the “Delete” field parameters in the trap destination configurations table are display only.

Delete

☑ Check to delete the entry. It will be deleted during the next save.

□ Do not delete the entry. (This is the default.)

Name

Shows the name of the specific trap

Enable

Shows the operation status of the specific trap (enabled/disabled)

Version

Show the SNMP trap supported version.

Destination Address

Show the SNMP trap destination address.

Destination Port

Show the SNMP trap destination port.

5.14.3 Trap Configuration Buttons

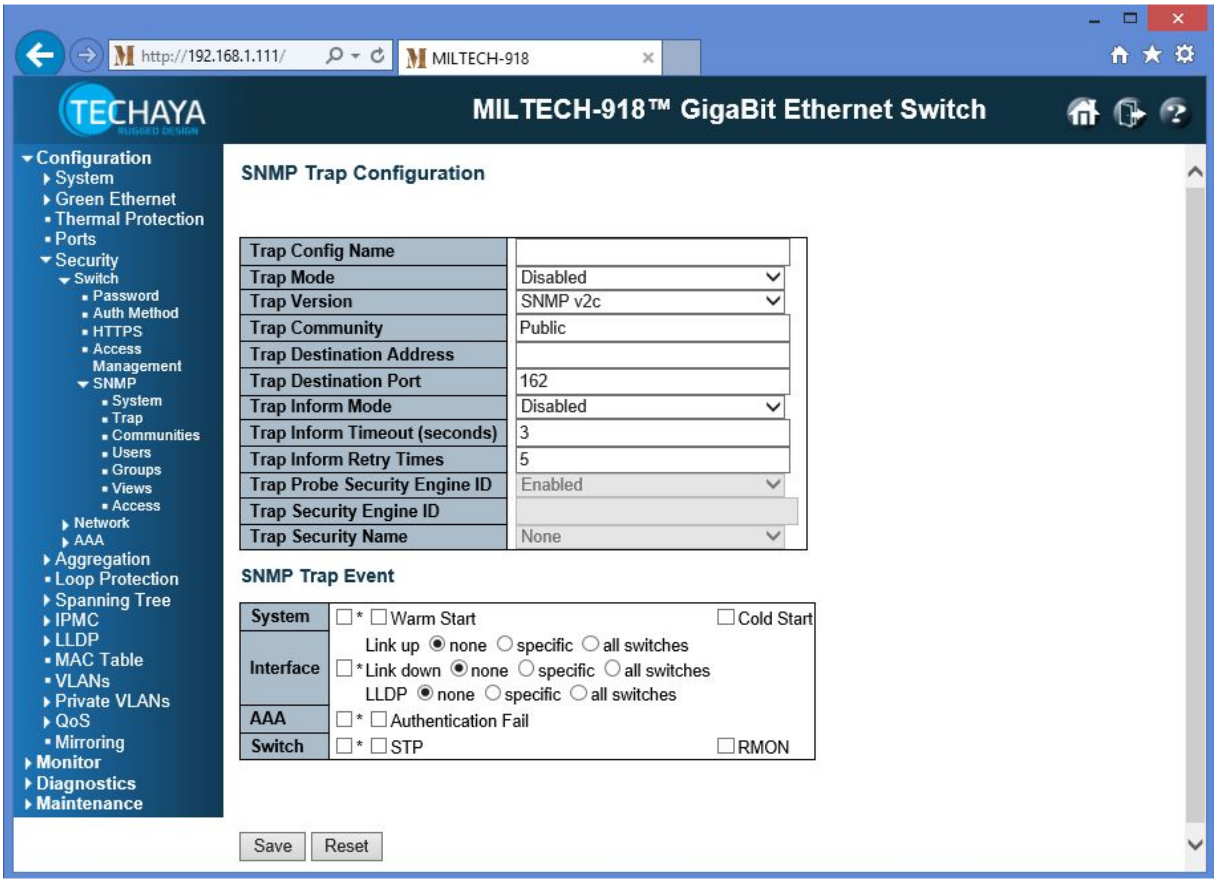
Add New Entry:
Click to add a new trap destination configuration

Save: Click to save all changes

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

5.14.3.1 SNMP Trap Configuration (Add or Reconfigure a Trap)

The user can create a new SNMP Trap or reconfigure an existing trap from this page. Open this page is by clicking the **Add New Entry** button on the Trap Configuration Page (see section 5.14 Security – Switch – SNMP – Trap on page 106).



SNMP Trap Configuration

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

SNMP Trap Event

System	□ * □ Warm Start	□ Cold Start
Interface	Link up ● none ○ specific ○ all switches □ * Link down ● none ○ specific ○ all switches LLDP ● none ○ specific ○ all switches	
AAA	□ * □ Authentication Fail	
Switch	□ * □ STP	□ RMON

Trap Config Name

Set a user defined name for the trap configuration. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126. (Existing trap names cannot be changed. To change a trap name, delete the trap and recreate it with a new name.)

Trap Mode

Set the SNMP trap mode operation:

Enabled: Enable SNMP trap mode operation

Disabled: Disable SNMP trap mode operation (This is the default mode.)

Trap Version

Show the SNMP trap supported version. Possible versions are:

SNMP v1: Set SNMP trap supported version 1

SNMP v2c: Set SNMP trap supported version 2c

SNMP v3: Set SNMP trap supported version 3

Trap Community

Set the community access string to be used when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126.

Trap Destination Address

Set the SNMP trap destination address. Requires a valid IP address in dotted decimal notation ('x.y.z.w')

Trap Destination Port

Set the SNMP trap destination port. The SNMP Agent will send an SNMP message via this port; the port range is 1 - 65535.

Trap Inform Mode

Set the SNMP trap inform mode operation:

Enabled: Enable SNMP trap inform mode operation

Disabled: Disable SNMP trap inform mode operation (This is the default mode.)

Trap Inform Timeout (seconds)

Set the SNMP trap inform timeout. The allowed range is 0 to 2147 seconds.

Trap Inform Retry Times

Set the SNMP trap inform retry times. The allowed range is 0 to 255.

Trap Probe Security Engine ID

Set the SNMP trap probe security engine ID mode of operation:

Enabled: Enable SNMP trap probe security engine ID mode of operation (This is the default mode.)

Disabled: Disable SNMP trap probe security engine ID mode of operation

Applicable Only to SNMP version: SNMPv3

Trap Security Engine ID

Set the SNMP trap security engine ID.

SNMPv3 sends traps information using USM protocol for authentication and privacy. A unique engine ID for these traps and informs is required. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

Applicable Only to SNMP version: SNMPv3

Trap Security Name

Set the SNMP trap security name.

SNMPv3 sends traps information using USM protocol for authentication and privacy. A unique security name is needed when traps and informs are enabled.

Applicable Only to SNMP version: SNMPv3

5.14.3.2 SNMP Trap Event (Add or Reconfigure a Trap)

☐ The first check box in each row of the table can be used to enable or disable all options in that row at the same time.

System

Enable/disable the interface group's traps. Possible traps are:

- Warm Start
- Cold Start

☑ Enable the specified Start Trap

☐ Disable the specified Start Trap (This is the default.)

The two traps may be enabled at the same time.

Interface

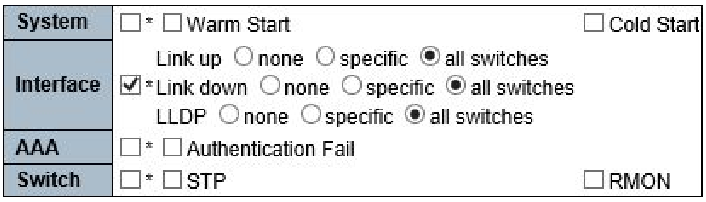
Enable/disable the SNMP entity's ability to generate authentication failure traps.

☑ Enable SNMP entity's ability

☐ Disable SNMP entity's ability (This is the default.)

When the interface is enabled all failure traps are enabled. Possible modes are:

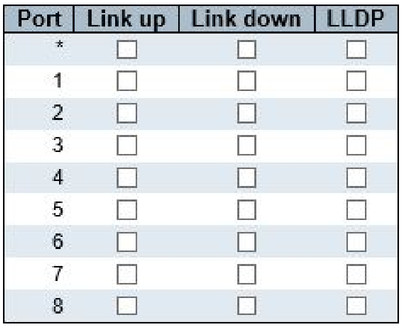
- **Link Up:** Enable/disable Link up trap
- **Link Down:** Enable/disable Link down trap
- **LLDP:** Enable/disable LLDP trap



System	☐ * ☐ Warm Start ☐ Cold Start
Interface	Link up ○ none ○ specific ● all switches ☑ * Link down ○ none ○ specific ● all switches LLDP ○ none ○ specific ● all switches
AAA	☐ * ☐ Authentication Fail
Switch	☐ * ☐ STP ☐ RMON

After the Interface is enabled the user can configure each trap type separately:

- **None:** Disable this trap
- **Specific:** Enable this trap only for specific ports (a table opens, see the table below)
- **All switches:** Enable this trap for all switches (This is the default mode.)



Port	Link up	Link down	LLDP
*	□	□	□
1	□	□	□
2	□	□	□
3	□	□	□
4	□	□	□
5	□	□	□
6	□	□	□
7	□	□	□
8	□	□	□

AAA

Set or show the AAA group's traps. Possible traps are:

- Authentication Fail

☑ Enable SNMP trap authentication failure trap

□ Disable SNMP trap authentication failure trap (This is the default.)

Switch

Set or show the Switch group's traps. Possible traps are:

- STP
- RMON

☑ Enable the specified Switch group Trap

□ Disable the specified Switch group Trap (This is the default.)

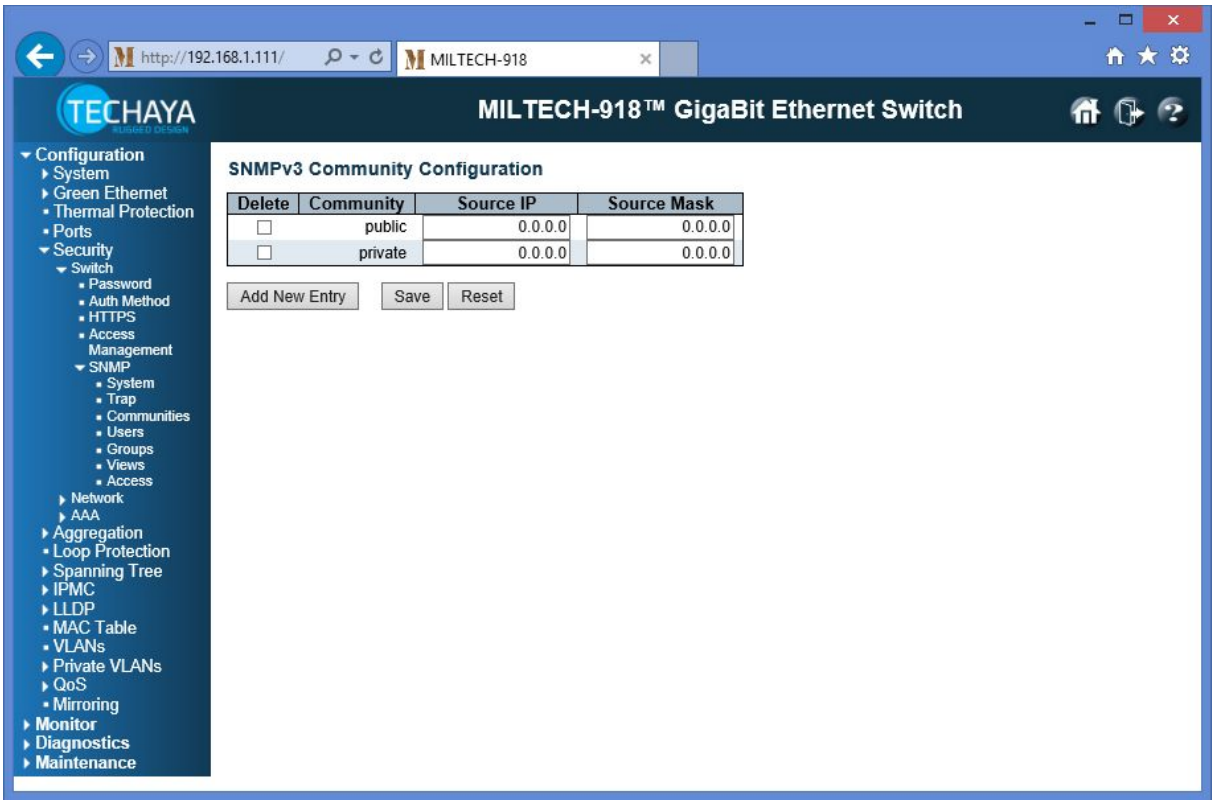
5.14.3.3 SNMP Trap Configuration Buttons

Save: Click to save all changes

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

5.15 Security – Switch – SNMP – Communities

The user can configure SNMPv3 from this page. The entry index key is Community.



SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
□	public	0.0.0.0	0.0.0.0
□	private	0.0.0.0	0.0.0.0

5.15.1 SNMPv3 Community Configuration

The SNMPv3 Community Configuration page has the following parameters:

Delete

☑ Check to delete the entry. It will be deleted during the next save.

□ Do not delete the entry. (This is the default.)

Community

Set or show the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.

Source IP

Set or show 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

Set or show the SNMP access source address mask.

5.15.2 Community Configuration Buttons

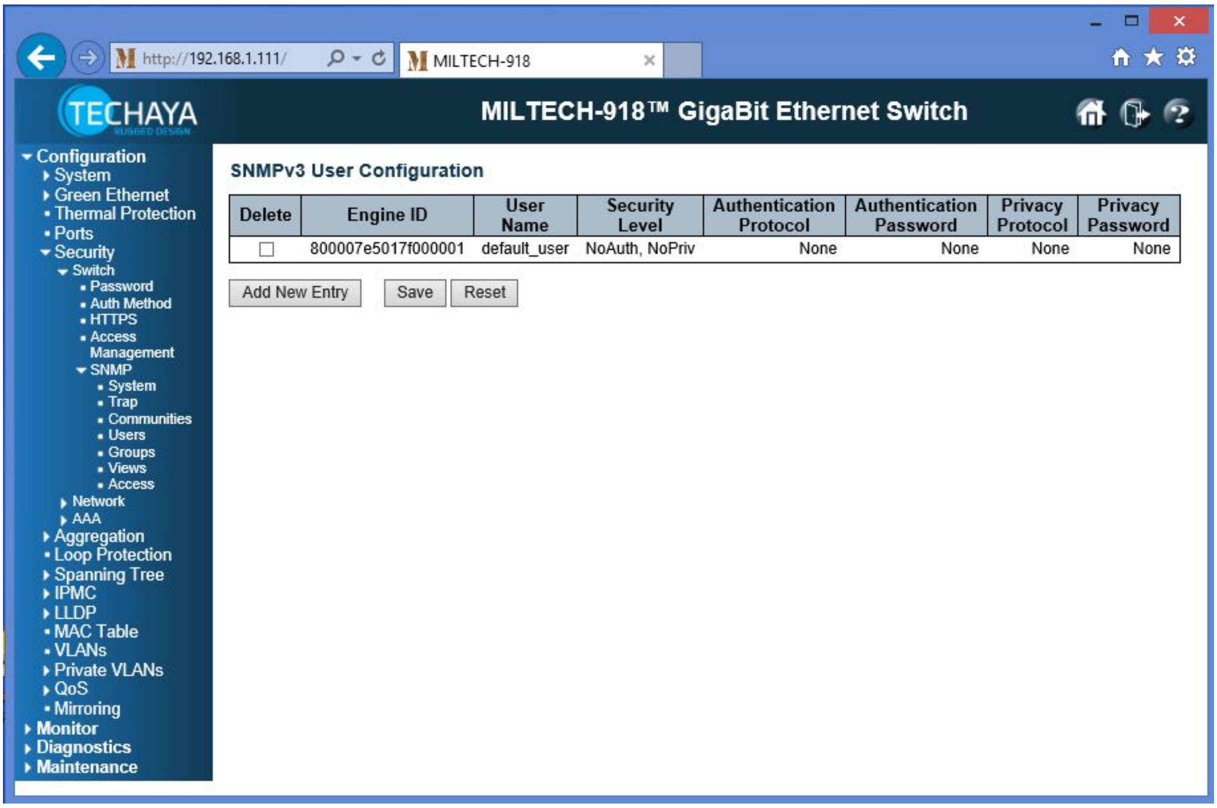
Add New Entry:
Click to add a new community configuration

Save: Click to save all changes

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

5.16 Security – Switch – SNMP – Users

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



SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
□	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

Add New Entry | Save | Reset

5.16.1 SNMPv3 User Configuration

The SNMPv3 User Configuration Page has the following parameters:

Delete

☑ Check to delete the entry. It will be deleted during the next save.

□ Do not delete the entry. (This is the default.)

Engine ID

An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. If the user engine ID equals the system engine ID then it is local user; otherwise it's remote user.

User Name

A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Level

Set or show the security level that this entry should belong to. Possible security models are:

- NoAuth, NoPriv: No authentication and no privacy
- Auth, NoPriv: Authentication and no privacy
- Auth, Priv: Authentication and privacy

The value of security level cannot be modified if entry already exists. Use care to ensure that the value is set correctly (otherwise the user will need to delete and recreate the entry in order to reset the security level).

Authentication Protocol

Set or show the authentication protocol that this entry should belong to. Possible authentication protocols are:

- None: No authentication protocol
- MD5: An optional flag to indicate that this user uses MD5 authentication protocol
- SHA: An optional flag to indicate that this user uses SHA authentication protocol

The value of security level cannot be modified if entry already exists. Use care to ensure that the value is set correctly (otherwise the user will need to delete and recreate the entry in order to reset the security level).

Authentication Password

Set or show the string identifying the authentication password phrase. Allowed string length depends on the authentication protocol:

- MD5: string length 8 to 32 characters
- SHA: string length 8 to 40 characters

The allowed content is ASCII characters from 33 to 126.

Privacy Protocol

Set or show the privacy protocol that this entry should belong to. Possible privacy protocols are:

- None: No privacy protocol
- DES: An optional flag to indicate that this user uses DES authentication protocol

- AES: An optional flag to indicate that this user uses AES authentication protocol.

Privacy Password

Set or show the 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.

5.16.2 User Configuration Buttons

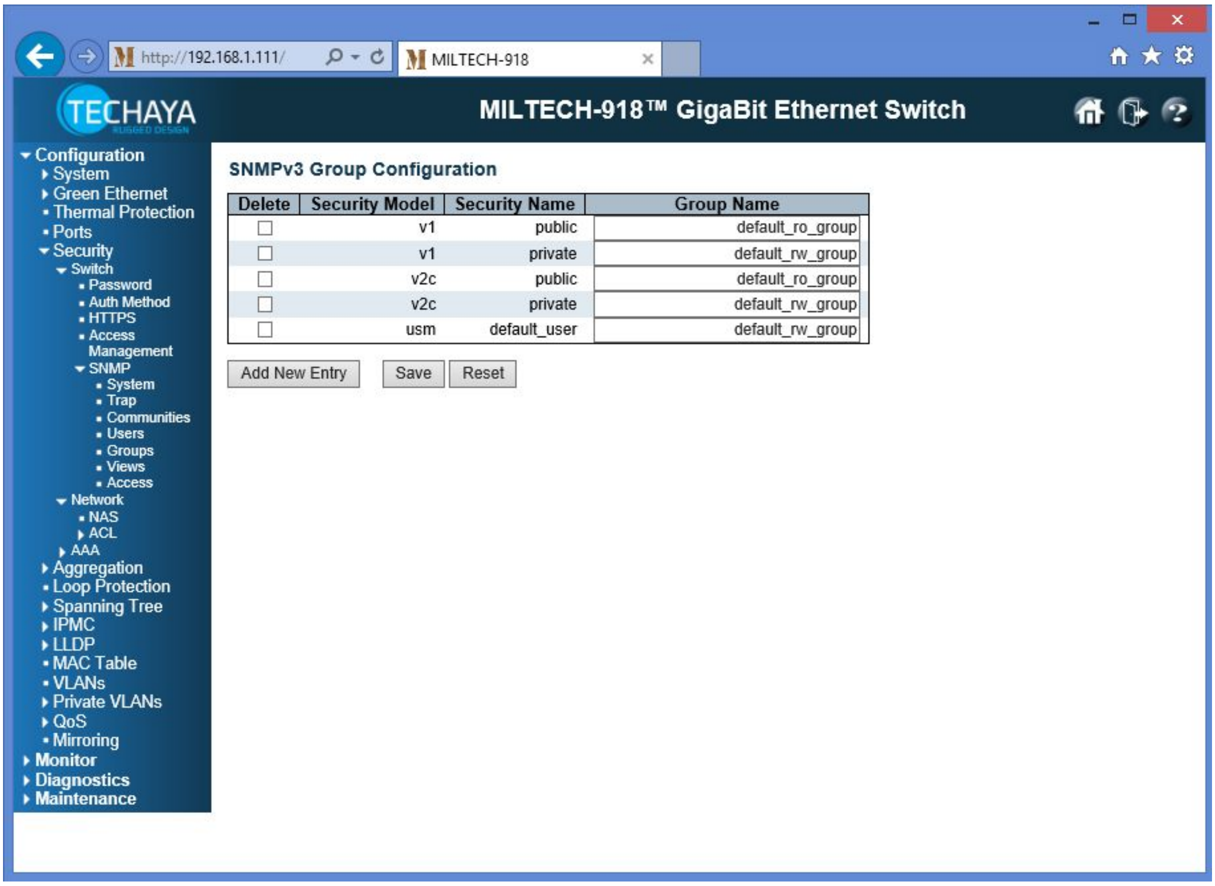
Add New Entry:
Click to add a new user configuration

Save: Click to save all changes

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

5.17 Security – Switch – SNMP – Groups

The user can configure the SNMPv3 group table on this page. The entry index keys are Security Model and Security Name.



SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
□	v1	public	default_ro_group
□	v1	private	default_rw_group
□	v2c	public	default_ro_group
□	v2c	private	default_rw_group
□	usm	default_user	default_rw_group

5.17.1 SNMPv3 Group Configuration

The SNMPv3 Group Configuration Page has the following parameters:

Delete

☑ Check to delete the entry. It will be deleted during the next save.

□ Do not delete the entry. (This is the default.)

Security Model

Set or show the security model that this entry should belong to. Possible security models are:

- v1: Reserved for SNMPv1
- v2c: Reserved for SNMPv2c
- usm: User-based Security Model (USM)

Security Name

A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Group Name

A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

5.17.2 Group Configuration Buttons

Add New Entry:

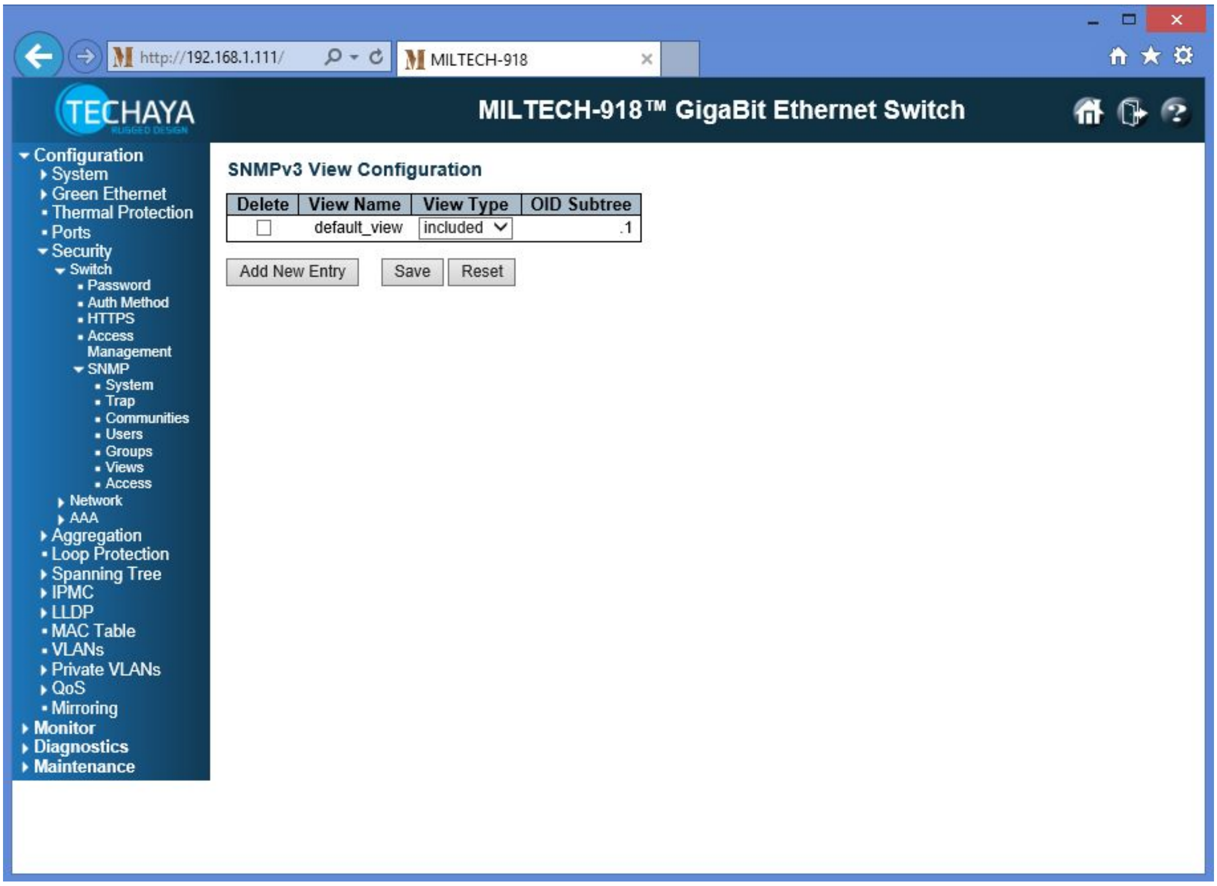
Click to add a new group configuration

Save: Click to save all changes

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

5.18 Security – Switch – SNMP – Views

The user can configure the SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.



SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
□	default_view	included	.1

5.18.1 SNMPv3 View Configuration

The SNMPv3 View Configuration Page has the following parameters:

Delete

☑ Check to delete the entry. It will be deleted during the next save.

□ Do not delete the entry. (This is the default.)

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

Set or show 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

If a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and its OID subtree should overstep the 'excluded' view entry.

OID Subtree

Set or show 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 (*).

5.18.2 View Configuration Buttons

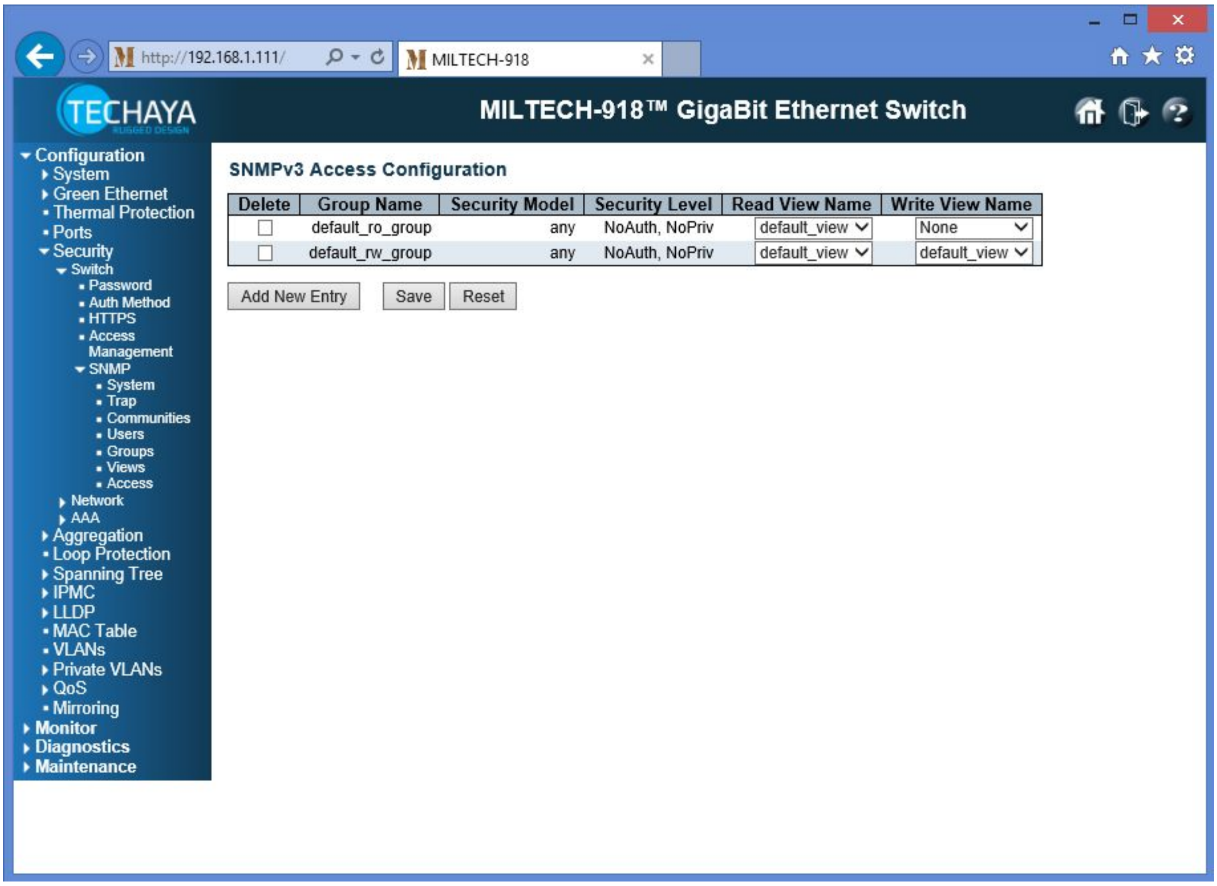
Add New Entry:
Click to add a new view configuration

Save: Click to save all changes

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

5.19 Security – Switch – SNMP – Access

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



SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	default_ro_group	any	NoAuth, NoPriv	default_view	None
□	default_rw_group	any	NoAuth, NoPriv	default_view	default_view

5.19.1 SNMPv3 Access Configuration

The SNMPv3 Access Configuration Page has the following parameters:

Delete

☑ Check to delete the entry. It will be deleted during the next save.

□ Do not delete the entry. (This is the default.)

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

Set or show 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

Set or show the security level 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

Set or show 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

Set or sow 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.

5.19.2 Access Configuration Buttons

Add New Entry: Click to add a new access configuration

Save: Click to save all changes

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

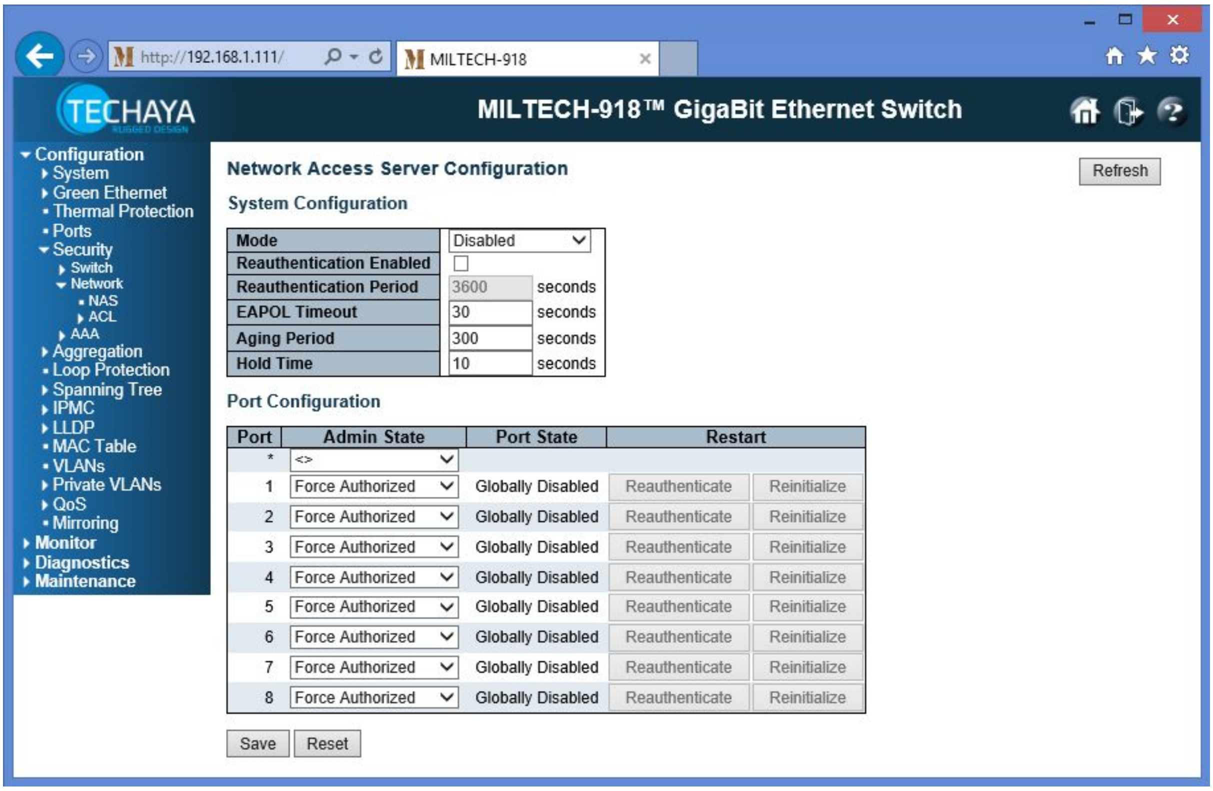
5.20 Security – Network – NAS

This page allows the user 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 and 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 (see section 5.24 Security – AAA – Radius on page 152). The IEEE 802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

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

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



Network Access Server Configuration

System Configuration

Mode	Disabled	
Reauthentication Enabled	□	
Reauthentication Period	3600	seconds
EAPOL Timeout	30	seconds
Aging Period	300	seconds
Hold Time	10	seconds

Port Configuration

Port	Admin State	Port State	Restart	
*	<>			
1	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize

5.20.1 System Configuration

Set or show the NAS system configuration parameters.

Mode

Set or show the NAS mode:

Enabled: NAS is globally enabled on the switchstack

Disabled: NAS is globally disabled on the switchstack (This is the default mode.)

If globally disabled, all ports are allowed forwarding of frames.

Reauthentication Enabled

Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn’t imply that a client is still present on a port (see Aging Period below).

☑ Successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period

□ Supplicants/clients are not reauthenticated (This is the default.)

Reauthentication Period

Set or show 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

Set or show the time for retransmission of Request Identity EAPOL frames.

Valid values are in the range 1 to 65535 seconds. This has no effect on MAC-based ports.

Aging Period

The Port Security module frees resources if no activity within a given period of time. The Aging Period parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.

This setting applies to 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 checks the specified MAC address at regular intervals, to see if there is activity.

If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.

For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

Hold Time

The Hold Time can be set to a number between 10 and 1000000 seconds.

This setting applies to the following modes, i.e. 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 (see section 5.24 Security – AAA – Radius on page 152) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.

The switch will ignore new frames coming from the client during the hold time.

5.20.2 Port Configuration

The table has one row for each port on the switch in the stack and a number of columns:

Port

Set or show the logical port for the settings contained in the same row.

Admin State

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

- Force Authorized:
  In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.
- Force Unauthorized:
  In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.
- 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. 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. (For a more detailed discussion of the Port-based 802.1X Admin State, see the online help.)

- 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.
  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. . (For a more detailed discussion of the MAC-based authentication Admin State, see the online help.)

Port State

Set or show 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.

Restart

Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port’s Admin State is in an EAPOL based or MAC based mode.

Clicking these buttons will not cause settings changed on the page to take effect.

- Reauthenticate:
  Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.
  The button only has effect for successfully authenticated clients on the port and will 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 will transfer to the unauthorized state while the reauthentication is in progress.

5.20.3 NAS Configuration Buttons

Refresh: Click to refresh the page

Save: Click to save all changes

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

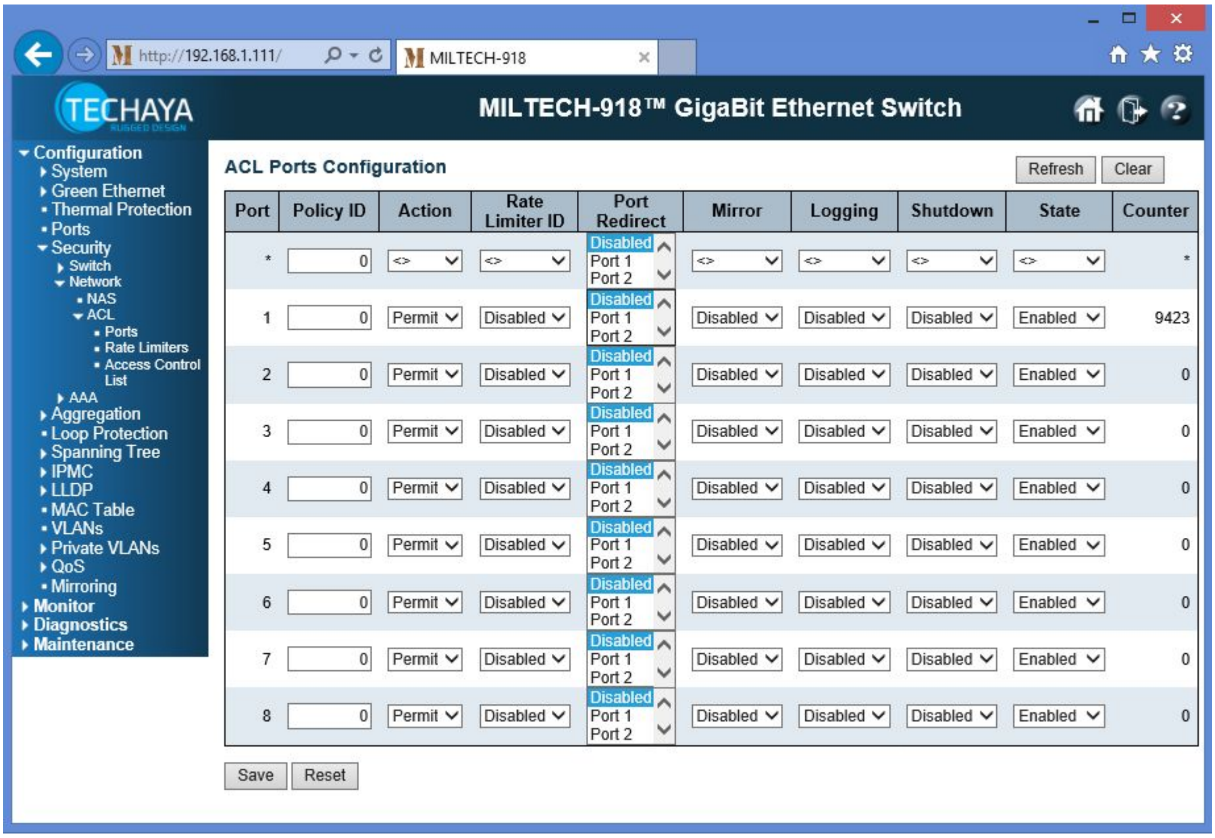
5.21 Security – Network – ACL – Ports

ACL is an acronym for Access Control List. It is the list table of ACEs (Access Control Entries), 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.

5.21.1 ACL Ports Configuration

This page allows the user to configure the ACL Ports parameters (Access Control Entry - ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.



ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	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	9423
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
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

Port

Show the logical port for the settings contained in the same row.

Policy ID

Set or show the policy to apply to this port. The allowed values are 0 through 255. The default value is 0.

Action

Set or show the forwarding status of the port:

Permit: Forwarding is permitted (The default value is "Permit".)

Deny: Forwarding is denied

Rate Limiter ID

Set or show the rate limiter to apply on this port. The Rate Limiter can be Disabled or set to a value from 1 through 16. The default value is "Disabled".

Port Redirect

Set or show which port frames are redirected on. The Port Redirect can be Disabled or set to a specific port number. It cannot be set when "Action" is permitted. The default value is "Disabled".

Mirror

Set or show the mirror operation of this port:

Enabled: Frames received on the port are mirrored

Disabled: Frames received on the port are not mirrored

The default value is "Disabled".

Logging

Set or show the logging operation of this port:

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 message does not include the 4 bytes CRC.
> - The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.

Shutdown

Set or show the port shut down operation of this port:

Enabled: If a frame is received on the port, the port will be disabled

Disabled: Port shut down is disabled (The default value is "Disabled".)

> **Note:** The shutdown feature only works when the packet length is less than 1518(without VLAN tags).

State

Set or show the port state of this port.

Enabled: To reopen ports by changing the volatile port configuration of the ACL user module (The default value is "Enabled".)

Disabled: To close ports by changing the volatile port configuration of the ACL user module

Counter

The Counter counts the number of frames that match this ACE.

5.21.2 ACL Ports Configuration Buttons

Refresh: Click to refresh the page, any changes made locally will be undone

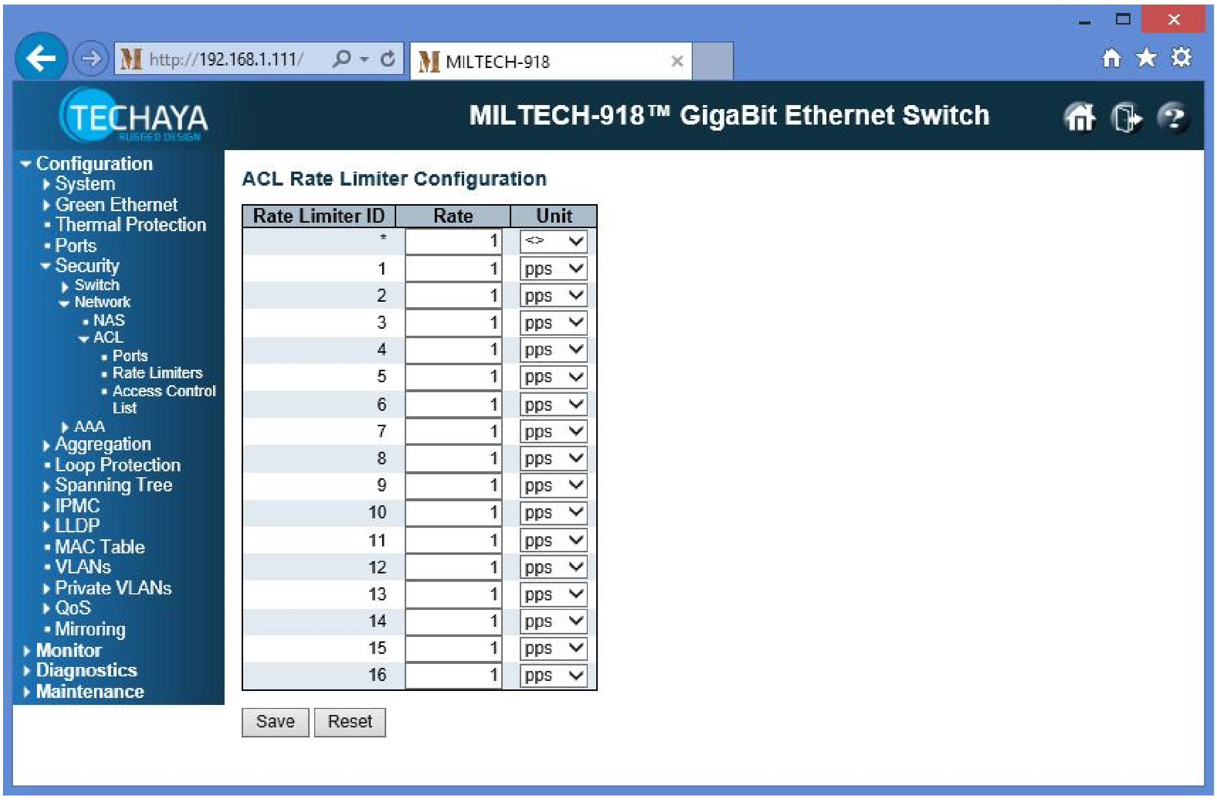
Clear: Click to clear the counters

Save: Click to save all changes

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

5.22 Security – Network – ACL – Rate Limiters

This page allows the user to configure the rate limiter for the ACL of the switch.



ACL Rate Limiter Configuration

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

5.22.1 ACL Rate Limiter Configuration

The ACL Rate Limiter Configuration Page has the following parameters:

Rate Limiter ID

Shows the Rate Limiter ID for the settings contained in the same row.

Rate

The rate range is located 0-3276700 in pps.

- The valid rate is 0 - -1, 0, 0, 0, ..., 3276700 in pps

Or

- 0, 100, 200, 300, ..., 1000000 in kbps

Unit

Set or show the rate unit:

pps:	packets per second
kbps:	Kbits per second

5.22.2 ACL Rate Limiter Configuration Buttons

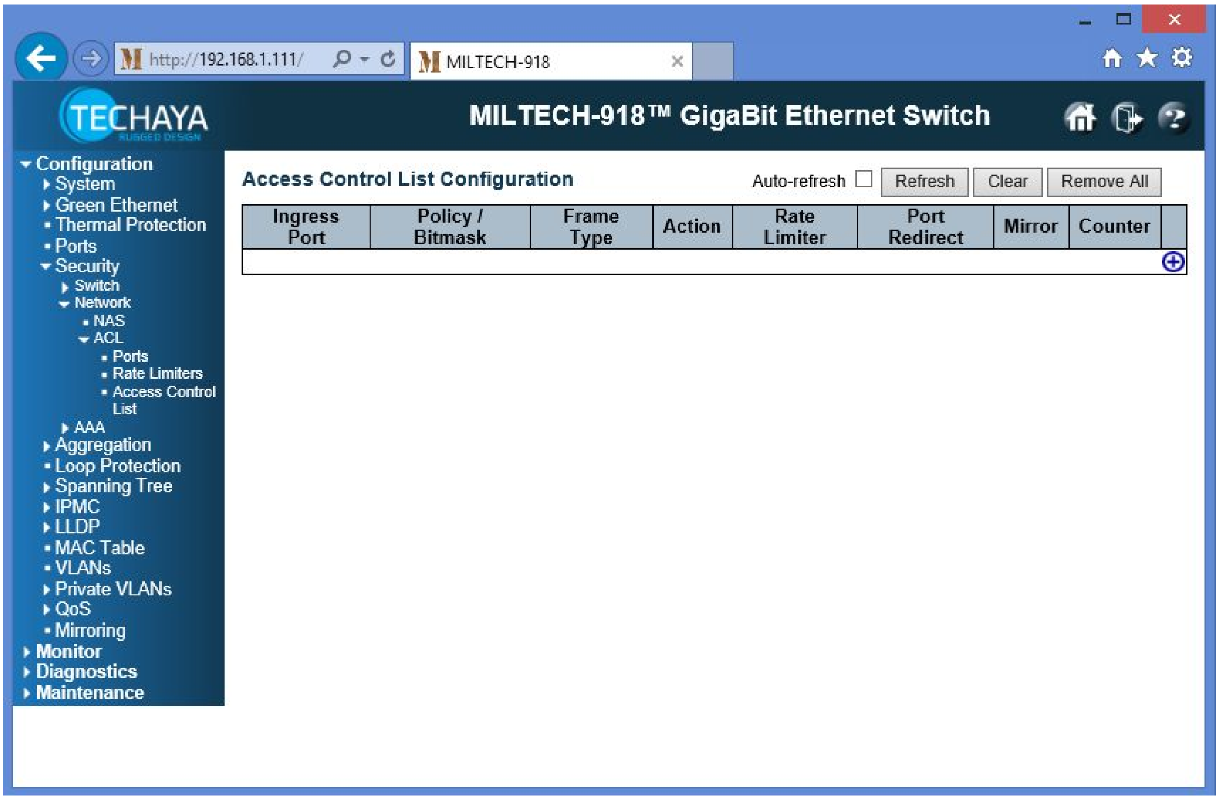
Save: Click to save all changes

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

5.23 Security – Network – ACL – Access Control List

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

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



Access Control List Configuration

Auto-refresh □ Refresh Clear Remove All

Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
								⊕

5.23.1 Access Control List Configuration

The ACL Access Control List Configuration Page has the following parameters:

Ingress Report

Display the ingress port of the ACE:

All: The ACE will match all ingress ports

Port: The ACE will match a specific ingress port

Policy/Bitmask

Display the policy number and bitmask of the ACE.

Frame Type

Display the frame type of the ACE:

Any: The ACE will match any frame type

EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames

ARP: The ACE will match ARP/RARP frames

IPv4: The ACE will match all IPv4 frames

IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol

IPv4/UDP: The ACE will match IPv4 frames with UDP protocol

IPv4/TCP: The ACE will match IPv4 frames with TCP protocol

IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP

IPv6: The ACE will match all IPv6 standard frames

Action

Display 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

Display the rate limiter number of the ACE.

The Rate Limiter can be Disabled or set to a value from 1 through 16. The default value is “Disabled”.

Port Redirect

Display the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number.

The port redirect operation can be Disabled or set to a specific port number. The default value is “Disabled”.

Mirror

Display the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port:

Enabled: Frames received on the port are mirrored

Disabled: Frames received on the port are not mirrored (The default value is “Disabled”.)

Counter

The counter indicates the number of times the ACE was hit by a frame.

Modification Buttons

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

⊕: 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

5.23.2 Access Control List Configuration Buttons

□ Auto-refresh – Click this box to refresh the page automatically (every three seconds)

Refresh: Click to refresh the page, any changes made locally will be undone

Clear: Click to clear the counters

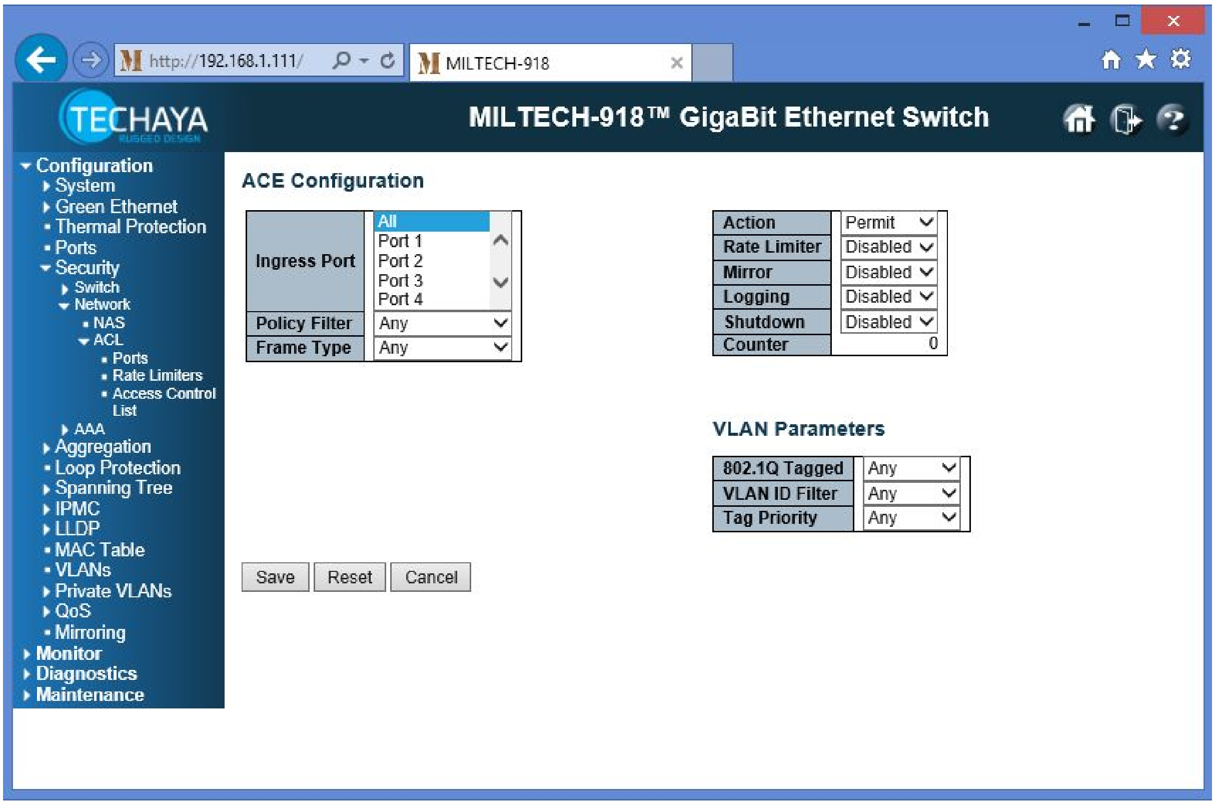
Remove All: Click to remove all ACEs

5.23.2.1 ACE Configuration

This page allows the user to configure an Access Control Entry (ACE). Open this page by clicking add (⊕) or edit (ⓔ) from the Access Control List Configuration table (see section 5.23 above).

An ACE consists of several parameters. These parameters vary according to the frame type that the user selects. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected.

A frame that hits this ACE matches the configuration that is defined here.



ACE Configuration

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

Action	Permit
Rate Limiter	Disabled
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Ingress Report

Set or show the ingress port for which this ACE applies:

All: The ACE applies to all port

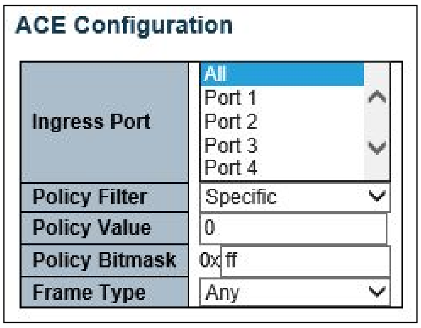
Port n: The ACE applies to this port number, where n is the number of the switch port.

Policy Filter

Set or show the policy number filter for this ACE.

Any: No policy filter is specified. (policy filter status is "don't-care".)

Specific: Filter a specific policy with this ACE. Two fields for entering a Policy Value and Policy Bitmask appear.



ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Specific
Policy Value	0
Policy Bitmask	0x ff
Frame Type	Any

Policy Value

Displayed only when Policy Filter = Specific.

The user can enter a specific policy value. The allowed range is 0 to 255.

Policy Bitmask

Displayed only when Policy Filter = Specific.

The user can enter a specific policy bitmask. The allowed range is 0x0 to 0xff.

> **Note:** 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 and 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

Set or show 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.

> **Note:** The ARP frames won't match the ACE with Ethernet type.

IPv4: Only IPv4 frames can match this ACE.

> **Note:** The IPv4 frames won't match the ACE with Ethernet type.

IPv6: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.

Action

Set or show 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

Set or show 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

Set or show the destination port number. Frames that hit the ACE are redirected to the port number specified here.

The rate limiter will affect these ports. The allowable values for port redirect are:

- “Disabled”
- A valid port number

When the Port Redirect is “Disabled the Port Redirect operation is disabled and the specific port number of ‘Port Redirect’ cannot be set when the action is permitted.

Mirror

Set or show the mirror operation of this port.

Enabled: Frames received on the port are mirrored

Disabled: Frames received on the port are not mirrored (The default value is “Disabled”.)

Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port.

Logging

Set or show the logging operation of the ACE:

Enabled: Frames matching the ACE are stored in the System Log

Disabled: Frames matching the ACE are not logged**.**

> **Note:**
>
> - The logging message doesn’t include the 4 bytes CRC information.
> - The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.

Shutdown

Set or show the port shut down operation of the ACE:

Enabled: If a frame matches the ACE, the ingress port will be disabled

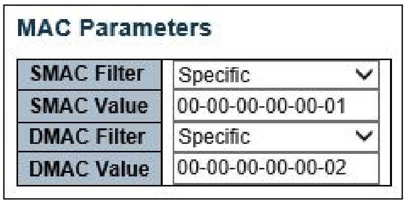
Disabled: Port shut down is disabled for the ACE

> **Note:** The shutdown feature only works when the packet length is less than 1518(without VLAN tags).

Counter

The counter indicates the number of times the ACE was hit by a frame.

5.23.2.2 MAC Parameters



MAC Parameters

SMAC Filter	Specific
SMAC Value	00-00-00-00-00-01
DMAC Filter	Specific
DMAC Value	00-00-00-00-00-02

SMAC Filter

SMAC Filter is displayed only when the Frame Type is Ethernet Type or ARP.

Set or show the source MAC filter for this ACE.

Any:	No SMAC filter is specified (SMAC filter status is "don't care".)
Specific:	Filter a specific source MAC address with this ACE. A field for entering a SMAC value appears.

SMAC Value

When "Specific" is selected for the SMAC filter, the user can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.

DMAC Filter

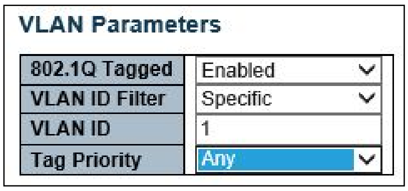
Set or show the destination MAC filter for this ACE.

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:	Filter a specific destination MAC address with this ACE. A field for entering a DMAC value appears.

DMAC Value

When "Specific" is selected for the DMAC filter, the user 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.

5.23.2.3 VLAN Parameters



VLAN Parameters

802.1Q Tagged	Enabled
VLAN ID Filter	Specific
VLAN ID	1
Tag Priority	Any

802.1Q tagged

Set or show 802.1Q Tagged operation status. The status determines whether or not frames can hit the action according to the 802.1Q Tagged:

Any: Any value is allowed ("don't care") (The default value is "Any".)

Enabled: Tagged frame only

Disabled: Untagged frame only

VLAN ID Filter

Set or show the VLAN ID filter for this ACE.

Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't care".)

Specific: Filter a specific VLAN ID with this ACE. A field for entering a VLAN ID number appears.

VLAN ID

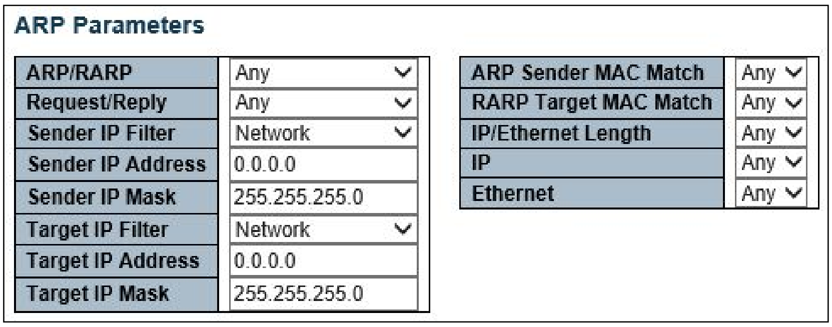
When "Specific" is selected for the VLAN ID filter, the user can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.

Tag priority

Set or show 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".)

5.23.2.4 ARP Parameters

The ARP parameters can be configured when Frame Type “ARP” is selected.



ARP Parameters

ARP/RARP	Any
Request/Reply	Any
Sender IP Filter	Network
Sender IP Address	0.0.0.0
Sender IP Mask	255.255.255.0
Target IP Filter	Network
Target IP Address	0.0.0.0
Target IP Mask	255.255.255.0

ARP Sender MAC Match	Any
RARP Target MAC Match	Any
IP/Ethernet Length	Any
IP	Any
Ethernet	Any

ARP/RARP

Set or show 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

Set or show 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

Send IP Filter

Set or show 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.

Send IP Address

When “Host” or “Network” is selected for the sender IP filter, the user can enter a specific sender IP address in dotted decimal notation.

Send IP Mask

When “Network” is selected for the sender IP filter, the user can enter a specific sender IP mask in dotted decimal notation.

Target IP Filter

Set or show 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, the user can enter a specific target IP address in dotted decimal notation.

Target IP Mask

When "Network" is selected for the target IP filter, the user 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: Not a Match

ARP frames where SHA is **not** equal to the SMAC address

1: Match

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: Not a Match

RARP frames where THA is **not** equal to the target MAC address

1: Match

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: Not a Match

ARP/RARP frames where the HLN is **not** equal to Ethernet (0x06) or the (PLN) is **not** equal to IPv4 (0x04)

1: Match

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: Not a Match

ARP/RARP frames where the HLD is **not** equal to Ethernet (1)

1: Match

ARP/RARP frames where the HLD is equal to Ethernet (1)

Any: Any value is allowed (“don’t-care”)

Ethernet

Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.

0: Not a Match

ARP/RARP frames where the PRO is **not** equal to IP (0x800)

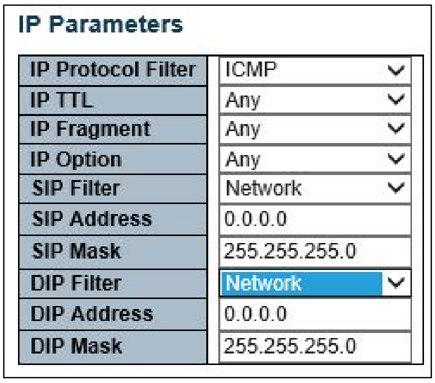
1: Match

ARP/RARP frames where the PRO is equal to IP (0x800)

Any: Any value is allowed (“don’t-care”)

5.23.2.5 IP Parameters

The IP parameters can be configured when Frame Type “IPv4” is selected.



IP Parameters

IP Protocol Filter	ICMP
IP TTL	Any
IP Fragment	Any
IP Option	Any
SIP Filter	Network
SIP Address	0.0.0.0
SIP Mask	255.255.255.0
DIP Filter	Network
DIP Address	0.0.0.0
DIP Mask	255.255.255.0

IP Protocol Filter

Set or show the IP protocol filter for this ACE.

Any: No IP protocol filter is specified (“don’t care”)

Specific: Filter a specific IP protocol filter with this ACE. 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, the user 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

Set or show 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

Set or show 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

Set or show 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

Set or show 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.

SIP Address

When “Host” or “Network” is selected for the source IP filter, the user can enter a specific SIP address in dotted decimal notation.

SIP Mask

When “Network” is selected for the source IP filter, the user can enter a specific SIP mask in dotted decimal notation.

DIP Filter

Set or show 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

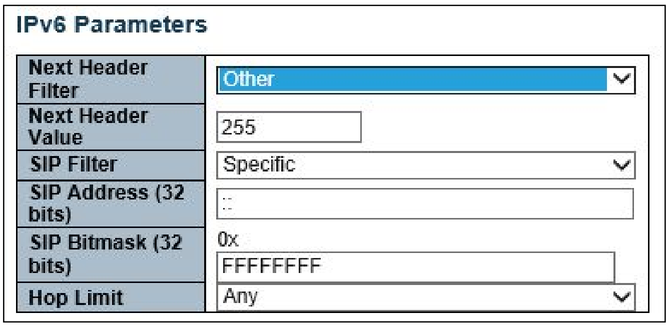
When “Host” or “Network” is selected for the destination IP filter, the user can enter a specific DIP address in dotted decimal notation.

DIP Mask

When “Network” is selected for the destination IP filter, the user can enter a specific DIP mask in dotted decimal notation.

5.23.2.6 IPv6 Parameters

The IPv6 parameters can be configured when Frame Type “IPv6” is selected.



IPv6 Parameters

Next Header Filter	Other
Next Header Value	255
SIP Filter	Specific
SIP Address (32 bits)	::
SIP Bitmask (32 bits)	0x FFFFFFFF
Hop Limit	Any

Next Header Filter

Set or show the IPv6 next header filter for this ACE.

Any: No IPv6 next header filter is specified ("don't-care")

Specific: Filter a specific IPv6 next header filter with this ACE. A field for entering an IPv6 next header filter appears.

ICMP: Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.

UDP: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.

TCP: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.

Next Header Value

When "Other" is selected for the IPv6 Next Header Filter, the user 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

Set or show 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, the user 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, the user can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address.

> **Note:** 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 and 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.

Hop Limit

Set or show the hop limit settings for this ACE.

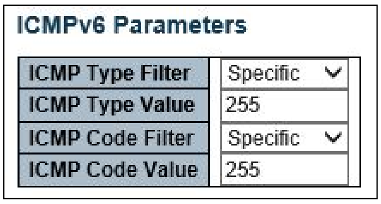
zero: IPv6 frames with a hop limit field greater than zero must **not** be able to match this entry

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”).

5.23.2.7 ICMPV6 Parameters

The ICMPV6 parameters can be configured when the Frame Type is “IPv6” and the Next Header Filter is “ICMP”.



ICMPv6 Parameters

ICMP Type Filter	Specific
ICMP Type Value	255
ICMP Code Filter	Specific
ICMP Code Value	255

ICMP Type Filter

Set or show the ICMP filter for this ACE.

Any: No ICMP filter is specified (ICMP filter status is “don’t care”)

Specific: To filter a specific ICMP filter with this ACE, the user can enter a specific ICMP value. A field for entering an ICMP value appears.

ICMP Type Value

When “Specific” is selected for the ICMP Type Filter, the user 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

Set or show the ICMP code filter for this ACE.

Any: No ICMP code filter is specified (ICMP code filter status is “don’t care”).

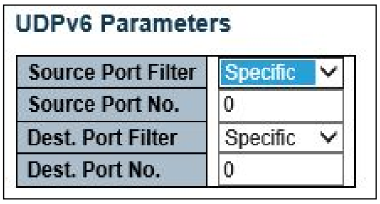
Specific: To filter a specific ICMP code filter with this ACE, the user can enter a specific ICMP code value. A field for entering an ICMP code value appears.

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.

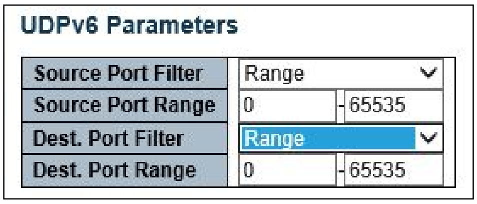
5.23.2.8 TCPv6/UDPv6 Parameters

The TCPv6/UDPv6 parameters can be configured when the Frame Type is “IPv6” and the Next Header Filter is “TCP” or “UDP”.



UDPv6 Parameters

Source Port Filter	Specific
Source Port No.	0
Dest. Port Filter	Specific
Dest. Port No.	0



UDPv6 Parameters

Source Port Filter	Range
Source Port Range	0 - 65535
Dest. Port Filter	Range
Dest. Port Range	0 - 65535

Source Filter: “Specific”

Destination Filter: “Specific”

Source Filter: “Range”

Destination Filter: “Range”

TCP/UDP Source Port Filter

Set or show 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: To filter a specific TCP/UDP source filter with this ACE, the user can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.

Range: To filter a specific TCP/UDP source range filter with this ACE, the user can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.

TCP/UDP Source Port Number

When “Specific” is selected for the TCP/UDP source filter, the user 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 Port Range

When “Range” is selected for the TCP/UDP source filter, the user 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 Port Filter

Set or show 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: To filter a specific TCP/UDP destination filter with this ACE, the user can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.

Range: To filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.

TCP/UDP Destination Port Number

When "Specific" is selected for the TCP/UDP destination filter, the user 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 Port Range

When "Range" is selected for the TCP/UDP destination filter, the user 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.

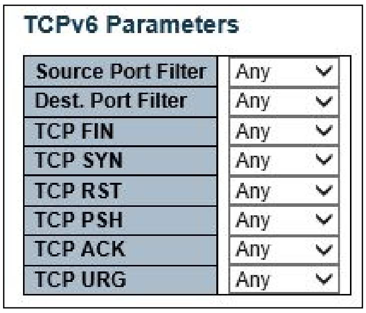
TCP FIN

Set or show 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")



TCPv6 Parameters

Source Port Filter	Any
Dest. Port Filter	Any
TCP FIN	Any
TCP SYN	Any
TCP RST	Any
TCP PSH	Any
TCP ACK	Any
TCP URG	Any

TCP SYN

Set or show 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

Set or show 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

Set or show 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

Set or show 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

Set or show the TCP "Urgent Pointer field significant" (URG) value for this ACE.

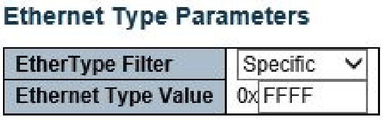
0: TCP frames where the URG field is set must **not** be able to match this entry

1: TCP frames where the URG field is set must be able to match this entry

Any: Any value is allowed ("don't care")

5.23.2.9 Ethernet Type Parameters

The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.



Ethernet Type Parameters

EtherType Filter	Specific
Ethernet Type Value	0x FFFF

EtherType Filter

Set or show the Ethernet type filter for this ACE.

Any: No EtherType filter is specified (EtherType filter status is "don't care")

Specific: To filter a specific EtherType filter with this ACE, the user can enter a specific EtherType value. A field for entering an EtherType value appears.

Ethernet Type Value

When “Specific” is selected for the EtherType filter, the user 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.

5.23.2.10 ACE Configuration Buttons

Save: Click to save all changes

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

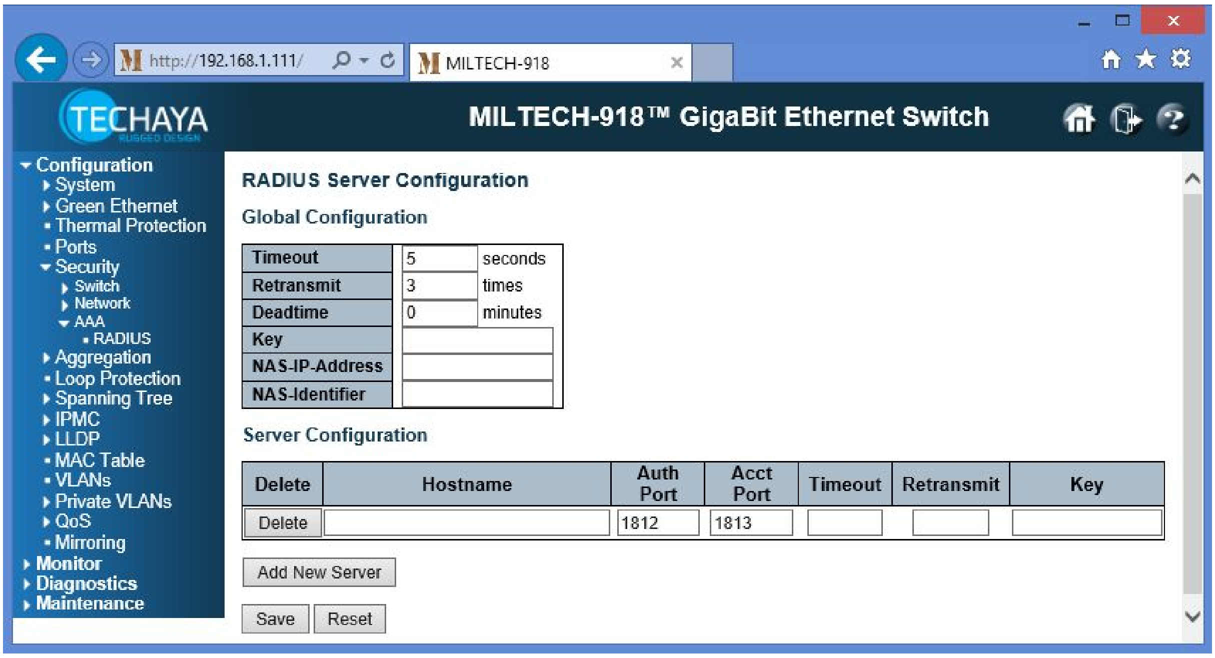
Cancel: Return to the previous page

5.24 Security – AAA – 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.

RADIUS Server Configuration

This page allows the user to configure RADIUS Server parameters.



RADIUS Server Configuration

Global Configuration

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

Server Configuration

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

Add New Server

Save Reset

5.24.1 Global Configuration

These setting are common for all of the RADIUS servers.

Timeout

Set or show the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.

Retransmit

Set or show 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

Set or show the period, a number between 0 to 1440 minutes, during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

Key

Set or show secret key - up to 63 characters long - shared between the RADIUS server and the switch.

NAS-IP-Address

IPv4 (Attribute 4)

Set or show 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.

IPv6 (Attribute 95)

Set or show 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)

Set or show the identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

5.24.2 Server Configuration

The table has one row for each RADIUS server and a number of columns, with the following parameters:

Delete

☑ Check to delete a RADIUS server entry. The entry will be deleted during the next save.

□ Do not delete the entry. (This is the default.)

Hostname

Set or show the IP address or hostname of the RADIUS server.

Auth Port

The UDP port to use on the RADIUS server for authentication.

Acct Port

Set or show the UDP port to use on the RADIUS server for accounting.

Timeout

Set or show this optional setting that overrides the global timeout value. Leaving it blank will use the global timeout value.

Retransmit

Set or show this optional setting that overrides the global retransmit value. Leaving it blank will use the global retransmit value.

Key

Set or show this optional setting that overrides the global key. Leaving it blank will use the global key.

5.24.3 RADIUS Server Configuration Buttons

Add New Server:

Click to add a new RADIUS Server entry. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported.

Delete: Click to undo the addition of the new server.

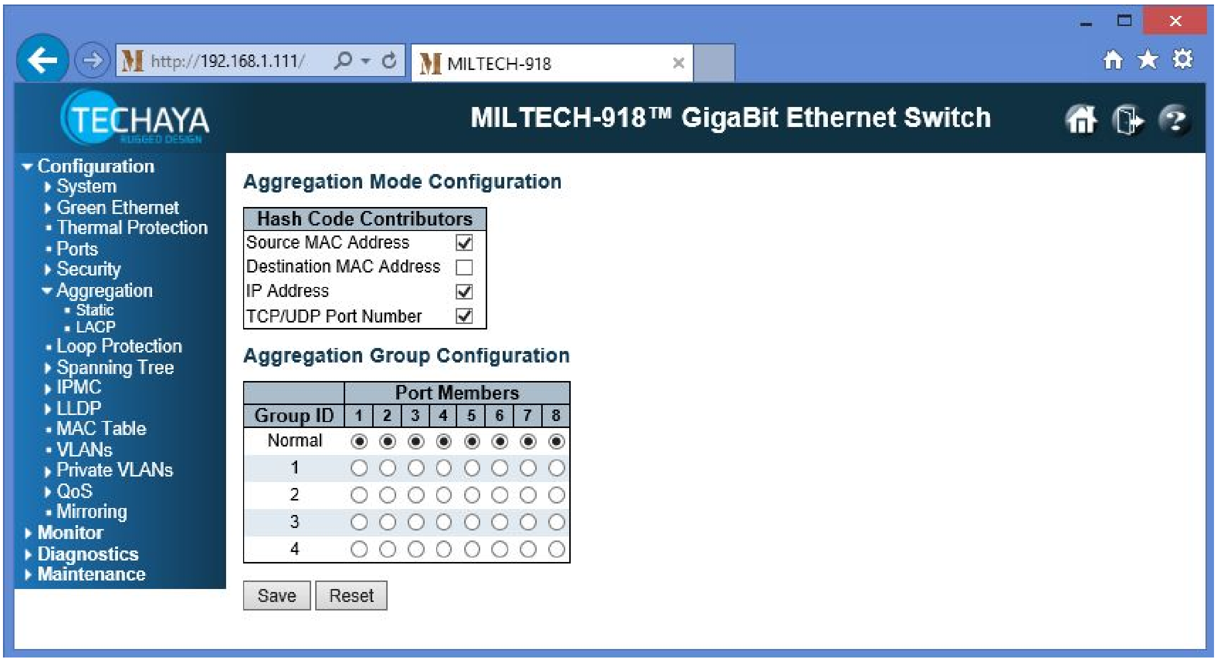
Save: Click to save all changes

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

5.25 Aggregation – Static

Aggregation mode uses multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

This page allows the user to configure Aggregation Mode parameters.



Aggregation Mode Configuration

Hash Code Contributors	
Source MAC Address	☑
Destination MAC Address	□
IP Address	☑
TCP/UDP Port Number	☑

Aggregation Group Configuration

	Port Members							
Group ID	1	2	3	4	5	6	7	8
Normal	●	●	●	●	●	●	●	●
1	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○

5.25.1 Aggregation Mode Configuration Hash Code Contributors

This section allows the user to configure Hash Code Contributors:

Source MAC Address

The Source MAC address can be used to calculate the destination port for the frame. By default, Source MAC Address is enabled.

☑ Check to enable the use of the Source MAC address (This is the default.)

□ Uncheck to disable the use of the Source MAC address

Destination MAC Address

The Destination MAC Address can be used to calculate the destination port for the frame. By default, Destination MAC Address is disabled.

☑ Check to enable the use of the Destination MAC Address

□ Uncheck to disable the use of the Destination MAC Address (This is the default.)

IP Address

The IP address can be used to calculate the destination port for the frame. By default, IP Address is enabled.

☑ Check to enable the use of the IP Address (This is the default.)

□ Uncheck to disable the use of the IP Address

TCP/UDP Port Number

The TCP/UDP port number can be used to calculate the destination port for the frame. By default, TCP/UDP Port Number is enabled.

☑ Check to enable the use of the TCP/UDP Port Number (This is the default.)

□ Uncheck to disable the use of the TCP/UDP Port Number

5.25.2 Aggregation Group Configuration

This section allows the user to configure aggregation groups.

Group ID

Set or show 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.

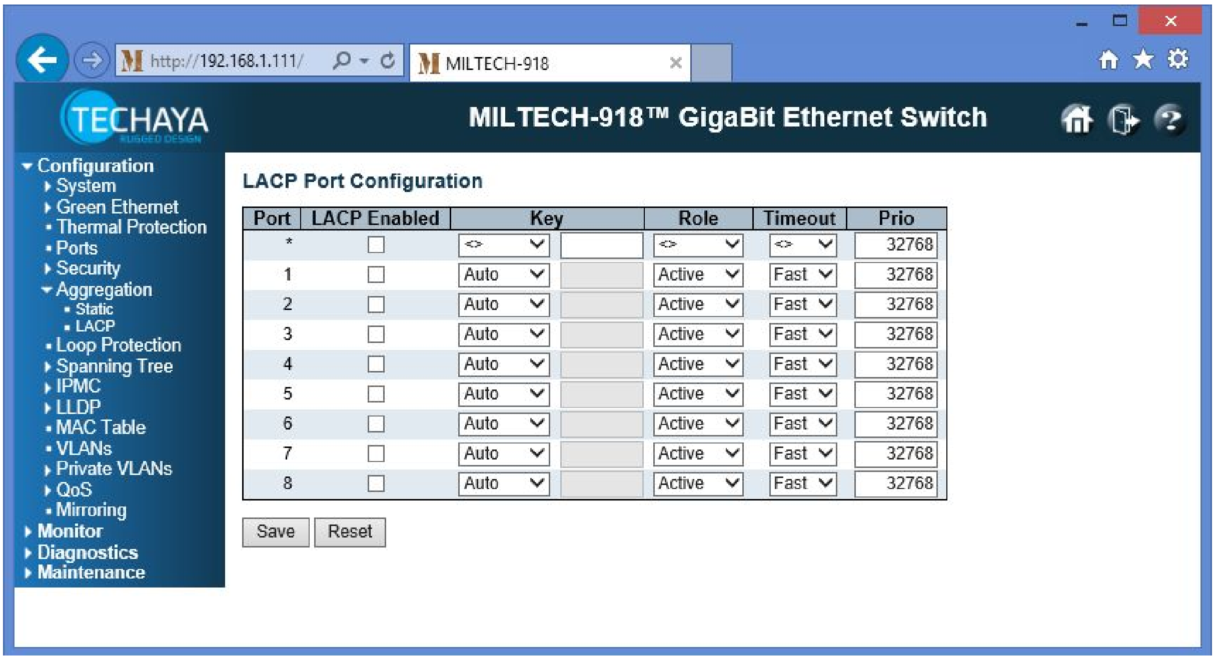
5.25.3 Aggregation Configuration Buttons

Save: Click to save all changes

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

5.26 Aggregation – 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.



LACP Port Configuration

Port	LACP Enabled	Key		Role	Timeout	Prio
*	☐	<>		<>	<>	32768
1	☐	Auto		Active	Fast	32768
2	☐	Auto		Active	Fast	32768
3	☐	Auto		Active	Fast	32768
4	☐	Auto		Active	Fast	32768
5	☐	Auto		Active	Fast	32768
6	☐	Auto		Active	Fast	32768
7	☐	Auto		Active	Fast	32768
8	☐	Auto		Active	Fast	32768

5.26.1 LACP Port Configuration

This page allows the user to inspect and change LACP Port configurations:

Port

This column displays the switch port number.

LACP Enabled

Set or show whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner.

☑ LACP is enabled on this switch port

☐ LACP is disabled on this switch port (This is the default.)

Up to 32 aggregations are supported (if stackable).

Key

Set or show the Key value incurred by the port, range 1-65535 . The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.

Role

Set or show the LACP activity status:

Active:	Transmit LACP packets each second
Passive	Wait for an LACP packet from a partner (speak if spoken to)

Timeout

Set or show the period between BPDU transmissions.

Fast	Transmit LACP packets each second
Slow	Wait for 30 seconds before sending a LACP packet

Prio

Set or show the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

5.26.2 LACP Port Configuration Buttons

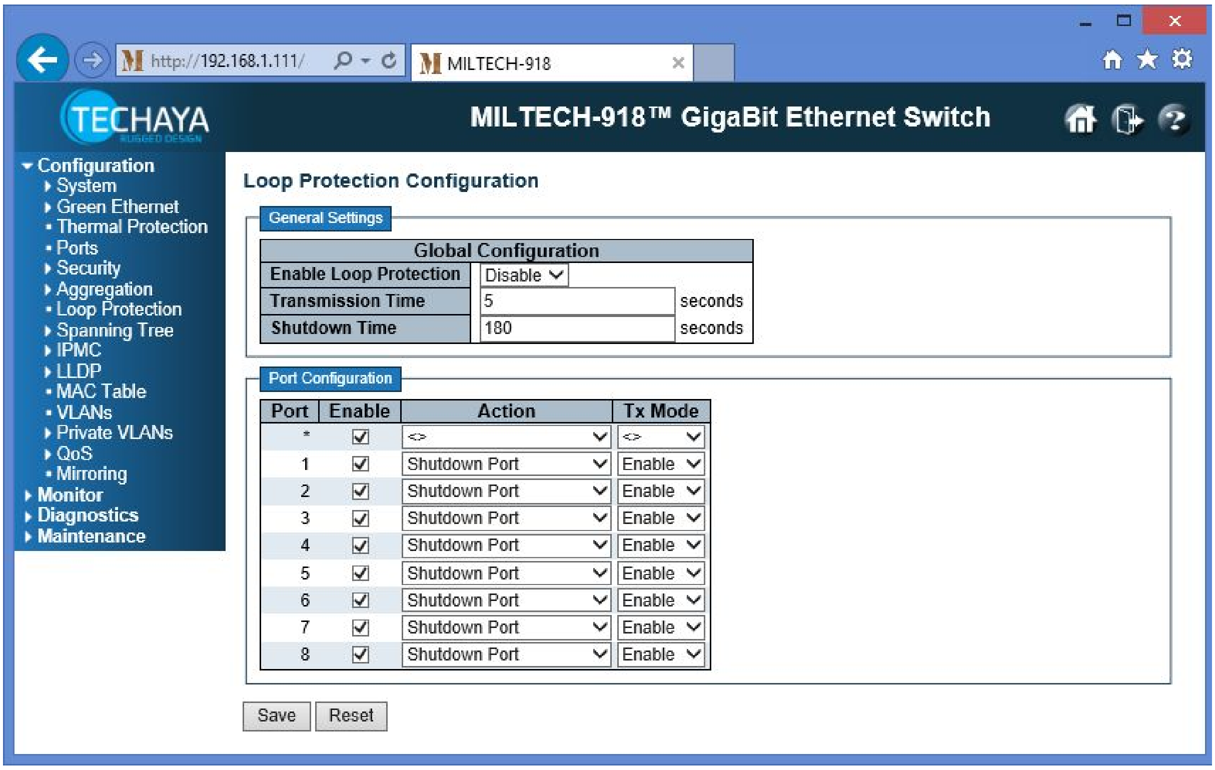
Save: Click to save all changes

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

5.27 Loop Protection (Configuration)

When loop protection is enabled, the spanning-tree topology detects root ports and blocked ports and makes sure both keep receiving BPDUs.

This page allows the user to inspect and change the Loop Protection Configuration.



Loop Protection Configuration

General Settings

Global Configuration		
Enable Loop Protection	Disable	
Transmission Time	5	seconds
Shutdown Time	180	seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	☑	<>	<>
1	☑	Shutdown Port	Enable
2	☑	Shutdown Port	Enable
3	☑	Shutdown Port	Enable
4	☑	Shutdown Port	Enable
5	☑	Shutdown Port	Enable
6	☑	Shutdown Port	Enable
7	☑	Shutdown Port	Enable
8	☑	Shutdown Port	Enable

5.27.1 General Settings

This section allows the user to configure the Global Configuration settings:

Enable Loop Protection

Set or show the global Loop Protection status:

Enabled: Loop Protection is enabled (globally)

Disabled: Loop Protection is disabled (globally)(This is the default.)

Transmission Time

Set or show the interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.

Shutdown Time

The period (in seconds) for which a port will be kept disabled in the event a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).

5.27.2 Port Configuration

Port

This column displays the switch port number.

Enable

Set or show whether Loop Protection is enabled on this switch port.

☑ Loop Protection is enabled on this switch port (This is the default.)

□ Loop Protection is disabled on this switch

Action

Set or show the action to perform when a loop is detected on a port. Valid values are:

- Shutdown Port
- Shutdown Port and Log
- Log Only.

Tx Mode

Set or show whether the port is actively generating loop protection PDUs

Enabled: Port is actively generating loop protection PDUs

Disabled: Port is passively looking for looped PDUs

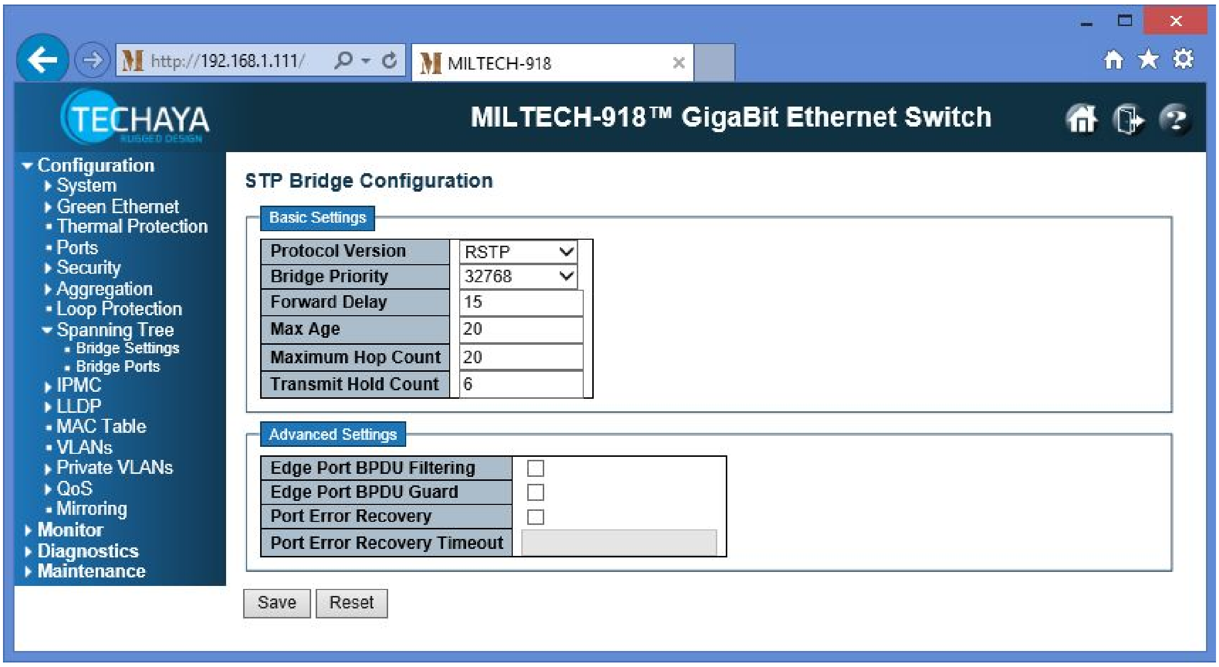
5.27.3 Loop Protection Configuration Buttons

Save: Click to save all changes

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

5.28 Spanning Tree – Bridge Settings

This page allows the user to configure Spanning Tree Protocol) STP system settings. The settings are used by all STP Bridge instances in the Switch.



STP Bridge Configuration

Basic Settings

Protocol Version	RSTP
Bridge Priority	32768
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	□
Edge Port BPDU Guard	□
Port Error Recovery	□
Port Error Recovery Timeout	

5.28.1 STP Bridge Configuration - Basic Settings

This section allows the user to configure the Bridge Configuration Basic settings:

Protocol Version

Set or show the MSTP/ RSTP/ STP protocol version setting. Valid values are STP, RSTP and MSTP.

Bridge Priority

Set or show the Bridge priority. Lower numeric values have higher 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

Set or show 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

Set or show the maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range from 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.

Maximum Hop Count

Set or show 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

Set or show the number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDUs per second.

5.28.2 STP Bridge Configuration – Advanced Settings

This section allows the user to configure the Bridge Configuration Advanced settings:

Edge Port BPDU Filtering

Set or show Edge Port BPDU Filtering status.

When Edge Port BPDU Filtering is enabled, a port explicitly configured as Edge will transmit and receive BPDUs.

☑ Edge Port BPDU Filtering is enabled

□ Edge Port BPDU Filtering is disabled (This is the default.)

Edge Port BPDU Guard

Set or show Edge Port BPDU Guard status.

When Edge Port BPDU Guard is enabled, a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

☑ Edge Port BPDU Guard is enabled

□ Edge Port BPDU Guard is disabled (This is the default.)

Port Error Recovery

Set or show Port Error Recovery status.

When Port Error Recovery is enabled, a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

☑ Port Error Recovery is enabled

□ Port Error Recovery is disabled (This is the default.)

Port Error Recovery Timeout

Set or show 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).

5.28.3 STP Bridge Configuration Buttons

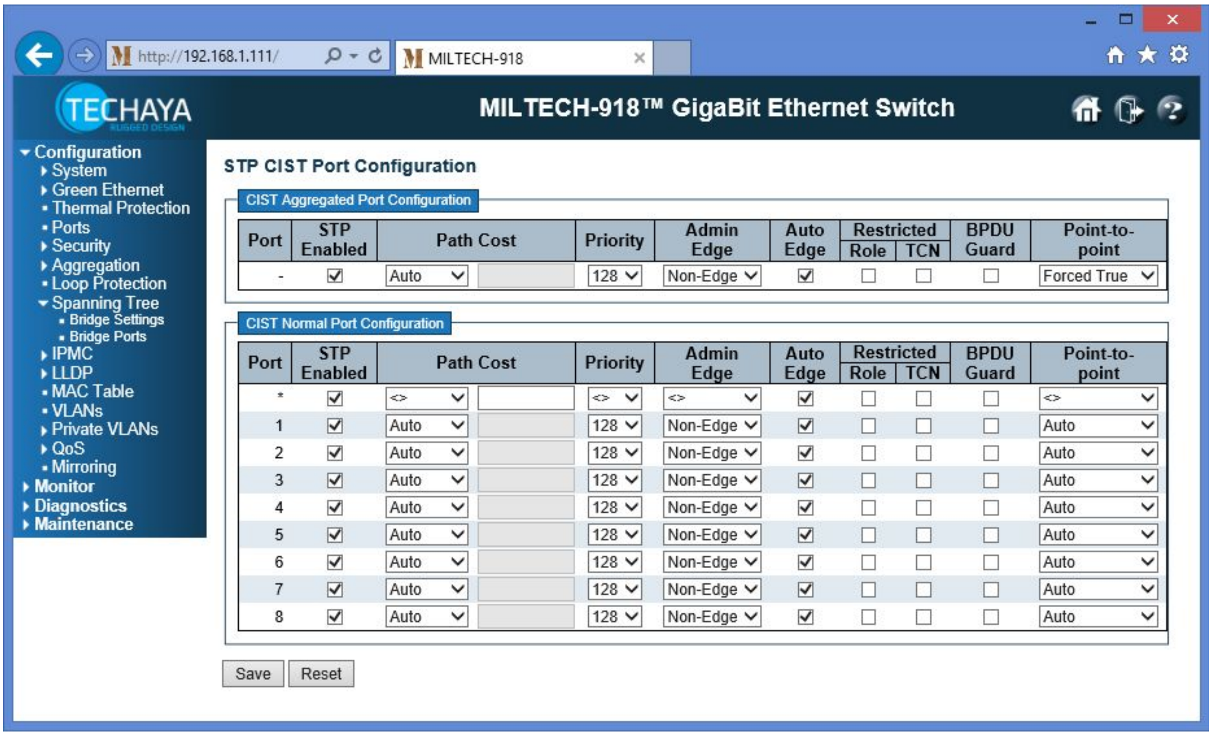
Save: Click to save all changes

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

5.29 Spanning Tree – Bridge Ports

This page allows the user to inspect and change the current Spanning Tree Protocol (STP) Common Internal Spanning Tree (CIST) port configurations.

This page contains settings for physical and aggregated ports.



STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
-	☑	Auto		128	Non-Edge	☑	□	□	□	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
*	☑	<>		<>	<>	☑	□	□	□	<>
1	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
2	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
3	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
4	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
5	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
6	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
7	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
8	☑	Auto		128	Non-Edge	☑	□	□	□	Auto

5.29.1 STP CIST Port Configuration

This section allows the user to configure the Bridge Configuration Basic settings (the parameters are the same for aggregated and normal ports):

Port

This column displays the switch port number of the logical STP port.

STP Enabled

Set or show the STP status for this switch port.

☑ STP is enabled on this switch port (This is the default.)

□ STP is disabled on this switch port

Path Cost

Set or show the path cost incurred by the port.

Auto: Sets the path cost as appropriately, for the physical link speed, using the 802.1D recommended values.

Specific: The user enters a value to define the path cost.

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 200,000,000.

Priority

Set or show the port priority. This can be used to control priority of ports having identical port cost. (See above).

operEdge (state flag)

Displays the operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.

AdminEdge

Set or show whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).

Edge: operEdge flag should start as set

Non- Edge: operEdge flag is not set

AutoEdge

Set or show the AutoEdge status for this bridge port.

☑ Enable automatic edge detection on the bridge port (This is the default.)

□ Disable 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

Set or show the Restricted Role status for this bridge port.

☑ Enabled – port will **not** be selected as a Root Port for the CIST or any MSTI

□ Disabled – port may be selected as a Root Port for the CIST or any MSTI (This is the default.)

If enabled, the port will not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If enabled, 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 influencing 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

Set or show the Restricted TCN (Topology Change Notification) status for this bridge port.

☑ Enabled – port will **not** propagate received topology change notifications and topology changes to other ports

□ Disabled – port may propagate received topology change notifications and topology changes to other ports (This is the default.)

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

Set or show the BPDU Guard status for this bridge port.

☑ Enabled – The Port will disable itself upon receiving valid BPDUs

□ Disabled – The Port will **not** disable itself upon receiving valid BPDUs (This is the default.)

Contrary to the similar bridge setting, the port Edge status does not affect this setting.

A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery (shown on page 161) setting as well.

Point-to-Point

Set or show whether the port connects to a point-to-point LAN rather than to a shared medium.

Auto:	Determine automatically
Forced True	Force to true
Forced False	Force to false

Transition to the forwarding state is faster for point-to-point LANs than for shared media.

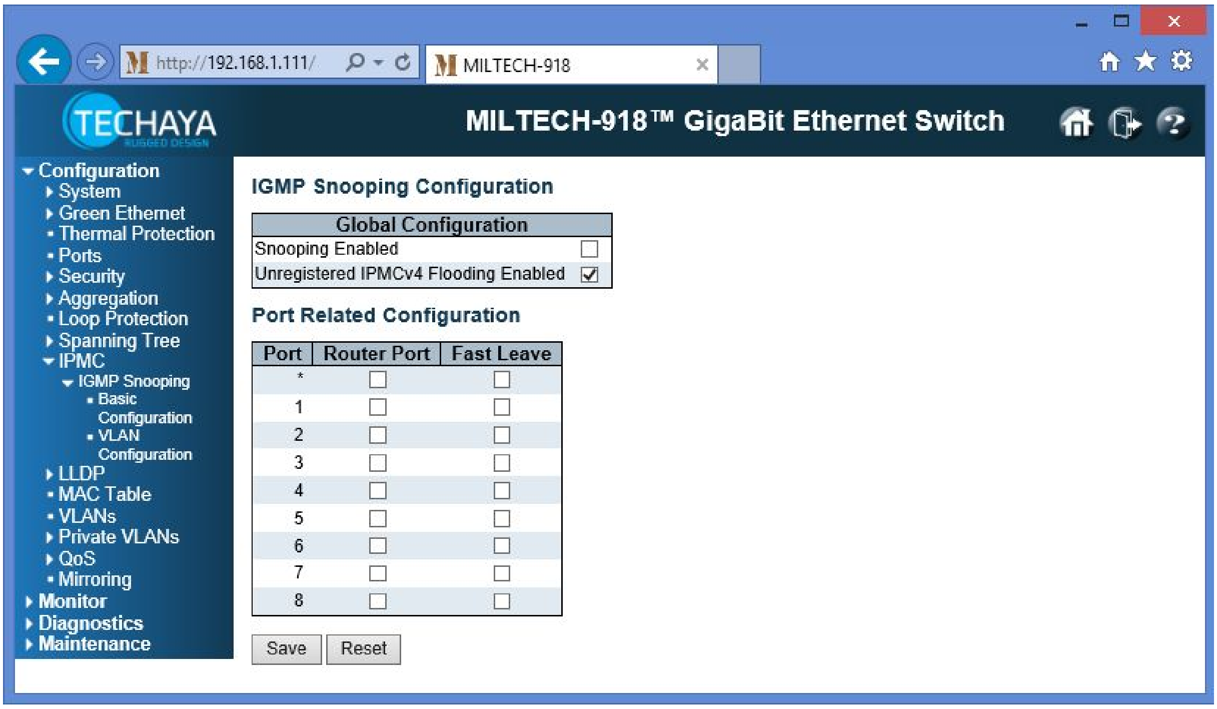
5.29.2 STP CIST Port Configuration Buttons

Save: Click to save all changes

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

5.30 IPMC – IGMP Snooping – Basic Configuration

This page allows the user to configure Internet Group Management Protocol (IGMP) Snooping related configuration.



IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	□
Unregistered IPMCv4 Flooding Enabled	☑

Port Related Configuration

Port	Router Port	Fast Leave
*	□	□
1	□	□
2	□	□
3	□	□
4	□	□
5	□	□
6	□	□
7	□	□
8	□	□

Save Reset

5.30.1 IGMP Snooping Configuration - Global

This section allows the user to configure the Bridge Configuration Basic settings:

Snooping Enabled

Set or show Snooping status.

☑ Enable the Global IGMP Snooping

□ Disable the Global IGMP Snooping (This is the default.)

Unregistered IPMCv4 Flooding Enabled

Set or show Unregistered IPMCv4 Flooding status

☑ Enable unregistered IPMCv4 traffic flooding (This is the default.)

□ Disable 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 despite this setting.

5.30.2 Port Related Configuration

This section allows the user to configure the Bridge Configuration Advanced settings:

Port

This column displays the switch port number.

Router Port

Set or show which ports act as router ports.

☑ Enable – the port is a Router port

□ Disable – the port is **not** a Router port (This is the default.)

A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP Querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave

Set or show whether a port has Fast Leave processing.

☑ Enable the Fast Leave on the port

□ Disable the Fast Leave on the port (This is the default.)

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.

5.30.3 IGMP Snooping Configuration Buttons

Save: Click to save all changes

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

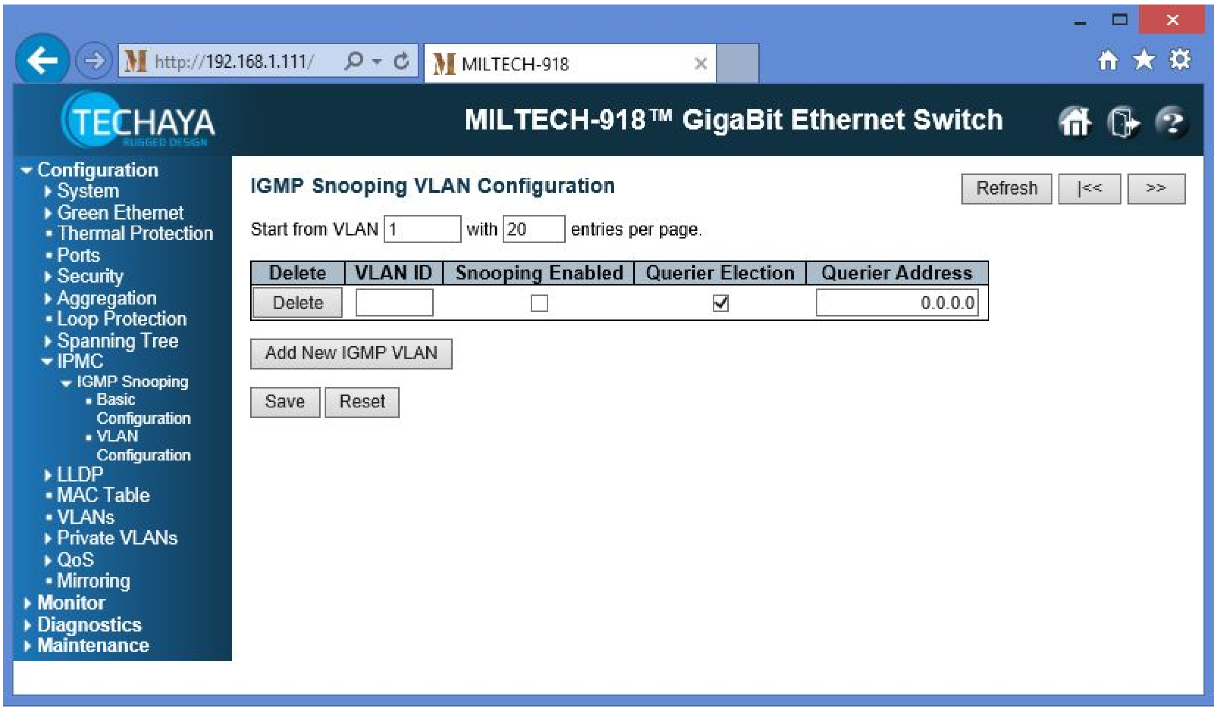
5.31 IPMC – IGMP Snooping – VLAN Configuration

Navigating the IGMP Snooping VLAN Table

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

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest VLAN Table match.

The **Forward Arrows (** >> **)** button will use the last entry of the currently displayed entry 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 **Back Arrows** button **(** |<< **)** to start over.



IGMP Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address
Delete		□	☑	0.0.0.0

5.31.1 IGMP Snooping VLAN Configuration

This page allows the user to configure the IGMP Snooping VLAN parameters:

Delete

☑ Check to delete a VLAN entry. The entry will be deleted during the next save.

□ Do not delete the entry. (This is the default.)

VLAN ID

Set or show the VLAN ID of the entry.

IGMP Snooping Enabled

Set or show the per VLAN IGMP Snooping status.

☑ Enable the Global IGMP Snooping

□ Disable the Global IGMP Snooping (This is the default.)

Up to 32 VLANs can be selected for IGMP Snooping.

Querier Election

☑ Enable this entry to join IGMP Querier election in the VLAN (This is the default.)

□ Disable this entry to act as an IGMP Non-Querier

Querier election is used to dedicate the Querier. This is the only Querier to which the sends Query messages, on a particular link.

Querier election rule determines that IGMP Querier or MLD Querier with the lowest IPv4/IPv6 address wins the election.

Querier Address

Set or show the IPv4 address as source address used in IP header for IGMP IGMP Querier election.

When the Querier address is not set, the system uses IPv4 management address of the IP interface associated with this VLAN.

When the IPv4 management address is not set, system uses the first available IPv4 management address.

Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

This column displays the switch port number of the logical STP port.

STP Enabled

Set or show the STP status for this switch port.

☑ STP is enabled on this switch port (This is the default.)

□ STP is disabled on this switch port

5.31.2 IGMP Snooping VLAN Configuration Buttons

Refresh: Refreshes the displayed table starting from the “VLAN” input fields.

Back Arrows (|<<): Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

Forward Arrows (>>): Updates the table, starting with the entry after the last entry currently displayed.

Add a New IGMP VLAN:
Click to add new IGMP VLAN. Specify the VID and configure the new entry. After creation of the new entry the user must click "Save". The specific IGMP VLAN starts working after the corresponding static VLAN is also created.

Save: Click to save all changes

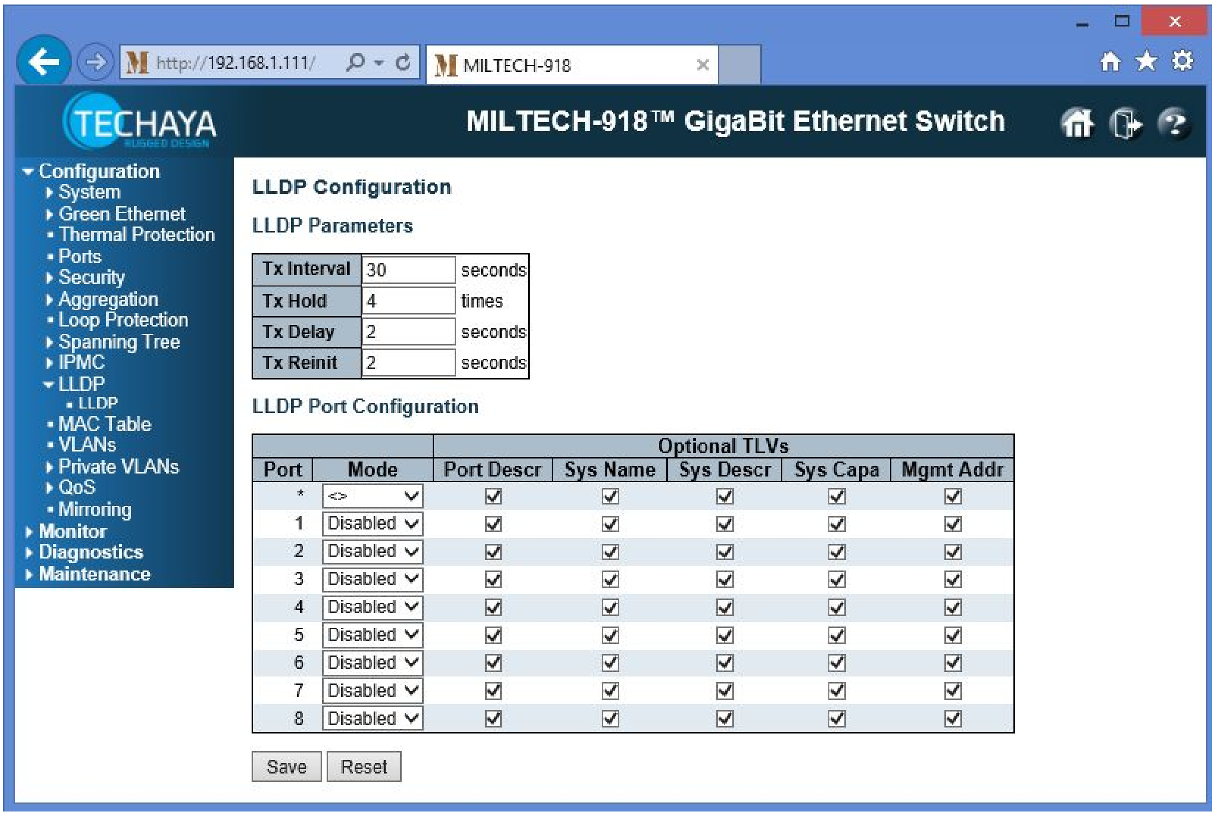
Reset: Click to undo any changes made locally and revert to previously saved values

5.32 LLDP – LLDP Configuration

The Link Layer Discovery Protocol (LLDP) is an IEEE 802.1ab standard protocol.

The 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 (for a more detailed explanation of this protocol, see the online help).

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



LLDP Configuration

LLDP Parameters

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

LLDP Port Configuration

		Optional TLVs				
Port	Mode	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☑	☑	☑	☑	☑
1	Disabled	☑	☑	☑	☑	☑
2	Disabled	☑	☑	☑	☑	☑
3	Disabled	☑	☑	☑	☑	☑
4	Disabled	☑	☑	☑	☑	☑
5	Disabled	☑	☑	☑	☑	☑
6	Disabled	☑	☑	☑	☑	☑
7	Disabled	☑	☑	☑	☑	☑
8	Disabled	☑	☑	☑	☑	☑

5.32.1 LLDP Parameters

This section allows the user to configure the LLDP Parameters per port:

Tx Interval

Set or show the Tx Interval. Valid values are restricted to 5 - 32768 seconds.

The switch periodically transmits LLDP frames to its neighbors to keep the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value.

Tx Hold

Set or show the Tx Hold value which is used to determine how long the information in the LLDP frame remains valid (the valid period). Values are restricted to 2 - 10 times.

The valid period equals Tx Hold multiplied by Tx Interval seconds. Each LLDP frame stores the valid period to know how long the information in the LLDP frame shall be considered valid.

Tx Delay

Set or show the Tx Delay value. Values are restricted to 1 - 8192 seconds.

If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value.

Tx Reinit

Set or show the Tx Reinit value. Values are restricted to 1 - 10 seconds

When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information is not valid anymore. Tx Reinit controls the number of seconds between the shutdown frame and a new LLDP initialization.

5.32.2 LLDP Port Configuration

This section allows the user to configure the LLDP Port Configuration Parameters:

Port

This column displays the switch port number of the logical LLDP port.

Mode

Set or show the LLDP mode:

Rx only The switch will **not** send out LLDP information, but LLDP information from neighbor units is analyzed

Tx only The switch will drop LLDP information received from neighbors, but will send out LLDP information

Disabled The switch will **not** send out LLDP information, and will drop LLDP information received from neighbors

Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbors

Port Descr

Set or show whether or not the “Port Description” is included in the LLDP information transmitted.

☑ “Port Description” is included (This is the default.)

□ “Port Description” is **not** included

(This is an optional TLV. For an explanation, see What is an optional TLV below.)

Sys Name

Set or show whether or not the “System Name” is included in the LLDP information transmitted.

☑ “System Name” is included (This is the default.)

□ “System Name” is **not** included

(This is an optional TLV. For an explanation, see What is an optional TLV below.)

Sys Descr

Set or show whether or not the “System Description” is included in the LLDP information transmitted.

☑ “System Description” is included (This is the default.)

□ “System Description” is **not** included

(This is an optional TLV. For an explanation, see What is an optional TLV below.)

Sys Capa

Set or show whether or not the “System Capability” is included in the LLDP information transmitted.

☑ “System Capability” is included (This is the default.)

□ “System Capability” is **not** included

(This is an optional TLV. For an explanation, see What is an optional TLV below.)

Mgmt Addr

Set or show whether or not the “Management Address” is included in the LLDP information transmitted.

☑ “Management Address” is included (This is the default.)

□ “Management Address” is **not** included

(This is an optional TLV. For an explanation, see What is an optional TLV below.)

What is an optional TLV

TLV is an acronym for Type Length Value. An LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

An LLDP frame contains multiple TLVs.

Optional TLVs are configurable; they can be enabled or disabled. If an optional TLV is disabled the corresponding information is not included in the LLDP frame.

5.32.3 LLDP Configuration Buttons

Save: Click to save all changes

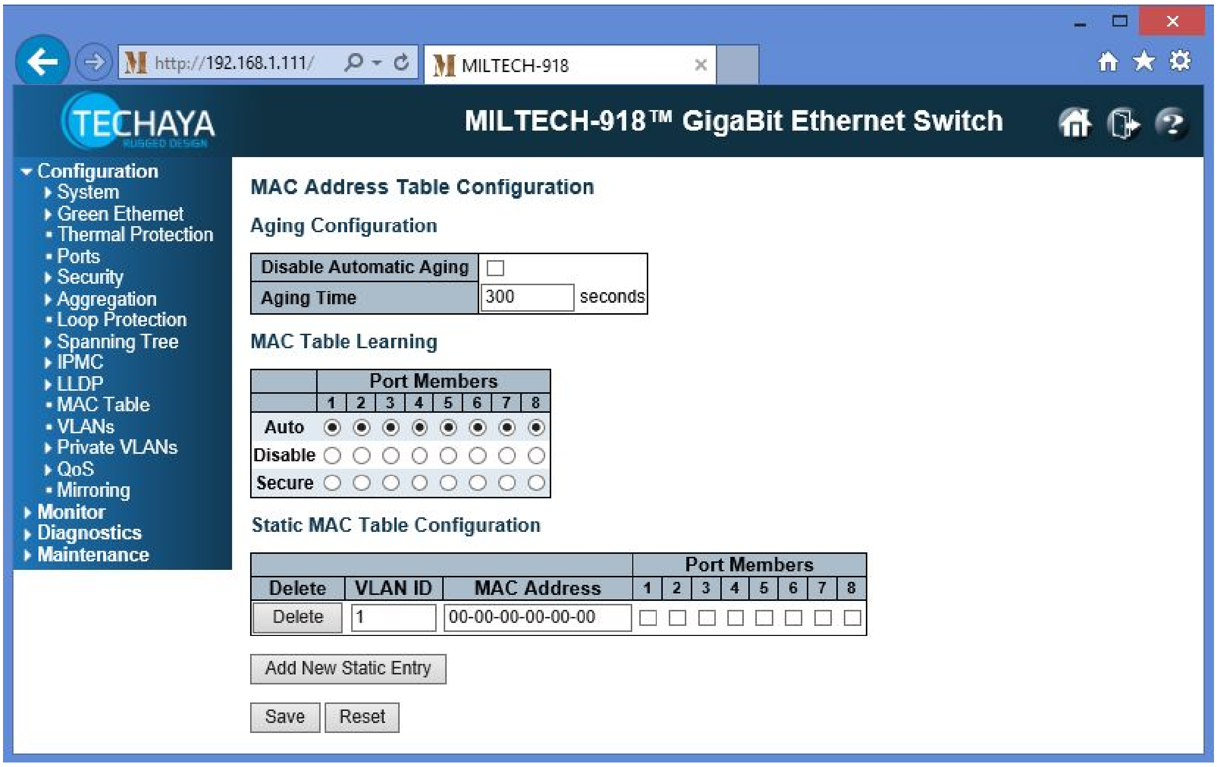
Reset: Click to undo any changes made locally and revert to previously saved values

5.33 MAC Table – MAC Address Table Configuration

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 has been seen after a configurable age time.

On this page, the user can configure the MAC Address Table, set timeouts for entries in the dynamic MAC Table, and configure the static MAC table here.



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds

MAC Table Learning

	Port Members							
	1	2	3	4	5	6	7	8
Auto	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○

Static MAC Table Configuration

			Port Members							
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8
Delete	1	00-00-00-00-00-00	□	□	□	□	□	□	□	□

Add New Static Entry

Save Reset

5.33.1 Aging Configuration

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is called aging.

Disable Automatic Aging

To disable the automatic aging of dynamic entries, check the box:

☑ Automatic aging disabled

□ Automatic aging enabled (This is the default.)

Aging Time

To configure aging time, enter a value in the box. The allowed range is 10 to 1,000,000 seconds.

5.33.2 MAC Table Learning

If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

Each port can do learning based upon the following settings:

Port Members

This column displays the switch port number of the logical LLDP port.

Learning Mode

Set or show the Learning mode per switch:

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.

5.33.3 Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The maximum of 64 entries is for the whole stack, and not per switch.

The MAC table is sorted first by VLAN IDand then by MAC address.

Delete

☑ Check to delete the entry. The entry will be deleted during the next save.

□ Do not delete the entry. (This is the default.)

VLAN ID

Set or show the VLAN ID of the entry.

MAC Address

Set or show the MAC address of the entry.

Port Members

☑ Checkmark indicates the corresponding port is a member of the entry

□ Unchecked box indicates the corresponding port is not a member of the entry (This is the default.)

5.33.4 MAC Configuration Buttons

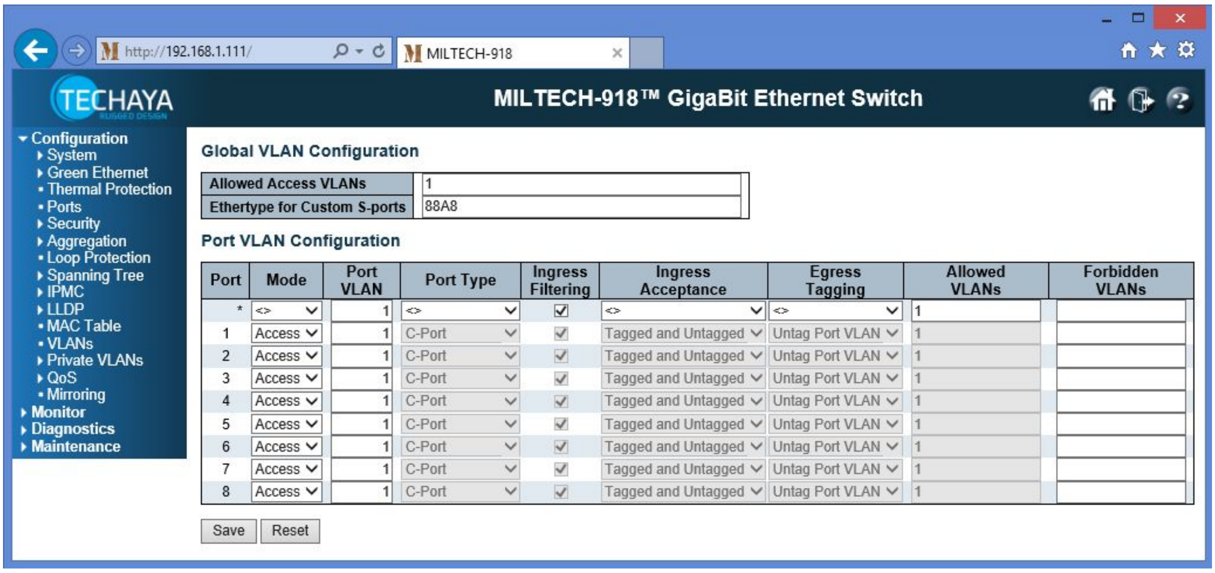
Add a New Static Entry Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

Save: Click to save all changes

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

5.34 VLANs –VLAN Configuration

This page allows the user to control the VLAN configuration on the switch stack. It is divided into a global section and a per-port configuration section.



Global VLAN Configuration

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

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

5.34.1 Global VLAN Configuration

Allowed Access VLANs

Set or show the allowed Access VLANs. “Allowed Access VLANs” only affect ports configured as Access Ports (for an explanation of Access Ports see the online help). 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 added by using list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will add VLANs 1, 10, 11, 12, 13, 200, and 300 to the list of Allowed Access VLANs:

1, 10-13,200,300. Spaces are allowed in between the delimiters.

Ethertype for Custom S-ports

Set or show 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.

5.34.2 Port VLAN Configuration

This section allows the user to configure the VLAN Parameters per port:

Port

This field displays the logical port number of this row.

Mode

Set or show the port mode (default is Access) to determine the fundamental behavior of the port in question. The remaining fields in that row will be either grayed out or made changeable depending on the mode selected.

The grayed out fields show the value that the port will get when the mode is applied to the port.

A port can have one of three modes:

Access: 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: 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 a 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 – except 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: Hybrid ports resemble trunk ports, but they have 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

  S-custom-tag aware
- Ingress filtering can be controlled

- Ingress acceptance of frames and configuration of egress tagging can be configured independently

Port VLAN

Set or show the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095 (the default is 1.

On ingress, frames get classified to the Port VLAN if:

- The port is configured as VLAN "Unaware"
- The frame is untagged
- 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.

Port Type

Ports in hybrid mode allow for changing the port type, so that the frame's VLAN tag can be 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. There are four Port Types:

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 will be 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 will be 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 will be tagged with the custom S-tag.

Ingress Filtering

Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.

☑ Enabled – frames classified to a VLAN of which the port is not a member get discarded (This is the default.)

□ Disabled – frames classified to a VLAN of which the port is not a member are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs of which it is not a member.

Ingress Acceptance

Set or show Ingress Acceptance type.

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.

Hybrid ports allow for changing the type of frames that are accepted on ingress.

Egress Tagging

Set or show Egress Tagging type.

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 can control which VLANs they are allowed to join as members. Access ports can be members of only one VLAN, the Access VLAN.

By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to 1-4095.

A list of specific VLANs may be created by using list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will allow the port to become a member of VLANs 1, 10, 11, 12, 13, 200, and 300:

1, 10-13,200,300. Spaces are allowed in between the delimiters.

The field may be left empty, which means that the port will not become member of any VLAN.

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.

By default, the field is left blank, which means that the port may become a member of all possible VLANs.

A list of specific VLANs may be created by using list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will forbid the port from becoming a member of VLANs 1, 10, 11, 12, 13, 200, and 300:

1, 10-13,200,300. Spaces are allowed in between the delimiters.

5.34.3 Global VLAN Configuration Buttons

Save: Click to save all changes

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

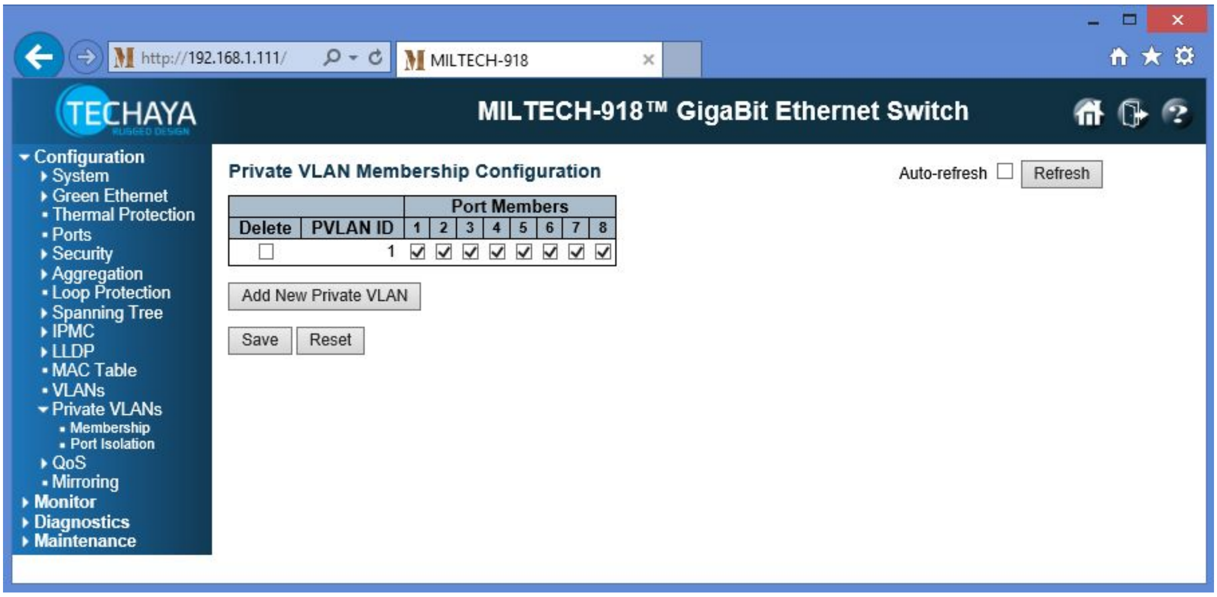
5.35 Private VLANs – Membership

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.

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

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

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



Private VLAN Membership Configuration

		Port Members							
Delete	PVLAN ID	1	2	3	4	5	6	7	8
□	1	☑	☑	☑	☑	☑	☑	☑	☑

5.35.1 Private VLAN Membership Configuration

From this page the user can:

- Configure, monitor, and modify Private VLAN membership configurations for the switch
- Add or delete Private VLANs
- Add or remove port members of each Private VLAN

Delete

☑ Check to delete a Private VLAN entry. It will be deleted during the next save.

□ Do not delete the entry. (This is the default.)

Private VLAN ID

Set or show ID of this particular private VLAN.

Port Members

A row of check boxes for each port is displayed for each private VLAN ID.

☑ Include this port in the Private VLAN (configured in this row)

□ Remove or exclude this port from the Private VLAN (configured in this row)

By default, no ports are members, and all boxes are unchecked.

5.35.2 Private VLAN Membership Configuration Buttons

Auto-refresh:

☑ Enable Auto-refresh - refresh the page automatically every 3 seconds

□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

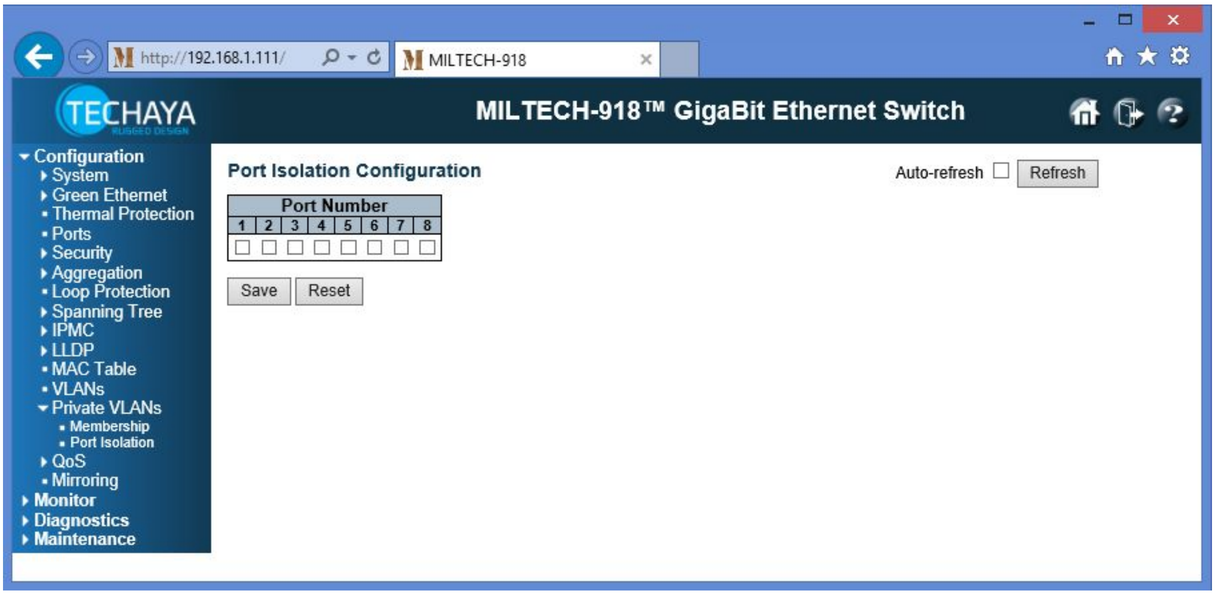
Add a New Private VLAN Click to add a new Private VLAN ID.
An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click “OK” to discard the incorrect entry, or click “Cancel” to return to the editing and make a correction.
Click the “Delete” button to undo the addition of a new Private VLAN. The Private VLAN is enabled when you click “Save”.

Save: Click to save all changes

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

5.36 Private VLANs – Membership

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.



Port Isolation Configuration

Port Number							
1	2	3	4	5	6	7	8
□	□	□	□	□	□	□	□

5.36.1 Port Isolation Configuration

From this page the user can enable or disable port isolation on ports in a Private VLAN.

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

Port Number

A check box is provided for each port of a private VLAN.

☑ Port Isolation is enabled on that port

□ Port Isolation is disabled on that port

By default, port isolation is disabled on all ports.

5.36.2 Port Isolation Configuration Buttons

Auto-refresh:

☑ Enable Auto-refresh - refresh the page automatically every 3 seconds

□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Save: Click to save all changes

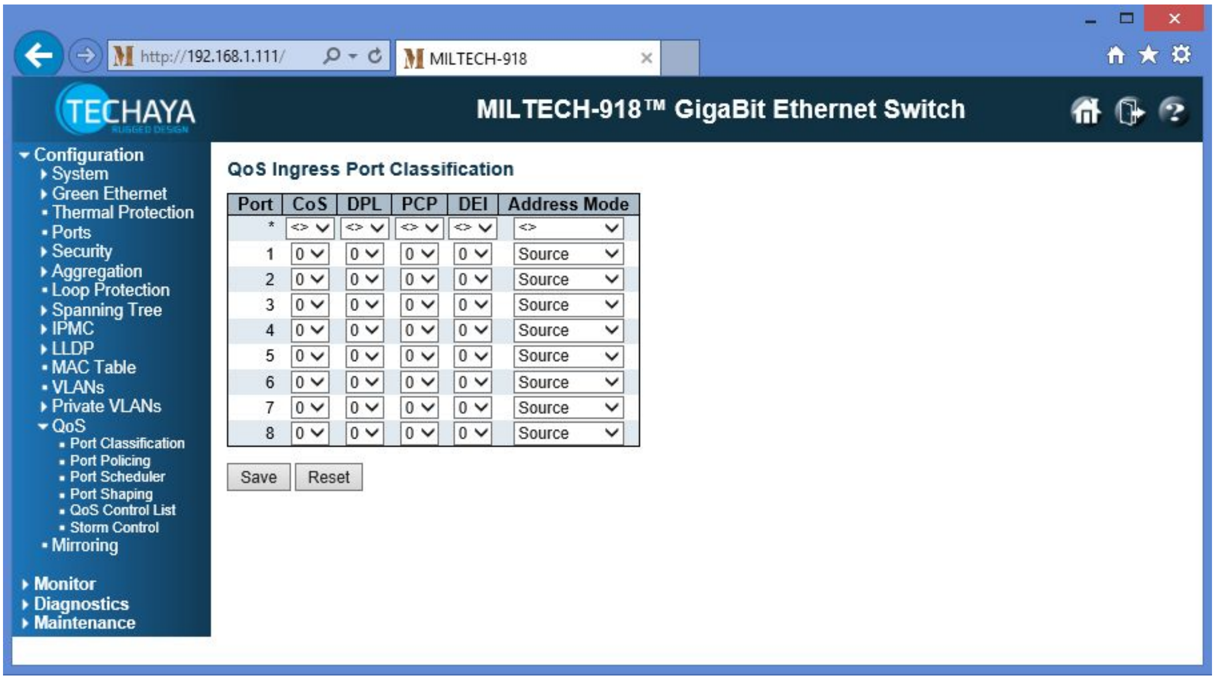
Reset: Click to undo any changes made locally and revert to previously saved values

5.37 QoS – Port Classification

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 Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Address Mode
*	<>	<>	<>	<>	<>
1	0	0	0	0	Source
2	0	0	0	0	Source
3	0	0	0	0	Source
4	0	0	0	0	Source
5	0	0	0	0	Source
6	0	0	0	0	Source
7	0	0	0	0	Source
8	0	0	0	0	Source

5.37.1 QoS Ingress Port Classification

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

The displayed settings are:

Port

This field displays the port number for this row. All configurations on this row apply to this port.

CoS

Set or show the 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.

The classified CoS can be overruled by a QCL (QoS Control List) 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

Set or show the default 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 or higher corresponds to ‘Discard Eligible’ (Yellow) frames.

The classified DPL can be overruled by a QCL (QoS Control List) entry.

PCP

Set or show the default PCP value.

All frames are classified to a PCP value.

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. A PCP of 0 (zero) has the lowest priority.

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.

DEI

Set or show the default DEI value.

All frames are classified to a DEI value.

DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag:

1: drop eligible

0: not drop eligible (default)

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.

Address Mode

The IP/MAC address mode specifying whether the QCL (QoS Control List) 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

5.37.2 QoS Ingress Port Classification Buttons

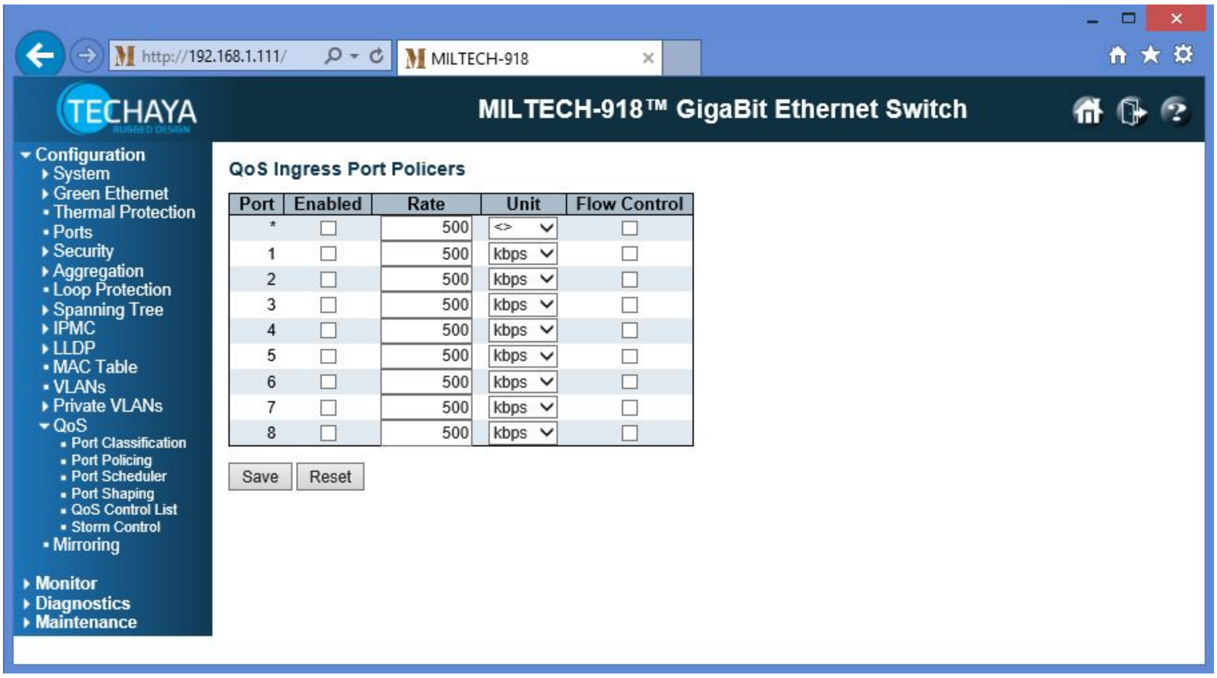
Save: Click to save all changes

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

5.38 QoS – Port Policing

A Policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

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



QoS Ingress Port Policers

Port	Enabled	Rate	Unit	Flow Control
*	□	500	<>	□
1	□	500	kbps	□
2	□	500	kbps	□
3	□	500	kbps	□
4	□	500	kbps	□
5	□	500	kbps	□
6	□	500	kbps	□
7	□	500	kbps	□
8	□	500	kbps	□

5.38.1 QoS Ingress Port Policers

The displayed settings are:

Port

This field displays the port number for this row. All configurations on this row apply to this port.

Enabled

Enable or disable the policer on this switch port.

☑ Enabled – the policer is enabled on this switch port

□ Disabled – the policer is disabled on this switch port (This is the default.)

Rate

Set or show the rate for the policer. The default value is 500.

This value is restricted to:	when the "Unit" is:
100-1,000,000	"kbps" or "fps"
1-3,300	"Mbps" or "kfps"

Unit

Set or show the unit of measure for the policer rate as kbps, Mbps, fps, or kfps. The default value is "kbps".

Flow Control

Enable or disable the flow control.

☑ Enabled – flow control is enabled on this switch port

□ Disabled – flow control is disabled on this switch port (This is the default.)

If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

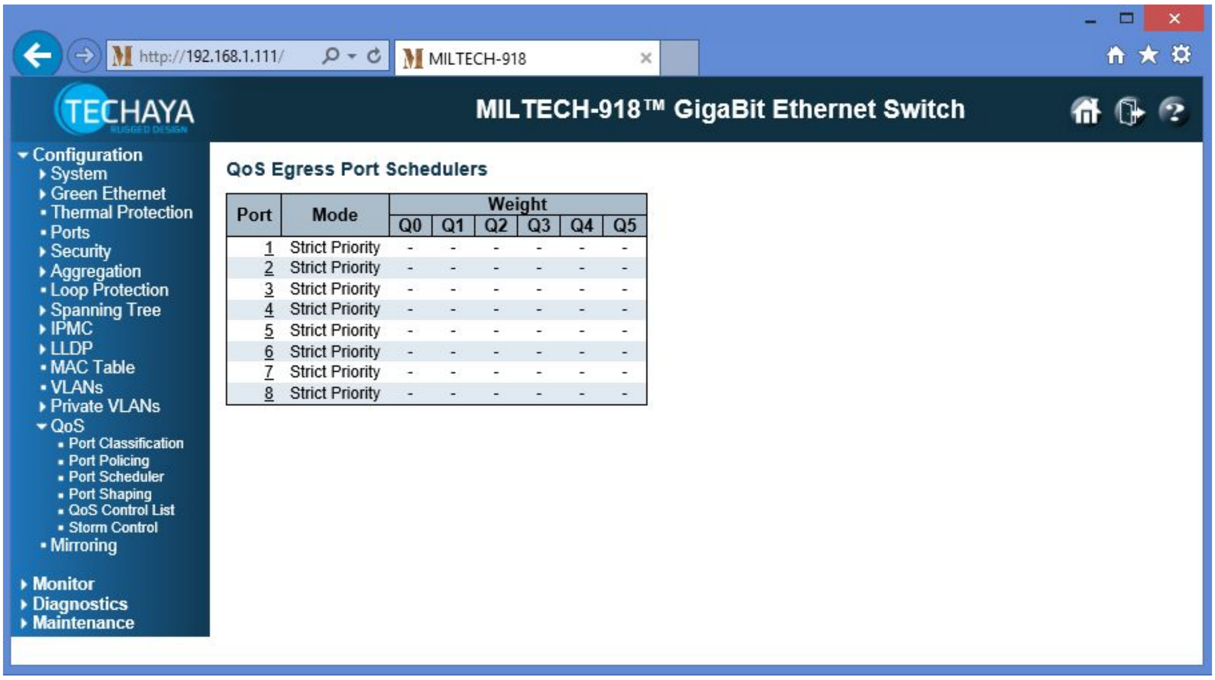
5.38.2 QoS Ingress Port Policers Buttons

Save: Click to save all changes

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

5.39 QoS – Port Scheduler

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



QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-

5.39.1 QoS Egress Port Schedulers

The displayed settings are:

Port

The logical port for the settings contained in the same row.

Click on the port number in order to configure the schedulers. The QoS Egress Port Schedulers and Shapers page opens (see section 5.39.2 QoS Egress Port Schedulers and Shapers Page on page 192).

Mode

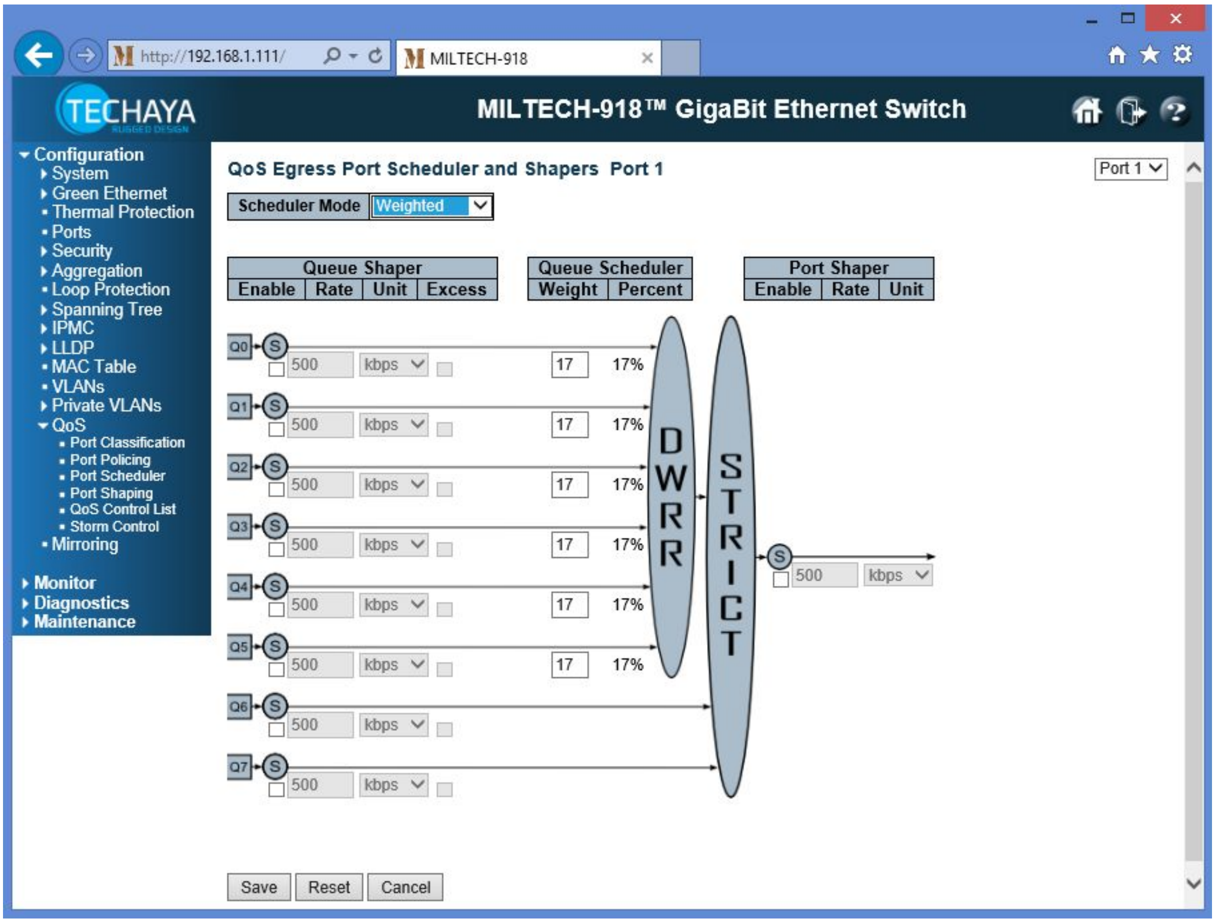
This column shows the scheduling mode for this port.

Qn

This column shows the we ight for this queue and port.

5.39.2 QoS Egress Port Schedulers and Shapers Page

This page allows the user to configure the Scheduler and Shapers for a specific port. It is opened from the QoS Egress Port Schedulers page, described in section 5.39.1 on page 191 and also from QoS – Port Shaping page described in section 5.40 on page 195. The port number is displayed at top of the page.



QoS Egress Port Scheduler and Shapers Port 1

Port 1

Scheduler Mode: Weighted

	Queue Shaper				Queue Scheduler	
	Enable	Rate	Unit	Excess	Weight	Percent
Q0	□	500	kbps	□	17	17%
Q1	□	500	kbps	□	17	17%
Q2	□	500	kbps	□	17	17%
Q3	□	500	kbps	□	17	17%
Q4	□	500	kbps	□	17	17%
Q5	□	500	kbps	□	17	17%
Q6	□	500	kbps	□		
Q7	□	500	kbps	□		

Port Shaper		
Enable	Rate	Unit
□	500	kbps

The displayed settings are:

Port

The box at the top right of the page shows the logical port for the settings contained in this page. Click the down arrow to select a different port to configure.

Scheduler Mode

Set or show whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

Queue Shaper Enable

Set or show whether the queue shaper is enabled for this queue on this switch port.

☑ Enabled – the queue shaper is enabled for this queue on this switch port

□ Disabled – the queue shaper is disabled for this queue on this switch port (This queue shaper is disabled by default.)

Queue Shaper Rate

Set or show the rate for the queue shaper. The default value is 500.

This value is restricted to:	when the "Unit" is:
100-1,000,000	"kbps"
1-3,300	"Mbps"

Queue Shaper Unit

Set or show the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

Queue Shaper Excess

Set or show whether the queue is allowed to use excess bandwidth.

☑ Enabled – the queue is allowed to use excess bandwidth

□ Disabled – the queue is **not** allowed to use excess bandwidth (The queue is not allowed to use excess bandwidth by default.)

Queue Scheduler Weight

Set or show the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent

Show the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Port Shaper Enable

Set or show whether the port shaper is enabled for this switch port.

☑ Enabled – the port shaper is enabled for this switch port

□ Disabled – the port shaper is disabled for this switch port (The port shaper is disabled for this switch port by default.)

Port Shaper Rate

Set or show the rate for the port shaper. The default value is 500.

This value is restricted to:	when the "Unit" is:
100-1,000,000	"kbps"
1-3,300	"Mbps"

Port Shaper Unit

Set or show the unit of measure for the port shaper rate as “kbps” or “Mbps”. The default value is “kbps”.

5.39.3 QoS Egress Port Schedulers Buttons

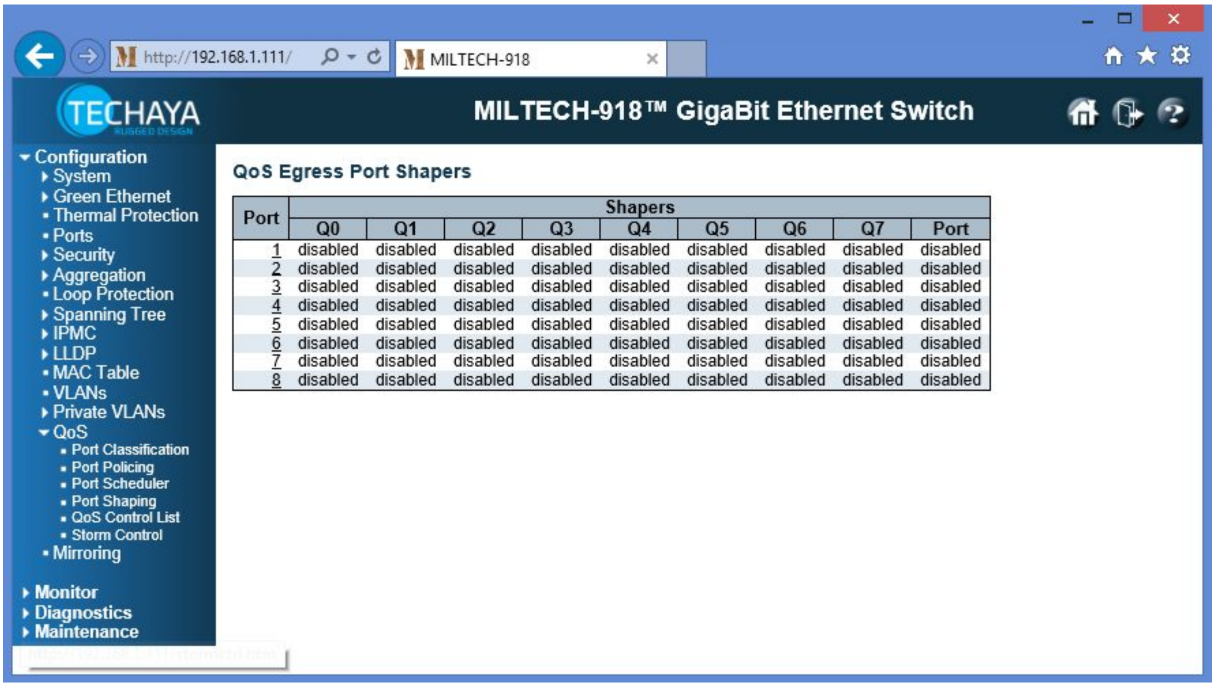
Save: Click to save all changes

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

Cancel: Click to undo any changes made locally and return to the previous page

5.40 QoS – Port Shaping

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



QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

5.40.1 QoS Egress Port Shapers

The displayed settings are:

Port

Displays the logical port for the settings contained in the same row.

Click on the port number in order to configure the shapers. The QoS Egress Port Schedulers and Shapers page opens. For an explanation of this page, see section 5.39.2 QoS Egress Port Schedulers and Shapers Page on page 192.

Qn

Shows “disabled” or actual queue shaper rate - e.g. “800 Mbps”.

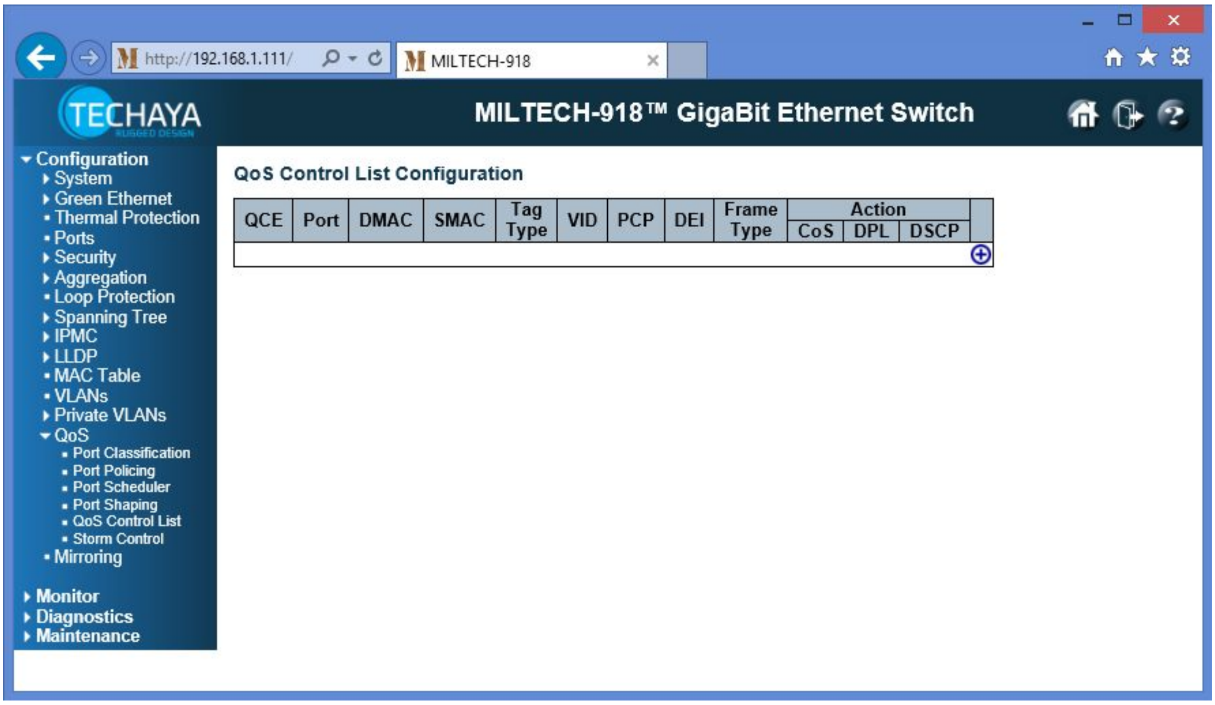
Port

Shows “disabled” or actual port shaper rate - e.g. “800 Mbps”.

5.41 QoS Control List

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

Click on the lowest plus sign to add a new QCE to the list (the QCE Configuration page opens, see the described in section 5.41.2 on page 199).



QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action			
									CoS	DPL	DSCP	
												⊕

5.41.1 QoS Control List Configuration

QCE

Display the QCE ID.

Port

Display the list of ports configured with the QCE.

DMAC

Display 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 the OUI field of source MAC address, i.e., first three octets (bytes) of MAC address or “Any”.

Match specific source MAC address or “Any”.

If a port is configured to match on DMAC/DIP, this field indicates the DMAC.

Tag Type

Display the 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

Display the VLAN ID, either a specific VID or range of VIDs. VID can be in the range 1-4095 or "Any".

PCP

Display the Priority Code Point. Valid values of PCP are:

Specific: (0, 1, 2, 3, 4, 5, 6, 7)

Range: (0-1, 2-3, 4-5, 6-7, 0-3, 4-7)

"Any"

DEI

Display the Drop Eligible Indicator. Valid values of DEI are 0, 1 or "Any".

Frame Type

Display 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

Display the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are:

CoS: Classify Class of Service

DPL: Classify Drop Precedence Level

DSCP: Classify DSCP value

PCP: Classify PCP value

DEI: Classify DEI value

Policy: Classify ACL Policy number

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

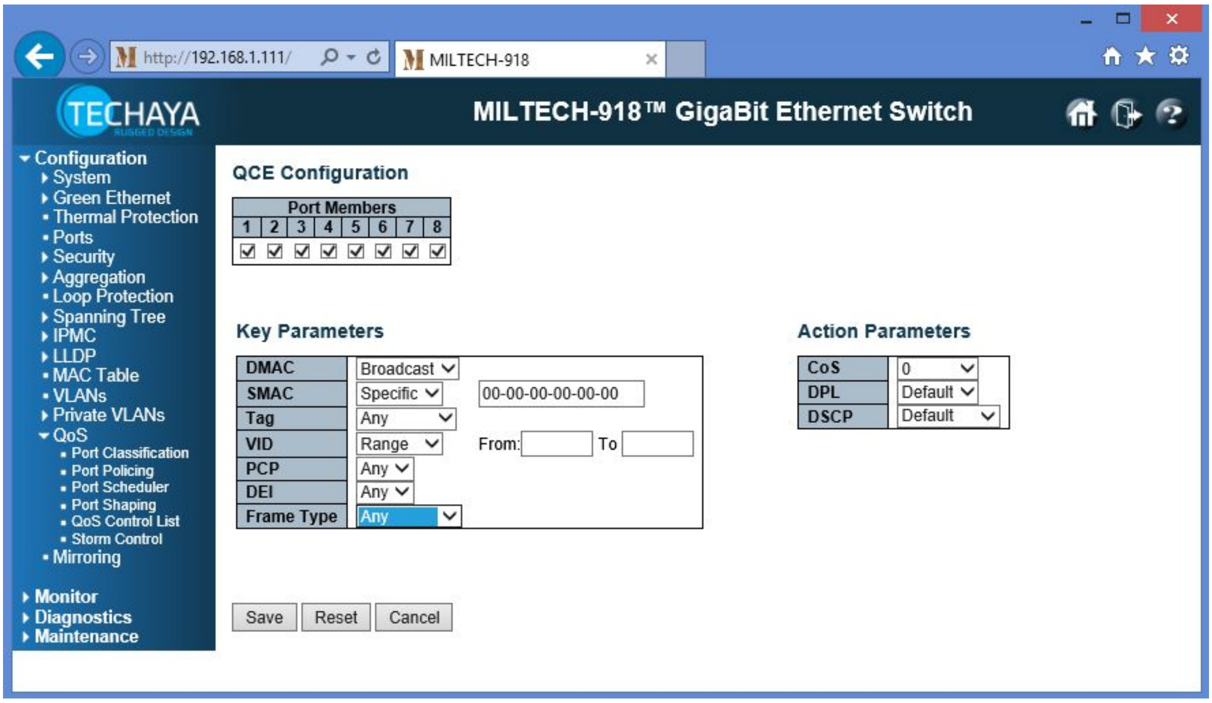
⊗: Deletes the QCE

⊕: The lowest plus sign adds a new entry at the bottom of the QCE listings

5.41.2 QCE Configuration

This page allows the user to edit and insert a single QoS Control Entry (QCE) at a time. A QCE consists of several parameters. These parameters vary according to the frame type that you select.

Open this page by clicking add (⊕) or edit (ⓔ) from the QoS Control List Configuration table (see section 5.41.1 QoS Control List Configuration above).



QCE Configuration

Port Members							
1	2	3	4	5	6	7	8
☑	☑	☑	☑	☑	☑	☑	☑

Key Parameters

DMAC	Broadcast	
SMAC	Specific	00-00-00-00-00-00
Tag	Any	
VID	Range	From: To
PCP	Any	
DEI	Any	
Frame Type	Any	

Action Parameters

CoS	0
DPL	Default
DSCP	Default

Port Members

Check the checkbox button to include the port in the QCL entry. By default all ports are included.

☑ Include the port in the QCL entry

☐ Do not include the port in the QCL entry

5.41.2.1 Key Parameters

Key configuration is described as below.

DMAC

Set or show the Destination MAC address. Possible values are:

- Unicast
- Multicast
- Broadcast
- Any

SMAC

Set or show the Source MAC address:

- Specific – a field opens for the user to enter the MAC address: xx-xx-xx-xx-xx-xx
- Any

If a port is configured to match on DMAC/DIP, this field is the Destination MAC address.

Tag

Set or show the value of the Tag. Possible values are:

- Untagged
- Tagged
- Any

VID

Set or show a valid VLAN ID.

- Specific – a field opens for the user to enter the VLAN ID
- Range – two field open for the user to enter the range of VLAN IDs
- Any

Possible values are in the range 1-4095 or "Any"

The user can enter either a specific value or a range of VIDs.

PCP

Set or show the value of the PCP, either a specific value (0, 1, 2, 3, 4, 5, 6, 7) or a range of values (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or "Any".

DEI

Set or show the value of the DEI. Values can be "0", "1", or "Any".

Frame Type

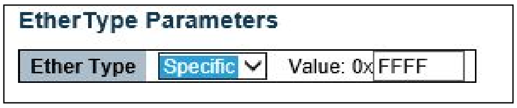
Frame Type can have any of the following values:

- Any
- EtherType
- LLC
- SNAP
- IPv4
- IPv6

After the user selects a Frame Type, a table will pop up with specific parameters for that Frame Type (except for "Any"). The parameters per Frame Type are given below:

EtherType Parameters

Set or show the EtherType Parameters. When the “Specific” option is selected for the EtherType parameter, the user must enter a valid value for that parameter.



EtherType Parameters

Ether Type	Specific	Value: 0x FFFF

Valid Ether Type can be:

Specific: Requires a specific **Value**. Valid EtherType values are:

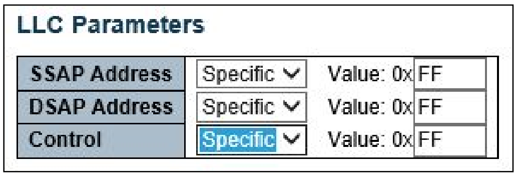
0x600-0xFFFF

Excluding: 0x800 (IPv4) and 0x86DD (IPv6)

Any

LLC Parameters

Set or show the LLC Parameters. When the “Specific” option is selected for an LLC parameter, the user must enter a valid value for that parameter.



LLC Parameters

SSAP Address	Specific	Value: 0x FF
DSAP Address	Specific	Value: 0x FF
Control	Specific	Value: 0x FF

SSAP Address:

Specific: **Value:** valid SSAP (Source Service Access Point) can vary from 0x00 to 0xFF

Any

DSAP Address:

Specific: **Value:** valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF

Any

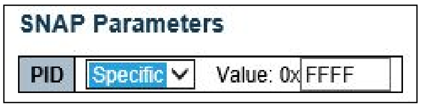
Control:

Specific: **Value:** Control field can vary from 0x00 to 0xFF

Any

SNAP Parameters

Set or show the SNAP Parameters. When the “Specific” option is selected for a SNAP parameter, the user must enter a valid value for that parameter.



SNAP Parameters

PID	Specific	Value: 0x FFFF

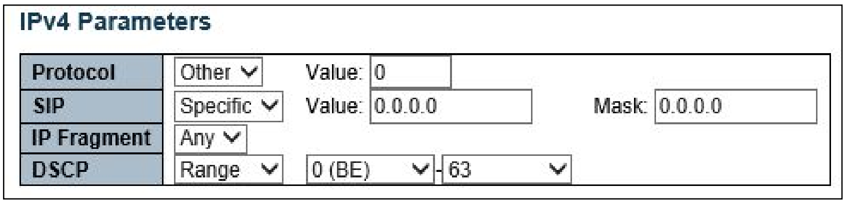
PID:

Specific: **Value:** valid PID (a.k.a Ether Type) can be 0x0000-0xFFFF

Any

IPv4 Parameters

Set or show the IPv4 Parameters. When one of the following options is selected for an IPv4 parameter: “Specific”, “Other”, or “Range” the user must enter a valid value in each of the value fields that open for that parameter.



IPv4 Parameters

Protocol	Other	Value: 0	
SIP	Specific	Value: 0.0.0.0	Mask: 0.0.0.0
IP Fragment	Any		
DSCP	Range	0 (BE) - 63	

Protocol:

Any

UDP

TCP

Other: **Value:** IP protocol number: 0-255

SIP:

Specific: **Value/Mask:** Source IP address in value/mask format

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 values:

Yes

No

Any

DSCP: Diffserv Code Point (DSCP) values:

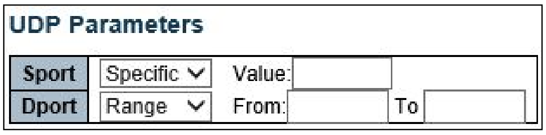
Specific value

Range of values

Any

Values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

IPv4 - TCP/UDP Parameters



UDP Parameters

Sport	Specific	Value:
Dport	Range	From: To

Sport: Source TCP/UDP port values:

Specific: Value: (0-65535)

Any

Set a specific or port range applicable for IP protocol TCP/UDP.

Dport: Destination TCP/UDP port values:

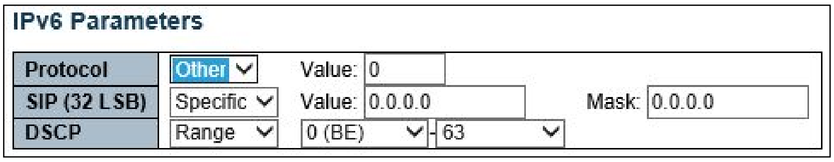
Specific: Value: (0-65535)

Any

Set a specific or port range applicable for IP protocol TCP/UDP.

IPv6 Parameters

Set or show the IPv6 Parameters. When one of the following options is selected for an IPv6 parameter: “Specific”, “Other”, or “Range” the user must enter a valid value in each of the value fields that open for that parameter.



IPv6 Parameters

Protocol	Other	Value: 0	
SIP (32 LSB)	Specific	Value: 0.0.0.0	Mask: 0.0.0.0
DSCP	Range	0 (BE) - 63	

Protocol:

Any

UDP

TCP

Other: Value: IP protocol number: 0-255

SIP:

Specific: **Value/Mask:** 32 LS bits of IPv6 source address in value/mask format

Any

If a port is configured to match on DMAC/DIP, this field is the Destination IP address.

DSCP: Diffserv Code Point (DSCP) values:

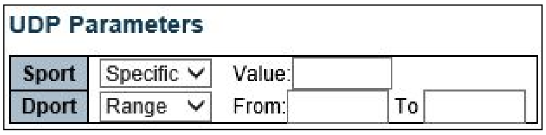
Specific value

Range of values

Any

Values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

IPv6 - TCP/UDP Parameters



UDP Parameters

Sport	Specific	Value:	
Dport	Range	From:	To

Sport: Source TCP/UDP port values:

Specific: Value: (0-65535)

Any

Set a specific or port range applicable for IP protocol TCP/UDP.

Dport: Destination TCP/UDP port values:

Specific: Value: (0-65535)

Any

Set a specific or port range applicable for IP protocol TCP/UDP.

Action Parameters

CoS: Class of Service values: (0-7) or “Default”

DP: Drop Precedence Level values: (0-1) or “Default”

DSCP: DSCP values: (0-63, BE, CS1-CS7, EF, or AF11-AF43) or “Default”

“Default” means that the default classified value is not modified by this QCE.

5.41.3 QCE Configuration Buttons

Save: Click to save all changes

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

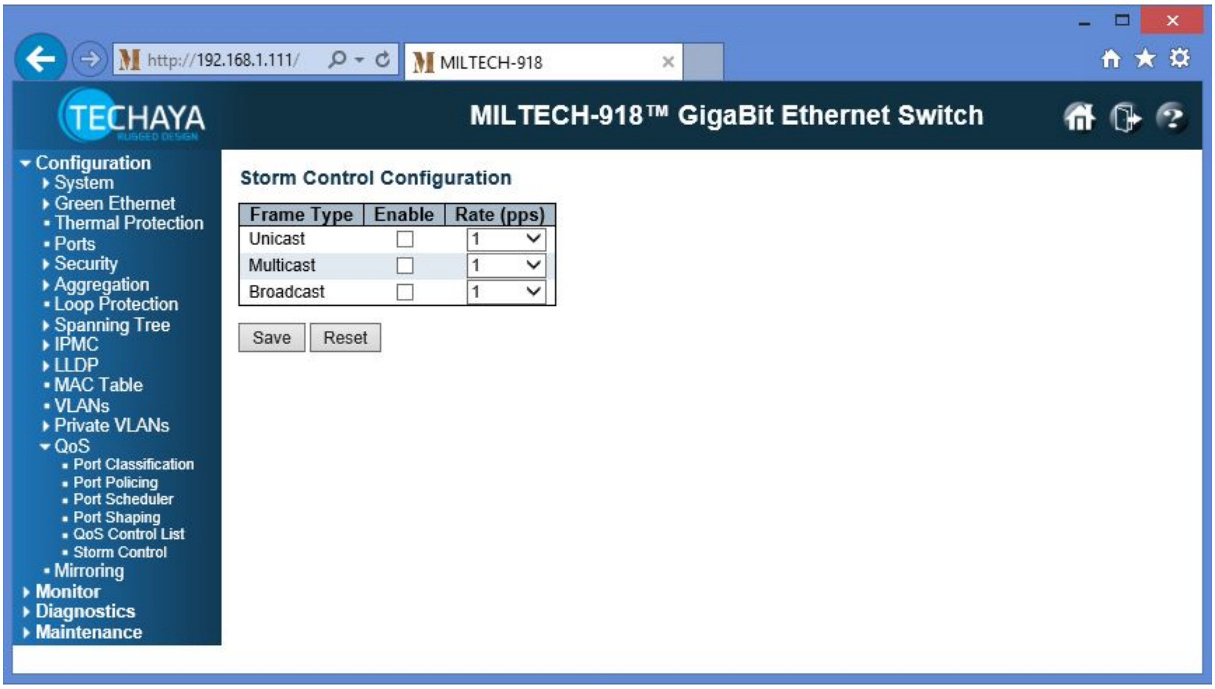
Cancel: Click to undo any changes made locally and return to the previous page

5.42 QoS – Storm Control

This page allows the user to configure the Storm control parameters for the switch.

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.



Storm Control Configuration

Frame Type	Enable	Rate (pps)
Unicast	□	1
Multicast	□	1
Broadcast	□	1

5.42.1 Storm Control Configuration

The displayed settings are:

Frame Type

This column displays the Frame Type to be configured in this row. The Frame Types are:

- Unicast
- Multicast
- Broadcast.

Enable

Enable or disable the storm control status for the given frame type.

☑ Enabled – the storm control status is enabled

□ Disabled – the storm control status is disabled (This is the default.)

Rate

Set or show the rate for Storm Control. The default value is 1.

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	1024K.			

5.42.2 Storm Control Configuration Buttons

Save: Click to save all changes

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

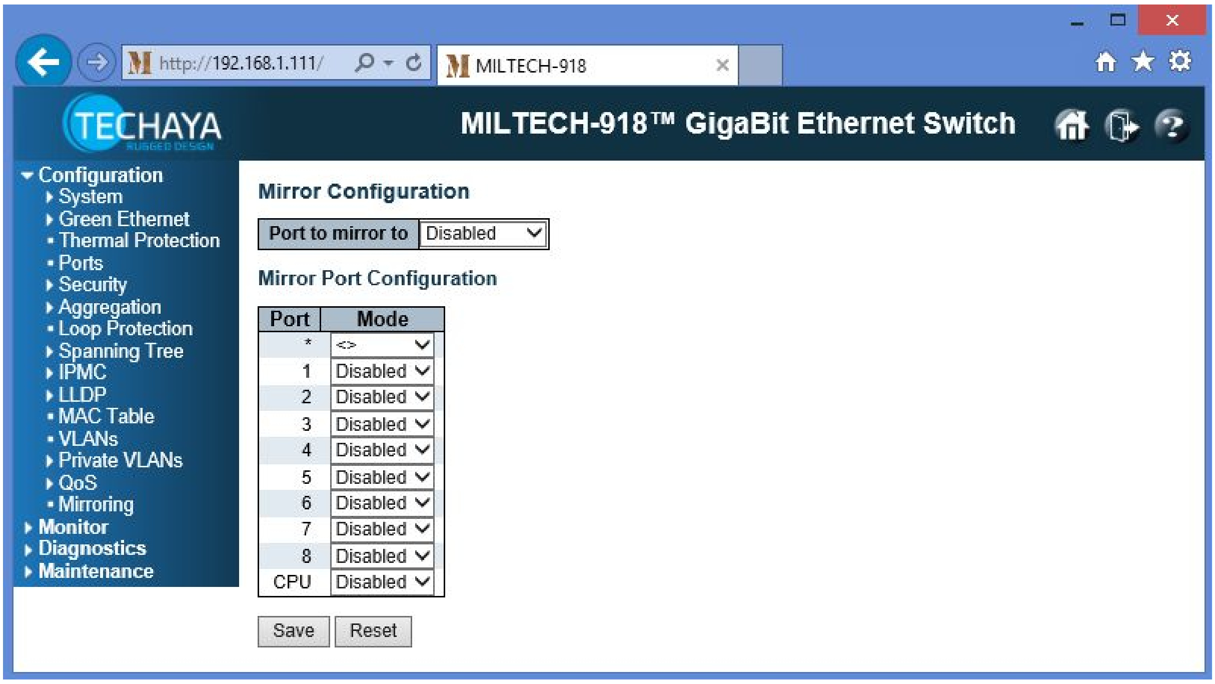
5.43 Mirroring

This page allows the user to configure the Mirroring parameters for the switch.

To debug network problems, selected traffic can be copied, or mirrored, to 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).



Mirror Configuration

Port to mirror to: Disabled

Mirror Port Configuration

Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
CPU	Disabled

5.43.1 Mirror Configuration

The displayed settings are:

Port to mirror to

Set or show the port destination (also known as the mirror port) for frames that are mirrored. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port.

Setting the “Disabled” option disables mirroring.

5.43.2 Mirror Port Configuration

Port

This column displays the logical port to be configured in this row.

Mode

Set or show the mirror mode.

Disabled: Neither frames transmitted nor frames received are mirrored

Rx only: Frames received on this port are mirrored on the mirror port, Frames transmitted are not mirrored

Tx only: Frames transmitted on this port are mirrored on the mirror port, Frames received are not mirrored

Enabled: Frames received and frames transmitted are mirrored on the mirror port

> **Note:** For a given port, a frame is only transmitted once. Therefore it is not possible to mirror the mirror port Tx frames. As a result, the mode for the selected mirror port is limited to Disabled or Rx only.

5.43.3 Mirror Configuration Buttons

Save: Click to save all changes

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

6 Web Interface - Monitor

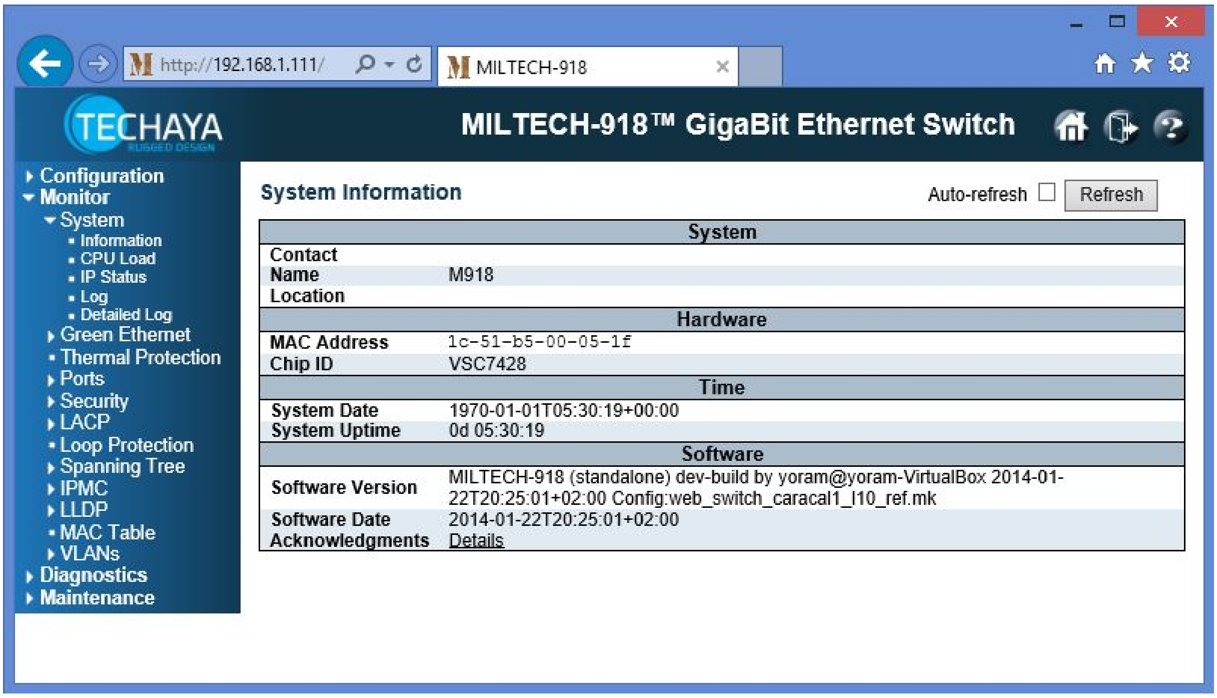
The Web Interface – Monitor section of this manual describes the monitoring features and screens of the MILTECH-912™ Gigabit Ethernet Switch User Interface.

From the Monitor section, the user can monitor the system by viewing:

- System information
- Statistics on the operation of the switch
- Status reports on different features on the switch and how they are operating

6.1 System – Information

The System Information page displays switch system information.



System Information

System	
Contact	
Name	M918
Location	
Hardware	
MAC Address	1c-51-b5-00-05-1f
Chip ID	VSC7428
Time	
System Date	1970-01-01T05:30:19+00:00
System Uptime	0d 05:30:19
Software	
Software Version	MILTECH-918 (standalone) dev-build by yoram@yoram-VirtualBox 2014-01-22T20:25:01+02:00 Config:web_switch_caracal1_l10_ref.mk
Software Date	2014-01-22T20:25:01+02:00
Acknowledgments	Details

6.1.1 System

Contact

The system contact is configured in Configuration->System->Information-> System Contact (see section 5.1 System Information Configuration on page 83).

Name

The system name is configured in Configuration->System->Information->System Name (see section 5.1 System Information Configuration on page 83).

Location

The system location is configured in Configuration->System->Information->System Location (see section 5.1 System Information Configuration on page 83).

6.1.2 Hardware

MAC Address

The MAC Address of this switch.

Chip ID

The Chip ID of this switch.

6.1.3 Time

System Date

This field displays 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.

6.1.4 Software

Software Version

This field displays the software version of this switch.

Software Date

This field displays the date when the switch software was produced.

Code Revision

The version control identifier of the switch software.

6.1.5 System Information Buttons

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

6.2 System – CPU Load

This page displays the CPU load, using an Scalable Vector Graphics (SVG) graph.

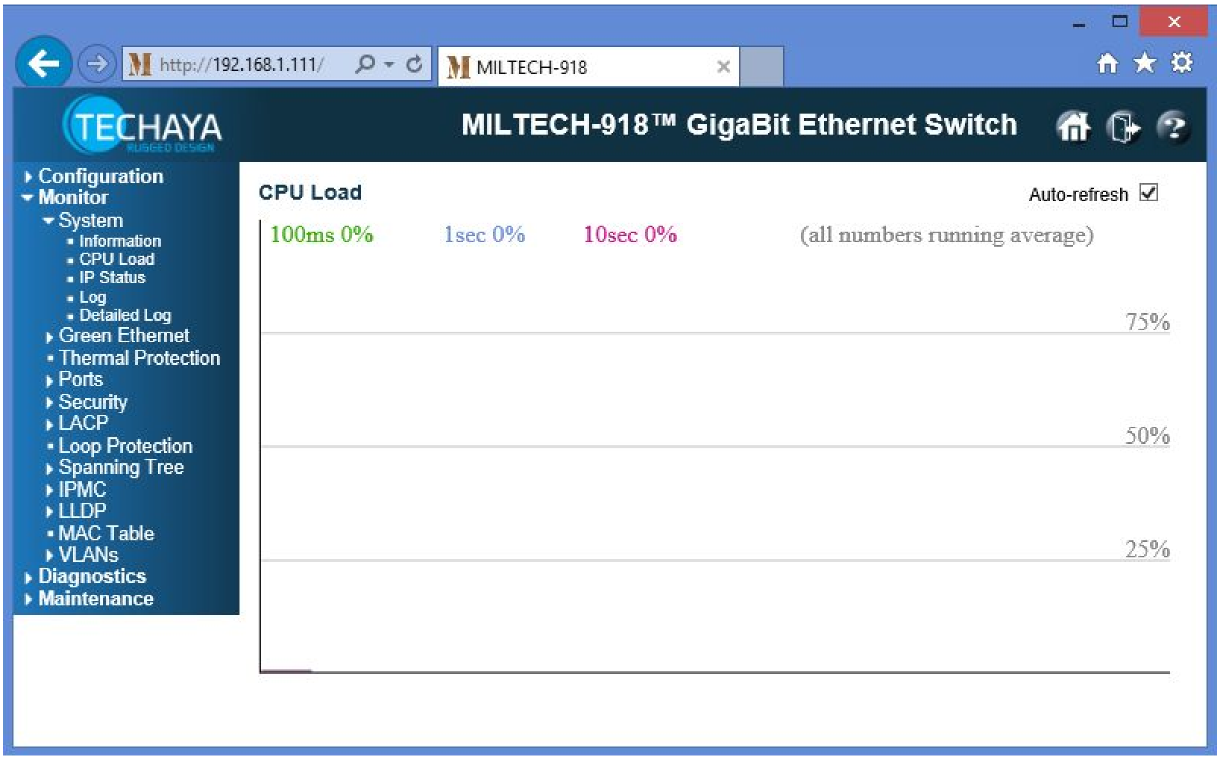
The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well.

In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds (This is the default.)

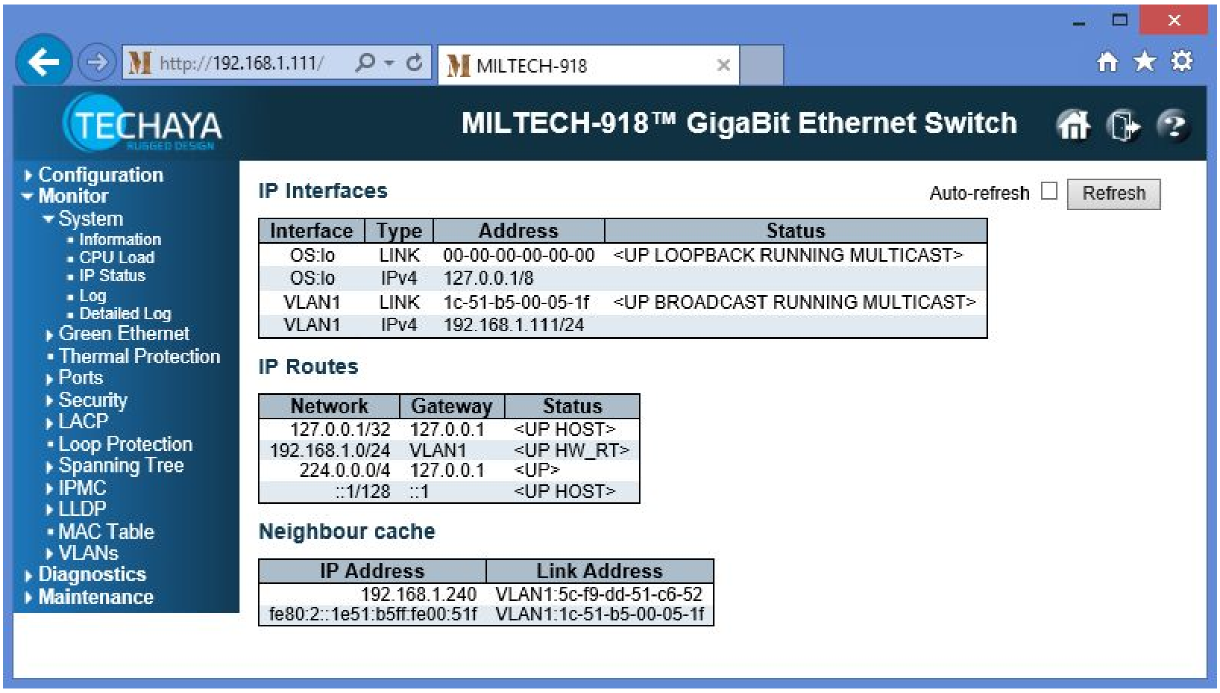
□Disable Auto-refresh (This is the default.)



100ms 0% 1sec 0% 10sec 0% (all numbers running average)

6.3 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.



IP Interfaces

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
VLAN1	LINK	1c-51-b5-00-05-1f	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.1.111/24	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
192.168.1.0/24	VLAN1	<UP HW_RT>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.1.240	VLAN1:5c-f9-dd-51-c6-52
fe80:2::1e51:b5ff:fe00:51f	VLAN1:1c-51-b5-00-05-1f

6.3.1 IP Interfaces

Interface

This column displays the name of the interface.

Type

This column displays the address type of the entry. This may be LINK or IPv4.

Address

This column displays the current address of the interface (of the given type).

Status

This column displays the status flags of the interface (and/or address).

6.3.2 IP Routes

Network

This column displays the destination IP network or host address of this route.

Gateway

This column displays the gateway address of this route.

Status

This column displays the status flags of the route.

6.3.3 Neighbour Cache

IP Address

This column displays the IP address of the entry.

Link Address

This column displays the Link (MAC) address for which a binding to the IP address given exists.

6.3.4 System Information Buttons

Auto-refresh:

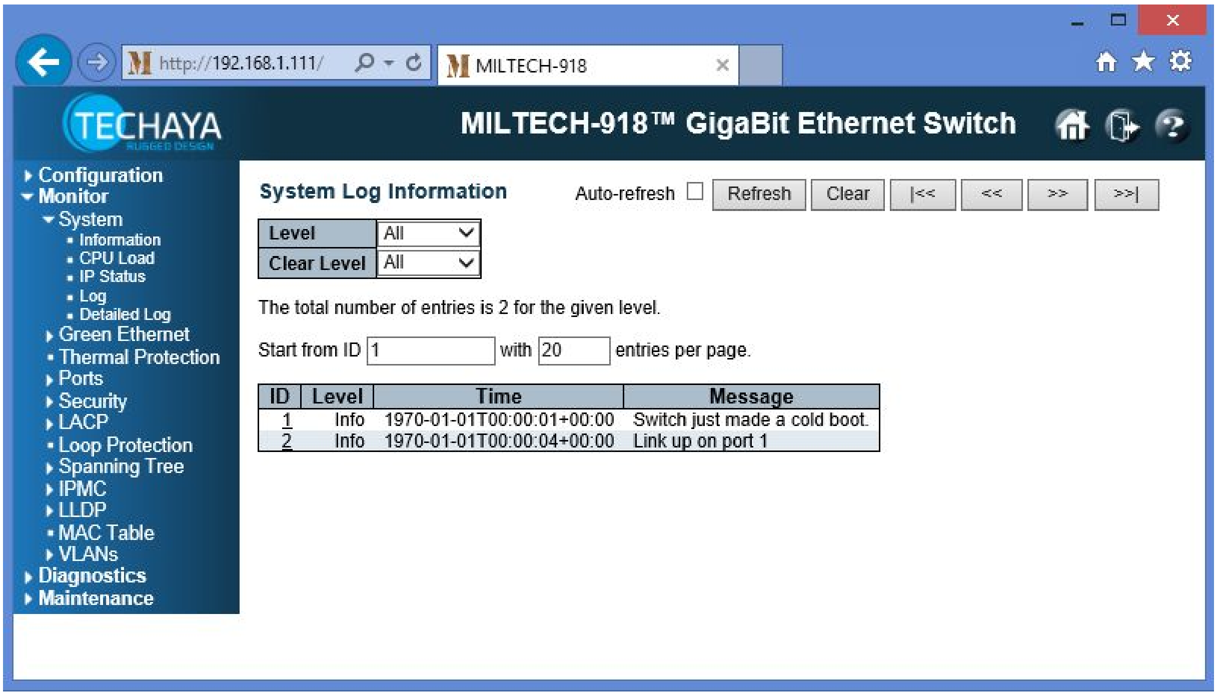
☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

6.4 System – Log

This page displays the system log information.



System Log Information

Level	All
Clear Level	All

The total number of entries is 2 for the given level.

Start from ID 1 with 20 entries per page.

ID	Level	Time	Message
1	Info	1970-01-01T00:00:01+00:00	Switch just made a cold boot.
2	Info	1970-01-01T00:00:04+00:00	Link up on port 1

6.4.1 Navigating the System Log Information Table

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

Level

The "Level" input field is used to filter the display system log entries. The following filtering levels are available:

- Info
- Warning
- Error
- All

Clear Level

The "Clear Level" input field is used to specify which system log entries will be cleared. The Clear Level has the same filtering levels as "Level" above.

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

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

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

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

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

6.4.2 System Log Information

ID

This column displays the identification number of the system log entry. Click on the ID number to open the Detailed System Log Information table, described on page 216

Level

This column displays the level of the system log entry.

Info: The system log entry is belongs to the information level

Warning: The system log entry is belongs to the warning level

Error: The system log entry is belongs to the error level

Time

This column displays the time the system log entry occurred.

Message

This column displays a detailed message of the system log entry.

6.4.3 System Log Information Buttons

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□Disable Auto-refresh (This is the default.)

Refresh: Updates the table entries, starting from the current entry

Clear: Flushes the selected entries

|<< Updates the table entries, starting from the first available entry

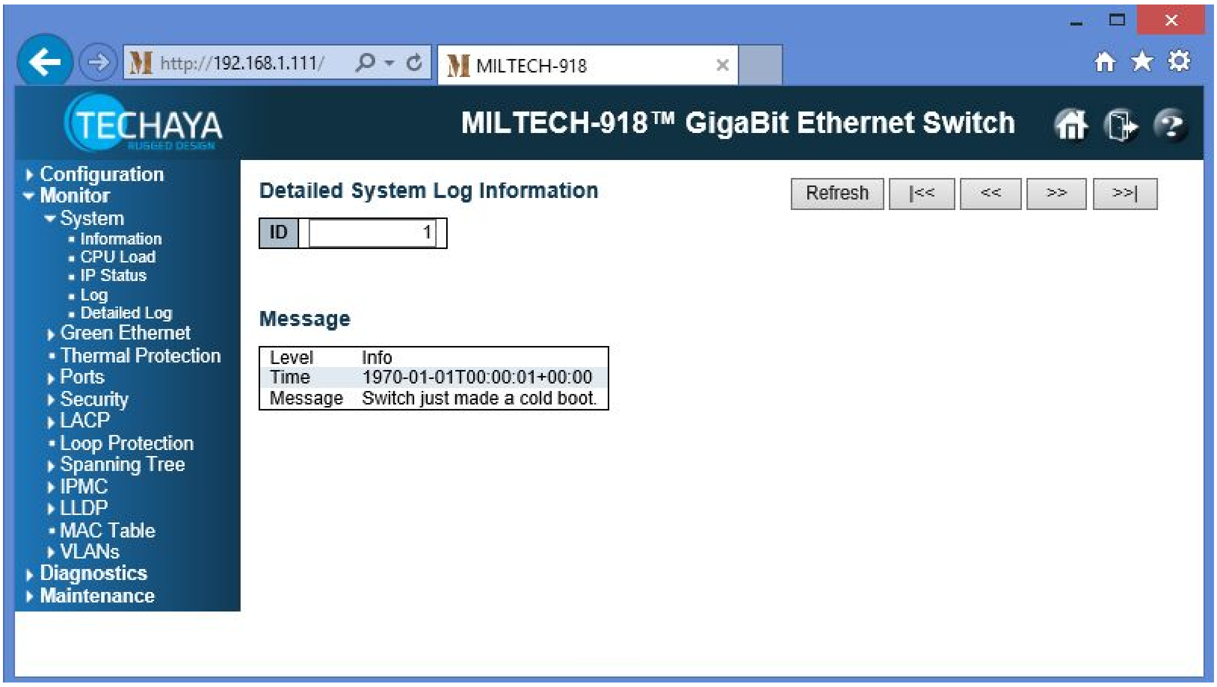
<< Updates the table entries, ending at the last entry currently displayed

>> Updates the table entries, starting from the last entry currently displayed

>>| Updates the table entries, ending at the last available entry

6.5 System – Detailed Log

This page displays the system detailed log information. The user can arrive at this page via the main menu on the left side of the page, or by clicking the ID number in the System Log Information table, described on page 215



Detailed System Log Information

ID: 1

Message

Level	Info
Time	1970-01-01T00:00:01+00:00
Message	Switch just made a cold boot.

6.5.1 Detailed System Log Information

ID

The ID (>= 1) of the system log entry.

Message

This column displays the detailed message of the system log entry.

6.5.2 System Log Information Buttons

Refresh: Updates the system log entry to the current entry ID

|<< Updates the system log entry to the first available entry ID

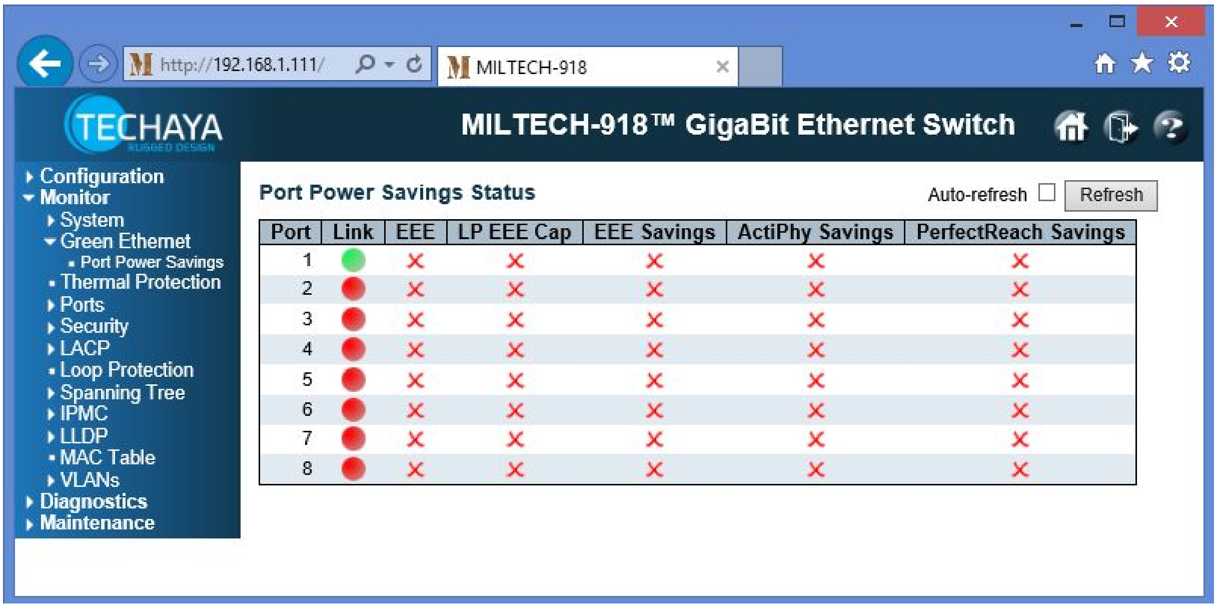
<< Updates the system log entry to the previous available entry ID

>> Updates the system log entry to the next available entry ID

>>| Updates the system log entry to the last available entry ID

6.6 Green Ethernet – Port Power Savings

This page displays the current status for Energy Efficient Ethernet (EEE).



Port Power Savings Status

Port	Link	EEE	LP EEE Cap	EEE Savings	ActiPhy Savings	PerfectReach Savings
1	🟢	✗	✗	✗	✗	✗
2	🔴	✗	✗	✗	✗	✗
3	🔴	✗	✗	✗	✗	✗
4	🔴	✗	✗	✗	✗	✗
5	🔴	✗	✗	✗	✗	✗
6	🔴	✗	✗	✗	✗	✗
7	🔴	✗	✗	✗	✗	✗
8	🔴	✗	✗	✗	✗	✗

6.6.1 Port Power Savings Status

The Port Power Savings are configured in the Port Power Savings Configuration Page. Navigate there as follows:

Configuration->Green Ethernet->Port Power Savings (for details, see section 5.6 Green Ethernet - Port Power Savings on page 92).

Port

This column displays the logical port number for this row.

Link

This column shows if the link is up for the port

Green = link up

Red = link down

EEE

This column shows if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page).

Green Check:	Enabled
Red X:	Disabled

LP EEE cap

This column shows if the link partner is EEE capable.

Green Check:	Enabled
Red X:	Disabled

EEE Savings

This column shows if the system is currently saving power due to EEE. When EEE is enabled, the system will powered down if no frame has been received or transmitted in 5 uSec.

Green Check:	Enabled
Red X:	Disabled

Actiphy Savings

This column shows if the system is currently saving power due to ActiPhy.

Green Check:	Enabled
Red X:	Disabled

PerfectReach Savings

This column shows if the system is currently saving power due to PerfectReach.

Green Check:	Enabled
Red X:	Disabled

6.6.2 Port Power Savings Status Buttons

Auto-refresh:

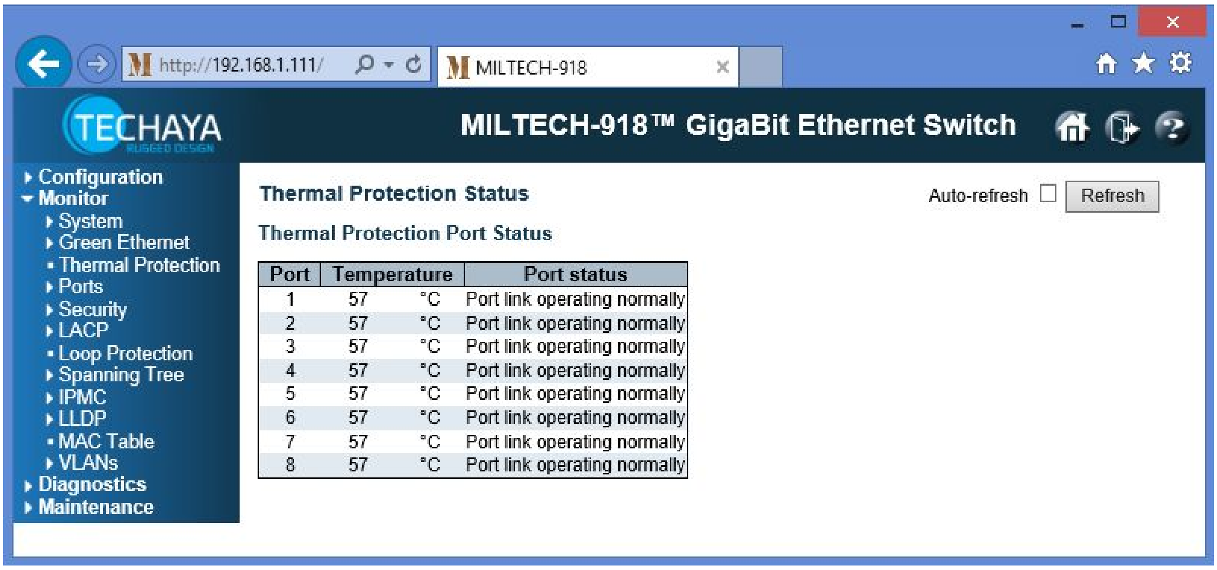
☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page

6.7 Thermal Protection Status

This page displays status information related to thermal protection.



Thermal Protection Status

Thermal Protection Port Status

Port	Temperature		Port status
1	57	°C	Port link operating normally
2	57	°C	Port link operating normally
3	57	°C	Port link operating normally
4	57	°C	Port link operating normally
5	57	°C	Port link operating normally
6	57	°C	Port link operating normally
7	57	°C	Port link operating normally
8	57	°C	Port link operating normally

6.7.1 Thermal Protection Port Status

Port

This column displays the switch port number for this row.

Temperature

This column shows the current chip temperature in degrees Celsius.

Port Status

This column shows if the port is thermally protected (link is down) or if the port is operating normally.

6.7.2 Port Power Savings Status Buttons

Auto-refresh:

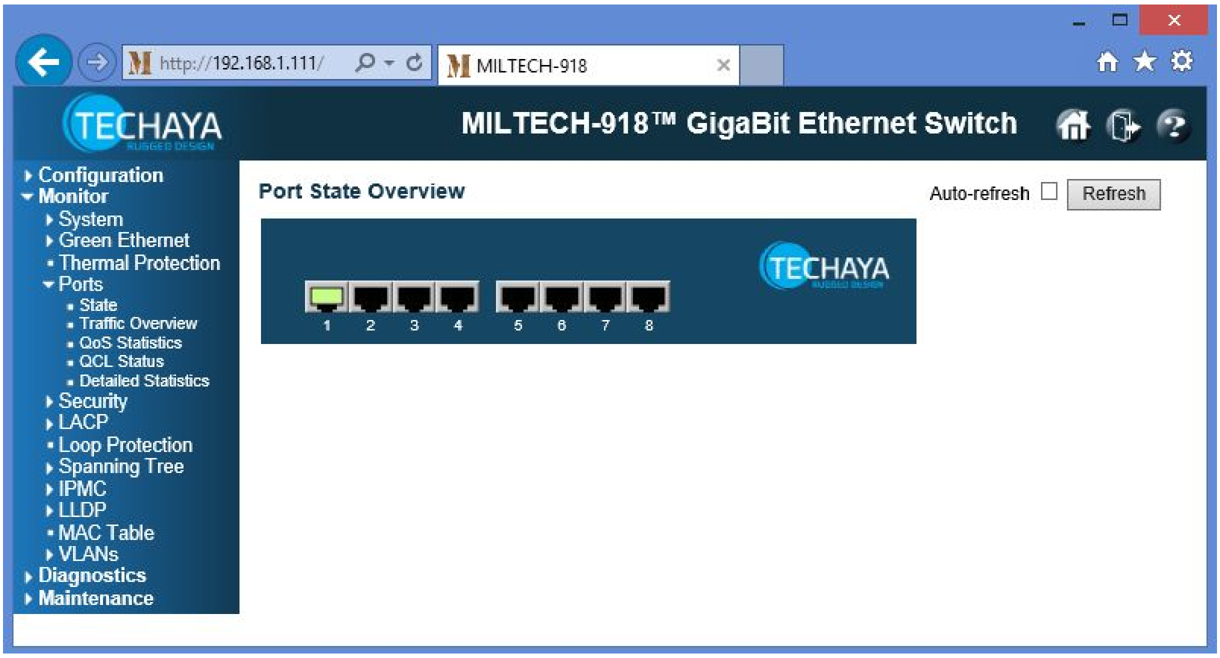
☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page

6.8 Ports - State

This page displays the current switch port states



6.8.1 Port State Overview

The port states are illustrated as follows:

	State		
	Disabled	Down	Link
RJ45 ports	⬜	⬛	🟩
SFP ports	⬜	⬛	🟨

6.8.2 Port State Overview Buttons

Auto-refresh:

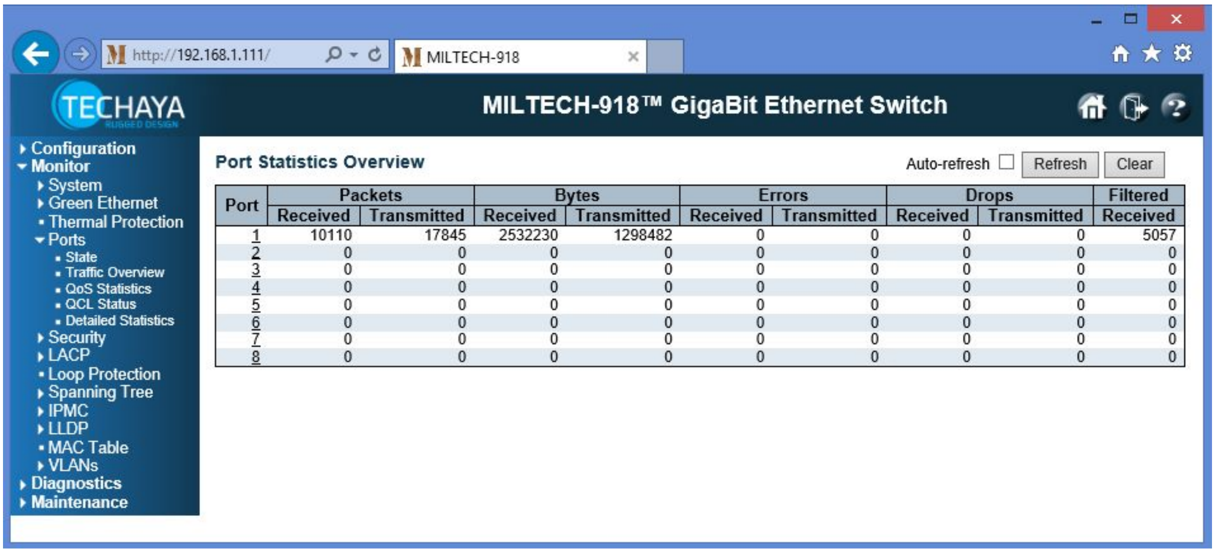
☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page

6.9 Ports – Traffic Overview

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



Port Statistics Overview

Auto-refresh □ Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	10110	17845	2532230	1298482	0	0	0	0	5057
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0

6.9.1 Port Statistics Overview

The displayed counters are:

Port

This column displays the logical port number for this row. Click on the Port number to view Detailed Port Statistics (described in section 6.12 Ports – Detailed Statistics on page 226).

Packets

This column displays the number of pa ckets received and transmitted per port.

Bytes

This column displays the number of bytes received and transmitted per port.

Errors

This column displays the number of frames received in error and the number of incomplete transmissions per port.

Drops

This column displays the number of frames discarded due to ingress or egress congestion.

Filtered

This column displays the number of received frames filtered by the forwarding process.

6.9.2 Port Statistics Overview Buttons

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

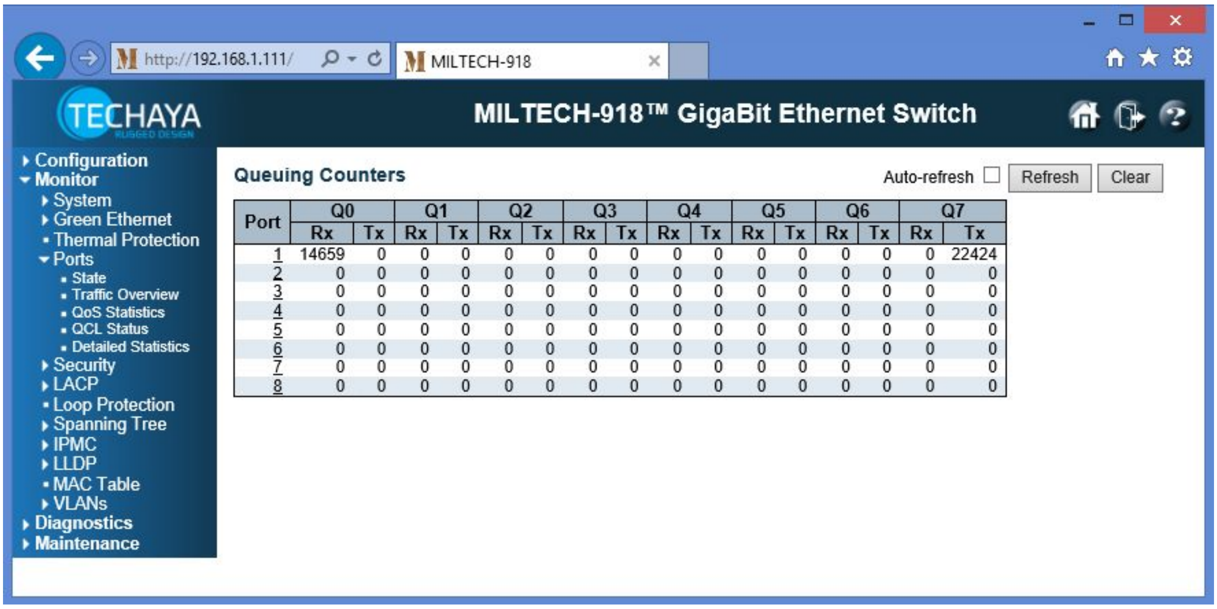
□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Clear: Click to clear the counters for all ports

6.10 Ports – QoS Statistics

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



Queuing Counters

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	14659	0	0	0	0	0	0	0	0	0	0	0	0	0	0	22424
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

6.10.1 Queuing Counters

The displayed counters are:

Port

This column displays the logical port number for this row. Click on the Port number to view Detailed Port Statistics (described in section 6.12 Ports – Detailed Statistics on page 226).

Qn

These column headers display the logical QoS queue for each column. There are 8 QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx

These columns display the number of received and transmitted packets per queue.

6.10.2 Queuing Counters Buttons

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

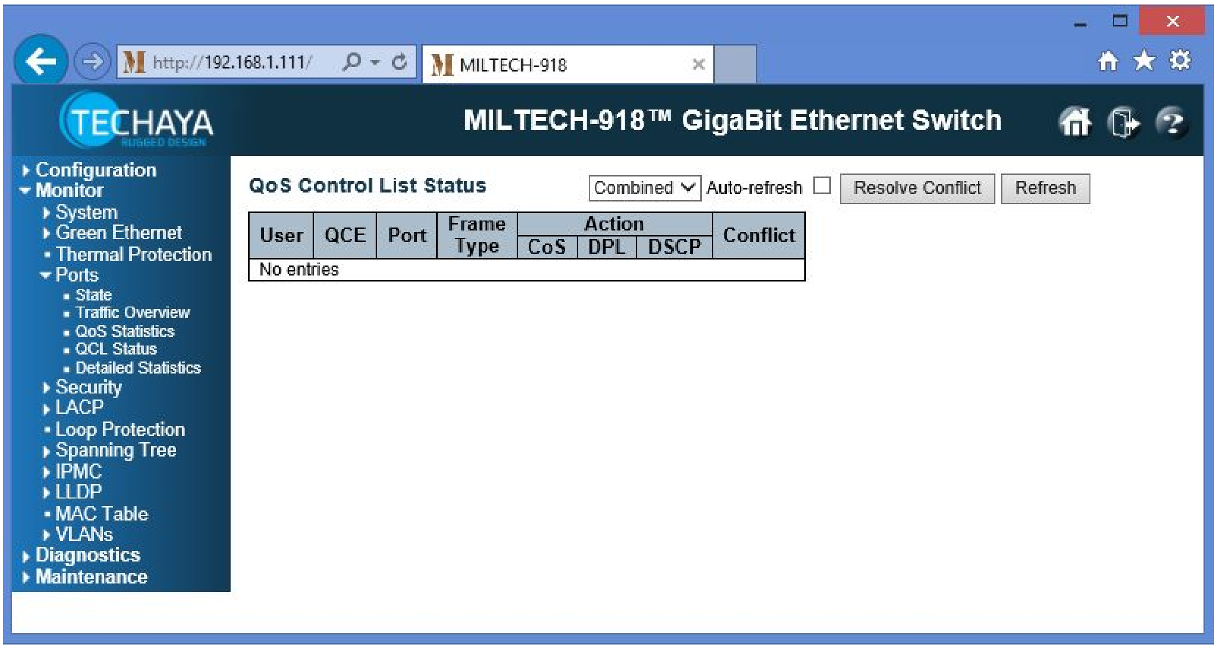
□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Clear: Click to clear the counters for all ports

6.11 Ports – QCL Status

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



QoS Control List Status

Combined Auto-refresh □

User	QCE	Port	Frame Type	Action			Conflict
				CoS	DPL	DSCP	
No entries							

6.11.1 QoS Control List Status

The following QCE details are displayed:

User

This column shows the QCL user.

QCE

This column shows the QCE id.

Port

This column shows the list of ports configured with the QCE.

Frame Type

This column shows 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

This column shows 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

This column shows Conflict status of QCL entries. Since H/W resources are shared by multiple applications, the resources required to add a QCE may not be available when needed. In that case the conflict status is "Yes", otherwise the conflict status "No".

> **Note:** To resolve conflict, click the **Resolve Conflict** button which releases the H/W resources required to add a QCL entry.

6.11.2 Queuing Counters Buttons

Combined

Select the QCL status from the drop down list (Combined, Static, Conflict).

Resolve Conflict:

Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

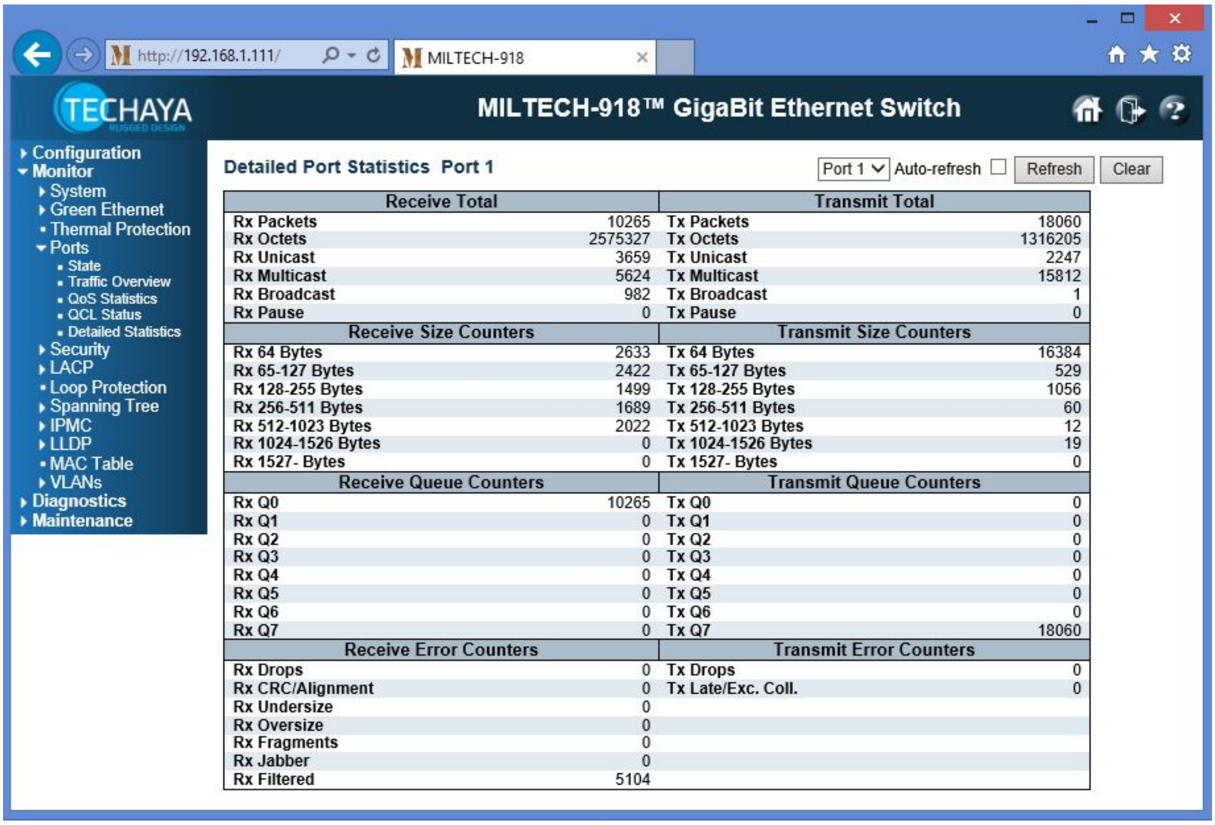
6.12 Ports – Detailed Statistics

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

6.12.1 Detailed Port Statistics

The selected port belongs to the currently selected stack unit, as reflected by the page header.

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



Detailed Port Statistics Port 1

Port 1 Auto-refresh □ Refresh Clear

Receive Total		Transmit Total	
Rx Packets	10265	Tx Packets	18060
Rx Octets	2575327	Tx Octets	1316205
Rx Unicast	3659	Tx Unicast	2247
Rx Multicast	5624	Tx Multicast	15812
Rx Broadcast	982	Tx Broadcast	1
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	2633	Tx 64 Bytes	16384
Rx 65-127 Bytes	2422	Tx 65-127 Bytes	529
Rx 128-255 Bytes	1499	Tx 128-255 Bytes	1056
Rx 256-511 Bytes	1689	Tx 256-511 Bytes	60
Rx 512-1023 Bytes	2022	Tx 512-1023 Bytes	12
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	19
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	10265	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	18060
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	5104		

6.12.1.1 Receive Total and Transmit Total

Rx and Tx Packets

This row shows the number of received and transmitted (good and bad) packets.

Rx and Tx Octets

This row shows the number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

Rx and Tx Unicast

This row shows the number of received and transmitted (good and bad) unicast packets.

Rx and Tx Multicast

This row shows the number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast

This row shows the number of received and transmitted (good and bad) broadcast packets.

Rx and Tx Pause

This row shows a count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

6.12.1.2 Receive and Transmit Size Counters

This section shows the number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

6.12.1.3 Receive and Transmit Queue Counters

This section shows the number of received and transmitted packets per input and output queue.

6.12.1.4 Receive Error Counters

Rx Drops

This row shows the number of frames dropped due to lack of receive buffers or egress congestion.

Rx CRC/Alignment

This row shows the number of frames received with CRC or alignment errors.

Rx Undersize

This row shows the number of short[1] frames received with valid CRC.

Rx Oversize

This row shows the number of long[2] frames received with valid CRC.

Rx Fragments

This row shows the number of short[1] frames received with invalid CRC.

Rx Jabber

The number of long[2] frames received with invalid CRC.

Rx Filtered

This row shows the number of received frames filtered by the forwarding process.

Footnotes

[1] Short frames are frames that are smaller than 64 bytes.

[2] Long frames are frames that are longer than the configured maximum frame length for this port.

6.12.1.5 Transmit Error Counters

Tx Drops

This row shows the number of frames dropped due to output buffer congestion.

Tx Late/Exc. Coll.

This row shows the number of frames dropped due to excessive or late collisions.

6.12.2 Detailed Port Statistics Buttons

Port select box:

The port select box determines which port is affected by clicking the buttons. Select a port from the drop-down list.

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

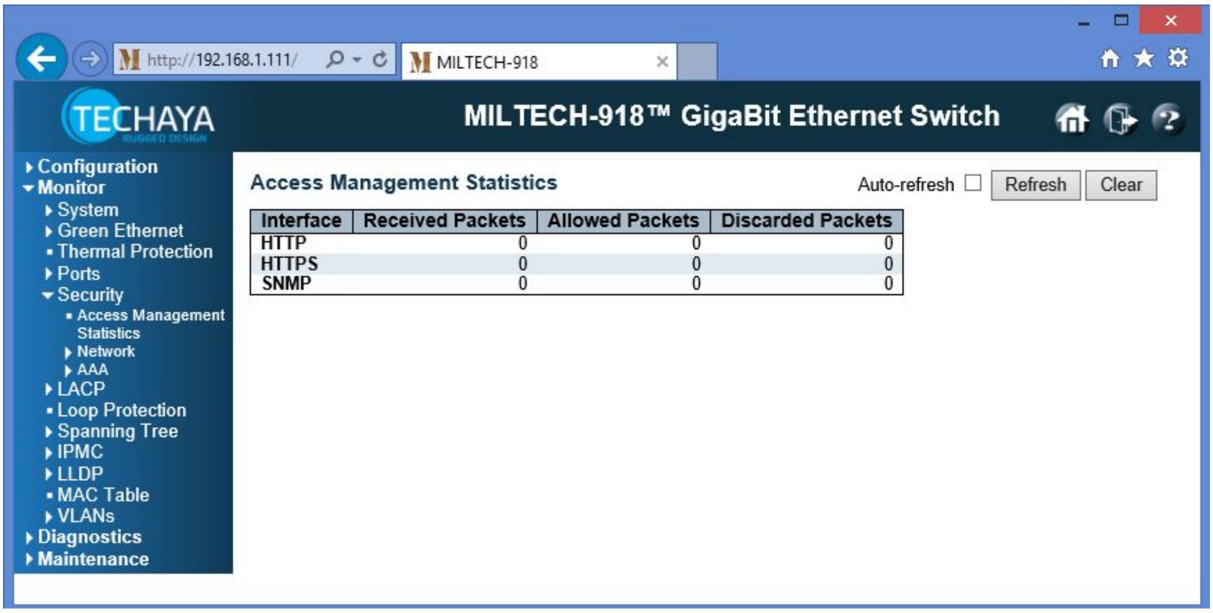
□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Clear: Click to clear the counters for the selected port

6.13 Security – Access Management

This page provides statistics for access management.



Access Management Statistics

Auto-refresh □ Refresh Clear

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0

6.13.1 Access Management Statistics

The displayed counters are:

Interface

This column displays the interface type through which the remote host can access the switch.

Received Packets

This column displays the number of received packets from the interface when access management mode is enabled.

Allowed Packets

This column displays the number of allowed packets from the interface when access management mode is enabled.

Discarded Packets

This column displays the number of discarded packets from the interface when access management mode is enabled.

6.13.2 Access Management Statistics Buttons

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

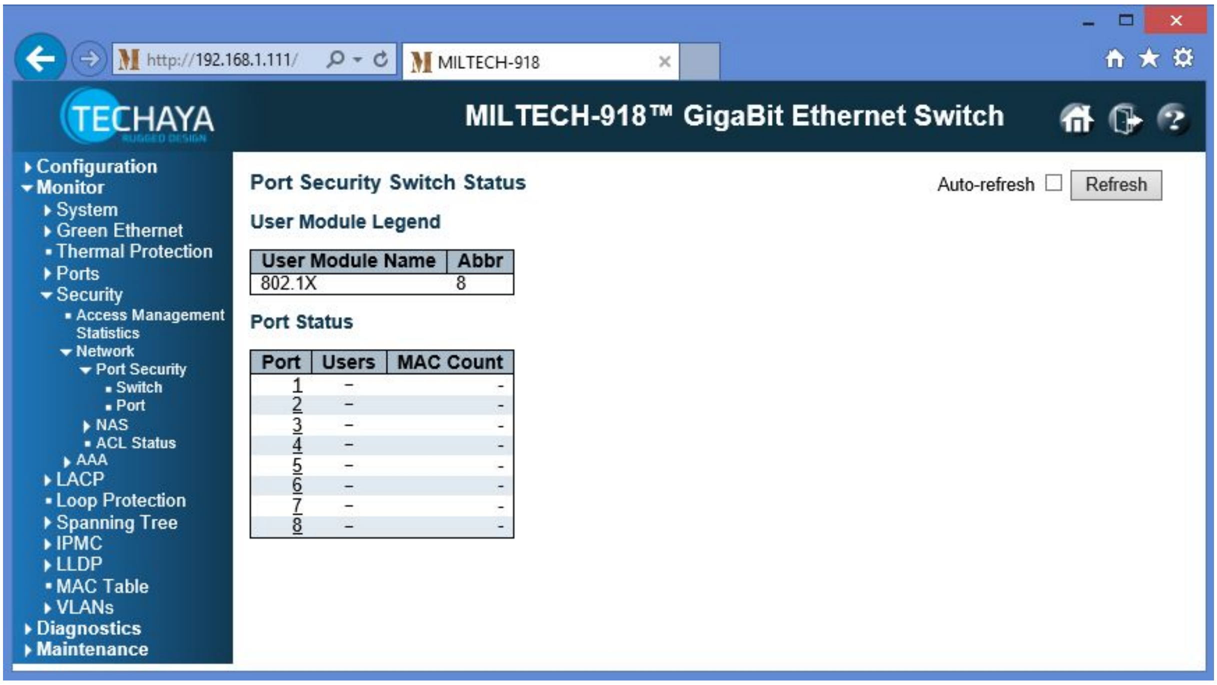
Clear: Click to clear the counters for all ports

6.14 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 will be blocked until that user module decides otherwise.

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



Port Security Switch Status

User Module Legend

User Module Name	Abbr
802.1X	8

Port Status

Port	Users	MAC Count
1	–	-
2	–	-
3	–	-
4	–	-
5	–	-
6	–	-
7	–	-
8	–	-

6.14.1 Port Security-Switch Status

6.14.1.1 User Module Legend

The legend shows all user modules that may request Port Security services.

User Module Name

This column displays the full name of a module that may request Port Security services.

Abbr

This column displays a one-letter abbreviation of the user module. This is used in the Users column in the port status table.

6.14.1.2 Port Status

The table has one row for each port on the switch and a number of columns:

Port

This column displays the port number for which the status applies. Click the Port number to see the status for this particular port (described in section 6.15.1 Port Security Port Status on page 233).

Users

This column displays Port Security status (enabled/disabled).

Each of the user modules has a column that shows whether that module has enabled Port Security or not.

A dash (“-”) means that the corresponding user module is not enabled.

A letter indicates that the user module abbreviated by that letter (see Abbr above) has enabled port security.

MAC Count

This column displays the number of currently learned MAC addresses (forwarding as well as blocked) on the port. If no user modules are enabled on the port, a dash (“-”) will be shown.

6.14.2 Access Management Statistics Buttons

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□Disable Auto-refresh (This is the default.)

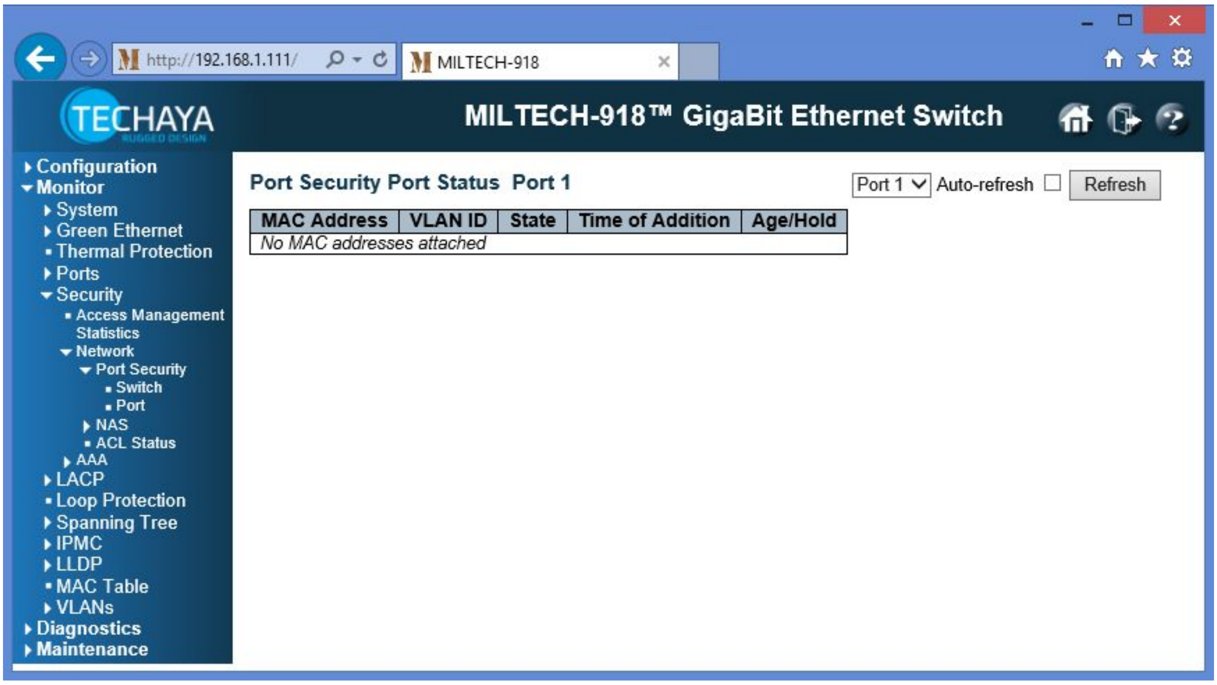
Refresh: Click to refresh the page immediately

6.15 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 will be blocked until that user module decides otherwise.

6.15.1 Port Security Port Status Port n



Port Security Port Status Port 1

Port 1 Auto-refresh □ Refresh

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
No MAC addresses attached				

MAC Address and VLAN ID

These columns display 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

This column displays the state of the corresponding MAC address: whether it is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition

This column displays the date and time when this MAC address was added to the port.

Age/Hold

If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash ("-") will be shown.

6.15.2 Port Security Port Status Buttons

Port select box:

The port select box determines which port's status to display. Select a port from the drop-down list.

Auto-refresh:

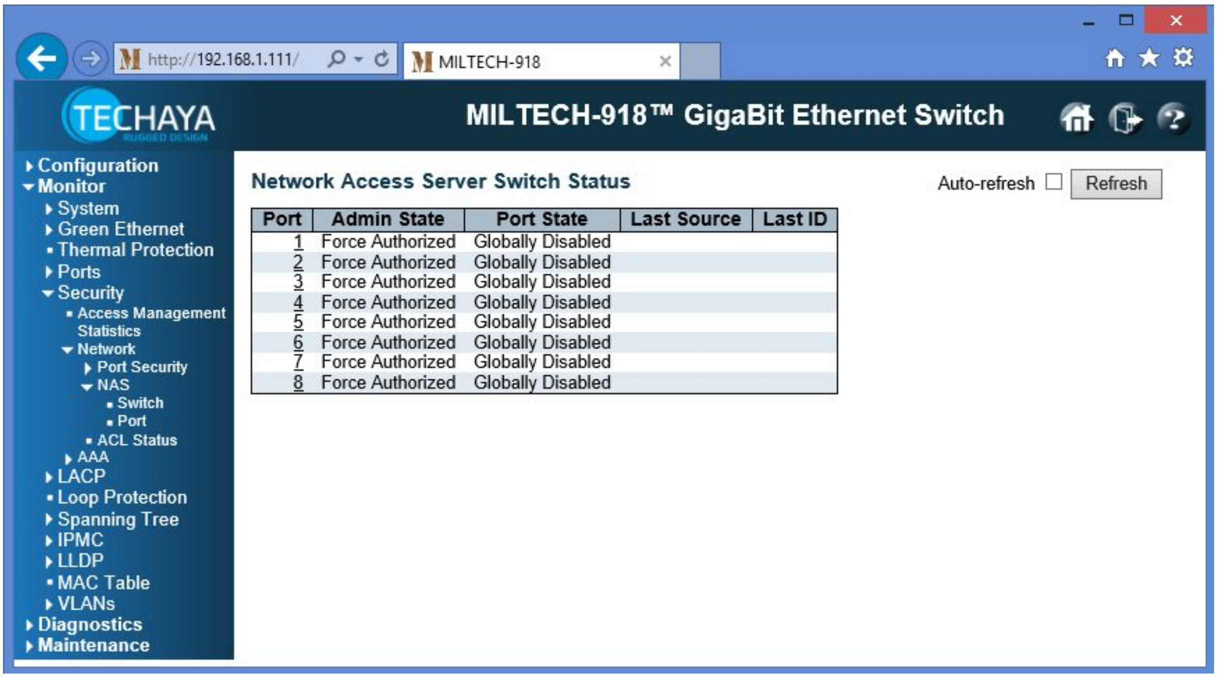
☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

6.16 Security – Network – NAS – Switch

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



Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID
1	Force Authorized	Globally Disabled		
2	Force Authorized	Globally Disabled		
3	Force Authorized	Globally Disabled		
4	Force Authorized	Globally Disabled		
5	Force Authorized	Globally Disabled		
6	Force Authorized	Globally Disabled		
7	Force Authorized	Globally Disabled		
8	Force Authorized	Globally Disabled		

6.16.1 Network Access Server Switch Status

Port

This column displays the port number for which the status applies. Click the Port number to navigate to detailed NAS statistics for this port (described in section 6.17 Security – Network – NAS – Port on page 237).

Admin State

This column displays the port's current administrative state. Refer to NAS Admin State in section 5.20.2 Port Configuration on page 125 for a description of possible values.

Port State

This column displays the current state of the port. Refer to NAS Port State in section 5.20.2 Port Configuration on page 125 for a description of the individual states.

Last Source

This column displays 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

This column displays 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.

6.16.2 Network Access Server Switch Status Buttons

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

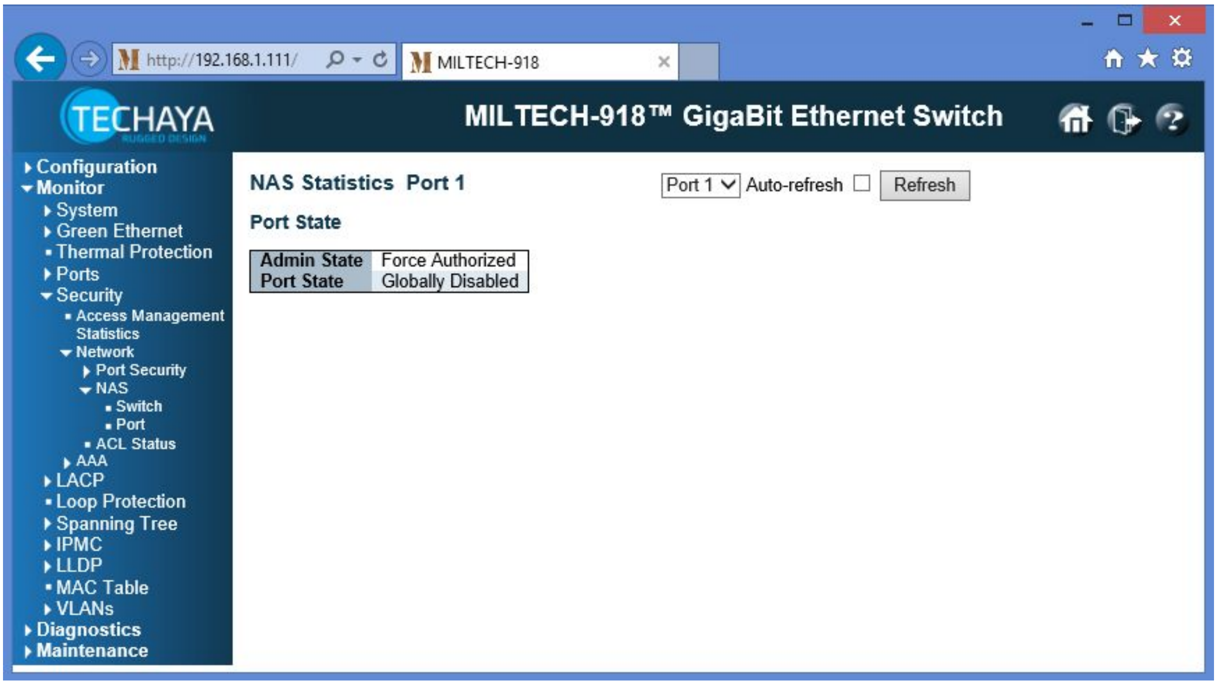
6.17 Security – Network – NAS – Port

This page shows the MAC addresses secured by the Port Security module.

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.

6.17.1 NAS Statistics Port n



NAS Statistics Port 1

Port State

Admin State	Force Authorized
Port State	Globally Disabled

6.17.1.1 Port State

Admin State

This column displays the port's current administrative state. Refer to NAS Admin State in section 5.20.2 Port Configuration on page 125 for a description of possible values.

Port State

This column displays the current state of the port. Refer to NAS Port State in section 5.20.2 Port Configuration on page 125 for a description of the individual states.

6.17.2 NAS Statistics Buttons

Port select box: Port 1

The port select box determines which port's details to display. Select a port from the drop-down list.

Auto-refresh:

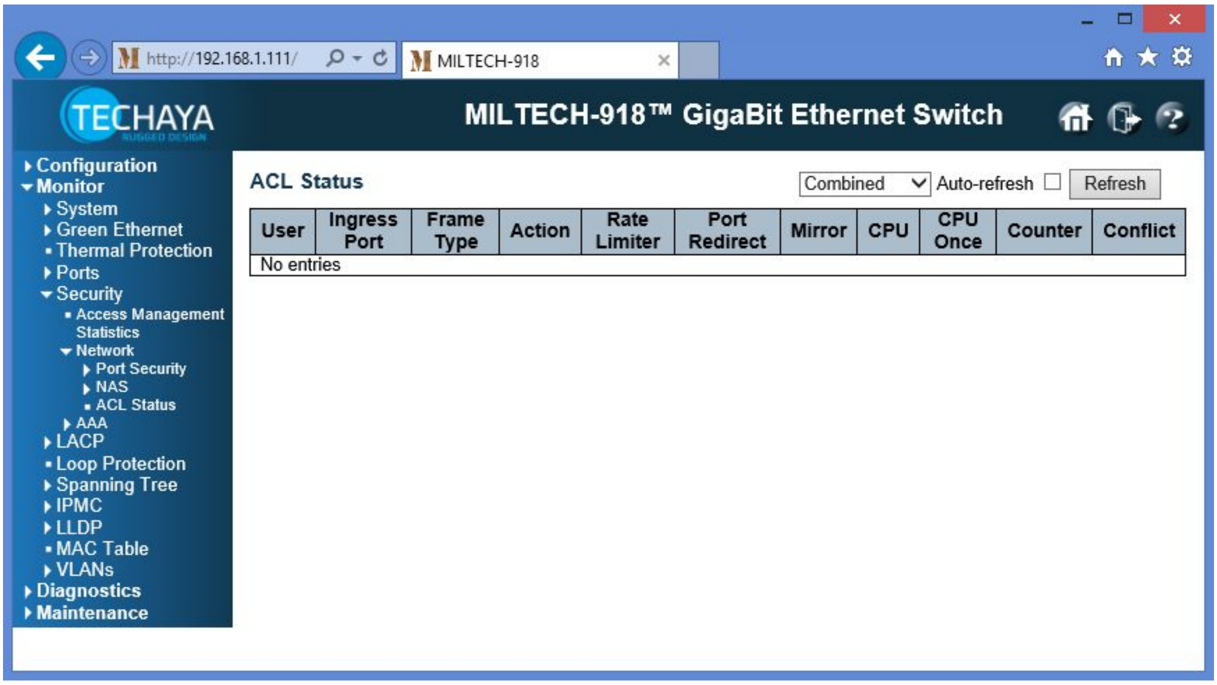
☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

6.18 Security – Network – ACL Status

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



ACL Status

Combined | Auto-refresh □ | Refresh

User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
No entries										

6.18.1 ACL Status

The following ACL Status details are displayed:

User

This column shows the ACL user.

Ingress Port

This column shows the ingress port of the ACE. Possible values are:

All: The ACE will match all ingress port

Port: The ACE will match a specific ingress port

Frame Type

This column shows the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type

EType: The ACE will match Ethernet Type frames.

ARP: The ACE will match ARP/RARP frames

IPv4: The ACE will match all IPv4 frames

IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol

IPv4/UDP: The ACE will match IPv4 frames with UDP protocol

IPv4/TCP: The ACE will match IPv4 frames with TCP protocol

IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP

IPv6: The ACE will match all IPv6 standard frames.

> **Note:** An Ethernet Type based ACE will not get matched by IP and ARP frames.

Action

This column shows the forwarding action of the ACE. Possible values are:

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

This column shows 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

This column shows the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are:

Disabled: The port redirect operation is disabled

Specific port number: Frames will be redirected to this port number

Mirror

This column shows 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

This column shows the number of times the ACE was hit by a frame.

Conflict

This column shows the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

6.18.2 ACL Status Buttons

Select Box

: The select box determines which ACL user is affected by clicking the buttons. Select a user from the drop down list:

Combined

Static

IPMC

Loop Protect

Conflict

Auto-refresh:

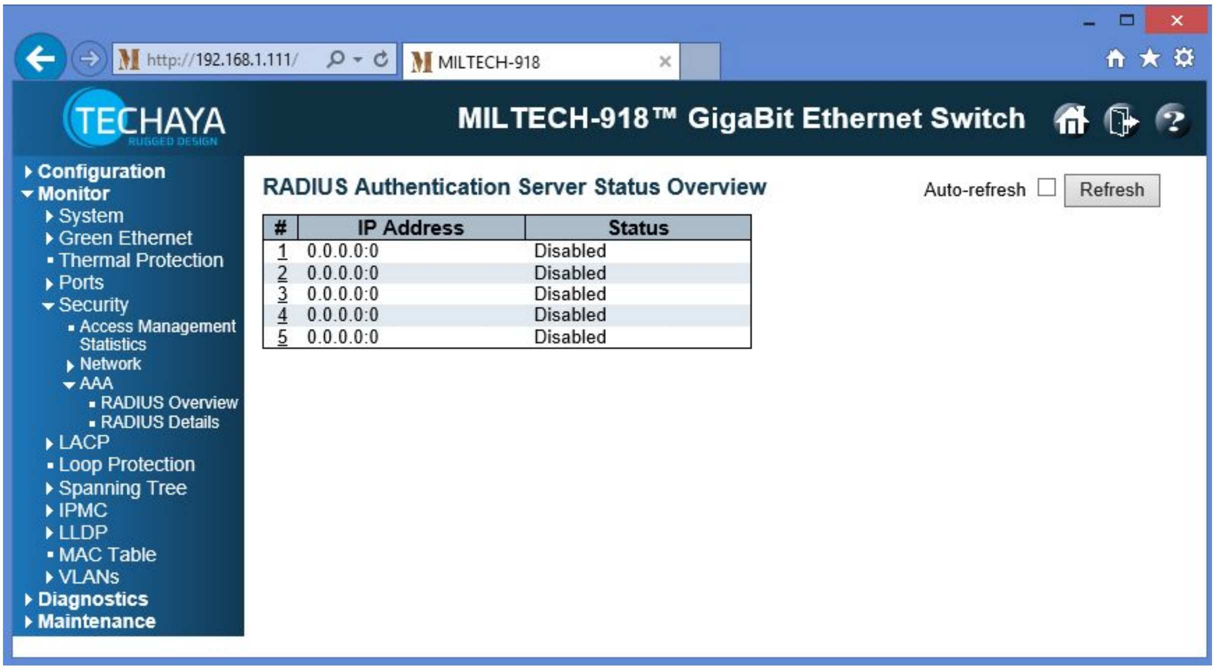
☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

6.19 Security – AAA – RADIUS Overview

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



RADIUS Authentication Server Status Overview

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

6.19.1 RADIUS Authentication Server Status Overview

#

This column displays the RADIUS server number. Click the RADIUS server number to navigate to detailed statistics for this server (described in section 6.20 Security – AAA – RADIUS Details on page 244).

IP Address

This column displays the IP address and UDP port number
(in <IP Address>:<UDP Port> notation) of this server.

Status

This column displays 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 will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

6.19.2 RADIUS Authentication Server Status Buttons

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

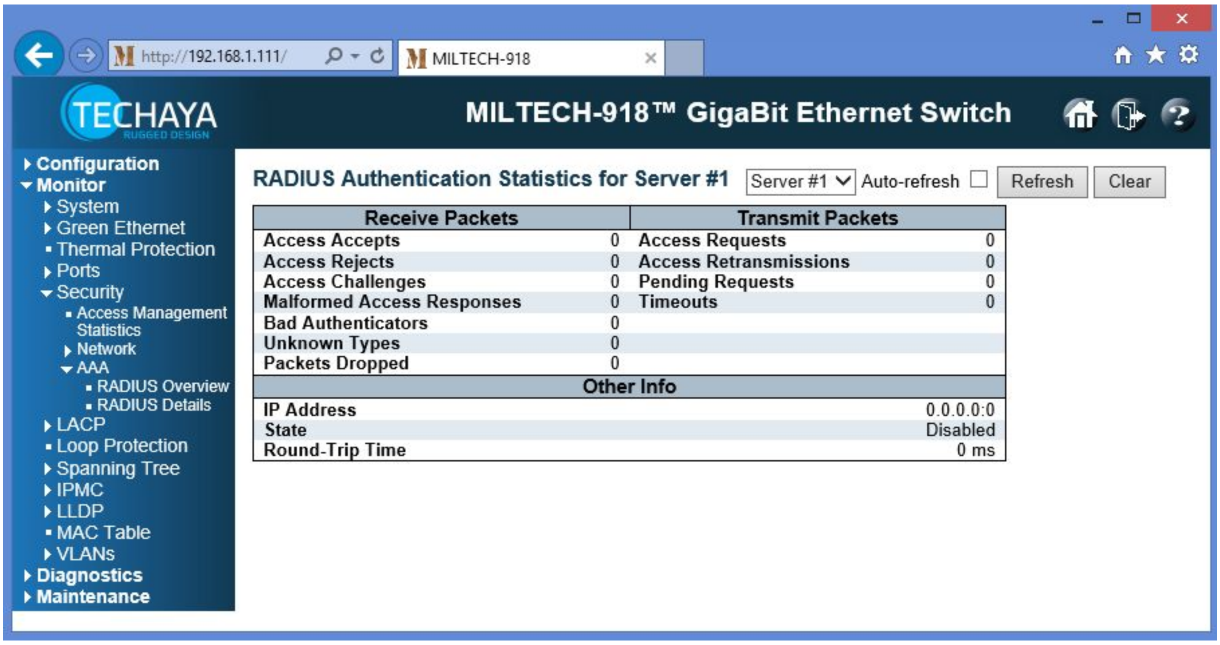
□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

6.20 Security – AAA – RADIUS Details

This page provides detailed statistics for a particular RADIUS server.

6.20.1 RADIUS Authentication Statistics for Server n



RADIUS Authentication Statistics for Server #1 Server #1 Auto-refresh □ Refresh Clear

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		

Other Info	
IP Address	0.0.0.0:0
State	Disabled
Round-Trip Time	0 ms

6.20.1.1 Receive Packets (Rx)

Name	Description
Access Accepts	Displays the number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Access Rejects	Displays the number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Access Challenges	Displays the number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Malformed Access Responses	Displays the number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. The following are not included as malformed access responses: Bad authenticators or Message Authenticator attributes or unknown types.
Bad Authenticators	Displays the number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.

Name	Description
Unknown Types	Displays the number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Packets Dropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason

6.20.1.2 Transmit Packets (Tx)

Name	Description
Access Requests	Displays the number of RADIUS Access-Request packets sent to the RADIUS authentication server. This does not include retransmissions.
Access Retransmissions	Displays the number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Pending Requests	Displays the number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Timeouts	Displays the number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

6.20.1.3 Other Info

IP Address

This field displays the IP address and UDP port for the authentication server in question.

State

This field displays the state of the server. It takes one of the following values:

Disabled: The selected 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 will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Round-Trip Time

This field displays the time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there has not been a round-trip communication with the server yet

6.20.2 RADIUS Authentication Statistics Buttons

Server select box:

The server select box determines which server is affected by clicking the buttons.

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

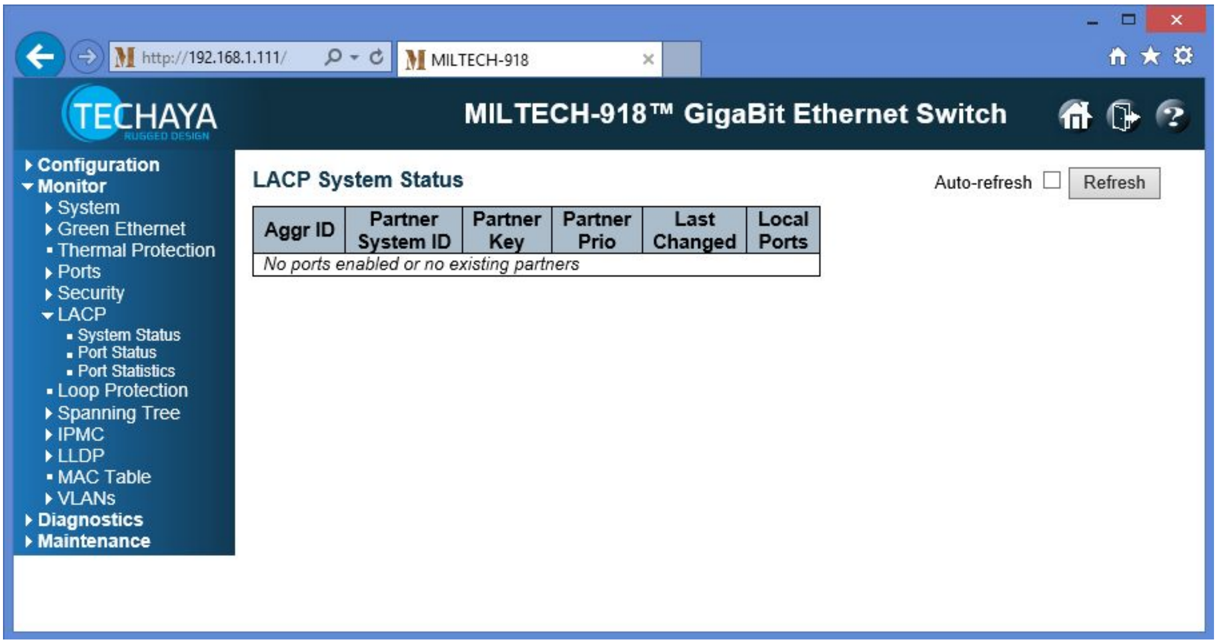
□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Clear: Click to clear the counters for the selected server. The “Pending Requests” counter will not be cleared by this operation.

6.21 LACP – System Status

This page provides a status overview for all LACP instances.



LACP System Status

Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
No ports enabled or no existing partners					

6.21.1 LACP System Status

Aggr ID

This column displays 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

This column displays the system ID (MAC address) of the aggregation partner.

Partner Key

This column displays the Key that the partner has assigned to this aggregation ID.

Partner Prio

This column displays the priority of the partner port.

Last changed

This column displays the time since this aggregation changed.

Local Ports

This column displays the ports that are a part of this aggregation for this switch.

6.21.2 LACP System Status Buttons

Auto-refresh:

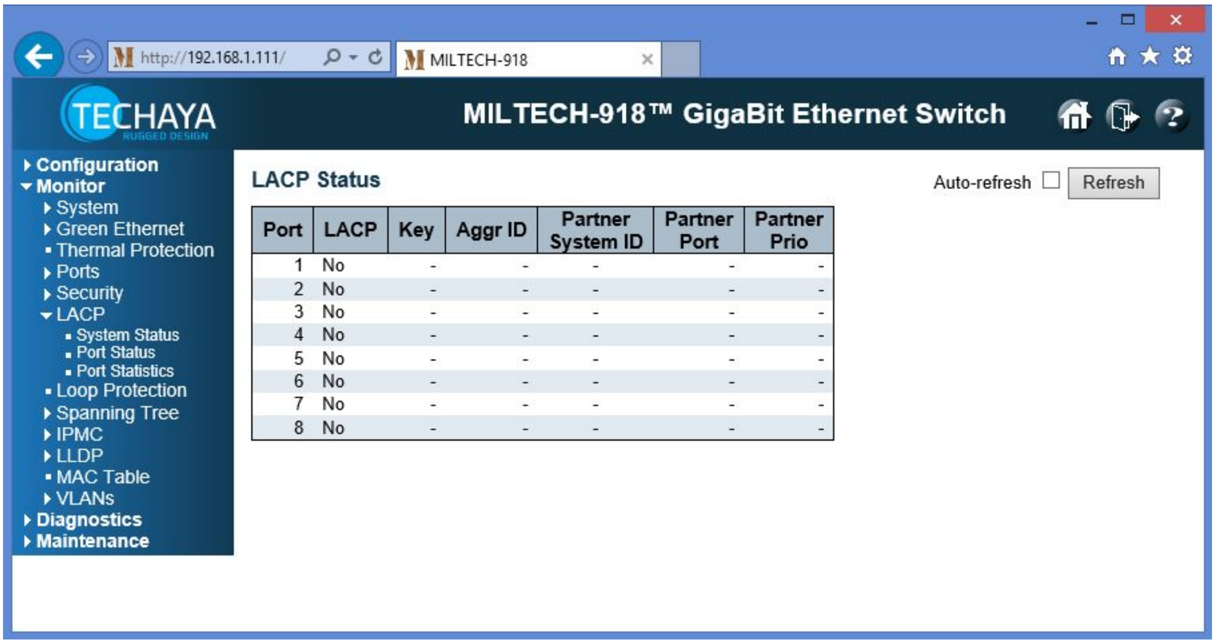
☑ Enable Auto-refresh – to refresh the page automatically every 3

seconds
□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

6.22 LACP – Port Status

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



LACP Status

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

6.22.1 LACP Status

Port

This column displays the switch port number for the row of status information.

LACP

This column displays the LACP operational status of the port. It takes one of the following values:

Yes: LACP is enabled and the port link is up

No: LACP is **not** enabled or the port link is down

Backup: The port could not join the aggregation group but will join if other port leaves. Meanwhile its LACP status is disabled.

Key

This column displays the key assigned to this port. Only ports with the same key can aggregate together.

Aggr ID

This column displays the Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.

Partner System ID

This column displays the partner’s System ID (MAC address).

Partner Port

This column displays the port number of the partner connected to this port.

Partner Prio

This column displays the partner's port priority.

6.22.2 LACP Status Buttons

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

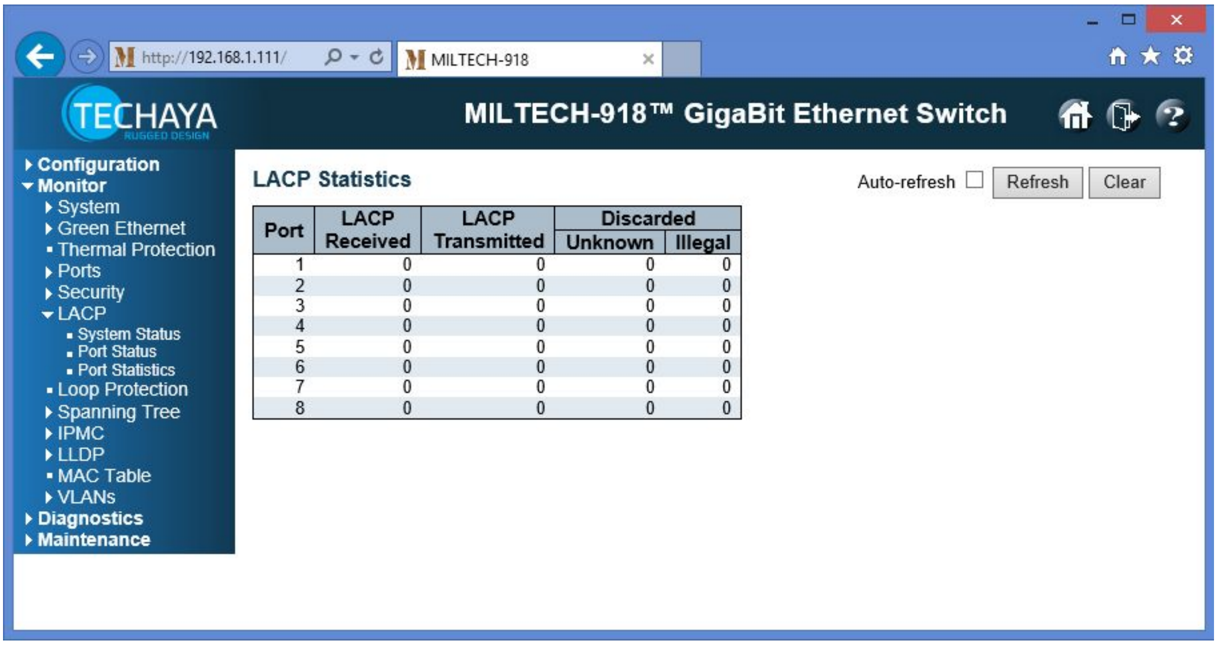
□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

6.23 LACP – Port Statistics

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

6.23.1 LACP Statistics



LACP Statistics

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

Port

This column displays the switch port number for the row of statistics.

LACP Received

This column shows how many LACP frames have been received at each port.

LACP Transmitted

This column shows how many LACP frames have been sent from each port.

Discarded

This column shows how many unknown or illegal LACP frames have been discarded at each port.

6.23.2 LACP Statistics Buttons

Server select box: Server #1

The server select box determines which server is affected by clicking the buttons.

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3

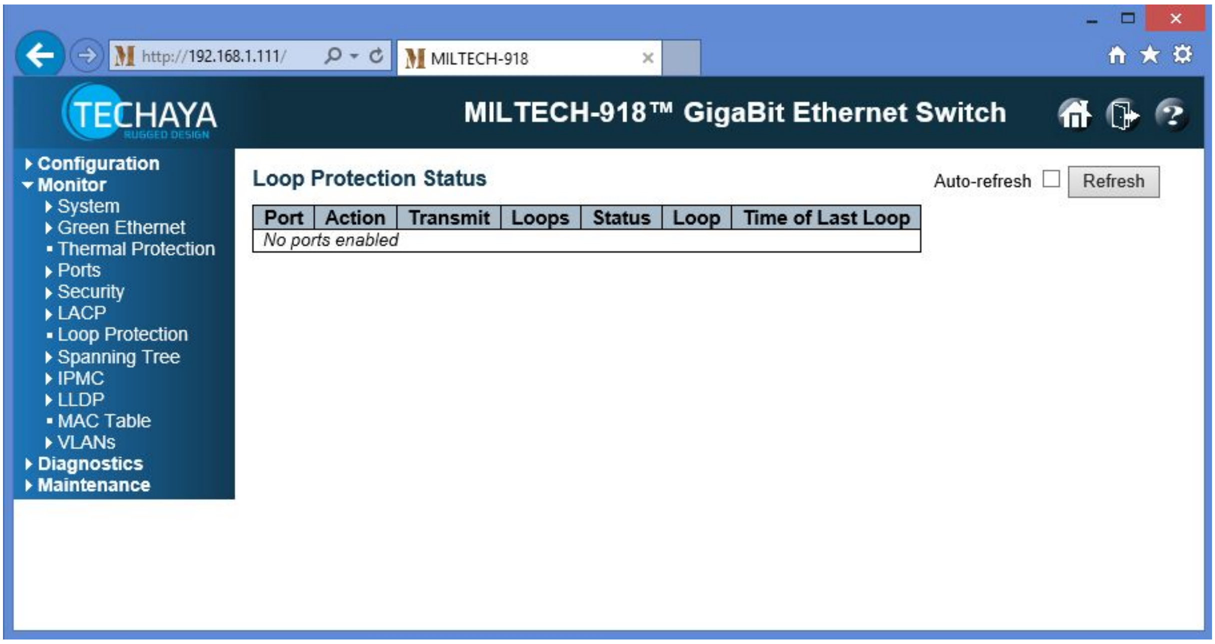
seconds
□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Clear: Click to clear the counters for all ports

6.24 Loop Protection

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



Loop Protection Status

Auto-refresh □ Refresh

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
No ports enabled						

6.24.1 Loop Protection Status

Port

This column displays the switch port number of the logical port.

Action

This column displays the currently configured port action.

Transmit

This column displays the currently configured port transmit mode.

Loops

This column displays the number of loops detected on this port.

Status

This column displays the current loop protection status of the port.

Loop

This column displays whether or not a loop is currently detected on the port.

Time of Last Loop

This column displays the time of the last loop event detected.

6.24.2 LACP Status Buttons

Auto-refresh:

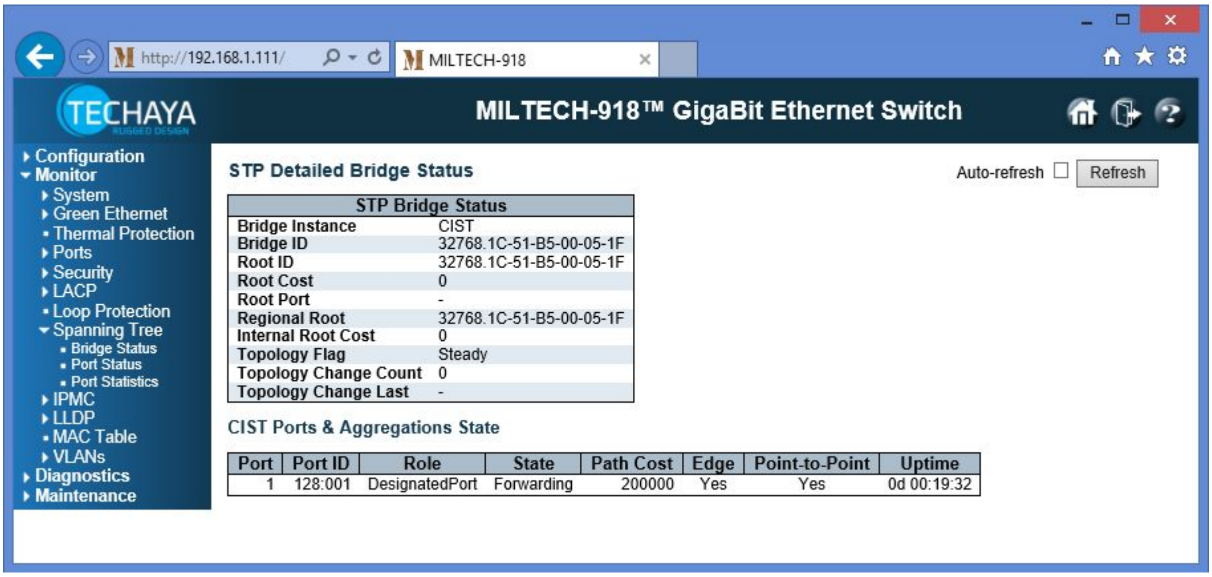
☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

6.25 Spanning Tree – Bridge Status

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



STP Detailed Bridge Status

Auto-refresh □ Refresh

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.1C-51-B5-00-05-1F
Root ID	32768.1C-51-B5-00-05-1F
Root Cost	0
Root Port	-
Regional Root	32768.1C-51-B5-00-05-1F
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
1	128:001	DesignatedPort	Forwarding	200000	Yes	Yes	0d 00:19:32

6.25.1 STP Detailed Bridge Status

6.25.1.1 STP Bridge Status

Bridge Instance

This field displays the Bridge instance: CIST, MST1, ...

Bridge ID

This field displays the Bridge ID of this Bridge instance.

Root ID

This field displays the Bridge ID of the currently elected root bridge.

Root Cost

This field displays the Root Path Costs:

- For the Root Bridge this is zero
- For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge

Root Port

This field displays the switch port currently assigned the root port role.

Regional Root

This field displays the Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge (for the CIST instance only).

Internal Root Cost

This field displays the Regional Root Path Cost:

- For the Regional Root Bridge this is zero
- For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge (for the CIST instance only).

Topology Flag

This field displays the current state of the Topology Change Flag of this Bridge instance.

Topology Change Count

This field displays the number of times where the topology change flag has been set (during a one-second interval).

Topology Change Last

This field displays the time passed since the Topology Flag was last set.

6.25.2 CIST Ports & Aggregations State

Port

This column displays the switch port number of the logical STP port.

Port ID

This column displays the port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.

Role

This column displays the current STP port role. The port role can be one of the following values:

- AlternatePort
- BackupPort
- RootPort
- DesignatedPort

State

This column displays the current STP port state. The port state can be one of the following values:

- Discarding
- Learning
- Forwarding

Path Cost

This column displays the current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value.

Edge

This column displays the current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.

Point-to-Point

This column displays the current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state.

Uptime

This column displays the time since the bridge port was last initialized.

6.25.3 STP Bridge Status Buttons

Auto-refresh:

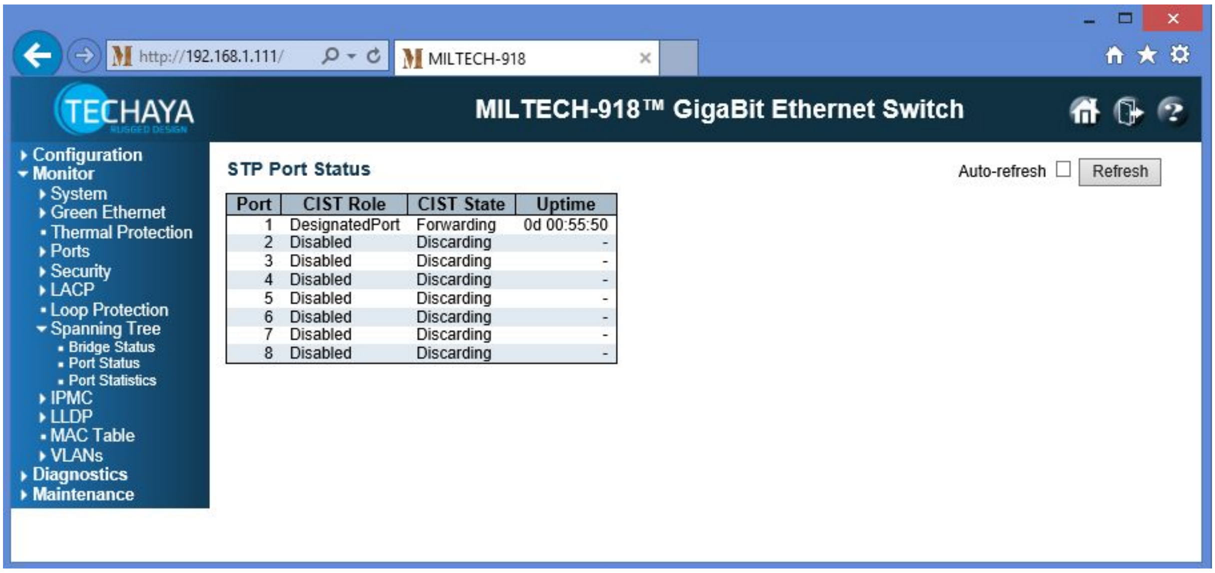
☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

6.26 Spanning Tree – Port Status

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



STP Port Status

Auto-refresh □ Refresh

Port	CIST Role	CIST State	Uptime
1	DesignatedPort	Forwarding	0d 00:55:50
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-

6.26.1 STP Port Status

Port

This column displays the switch port number of the logical STP port.

CIST Role

This column displays the current STP port role of the CIST port. The port role can be one of the following values:

- AlternatePort
- BackupPort
- RootPort
- DesignatedPort
- Disabled

CIST State

This column displays the current STP port state of the CIST port. The port state can be one of the following values:

- Discarding
- Learning
- Forwarding

Uptime

This column displays the time since the bridge port was last initialized.

6.26.2 STP Port Status Buttons

Auto-refresh:

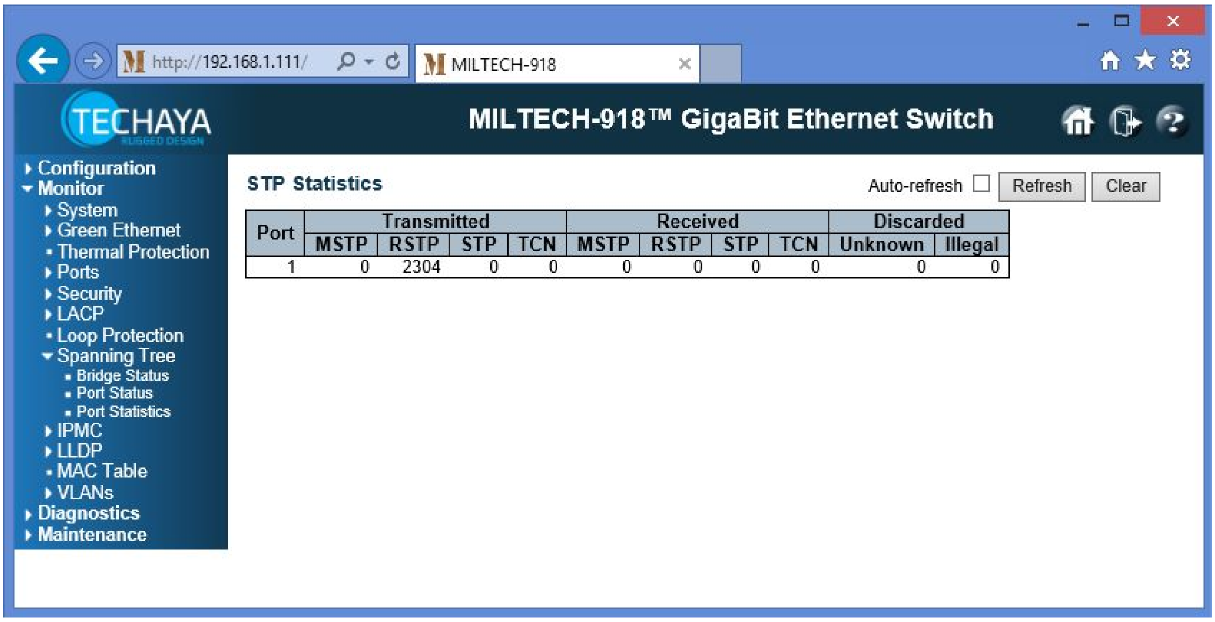
☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

6.27 Spanning Tree – Port Statistics

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



STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	0	2304	0	0	0	0	0	0	0	0

6.27.1 STP Statistics

Port

This column displays the switch port number of the logical STP port.

6.27.1.1 Transmitted/Received

MSTP

This column displays the number of MSTP BPDUs received/transmitted on the port.

RSTP

This column displays the number of RSTP BPDUs received/transmitted on the port.

STP

This column displays the number of legacy STP Configuration BPDUs received/transmitted on the port.

TCN

This column displays the number of (legacy) Topology Change Notification BPDUs received/transmitted on the port.

6.27.1.2 Discarded

Unknown

This column displays the number of unknown Spanning Tree BPDUs received (and discarded) on the port.

Illegal

This column displays the number of illegal Spanning Tree BPDUs received (and discarded) on the port.

6.27.2 STP Port Status Buttons

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

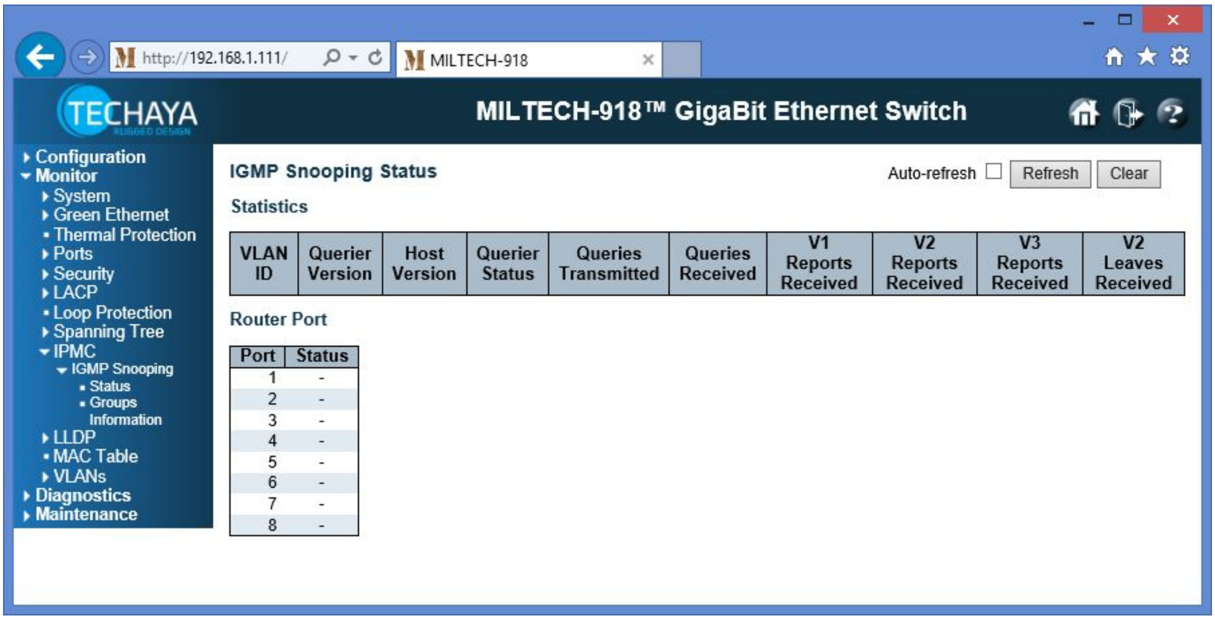
□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Clear: Click to reset the counters

6.28 IPMC – IGMP Snooping – Status

This page provides Internet Group Management Protocol (IGMP) Snooping status.



IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

6.28.1 IGMP Snooping Status

6.28.1.1 Statistics

VLAN ID

This column displays the VLAN ID of the entry.

Querier Version

This column displays the Version of the current Working Querier.

Host Version

This column displays the Version of the current Working Host.

Querier Status

This column displays the Querier status as

- ACTIVE
- IDLE
- DISABLE (denotes the specific interface is administratively disabled)

Queries Transmitted

This column displays the number of Transmitted Queries.

Queries Received

This column displays the number of Received Queries.

V1 Reports Received

This column displays the number of Received V1 Reports.

V2 Reports Received

This column displays the number of Received V2 Reports.

V3 Reports Received

This column displays the number of Received V3 Reports.

V2 Leaves Received

This column displays the number of Received V2 Leaves.

6.28.1.2 Router Port

This table displays the router status of each port (indicates 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.

Port

This column displays the switch port number.

Status

This column indicates whether specific port is a router port or not:

Static:	the port is configured to be a router port
Dynamic:	the port has learned to be a router port
Dash ("-"):	the port is **not** a router port

6.28.2 STP Port Status Buttons

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

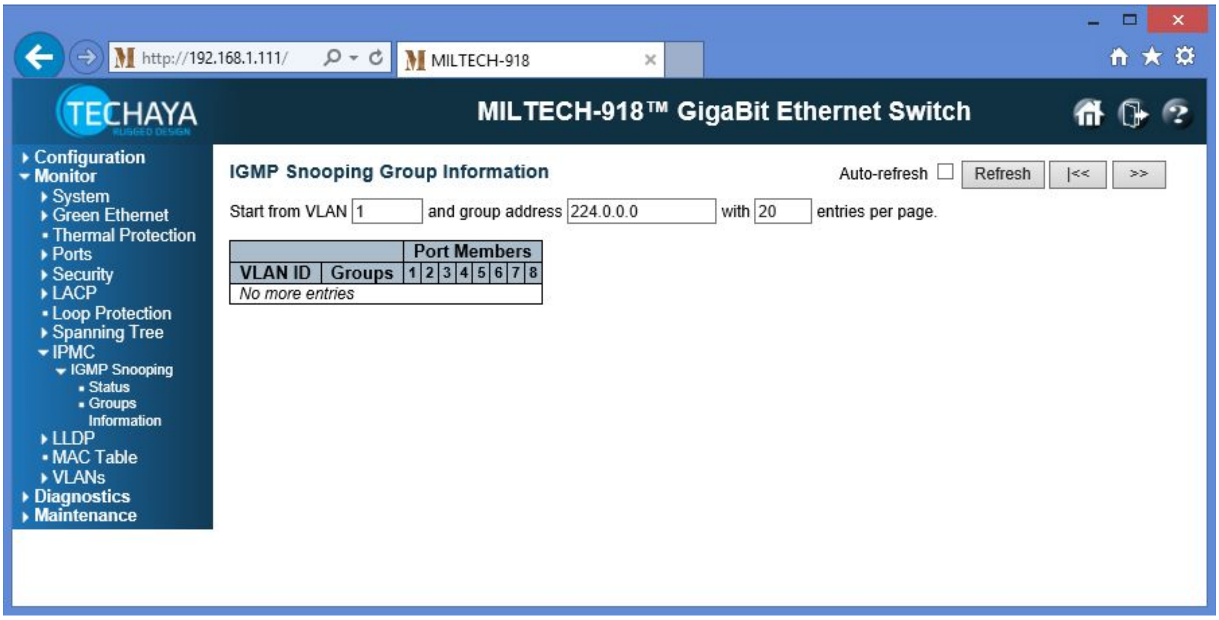
□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Clear: Click to clear all statistics counters

6.29 IPMC – IGMP Snooping – Groups

This page provides Internet Group Management Protocol (IGMP) Snooping status.



IGMP Snooping Group Information

Start from VLAN 1 and group address 224.0.0.0 with 20 entries per page.

		Port Members							
VLAN ID	Groups	1	2	3	4	5	6	7	8
No more entries									

6.29.1 Navigating the IGMP Group Table

Each page can show up to 99 entries from the IGMP Group table. Set the number of entries per page in the “entries per page” input field (the default is 20). When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

The “Start from VLAN”, and “group address” input fields allow the user to set the starting point in the IGMP Group Table. Click the **Refresh** button to update the displayed table starting from the current settings or the closest next IGMP Group Table match. After clicking the **Refresh** button, the two input fields will assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

6.29.2 IGMP Snooping Groups Information

VLAN ID

This column displays the VLAN ID of the group.

Groups

This column displays the Group address of the group displayed.

Port Members

This column displays Ports that are members of this group.

6.29.3 STP Port Status Buttons

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□Disable Auto-refresh (This is the default.)

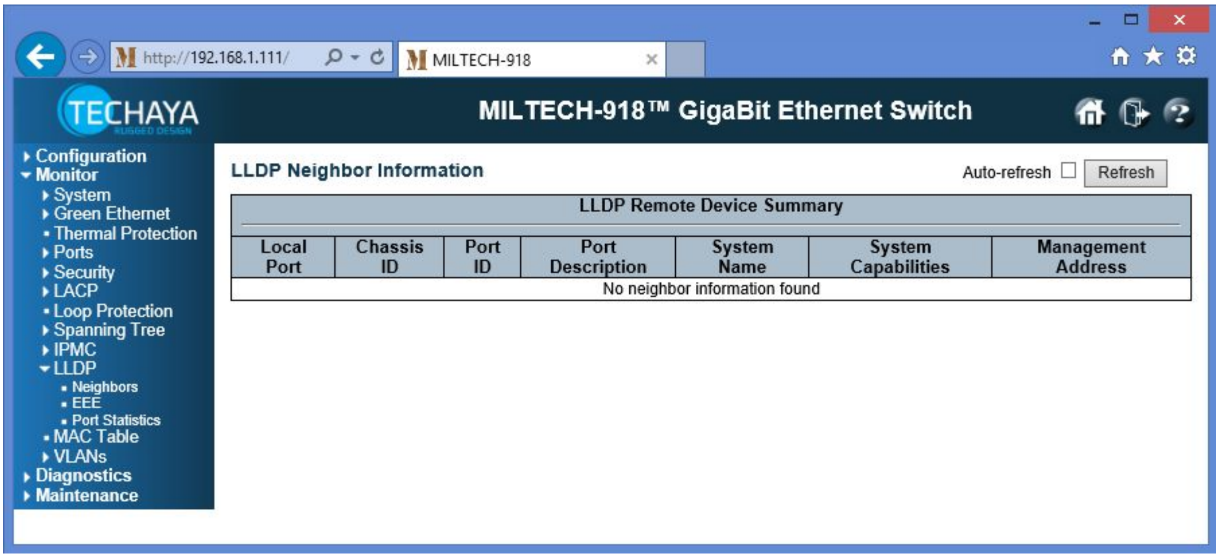
Refresh: Click to refresh the page immediately

Back Arrows (|<<): Updates the table, starting with the first entry in the IGMP Group Table.

Forward Arrows (>>): Updates the table, starting with the entry after the last entry currently displayed.

6.30 LLDP – Neighbors

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



LLDP Neighbor Information

LLDP Remote Device Summary						
Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
No neighbor information found						

6.30.1 LLDP Neighbor Information

6.30.1.1 LLDP Remote Device Summary

Local Port

This column displays the port on which the LLDP frame was received.

Chassis ID

This column displays the Chassis ID (Identification) of the neighbor's LLDP frames.

Port ID

This column displays the Port ID of the neighbor port.

Port Description

This column displays the Port Description advertised by the neighbor unit.

System Name

This column displays the System Name advertised by the neighbor unit.

System Capabilities

This column displays the System Capabilities of the neighbor unit. The possible capabilities are:

- Other

- Repeater
- Bridge
- WLAN Access Point
- Router
- Telephone
- DOCSIS cable device
- Station only
- Reserved

When a capability is enabled, it is followed by (+). If the capability is disabled, it is followed by (-).

Management Address

This column displays the Management Address of the neighbor unit used for higher layer entities to assist discovery by the network management. For example, this might hold the neighbor's IP address.

6.30.2 LLDP Neighbor Information Buttons

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□Disable Auto-refresh (This is the default.)

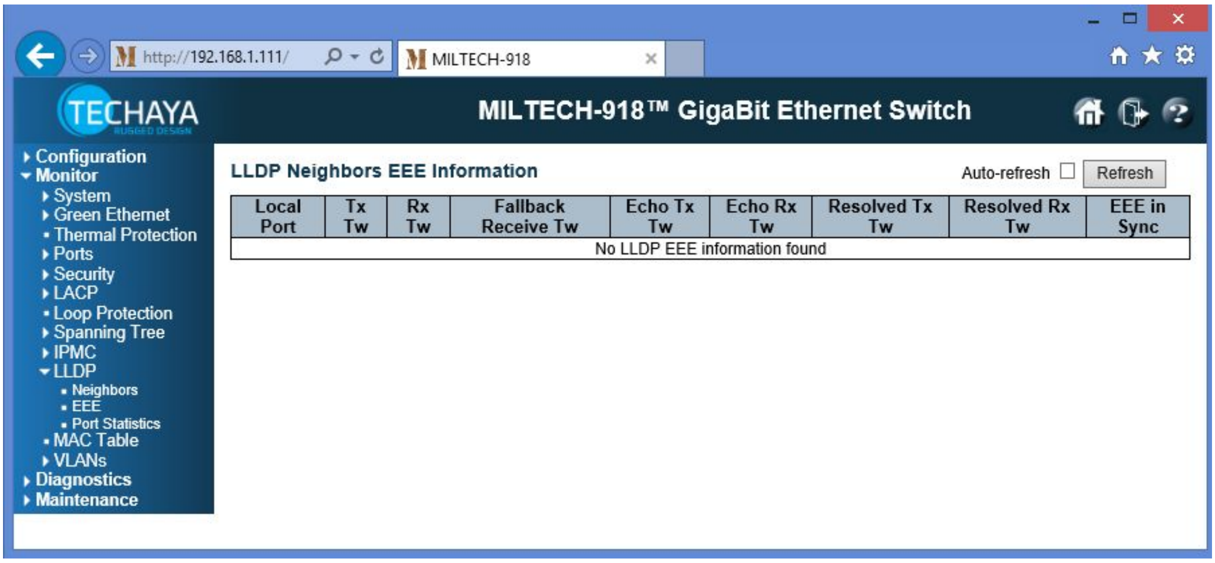
Refresh: Click to refresh the page immediately

6.31 LLDP – EEE

By using Energy Efficient Ethernet (EEE) power savings can be achieved at the expense of traffic latency. This latency results from the time required to boot up circuits that were turned off by EEE to save power. This time is called "wakeup time".

To achieve minimal latency, devices can use Link Layer Discovery Protocol (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.



LLDP Neighbors EEE Information

Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
No LLDP EEE information found								

6.31.1 LLDP Neighbors EEE Information

The displayed table contains a row for each port. The columns display the following information:

Local Port

This column displays the port on which LLDP frames are received or transmitted.

Tx Tw

This column displays the maximum time that link partner's transmit path can hold-off sending data after de-assertion of LPI.

Rx Tw

This column displays the time that link partner's receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.

Fallback Receive Tw

This column displays 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 to the same value as that of the Receive Tw_sys_tx.

Echo Tx Tw

This column displays the link partner's Echo Tx Tw value.

The respective echo values shall be defined as the local link partner's reflection (echo) of the remote link partner's 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

This column displays the link partner's Echo Rx Tw value.

Resolved Tx Tw

This column displays the Resolved Tx Tw for this link.

> **Note:** NOT the link partner

The Resolved Tx Tw value is the actual "tx wakeup time" used for this link (based on EEE information exchanged via LLDP).

Resolved Rx Tw

This column displays the Resolved Rx Tw for this link.

> **Note:** NOT the link partner

The Resolved Rx Tw value is the actual "tx wakeup time" used for this link (based on EEE information exchanged via LLDP).

EEE in Sync

This column displays 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

6.31.2 EEE Neighbor Information Buttons

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

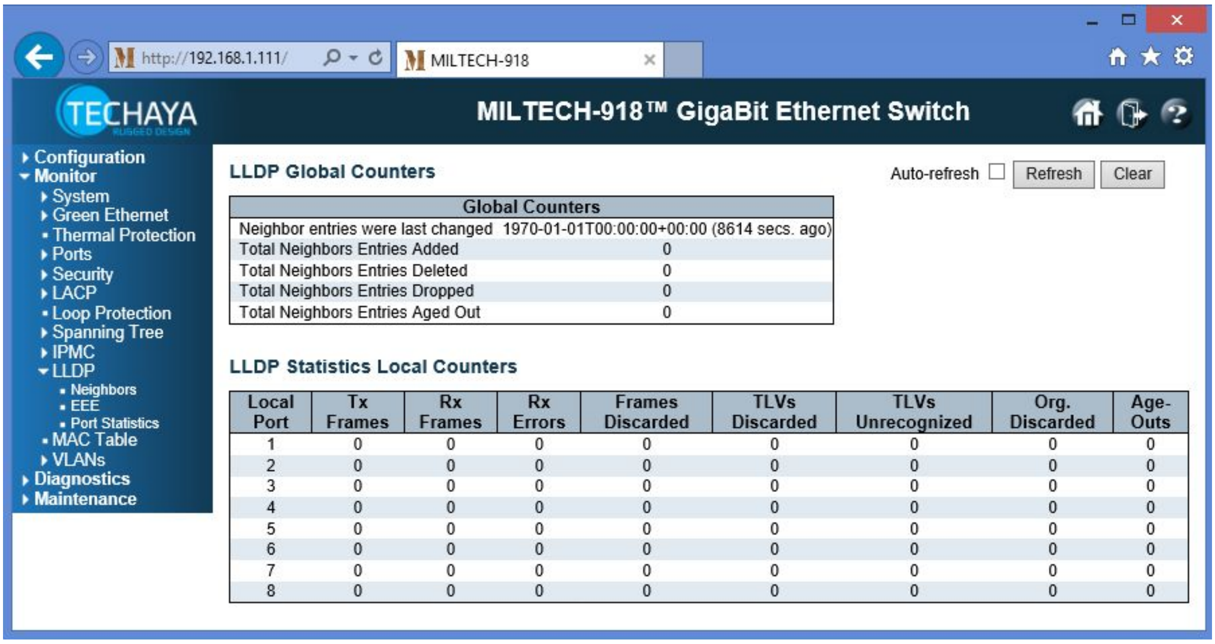
□ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

6.32 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 stack, switch, while local counters refer to per port counters for the currently selected switch..



LLDP Global Counters

Global Counters	
Neighbor entries were last changed	1970-01-01T00:00:00+00:00 (8614 secs. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

6.32.1 LLDP Global Counters

6.32.1.1 Global Counters

Neighbor entries were last changed

This column displays 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

This column displays the number of new entries added since switch reboot.

Total Neighbors Entries Deleted

This column displays the number of new entries deleted since switch reboot.

Total Neighbors Entries Dropped

This column displays the number of LLDP frames dropped due to the entry table being full.

Total Neighbors Entries Aged Out

This column displays the the number of entries deleted due to Time-To-Live expiring.

6.32.2 LLDP Statistics Local Counters

Local Port

This column displays the port on which LLDP frames are received or transmitted.

Tx Frames

This column displays the number of LLDP frames transmitted on the port.

Rx Frames

This column displays the number of LLDP frames received on the port.

Rx Errors

This column displays the number of received LLDP frames containing some kind of error.

Frames Discarded

This column displays the number of LLDP frames discarded.

If an 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

This column displays the number of TLVs discarded.

Each LLDP frame can contain multiple pieces of information, known as TLVs (Type Length Value). If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized

This column displays the number of TLVs unrecognized.

This is the number of well-formed TLVs that have an unknown type value.

Org. Discarded

This column displays the number of Organizational TLVs unrecognized.

If an LLDP frame is received with an Organizational TLV, but the TLV is not supported the TLV is discarded and counted.

Age-Outs

This column displays the number of Age-Outs.

Each LLDP frame contains information about how long 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.

6.32.3 LLDP Counters Buttons

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

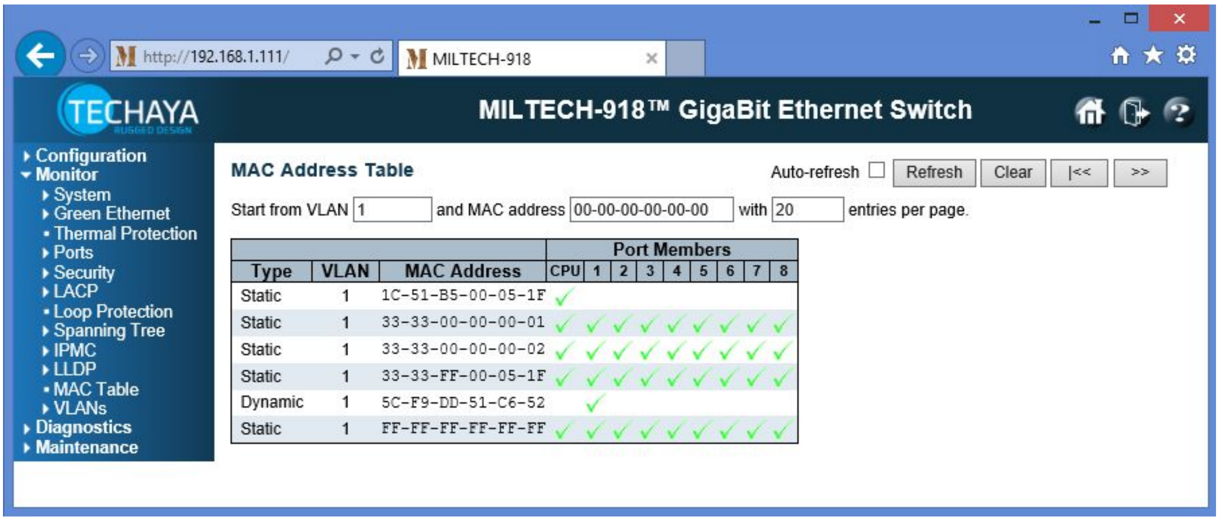
□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Clear: Click to clear the local counters. All counters (including Global Counters) are cleared upon reboot.

6.33 MAC Table

This page displays the entries in the MAC Table. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID , then by MAC address.



MAC Address Table

Auto-refresh □

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

			Port Members								
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8
Static	1	1C-51-B5-00-05-1F	✓								
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-00-05-1F	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic	1	5C-F9-DD-51-C6-52		✓							
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓

6.33.1 Navigating the MAC Table

Each page can show up to 999 entries from the MAC table. Set the number of entries per page in the “entries per page” input field (the default is 20). When first visited, the web page will show the first 20 entries from the beginning of the MAC Table.

The “Start from VLAN”, and “MAC address” input fields allow the user to set the starting point in the MAC Table. Click the **Refresh** button to update the displayed table starting from the current settings or the closest next MAC Table match. After clicking the **Refresh** button, the two input fields will assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The **Forward Arrows** button (>>) will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text “No more entries” is shown in the displayed table. Use the **Back Arrows** button **(** |<< **)** to start over.

6.33.2 MAC Address Table

Type

This column displays the entry type:

- Static
- Dynamic

VLAN

This column displays the VLAN ID of the entry.

MAC address

This column displays the MAC address of the entry.

Port Members

This column displays the ports that are members of the entry.

☑ Port is a member of the entry

□ Port is **not** a member of the entry

6.33.3 MAC Address Table Buttons

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□Disable Auto-refresh (This is the default.)

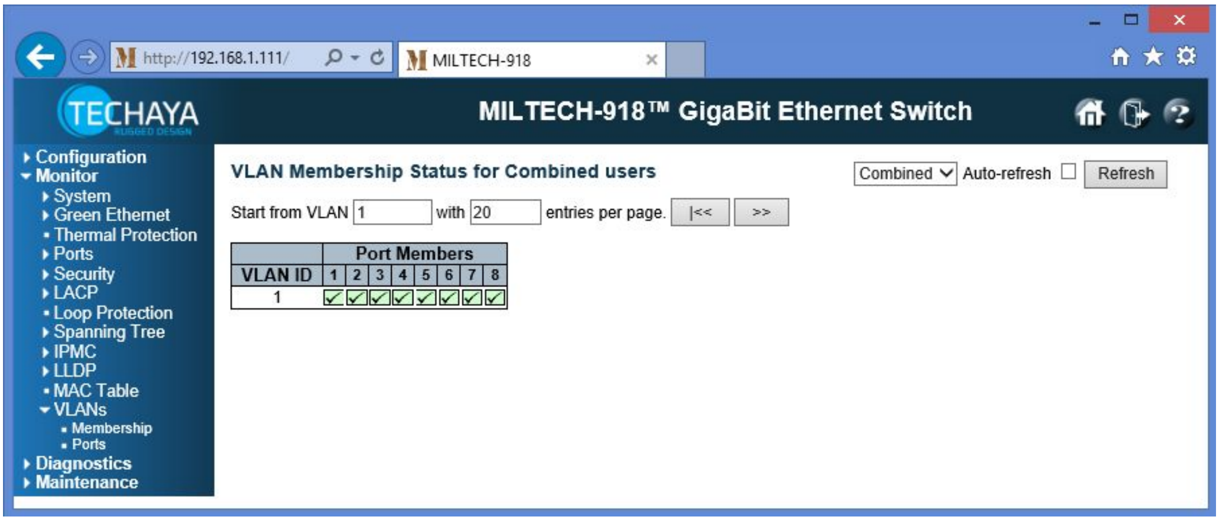
Refresh: Click to refresh the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

Back Arrows (|<< **):** Updates the table, starting from the first entry in the MAC Table (i.e. the entry with the lowest VLAN ID and MAC address).

Forward Arrows (>> **):** Updates the table, starting with the entry after the last entry currently displayed.

6.34 VLANs – Membership

This page provides an overview of membership status of VLAN users.



VLAN Membership Status for Combined users

Combined Auto-refresh □ Refresh

Start from VLAN 1 with 20 entries per page. |<< >>

	Port Members							
VLAN ID	1	2	3	4	5	6	7	8
1	✓	✓	✓	✓	✓	✓	✓	✓

6.34.1 Navigating the VLAN Membership Status Page

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

The “VLAN” input field allows the user to set the starting point in the VLAN Table. Click the **Refresh** button to update the displayed table starting from the current setting or the closest next VLAN Table match.

The **Forward Arrows** button (>>) will use the last entry of the currently displayed VLAN Table 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 **Back Arrows** button (|<<) to start over.

VLAN User

Various internal software modules may use VLAN services to configure VLAN memberships on the fly.

The drop-down list Combined ▾ on the top of the page allows the user to select the type of VLAN membership to display. The type of VLAN membership is determined by how it was configured; administrator or one of the internal software modules. The current options are:

- Combined
- Admin
- NAS

The "Combined" entry will show a combination of the administrator and internal software modules configuration. It reflects what is actually configured in the hardware.

6.34.2 VLAN Membership for ___ user(s)

The following VLAN Membership details are displayed:

VLAN ID

This column displays the VLAN ID for which the Port members are displayed.

Port Members

This column displays a row of check boxes for – one for each port is displayed for each VLAN ID:

☑ Indicates that the port is included in the VLAN

☒ Indicates that the port is in the forbidden port list

☒ Indicates that the port is in the forbidden port list, but attempted to be included in the VLAN. The port will not be a member of the VLAN in this case.

6.34.3 VLAN Membership Status Buttons

Select Box Combined ▾**:** Select a VLAN user from the drop down list:

Combined

Admin

NAS

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐Disable Auto-refresh (This is the default.)

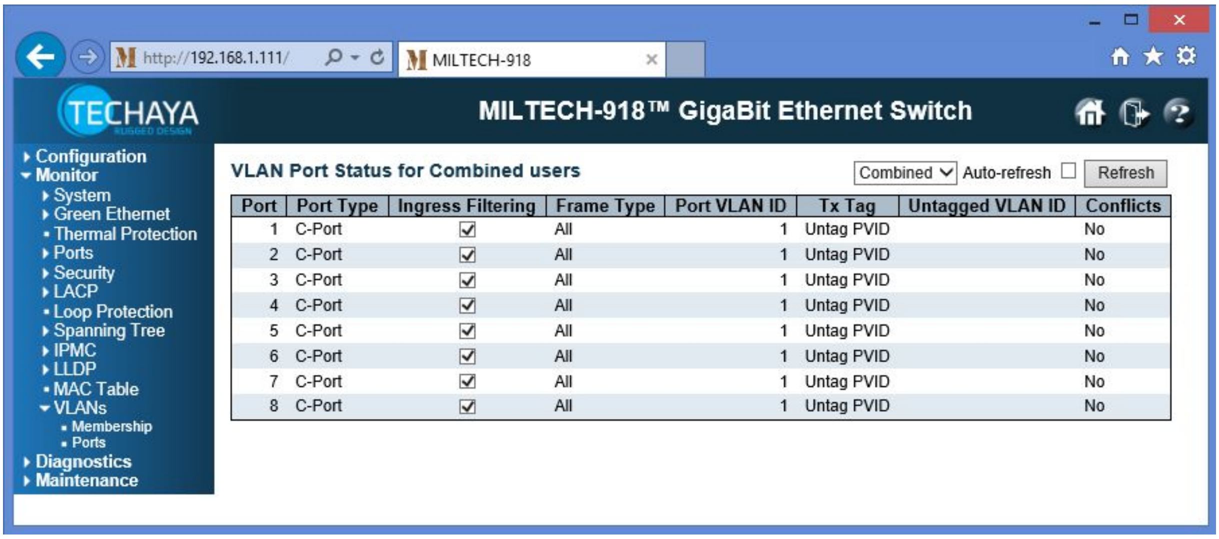
Refresh: Click to refresh the page immediately

Back Arrows (|<<): Updates the table, starting from the first entry in the MAC Table (i.e. the entry with the lowest VLAN ID and MAC address).

Forward Arrows (>>): Updates the table, starting with the entry after the last entry currently displayed.

6.35 VLANs – Ports

This page provides VLAN Port Status.



VLAN Port Status for Combined users

Combined | Auto-refresh □

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

6.35.1 VLAN Port Status for ___ user(s)

The following VLAN Port Status details are displayed:

VLAN User

Various internal software modules may use VLAN services to configure VLAN memberships on the fly.

The drop-down list Combined on the top of the page allows the user to select the type of VLAN membership to display. The type of VLAN membership is determined by how it was configured; administrator or one of the internal software modules. The current options are:

- Combined
- Admin
- NAS
- MSTP

The “Combined” entry will show a combination of the administrator and internal software modules configuration. It reflects what is actually configured in the hardware.

If a given software modules has not overridden any of the port settings, the text “No data exists for the selected user” is shown in the table.

Port

This column displays the logical port for the settings contained in the same row.

Port Type

This column displays the Port Type that a given user wants to configure on the port. The values are:

- Unaware
- C-Port
- S-Port
- S-Custom-Port

The field is empty if not overridden by the selected user.

Ingress Filtering

This column displays the whether a given user wants ingress filtering enabled or not:

☑ Ingress Filtering enabled

□ Ingress Filtering disabled

The field is empty if not overridden by the selected user.

Frame Type

This column displays the acceptable frame types that a given user wants to configure on the port:

- All
- Tagged
- Untagged

The field is empty if not overridden by the selected user.

Port VLAN ID

This column displays 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

This column displays the Tx Tag requirements that a given user has on a port. The values are:

- Tag All
- Tag PVID
- Tag UVID
- Untag All
- Untag PVID
- Untag UVID)

The field is empty if not overridden by the selected user.

Untagged VLAN ID

This column displays a VLAN ID. It is the VLAN ID that the user wants to tag or untag on egress, when Tx Tag is overridden by the selected user and is set to Tag or Untag UVID.

The field is empty if not overridden by the selected user.

Conflicts

This column displays the Conflicts status:

Yes: There is a conflict

No: There is **no** conflict

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 lowest 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 will be displayed as "Yes" for the "Combined" user and the offending software module.

6.35.2 VLAN Port Status Buttons

Select Box Combined ⌄**:** Select a VLAN user from the drop down list:

Combined

Admin

NAS

MSTP

Auto-refresh:

☑ Enable Auto-refresh – to refresh the page automatically every 3 seconds

□Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

7 Web Interface – Diagnostics

The Web Interface – Diagnostics section of this manual describes the diagnostic features and screens of the MILTECH-912™ Gigabit Ethernet Switch User Interface.

From the Diagnostics section of the Web interface the user can troubleshoot IP connectivity issues and cable diagnostics. See the following sections:

- Ping
- VeriPHY

7.1 Ping

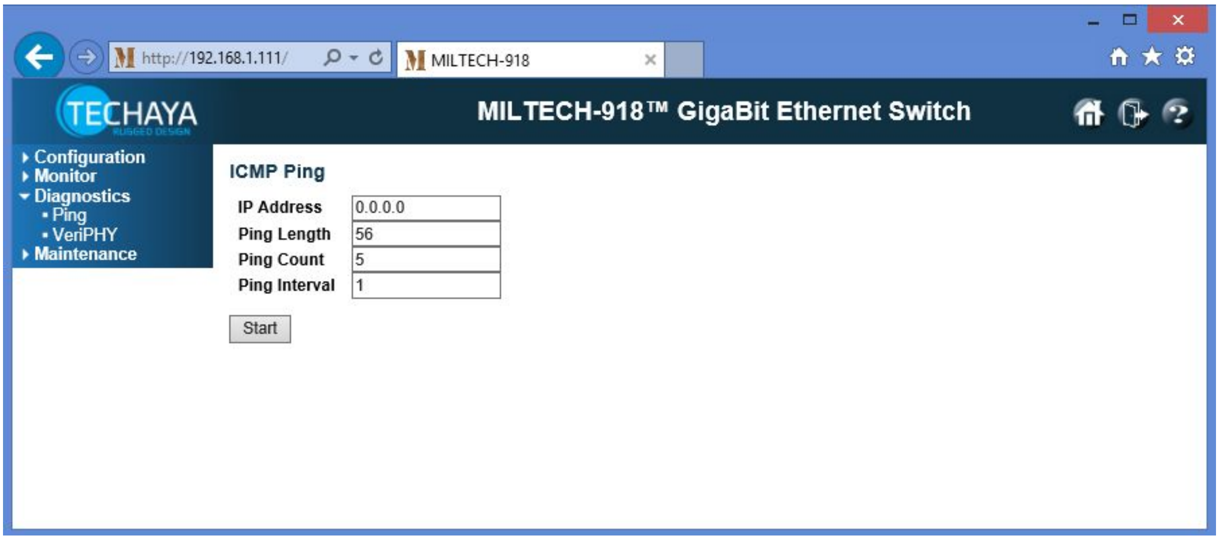
This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

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.

After you press the **Start** button (Start), ICMP packets are transmitted, and the sequence number and round trip time are displayed upon receipt of a reply. The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested data space (the ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
PING server 10.10.132.20, 56 bytes of data.
64 bytes from 10.10.132.20: icmp_seq=0, time=0ms
64 bytes from 10.10.132.20: icmp_seq=1, time=0ms
64 bytes from 10.10.132.20: icmp_seq=2, time=0ms
64 bytes from 10.10.132.20: icmp_seq=3, time=0ms
64 bytes from 10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```



ICMP Ping

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

7.1.1 ICMP Ping

The user can configure the following properties of the issued ICMP packets:

IP Address

Set or show the destination IP Address.

Ping Length

Set or show the payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Ping Count

Set or show the count of the ICMP packet. Values range from 1 time to 60 times.

Ping Interval

Set or show the interval of the ICMP packet. Values range from 0 second to 30 seconds.

Egress Interface (Only for IPv6)

Set or show the VLAN ID (VID) of the specific egress IPv6 interface where the ICMP packet goes.

The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.

When the egress interface is not given, PING6 finds the best match interface for destination.

Do not specify egress interface for loopback address.

Do specify egress interface for link-local or multicast address.

7.1.2 ICMP Ping Buttons

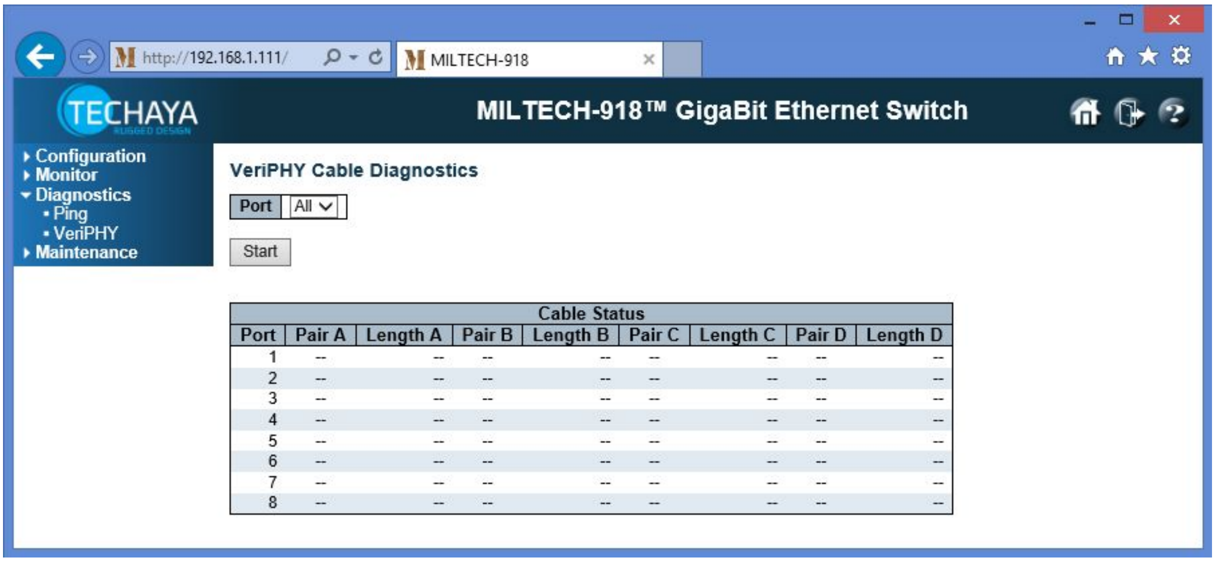
	Click to start transmitting ICMP packets
	Click to re-start diagnostics with PING

7.2 VeriPHY

This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.

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

> **Note:**
>
> - VeriPHY is only accurate for cables of length 7 - 140 meters.
> - 10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.



VeriPHY Cable Diagnostics

Port: All

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--
7	--	--	--	--	--	--	--	--
8	--	--	--	--	--	--	--	--

7.2.1 VeriPHY Cable Diagnostics

Port

Set or show the port requesting VeriPHY Cable Diagnostics.

7.2.2 Cable Status Table

Port:

This column displays the port number for the status row

Pair n:

This column displays the status of the cable pair. The possible values are:

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:

This column displays the length (in meters) of the cable pair. The resolution is 3 meters.

7.2.3 VeriPHY Cable Diagnostics Buttons

Start	Click to start VeriPHY Cable Diagnostics

8 Web Interface – Maintenance

The Web Interface – Maintenance section of this manual describes the maintenance features and screens of the MILTECH-912™ Gigabit Ethernet Switch User Interface.

From the Maintenance section of the Web interface the user can restart the device, revert to factory default settings, and update the firmware software that controls the switch. See the following sections:

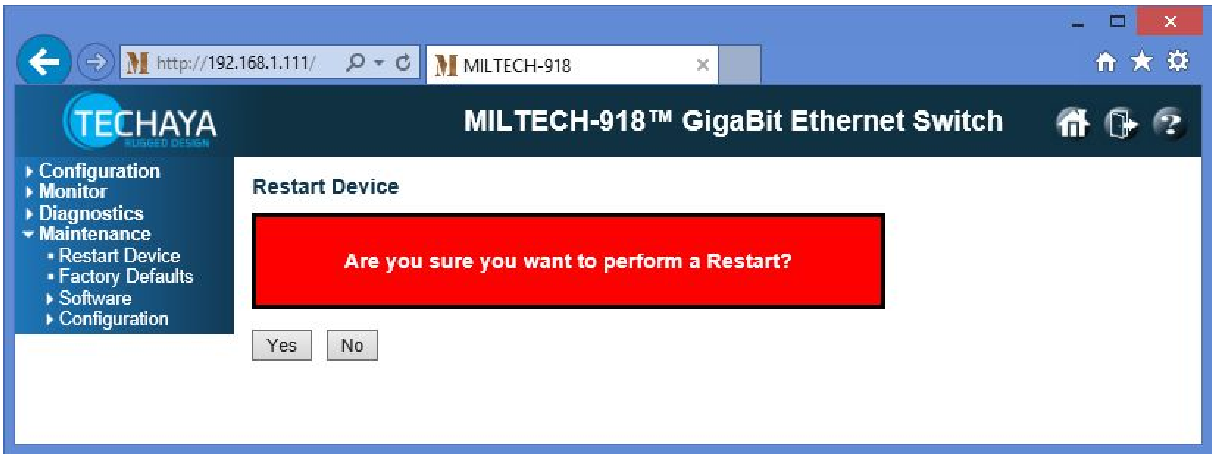
- Restart Device
- Factory Defaults
- Software – Upload
- Software – Image Select

From the Maintenance section of the Web interface the user may also save multiple configuration files for the device and easily reset the device with the desired configuration file for different performance purposes. These features can be found in the following sections:

- Configuration – Save Startup-Config
- Configuration – Download
- Configuration – Upload
- Configuration – Activate
- Configuration – Delete

8.1 Restart Device

The user can restart the stack switch from this page.



Restart Device

Are you sure you want to perform a Restart?

8.1.1 Restart Device Buttons

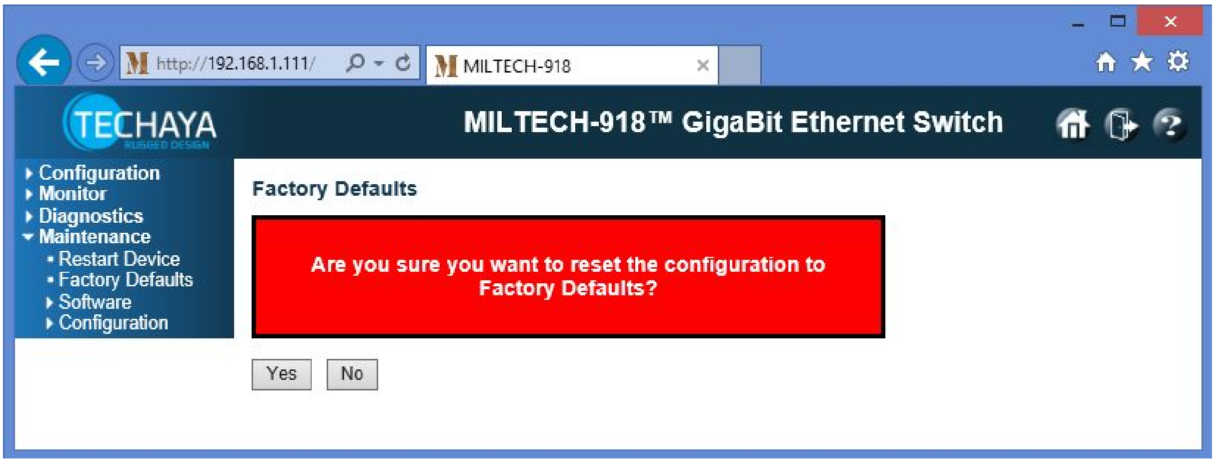
Yes	Click to restart the device
No	Click to return to the Port State page without restarting the device

8.2 Factory Defaults

The user can reset the configuration of the stack switch from this page. Only the IP configuration is retained.

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

> **Note:** Restoring factory defaults can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, "loopback" packets will be transmitted at port 1. If a "loopback" packet is received at port 2 the switch will do a restore to default.



Factory Defaults

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

8.2.1 Factory Defaults Buttons

Yes	Click to reset the configuration to Factory Defaults
No	Click to return to the Port State page without resetting the configuration

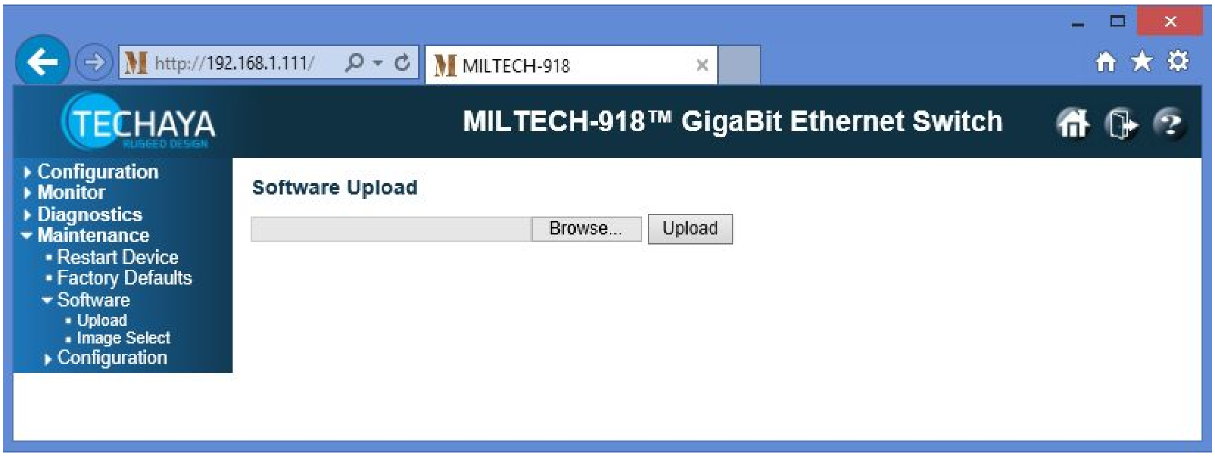
8.3 Software – Upload

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

Browse (Browse...) to the location of a software image and click the **Upload** button (Upload).

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

Warning: While the firmware is being updated, Web access appears to be defunct. 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.**

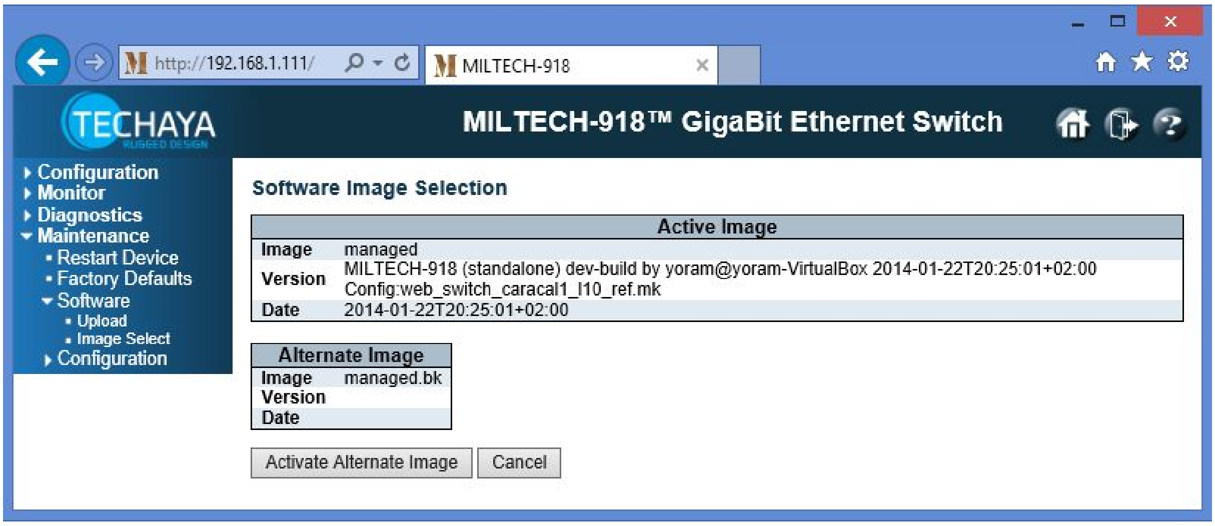


8.4 Software – Image Select

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

> **Note:**
>
> - 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.
> - If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this image.
> - The firmware version and date information may be empty for older firmware releases. This does not constitute an error.



Software Image Selection

Active Image	
Image	managed
Version	MILTECH-918 (standalone) dev-build by yoram@yoram-VirtualBox 2014-01-22T20:25:01+02:00 Config:web_switch_caracal1_l10_ref.mk
Date	2014-01-22T20:25:01+02:00

Alternate Image	
Image	managed.bk
Version	
Date	

8.4.1 Software Image Selection

Image

This field displays the flash index name of the firmware image. The name of primary (preferred) image is "image", the alternate image is named "image.bk".

Version

This field displays the version of the firmware image.

Date

This field displays the date when the firmware was produced.

8.4.2 Software Image Selection Buttons

Click to use the alternate image. This button may be disabled depending on system state

Click to cancel activating the backup image. Navigates away from this page

8.5 Configuration – Save Startup-Config

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch.

There are three system files:

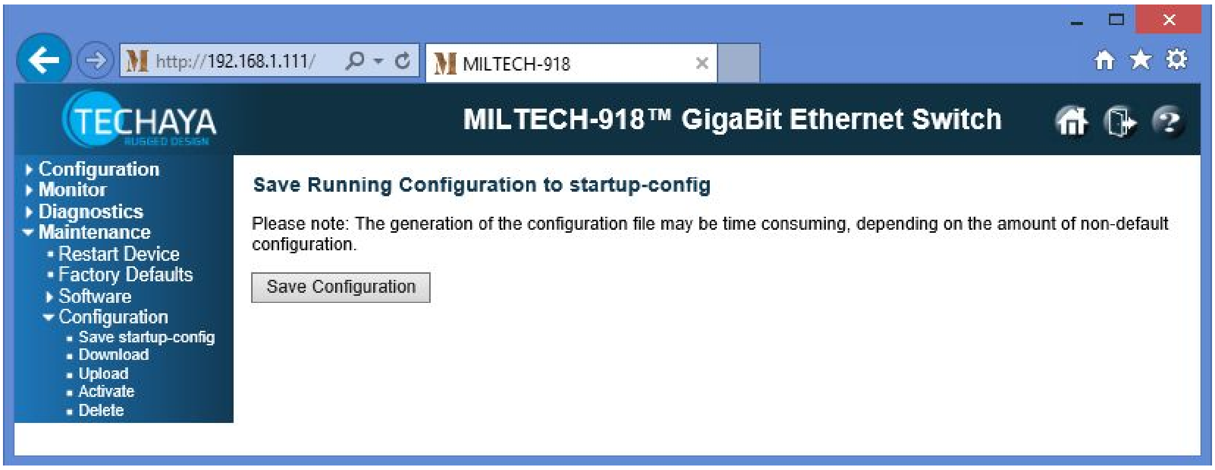
running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.

startup-config: The startup configuration for the switch, read at boot time.

default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

It is also possible to store up to two other files and apply them to running-config, thereby switching configuration.

This page allows the user to copy the running-config to the startup-config and save it, thereby ensuring that the currently active configuration will be used at the next reboot.



Save Running Configuration to startup-config

Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

Save Configuration

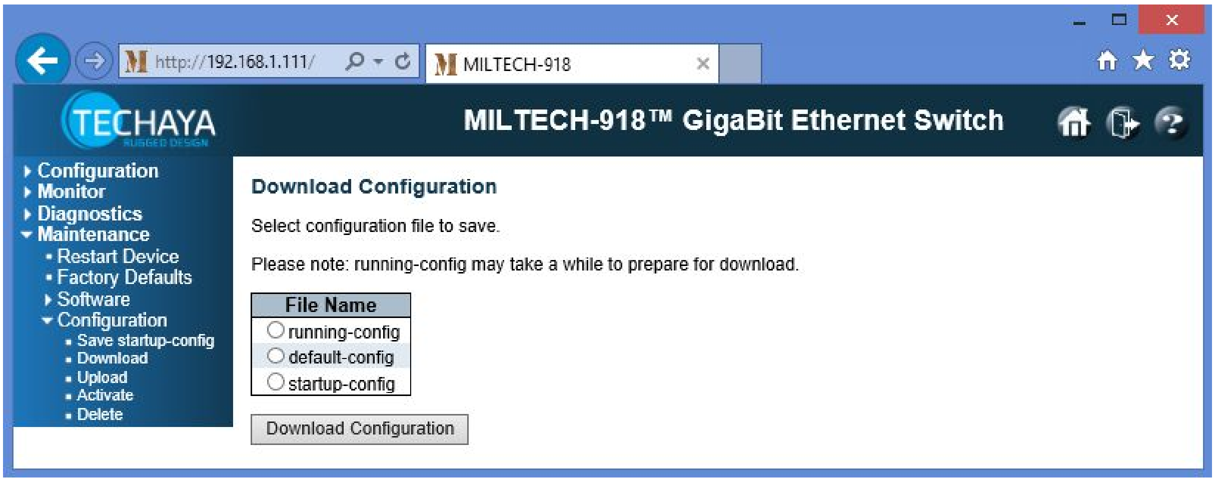
8.5.1 Save Running Configuration to Startup-Config

Click Save Configuration to copy the running-config to the startup-config and save it.

8.6 Configuration – Download

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch. For a more detailed description of system files see section 8.5 Configuration – Save Startup-Config on page 293.

It is possible to download any of the files on the switch to the web browser. This page allows the user to download a file from the switch.



Download Configuration

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

File Name
○ running-config
○ default-config
○ startup-config

Download Configuration

8.6.1 Download Configuration

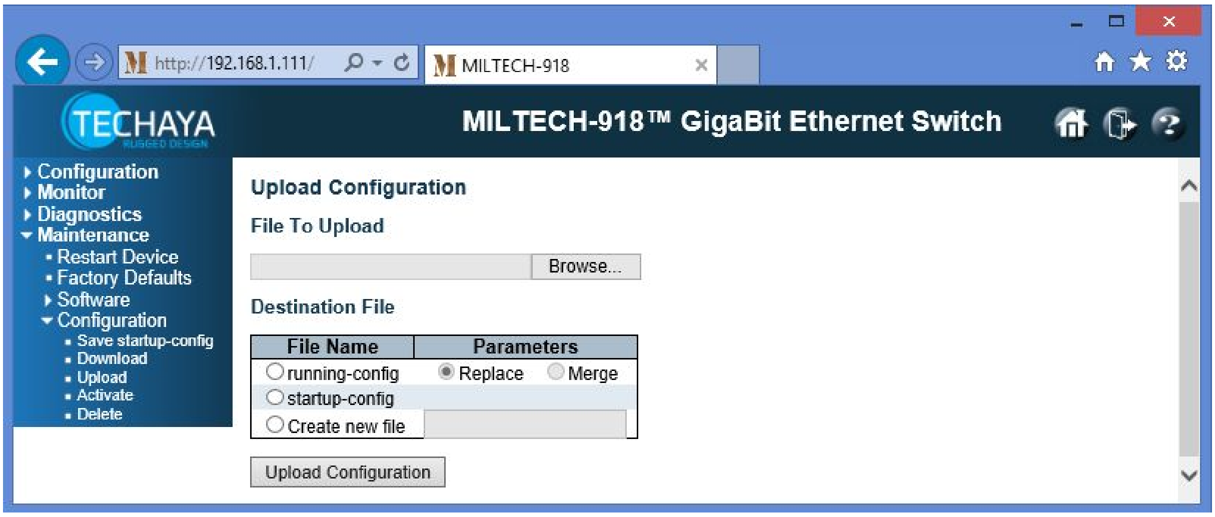
To download one of the configuration files:

1. Click one of the radio buttons to select the file.
2. Click the **Download Configuration** button (Download Configuration).
   Download of running-config may take a little while to complete, as the file must be prepared for download.

8.7 Configuration – Upload

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch. For a more detailed description of system files see section 8.5 Configuration – Save Startup-Config on page 293.

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



Upload Configuration

File To Upload

Browse...

Destination File

File Name	Parameters	
○ running-config	● Replace	○ Merge
○ startup-config		
○ Create new file		

Upload Configuration

8.7.1 File to Upload

Browse (Browse...) to the location of the configuration file to upload.

8.7.2 Destination File

To upload the selected configuration file:

1. Click one of the radio buttons to select the destination file to replace.
2. Click the **Upload Configuration** button (Upload Configuration).
   Download of running-config may take a little while to complete, as the file must be prepared for download.

If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:

Replace mode: The current configuration is fully replaced with the configuration in the uploaded file.

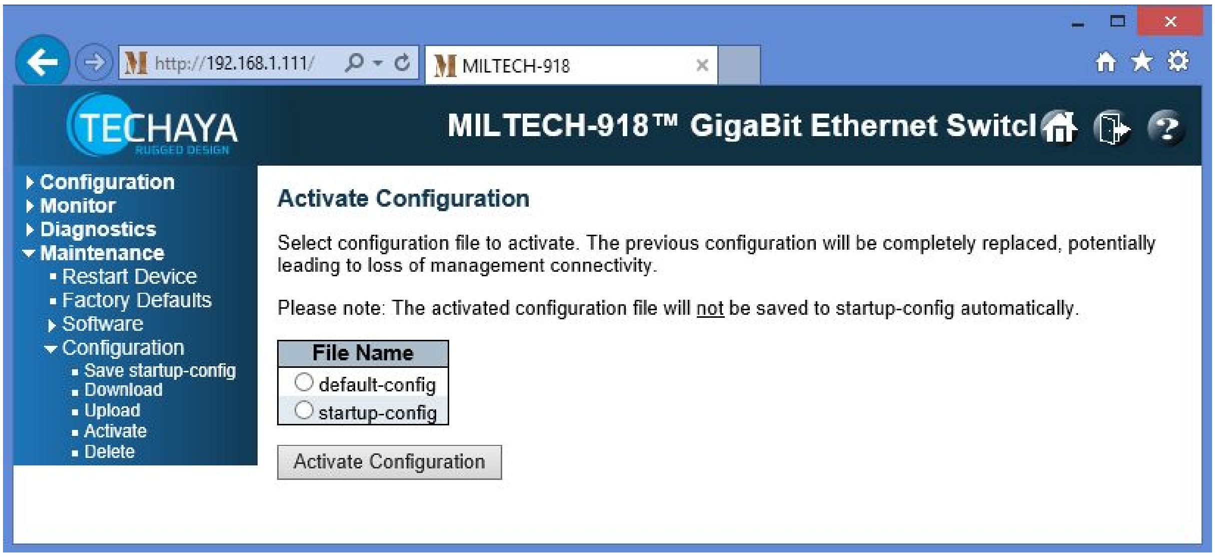
Merge mode: The uploaded file is merged into running-config.

> **Note:** 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.

8.8 Configuration – Activate

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch. For a more detailed description of system files see section 8.5 Configuration – Save Startup-Config on page 293.

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



Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will not be saved to startup-config automatically.

File Name
○ default-config
○ startup-config

8.8.1 Activate Configuration

To activate a configuration file:

1. Click one of the radio buttons to select the file.
2. Click the **Activate Configuration** button (Activate Configuration).

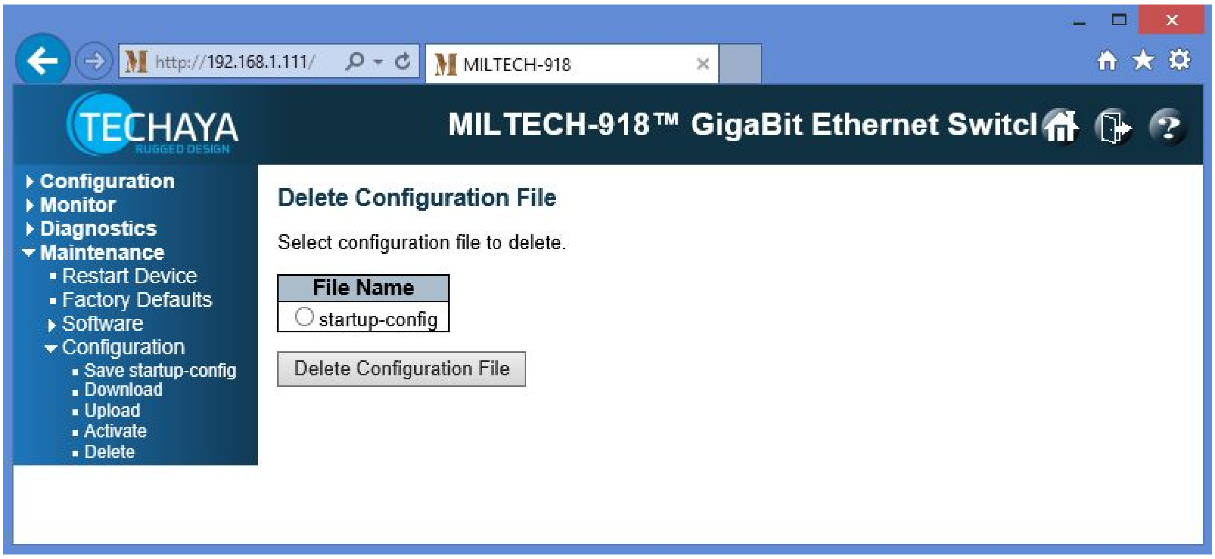
This will initiate the process of completely replacing the existing configuration with that of the selected file.

8.9 Configuration – Delete

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch. For a more detailed description of system files see section 8.5 Configuration – Save Startup-Config on page 293.

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.

This page allows the user to delete a configuration file on the switch.



Delete Configuration File

Select configuration file to delete.

File Name
○ startup-config

Delete Configuration File

8.9.1 Delete Configuration

To delete a configuration file:

1. Click one of the radio buttons to select the file.
2. Click the **Delete Configuration** File button (Delete Configuration File).

9 Warranty

1. Seller expressly warrants that all goods and services shall be free from defects, shall be of good materials and workmanship, and shall conform to applicable:
   - Specifications
   - Drawings
   - Samples
   - Performance specifications.
2. The Seller warranty shall remain in effect for a period of one year after the item is shipped, or the service is completed, from or by the Seller.
3. In the event that the Seller is required to replace or correct any component of any item, the warranty period for the defective item or the item containing a defective component shall be suspended from the date Seller receives the item until the date the item is replaced or corrected, and this warranty shall apply to such replacement or corrected items furnished for the unexpired portion of the warranty period.
4. The Seller shall not be responsible for any liabilities, loss, costs, damages, and/or expense resulting from any breach of any, or all, of Seller's warranties, express, or implied. Seller shall not be responsible for any cost of removing such items from property, equipment, or products, and/or any additional costs of disassembly, fault isolation, failure analysis, reinstallation, reinspection, retesting in which such items have been incorporated and/or transportation to or from the Seller.

The MILTECH-912 does not contain any user serviceable parts. Any modification or use other than consistent with the intended design shall void the warranty. Owner must contact Techaya at (972) (4)637-7741 and be issued a Return Material Authorization (RMA) number before returning a unit for warranty repair.

10Accessories and Services

Techaya offers an extensive line of Engineering Services and custom made cable sets to match your MILTECH-912 application.

Visit the Techaya Web site at www.techaya.com for additional information about our products and services.