
OPTICAL

SYSTEMS

DESIGN

User Manual

OSD2790SFP

MANAGED ETHERNET SWITCH

**24 x 100/1000M SFP AND 4 x 1G
TRUNK/UPLINK SFP**

OPTICAL SYSTEMS DESIGN

INDEX 1

1	PRODUCT DESCRIPTION	8
2	FUNCTIONAL DESCRIPTION	8
2.1	TECHNICAL SPECIFICATIONS	10
3	QUICK START GUIDE	11
3.1	OSD2790SFP FRONT AND REAR PANELS	11
3.2	POWER SUPPLY CONNECTIONS.....	12
3.3	LED INDICATORS	13
3.4	FITTING SFP CONNECTORS	13
3.5	CLI OVERVIEW.....	14
	CONNECT TO CLI	14
	CLI COMMANDS (TOP LEVEL)	16
	RESET CONFIGURATION TO FACTORY DEFAULT	17
	SET HOSTNAME AND ADMIN USER PASSWORD	18
	SET VLAN 1 IP ADDRESS	19
	SAVE CONFIGURATION TO FLASH.....	19
3.6	GUI OVERVIEW	20
	DEFAULT SETTING	20
	LOG INTO THE SWITCH	20
	IP CONFIGURATION.....	21
	USERS AUTHENTICATION.....	22
	SAVE CONFIGURATION TO START-UP.....	23
4	USER MANUAL	24
4.1	INSTALLATION	24
4.2	OSD2790SFP DIMENSIONS	25
5	GUI CONFIGURATION	26
5.1	GUI MENU	27
5.2	CONFIGURATION	28
	SYSTEM	28
	TIME ZONE	34
	DAYLIGHT SAVING TIME	35
	GREEN ETHERNET	38
	LEDs INTENSITY	39
	MAINTENANCE	40
	WHAT IS EEE	41
	OPTIMIZE EEE FOR	42
	PORT CONFIGURATION	42
	PORT CONFIGURATION	43
	DHCP	46
	GLOBAL MODE	47
	VLAN MODE	47
	EXCLUDED IP ADDRESS	48
	POOL SETTING	49
	SECURITY.....	54
	COMMAND AUTHORIZATION METHOD CONFIGURATION HELP	59
	ACCOUNTING METHOD CONFIGURATION HELP	59
	GLOBAL SETTINGS	68
	TRAP DESTINATION CONFIGURATIONS	68
	SYSTEM CONFIGURATION	83
	PORT CONFIGURATION	83
	SYSTEM CONFIGURATION	86
	PORT CONFIGURATION	88
	FORCE AUTHORIZED	88

OPTICAL SYSTEMS DESIGN

FORCE UNAUTHORIZED	88
PORT-BASED 802.1X	88
SINGLE 802.1X	89
MULTI 802.1X	89
MAC-BASED AUTH.	90
NAVIGATING THE VLAN CONFIGURATION	104
NAVIGATING THE ARP INSPECTION TABLE	107
ARP INSPECTION TABLE COLUMNS	107
GLOBAL CONFIGURATION	110
SERVER CONFIGURATION	110
ADDING A NEW SERVER	111
GLOBAL CONFIGURATION	112
SERVER CONFIGURATION	113
ADDING A NEW SERVER	113
AGGREGATION	114
HASH CODE CONTRIBUTORS	114
AGGREGATION GROUP CONFIGURATION	115
LINK OAM CONFIGURATION	118
LOOP PROTECTION	122
SPANNING TREE	124
IPMC PROFILE CONFIGURATIONS	133
MVR CONFIGURATIONS	137
IPMC	140
NAVIGATING THE IGMP SNOOPING VLAN TABLE	143
IGMP SNOOPING VLAN TABLE COLUMNS	143
NAVIGATING THE MLD SNOOPING VLAN TABLE	149
MLD SNOOPING VLAN TABLE COLUMNS	149
LLDP	152
LLDP PARAMETERS	153
LLDP INTERFACE CONFIGURATION	153
FAST START REPEAT COUNT	156
TRANSMIT TLVs	156
COORDINATES LOCATION	157
CIVIC ADDRESS LOCATION	158
EMERGENCY CALL SERVICE	159
POLICIES	160
POLICIES INTERFACE CONFIGURATION	162
MAC ADDRESS TABLE CONFIGURATION	163
AGING CONFIGURATION	163
MAC TABLE LEARNING	164
STATIC MAC TABLE CONFIGURATION	164
GLOBAL VLAN CONFIGURATION	166
GLOBAL VLAN CONFIGURATION	166
PORT VLAN CONFIGURATION	167
VLAN TRANSLATION	171
PRIVATE VLANS	174
OVERVIEW	176
CONFIGURATION	176
VCL	177
VOICE VLAN CONFIGURATION	185
QOS	189
GLOBAL STORM POLICER CONFIGURATION	209
PORT STORM POLICER CONFIGURATION	209

OPTICAL SYSTEMS DESIGN

RED DROP PROBABILITY FUNCTION	211
UPNP CONFIGURATION	213
PTP EXTERNAL CLOCK MODE	214
PTP EXTERNAL CLOCK CONFIGURATION	214
PTP CLOCK CONFIGURATION	215
GVRP CONFIGURATION	217
SFLOW CONFIGURATION	219
AGENT CONFIGURATION	220
RECEIVER CONFIGURATION	220
PORT CONFIGURATION	221
UDLD PORT CONFIGURATION	222
PROGRAMMABLE ALARM	224
ALARM RESET OPTION	225
ALARM SELECTION	225
PORT LINK ALARM CONFIGURATION	225
TEMPERATURE ALARM SETTING	225
5.3 MONITOR	226
SYSTEM	226
NAVIGATING THE SYSTEM LOG INFORMATION TABLE	231
SYSTEM LOG INFORMATION ENTRY COLUMNS	231
GREEN ETHERNET	234
FAN STATUS	236
PORTS	237
RECEIVE TOTAL AND TRANSMIT TOTAL	242
RECEIVE AND TRANSMIT SIZE COUNTERS	243
RECEIVE AND TRANSMIT QUEUE COUNTERS	243
RECEIVE ERROR COUNTERS	243
TRANSMIT ERROR COUNTERS	243
LINK OAM	245
RECEIVE TOTAL AND TRANSMIT TOTAL	245
LOCAL AND PEER	247
DHCP	252
DATABASE COUNTERS	253
BINDING COUNTERS	253
DHCP MESSAGE RECEIVED COUNTERS	253
DHCP MESSAGE SENT COUNTERS	254
BINDING IP ADDRESS	255
DECLINED IP ADDRESSES	257
NAVIGATING THE DHCP SNOOPING TABLE	258
DHCP SNOOPING TABLE COLUMNS	258
SERVER STATISTICS	260
SERVER STATISTICS	260
RECEIVE AND TRANSMIT PACKETS	262
SECURITY	264
USER MODULE LEGEND	266
PORT STATUS	266
PORT STATE	272
PORT COUNTERS	272
SELECTED COUNTERS	275
ATTACHED MAC ADDRESSES	276
NAVIGATING THE ARP INSPECTION TABLE	280
ARP INSPECTION TABLE COLUMNS	280
NAVIGATING THE IP SOURCE GUARD TABLE	282

OPTICAL SYSTEMS DESIGN

IP SOURCE GUARD TABLE COLUMNS	282
RADIUS SERVERS	284
RADIUS AUTHENTICATION STATISTICS	286
RADIUS ACCOUNTING STATISTICS	289
AGGREGATION	300
AGGREGATION GROUP STATUS	300
LOOP PROTECTION STATUS.....	305
SPANNING TREE.....	306
MVR.....	309
NAVIGATING THE MVR CHANNELS (GROUPS) INFORMATION TABLE	310
MVR CHANNELS (GROUPS) INFORMATION TABLE COLUMNS	310
NAVIGATING THE MVR SFM INFORMATION TABLE	312
MVR SFM INFORMATION TABLE COLUMNS	312
IPMC	314
NAVIGATING THE IGMP GROUP TABLE	316
IGMP GROUP TABLE COLUMNS	316
NAVIGATING THE IGMP SFM INFORMATION TABLE	318
IGMP SFM INFORMATION TABLE COLUMNS	318
NAVIGATING THE MLD GROUP TABLE	322
MLD GROUP TABLE COLUMNS	322
NAVIGATING THE MLD SFM INFORMATION TABLE	323
MLD SFM INFORMATION TABLE COLUMNS	323
LLDP	325
LLDP NEIGHBORS EEE INFORMATION	331
GLOBAL COUNTERS	333
LOCAL COUNTERS	334
PTP	335
PTP EXTERNAL CLOCK DESCRIPTION	335
PTP CLOCK DESCRIPTION	336
MAC TABLE	337
NAVIGATING THE MAC TABLE	338
MAC TABLE COLUMNS	338
VLANS.....	339
NAVIGATING THE VLAN MEMBERSHIP STATUS PAGE	339
SFLOW	343
RECEIVER STATISTICS	343
PORT STATISTICS	344
UDLD.....	345
UDLD PORT STATUS	345
NEIGHBOUR STATUS	345
ALARM.....	347
ALARM 348	
ALARM STATUS	348
LINK ALARM STATUS	348
TEMPERATURE ALARM STATUS	348
5.4 DIAGNOSTICS	350
PING.....	350
LINK OAM	351
LINK OAM MIB RETRIEVAL	351
PING6 (ICMPV6 PING)	352
5.5 MAINTENANCE	354
RESTART DEVICE.....	354
FACTORY DEFAULTS	355

OPTICAL SYSTEMS DESIGN

SOFTWARE.....	356
IMAGE INFORMATION	357
CONFIGURATION	358
6 WARRANTY	363
6.1 WARRANTY PERIOD.....	363
6.2 REPAIRS.....	363
WARRANTY REPAIRS.....	363
OUT-OF-WARRANTY REPAIRS.....	363
SITE REPAIRS	363
EXCLUSIONS	363
FIGURE 1: FRONT PANEL.....	11
FIGURE 2: REAR PANEL	11
FIGURE 3: POWER CONNECTION.....	12
FIGURE 4: FITTING/REMOVING SFP CONNECTORS	13
FIGURE 5: CLI DRIVER DOWNLOAD	14
FIGURE 6: DIMENSIONS	25
TABLE 1: TECHNICAL SPECIFICATIONS.....	10
TABLE 2: DC POWER CONNECTION.....	12
TABLE 3: LED FUNCTION	13

1 PRODUCT DESCRIPTION

This manual describes how to install and setup the OSD2790SFP Managed Ethernet Switch. To get the most out of this manual, the user should have an understanding of Ethernet networking concepts. This manual is in two parts – A Quick Start Guide section and a detailed user manual format.

The OSD2790SFP is a managed 24 port 100M/1G SFP + 4 port 1G Trunk/Uplink SFP Ethernet Switch. Various SFPs can be used including 100Mbps, 1Gbps duplex, single-fiber and RJ45 Copper. Please see OSD SFP datasheets for available options.

2 FUNCTIONAL DESCRIPTION

- ▲ Managed L2/3 switch for small to medium-sized enterprise networks requiring high throughput
- ▲ Redundant and self-healing network
- ▲ Ideal for star configured optical networks
- ▲ Industrial IP communications for rugged environments
- ▲ Available with either DC or AC powering. The DC version has dual redundant inputs as standard whereas redundant AC powering is optional for the AC version

▲ General

- △ L2/L3 managed Ethernet switch
- △ Supports RSTP/MRSTP/STP for Ethernet redundancy
- △ CPU Memory 128MB RAM
- △ User-friendly web browser based GUI
- △ CLI and SNMP management

▲ Port Control

- △ Port speed, duplex mode, and flow control
- △ Port status -- link monitoring
- △ Port statistics -- MIB counters

▲ QoS

- △ Traffic classes (1, 2, or 4, 8 active priorities)
- △ Port default priority and user assigned priority
- △ Scheduler priority
- △ QoS control
- △ Storm control

▲ L2 Switching

- △ IEEE 802.1D Bridge with auto MAC learning/aging
- △ IEEE 802.1Q static VLAN
- △ Private VLAN (static)
- △ 80Gbps switching backplane
- △ IEEE 802.1Q-2005 - Rapid spanning tree (RSTP)
- △ IEEE 802.3ad Link aggregation, static and LACP
- △ DHCP client
- △ Port mirroring

▲ Security

- △ Port-based 802.1X
- △ Web and CLI authentication and authorization

OPTICAL SYSTEMS DESIGN

▲ QAM

- △ IEEE 802.3ah Link OAM

▲ Multicasting

- △ IGMP Snooping (IGMPv2, IGMPv3)
- △ Multicast Listener Discovery (MLD) v1 and v2

▲ Power Saving

- △ Ethernet energy efficient
 - Link down power savings
 - Scales power based on cable length
- △ Thermal protection

▲ Management

- △ HTTP server
- △ Web management
- △ CLI console port
- △ Management access filtering
- △ System log
- △ Software download through web
- △ SNMPv1/v2c/v3Agent
- △ IEEE 802.1AB-2005 Link Layer Discovery, LLDP
- △ Configuration download or upload
- △ RFC 1213 MIB II
- △ RFC 3635 Ethernet-like MIB
- △ RFC 4188 Bridge MIB
- △ Private MIB framework
- △ IEEE 802.1 MSTP MIB
- △ IEEE802.1AB LLDP MIB

OPTICAL SYSTEMS DESIGN

2.1 TECHNICAL SPECIFICATIONS

TABLE 1: TECHNICAL SPECIFICATIONS

SPECIFICATION	PERFORMANCE
Electrical Data Interface	IEEE802.3z 1000Base-Lx, 1000Base-Sx IEEE802.3u 100Base-Fx
Operating Mode	Full duplex for 100M/1G Store-and-Forward IEEE802.3x full-duplex flow control
Number of Optical Port Connectors	SFP x 28: 24 for 100/1000SFP Port1-24, 4 for the 1G uplink/trunk ports
Optical Port Connector Type	SFP (LC or SC)
SFP Options	Short haul, long haul, single fiber operation, etc. Please see OSD Datasheets #102100XX and #1021000XX for 100Mbps and 1Gbps SFP optical modules
Indicators	28 x 100M/1G Link/Activity/Speed 2 x Power 1 x Status
Configuration Connector	Mini USB Console Port
Alarms	Four: Two for Power Supply Status Two user definable via the GUI as specified in the user manual
Alarm Interface	Four opto-isolated relay drivers via two 4-way 3.5mm terminal blocks
Control	System Reset
Operating Temperature	-20°C to +75°C for OSD2790SFPDC -20°C to +65°C for OSD2790SFPAC and OSD2790SFPDAC
Relative Humidity	0 to 95% non-condensing
Power Requirements	+10 to +36V _{DC} @ 40VA Max for DC version 90 to 264V _{AC} @ 50VA Max for standard single AC version 90 to 264V _{AC} @ 55VA Max for optional redundant AC version
Power Connector	4 way 5.08mm Terminal Block for DC powered version One IEC power inlet module for the standard AC powered version Two IEC power inlet modules for the optional redundant AC powered version
Dimensions of Enclosure (mm)	443W x 300D x 44H
Weight (kg)	5.1

1022790SFP02

OPTICAL SYSTEMS DESIGN

3 QUICK START GUIDE

3.1 OSD2790SFP FRONT AND REAR PANELS

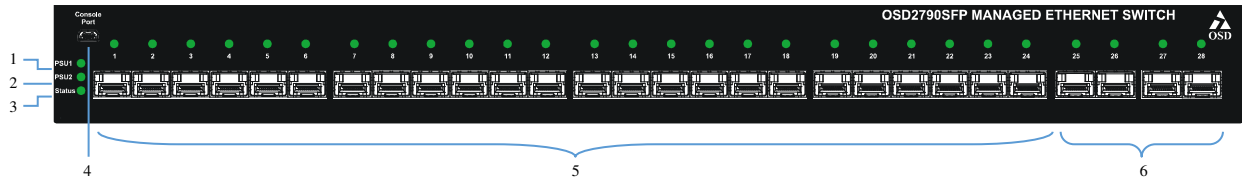


FIGURE 1: FRONT PANEL

1. PSU1 Status LED
2. PSU2 Status LED
3. Status LED
4. Mini USB Console Port
5. 24 x 100/1000M SFP ports with 100M/1G Link/Activity/Speed LEDs
6. 4 x 1G Trunk/Uplink SFP ports with 100M/1G Link/Activity/Speed LEDs

Single AC Power Input



Dual Redundant AC Power Input



DC Power Input



FIGURE 2: REAR PANEL

- | | |
|------------------------------|------------------------------|
| 7. Reset Switch | 12. AC PSU 2 IEC Power Inlet |
| 8. PSU Alarm Relay | 13. Power 1 LED |
| 9. Programmable Alarm Relay | 14. DC Dual Power Inlet |
| 10. Earth Connection Point | 15. Power 2 LED |
| 11. AC PSU 1 IEC Power Inlet | |

OPTICAL SYSTEMS DESIGN

3.2 POWER SUPPLY CONNECTIONS

The OSD2790 comes in three power input variations: Single Input AC powered, Dual Redundant AC Powered and Dual Redundant DC Powered. Power requirements are as follows;

SINGLE AC POWERED: 90-264V_{AC} @ 50VA Max. IEC Inlet.

DUAL REDUNDANT AC POWERED: 90-264V_{AC} @ 50VA Max. IEC Inlet.

DUAL REDUNDANT DC POWERED: +10 to +36V_{DC} @ 55VA Max. 4-way terminal block.

FUSE (AC VERSIONS ONLY): 1A 250V Anti-Surge, 5x20mm.



FIGURE 3: POWER CONNECTION

TABLE 2: DC POWER CONNECTION

External Power Pin	Specification
Pin 1, Pin 3	0V (Ground Isolated)
Pin 2, Pin 4	+10 to +36V _{DC} @ 40VA max

OPTICAL SYSTEMS DESIGN

3.3 LED INDICATORS

TABLE 3: LED FUNCTION

LED	Function
PSU 1	<ul style="list-style-type: none"> • Red – PSU 1 Not connected or faulty • Green – PSU 1 On
PSU 2	<ul style="list-style-type: none"> • Red – PSU 2 Not connected or faulty • Green – PSU 2 On
Status	<ul style="list-style-type: none"> • Red – Standby/Initialization Mode • Green – Normal status
SFP 1-24	Port Status LED will indicate the below information. <ul style="list-style-type: none"> • Green – 1Gbps • Amber – 100MBps • Off – No Connection
SFP 25-28	Port Status LED will indicate the below information. <ul style="list-style-type: none"> • Green – 1Gbps • Off – No Connection

3.4 FITTING SFP CONNECTORS

Care should be taken when inserting/removing the SFP connectors from the SFP port as SFP modules are Electrostatic (ES) sensitive and Electrostatic Discharge (ESD) precautions should be taken when installing. Ensure that the SFP is fully engaged and latched into position.

Inserting SFP – Ensure that the SFP lever is in the locked position and insert into appropriate SFP port. Gently push the SFP until it locks into place. Remove plastic/rubber dust cap and fit appropriate fiber cable.

Removing SFP – Remove fiber connector. Pull the SFP lever down to unlock SFP from housing. Using the lever, gently pull the SFP out.

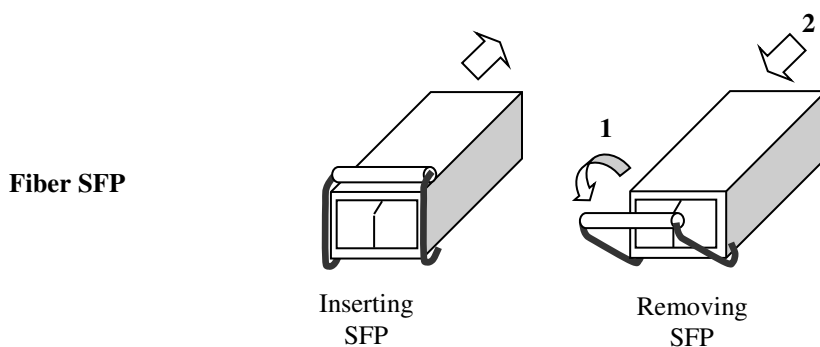


FIGURE 4: FITTING/REMOVING SFP CONNECTORS

OPTICAL SYSTEMS DESIGN

3.5 CLI OVERVIEW

CONNECT TO CLI



The OSD2790SFP has a Mini USB console port connector located on the front of the unit that is used for Command Line Interface (CLI) from the PC to the OSD2790SFP via the PC's USB connector.

To operate and control the OSD2790SFP using the CLI, a proprietary driver will be required to be installed onto the PC being used. The driver can be found and downloaded via the following site: www.silabs.com and searching for the CP210x driver. Download the relevant driver for your operating system, install and follow the installation instructions from your PC.


Download for Windows 10 Universal (v10.1.7)

Platform	Software	Release Notes
 Windows 10 Universal	Download VCP (2.3 MB)	Download VCP Revision History

Download for Windows 7/8/8.1 (v6.7.6)

Platform	Software	Release Notes
 Windows 7/8/8.1	Download VCP (5.3 MB) (Default)	Download VCP Revision History
 Windows 7/8/8.1	Download VCP with Serial Enumeration (5.3 MB) Learn More >	Download VCP Revision History

Download for Windows XP/Server 2003/Vista/7/8/8.1 (v6.7)

Platform	Software	Release Notes
 Windows XP/Server 2003/Vista/7/8/8.1	Download VCP (3.66 MB)	Download VCP Revision History

Download for Windows ZK (v6.3a)

Platform	Software	Release Notes
 Windows ZK	Download VCP (4.79 MB)	Download WinZK VCP Revision History


Download for WinCE

Platform	Software	Release Notes
 WinCE 6.0 (2.1)	Download VCP (276 KB)	Download WinCE 6.0 Revision History
 WinCE 5.0 (2.1)	Download VCP (271 KB)	Download WinCE 5.0 Revision History

Download for Macintosh OSX (v5.1.0)

Platform	Software	Release Notes
 Mac OS X	Download VCP (832 KB)	Download Mac VCP Revision History

Download for Linux

Platform	Software	Release Notes
 Linux 3.x.x and 4.x.x	Download VCP (10.0 KB)	Download Linux 3.x.x and 4.x.x VCP Revision History
 Linux 2.6.x	Download VCP (10.2 KB)	Download Linux 2.6.x VCP Revision History

*Note: The Linux 3.x.x and 4.x.x version of the driver is maintained in the current Linux 3.x.x and 4.x.x tree at www.kernel.org.

Download for Android

Platform	Application Note
 Android 4.2	AN809: Integrating the CP210x Virtual COM Port Driver into the Android Platform

FIGURE 5: CLI DRIVER DOWNLOAD

OPTICAL SYSTEMS DESIGN

1. Connect the Console Port on OSD2790SFP (Mini USB) to PC with USB cable.
2. Using HyperTerminal, SecureCRT, etc to set up the following parameters.
 - Baud Rate: 115200
 - Data Bits: 8
 - Parity: None
 - Stop Bits: 1
 - Flow Control: None
3. Check the link by pressing <ENTER>. The line should jump to the next line.
4. Using the Username and password to login the switch

```
Username: admin
Password:
#
```

5. If there is no user input for a period of time, the user will be locked out and will require to re-enter by pressing ENTER.

```
Username: admin
Password:
#
Press ENTER to get started█
```

6. The admin username is operating at the highest privilege level (level 15) and has full control over the OSD2790SFP and its configuration. On this level, the admin can reset the OSD2790SFP configuration to factory default.

OPTICAL SYSTEMS DESIGN

CLI COMMANDS (TOP LEVEL)

By entering “?” a list of CLI commands available with a brief description will be displayed

```
# ?
clear          Reset functions
configure     Enter configuration mode
copy          Copy from source to destination
delete        Delete one file in flash: file system
dir           Directory of all files in flash: file system
disable       Turn off privileged commands
do            To run exec commands in the configuration mode
dot1x         IEEE Standard for port-based Network Access Control
enable        Turn on privileged commands
erps          Ethernet Ring Protection Switching
exit          Exit from EXEC mode
firmware      Firmware upgrade/swap
help          Description of the interactive help system
ip            IPv4 commands
ipv6          IPv6 configuration commands
link-oam      Link OAM configuration
logout        Exit from EXEC mode
more          Display file
no            Negate a command or set its defaults
ping          Send ICMP echo messages
platform      Platform configuration
ptp           Misc non persistent 1588 settings
reload        Reload system.
send          Send a message to other tty lines
show          Show running system information
terminal      Set terminal line parameters
verify        VeriPHY keyword
```

Some terminal emulators like SecureCRT support the “Tab” key. At the # prompt pressing the “Tab” key will also produce a list of available commands within the command level. Partially typing a command and hitting “Tab” key will autocomplete the command.

```
#
clear      configure  copy      delete    dir        disable   do
dot1x      enable     erps      exit      firmware  help      ip
ipv6       link-oam   logout    more      no         ping      platform
ptp        reload     send      show      terminal   verify
#
```


OPTICAL SYSTEMS DESIGN

Help may be requested at any point in a command by entering a question mark “?”. If there are no command arguments available, the help list will be empty and the user must backup (backspace) until entering a “?” shows the available options. There are two types of help provided;

1. Full help is available when the user is ready to enter a command argument (eg. “show”) and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and user wants to know what arguments match the input (eg “show pr?”)

Note that there are sub-commands for every 1st level commands eg. **# clear ?** will display all sub command arguments associated with the **clear** command. The CLI will then display # clear and wait for the sub command.

```
# clear ?
access          Access management
access-list     Access list
dot1x           IEEE Standard for port-based Network Access Control
eps            Ethernet Protection Switching.
erps           Ethernet Ring Protection Switching
evc            Ethernet Virtual Connections
ip             Interface Internet Protocol configuration commands
ipv6           IPv6 configuration commands
lACP           Clear LACP statistics
link-oam        Clear Link OAM statistics
lldp           Clears LLDP statistics.
logging         System logging message
mac            MAC Address Table
mep            Maintenance Entity Point
mvr            Multicast VLAN Registration configuration
network-clock  Clear active WTR timer.
ptp
sflow          Statistics flow.
spanning-tree  STP Bridge
statistics     Clear statistics for one or more given interfaces
# clear
```

RESET CONFIGURATION TO FACTORY DEFAULT

To reset the configuration to factory defaults;

reload defaults

When the prompt returns, the unit has reverted to factory defaults

OPTICAL SYSTEMS DESIGN

SET HOSTNAME AND ADMIN USER PASSWORD

The CLI has several different modes. When entering the CLI through the admin entry, the mode is in exec mode. This allows the user to modify configuration files, reload defaults, system information etc. When the unit is in configuration mode, the user can change detailed configurations.

To set the OSD2790SFP host name, the unit needs to be first set to configuration mode then enter the hostname command, then a chosen hostname. After this is entered, the units requires an 'exit' from configuration mode.

```
# configure terminal
(config)# hostname OSD2512-sec1
OSD2512-sec1(config)# exit
OSD2512-sec1#
```

The host name has now changed to "OSD2790SFP-Sec1" and can be seen on the prompt.

A new password for the 'admin' user is recommended to be set.

```
OSD2512-sec1#
OSD2512-sec1#
OSD2512-sec1# configure terminal
OSD2512-sec1(config)# username admin privilege 15 password unencrypted OSD
OSD2512-sec1(config)# exit
OSD2512-sec1# █
```

In the example above the password was changed to "OSD". Other users can be added using the above method.

OPTICAL SYSTEMS DESIGN

SET VLAN 1 IP ADDRESS

To display current IP address and subnet mask details;

```
# show ip interface brief
```

To configure a new IP address the unit needs to be first set to configuration mode then enter the interface VLAN number, then a chosen IP address. An 'exit' from configuration mode is also required when changes are made. Note that the chosen input arguments (IP address/Subnet mask) are not in bold shown in the example below.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if-vlan)# ip address 192.168.0.99 255.255.0.0
Switch(config-if-vlan)# end
```

Note: IP addresses can only be assigned to VLAN interfaces.

After configuration the IP address is completed, the newly allocated IP address can be checked again by typing in;

```
# show ip interface brief
```

If the DHCP negotiation failed, the fallback IP is assigned (192.168.0.99)

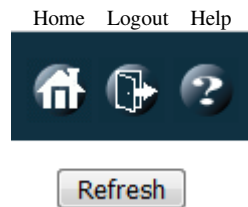
SAVE CONFIGURATION TO FLASH

It is necessary to save any changes to FLASH storage in the 'startup-config' otherwise the changes will not take effect when the unit is powered off. To save the changes the configuration needs to be copied to the startup configuration.

```
# copy running-config startup-config
```

3.6 GUI OVERVIEW

The Quick Start Guide section will only show a few main or important features to get the user started and running the OSD2790SFP successfully. On the top right hand of the GUI screen there are three icons available to quickly navigate or obtain help for each GUI menu item. *Note: Some screen captures will not display the full port channel count for the product. Port Number screen captures are indicative only!*



HOME: Clicking the Home button will exit any GUI current screen and display the panel status.

LOGOUT: Clicking the Logout button will logout the current user.

HELP: Clicking the Help button will open a help window for the current open menu window and display all functions and input arguments for that page.

DEFAULT SETTING

- IP Address: 192.168.0.99
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.0.1
- User Name: admin
- Password: (None)

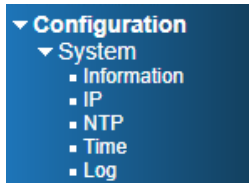
LOG INTO THE SWITCH

- Connect a switch port to a PC, Change the PC's network IP address to connect to the switch (i.e.: 192.168.0.2).
- In a web browser, enter the URL 192.168.0.99.
- Enter the username and password.

OPTICAL SYSTEMS DESIGN

IP CONFIGURATION

In the treemap on the left, expand the **Configuration** → **System** → **IP**.



IP Configuration

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

IP Interfaces

Delete	VLAN	DHCPv4			IPv4		DHCPv6			IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
<input type="checkbox"/>	1	<input type="checkbox"/>	0		192.168.0.99	24	<input type="checkbox"/>	<input type="checkbox"/>			

Add Interface

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
--------	---------	-------------	---------	---------------

Add Route

Save Reset

Enter the **IPv4 address** and **Mask Length** in the table.

Choose the management VLAN ID to access that IP in **VLAN** table if VLAN function is required.

If the multiple IP addresses are required, click **Add Interface** to add more IP interface.

Click **Save** to save the configuration.

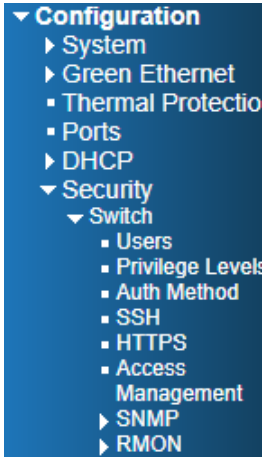
Use new IP address to access the switch.

PS: All configuration changes must be saved otherwise all the changes will be lost after rebooting!

OPTICAL SYSTEMS DESIGN

USERS AUTHENTICATION

In the tree map on the left, expand the **Configuration** → **Security** → **Switch** → **Users**



Users Configuration

User Name	Privilege Level
admin	15

Click **admin** to change the current admin account setting.

Edit User

User Settings	
User Name	admin
Password	
Password (again)	
Privilege Level	15 ▼

If multiple users are required, click **Add New User**

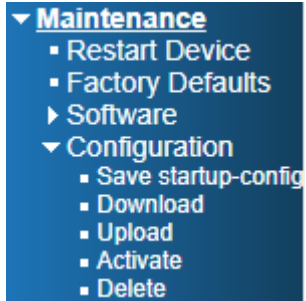
Add User

User Settings	
User Name	
Password	
Password (again)	
Privilege Level	0 ▼

PS: All configuration changes must be saved otherwise all the changes will be lost after rebooting!

SAVE CONFIGURATION TO START-UP

In the treemap below, expand the **Maintenance** and expand **Configuration**, then select Save startup-config



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.

Click **Save Configuration** to save the configuration on start-up.

4 USER MANUAL

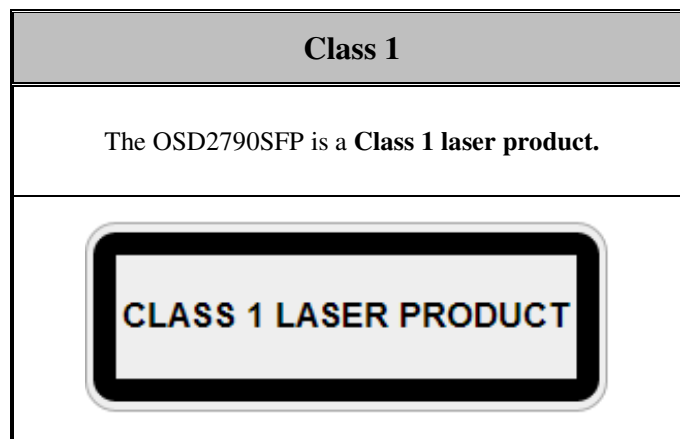
4.1 INSTALLATION

ELECTROMAGNETIC COMPATIBILITY

WARNING: This is a **Class A product**. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

OPTICAL OUTPUT OPERATION

WARNING: Laser Safety: Class 1 Laser Product (SFP) per IEC 60825-1:2014 standard.



PRECAUTIONS

- ▲ All service personnel should be provided training as to the hazards of direct viewing of laser radiation and of the precautionary measures during servicing of equipment
- ▲ Areas where laser products are installed should be restricted in access to trained service personnel only and appropriate warning signs posted in the work area.
- ▲ All laser apertures should be covered by protective covers when not connected to optical fibers. Never leave outputs uncovered.
- ▲ Laser equipment should be positioned above or below eye level where possible. Apertures should be positioned away from personnel.
- ▲ Protective eyewear should be worn in the vicinity of laser equipment.

4.2 OSD2790SFP DIMENSIONS

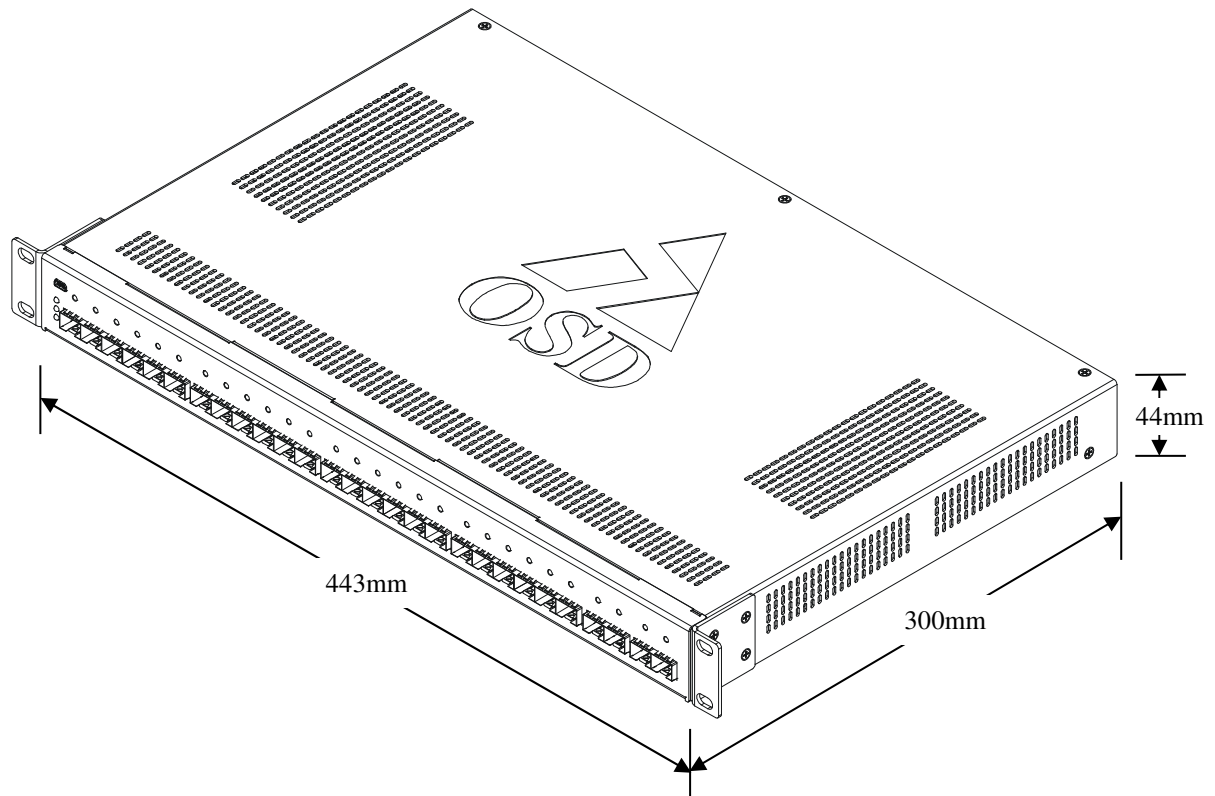
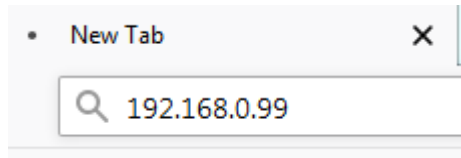


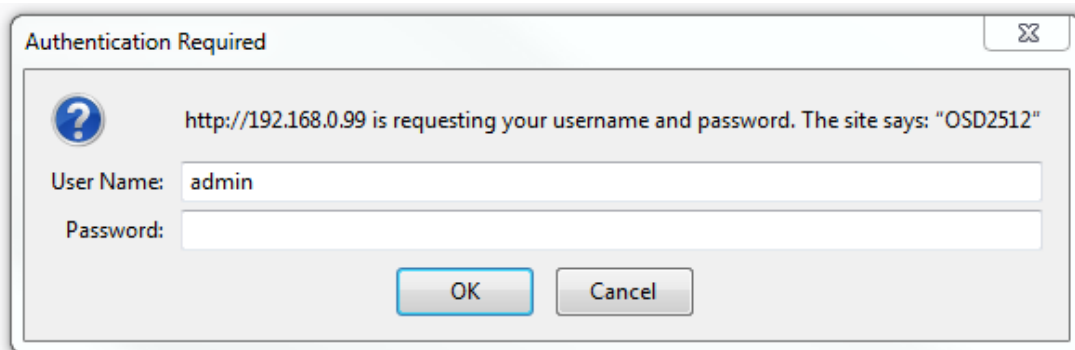
FIGURE 6: DIMENSIONS

5 GUI CONFIGURATION

- Connect the OSD2790SFP to a network using Cat5 (or greater) cable to any switch port fitted with an appropriate SFP and power the unit.
- Open a web browser window (Firefox, IEx, etc) Enter the IP address of the switch on the web browser - *The default IP address assigned to the OSD2790SFP is 192.168.0.99*. A login window will be shown as below:



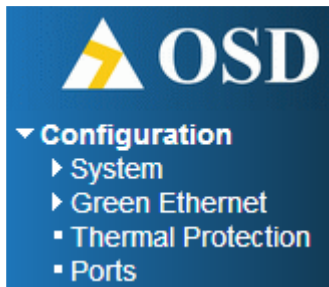
- Enter the username and password. Below diagram shows default login parameters. If this has been changed, enter a valid username and password.



5.1 GUI MENU

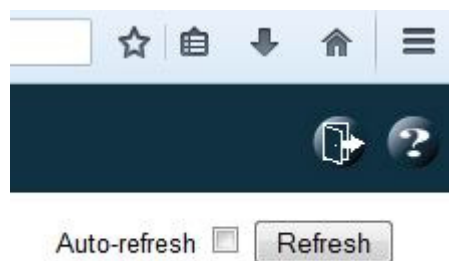
The GUI Menu allows the user to change many parameters and settings. The example below shows a snapshot of the menu. The following symbols and actions are as follows;

- ▶ Menu can be expanded to show sub menus by clicking the heading
- ▼ Menu is expanded and sub menus are displayed. Clicking the heading will close the submenu
- Menu title. Clicking will open the GUI window for this parameter



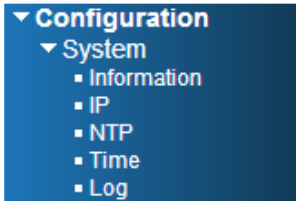
The help “?” button is located on the right hand side of the browser. Clicking this button will open the help menu with control syntax for the selected open directory.

Clicking the door symbol will bring up the “Logout” screen.



5.2 CONFIGURATION

SYSTEM



SYSTEM INFORMATION CONFIGURATION

Configuration → *System* → *Information*

System Information Configuration

System Contact	<input type="text"/>
System Name	<input type="text"/>
System Location	<input type="text"/>

The switch system information is provided here.

System Contact

The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

System Name

An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z, a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.

System Location

The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Buttons

: Click to save changes.

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

OPTICAL SYSTEMS DESIGN

IP CONFIGURATION

Configuration → System → IP

IP Configuration

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

IP Interfaces

Delete	VLAN	DHCPv4			IPv4		DHCPv6			IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
<input type="checkbox"/>	1	<input type="checkbox"/>	0		192.168.0.99	24	<input type="checkbox"/>	<input type="checkbox"/>			

Add Interface

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
--------	---------	-------------	---------	---------------

Add Route

Save Reset

Configure IP basic settings, control IP interfaces and IP routes.

The maximum number of interfaces supported is 128 and the maximum number of routes is 128.

IP Configuration

Mode

Configure whether the IP stack should act as a *Host* or a *Router*. In *Host* mode, IP traffic between interfaces will not be routed. In *Router* mode traffic is routed between all interfaces.

DNS Server

This setting controls the DNS name resolution done by the switch.

There are four servers available for configuration, and the index of the server presents the preference (less index has higher priority) in doing DNS name resolution.

System selects the active DNS server from configuration in turn, if the preferred server does not respond in five attempts.

The following modes are supported:

- From any DHCPv4 interfaces

The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used.

- No DNS server

No DNS server will be used.

OPTICAL SYSTEMS DESIGN

- Configured IPv4
Explicitly provide the valid IPv4 unicast address of the DNS Server in dotted decimal notation.
Make sure the configured DNS server could be reachable (e.g. via PING) for activating DNS service.
- From this DHCPv4 interface
Specify from which DHCPv4-enabled interface a provided DNS server should be preferred.
- Configured IPv6
Explicitly provide the valid IPv6 unicast (except linklocal) address of the DNS Server.
Make sure the configured DNS server could be reachable (e.g. via PING6) for activating DNS service.
- From this DHCPv6 interface
Specify from which DHCPv6-enabled interface a provided DNS server should be preferred.
- From any DHCPv6 interfaces
The first DNS server offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used.

DNS Proxy

When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.
Only IPv4 DNS proxy is now supported.

IP Interfaces

Delete

Select this option to delete an existing IP interface.

VLAN

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

IPv4 DHCP Enabled

Enable the DHCPv4 client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol. The DHCPv4 client will announce the configured System Name as hostname to provide DNS lookup.

OPTICAL SYSTEMS DESIGN

IPv4 DHCP Fallback Timeout

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

IPv4 DHCP Current Lease

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

IPv4 Address

The IPv4 address of the interface in dotted decimal notation.

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

IPv4 Mask

The IPv4 network mask, in number of bits (*prefix length*). Valid values are between 0 and 30 bits for a IPv4 address.

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

DHCPv6 Enable

Enable the DHCPv6 client by checking this box. If this option is enabled, the system will configure the IPv6 address of the interface using the DHCPv6 protocol.

DHCPv6 Rapid Commit

Enable the DHCPv6 Rapid-Commit option by checking this box. If this option is enabled, the DHCPv6 client terminates the waiting process as soon as a Reply message with a Rapid Commit option is received.

This option is only manageable when DHCPv6 client is enabled.

DHCPv6 Current Lease

For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server.

IPv6 Address

The IPv6 address of the interface. A IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once.

System accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address.

The field may be left blank if IPv6 operation on the interface is not desired.

IPv6 Mask

The IPv6 network mask, in number of bits (*prefix length*). Valid values are between 1 and 128 bits for a IPv6 address.

The field may be left blank if IPv6 operation on the interface is not desired.

OPTICAL SYSTEMS DESIGN

Resolving IPv6 DAD

The link-local address is formed from an interface identifier based on the hardware address which is supposed to be uniquely assigned. Once the DAD (Duplicate Address Detection) detects the address duplication, the operation on the interface SHOULD be disabled.

At this moment, manual intervention is required to resolve the address duplication. For example, check whether the loop occurs in the VLAN or there is indeed other device occupying the same hardware address as the device in the VLAN.

After making sure the specific link-local address is unique on the IPv6 link in use, delete and then add the specific IPv6 interface to restart the IPv6 operations on this interface.

IP Routes

Delete

Select this option to delete an existing IP route.

Network

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

Mask Length

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

Gateway

The IP address of the IP gateway. Valid format is 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.

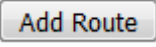
The given VID ranges from 1 to 4095 and will be effective only when the corresponding IPv6 interface is valid.


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.

Buttons

 : Click to add a new IP interface. A maximum of 128 interfaces is supported.

 : Click to add a new IP route. A maximum of 128 routes is supported.

 : Click to save changes.

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

OPTICAL SYSTEMS DESIGN

NTP CONFIGURATION

Configuration → System → NTP

NTP Configuration

Mode	Disabled ▾
Server 1	
Server 2	
Server 3	
Server 4	
Server 5	

Save

Reset

Configure NTP on this page.

Mode

Indicates the NTP mode operation. Possible modes are:

Enabled: Enable NTP client mode operation.

Disabled: Disable NTP client mode operation.

Server

Provide the IPv4 or IPv6 address of a NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'. In addition, it can also accept a domain name address.

Buttons

Save

: Click to save changes.

Reset

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

OPTICAL SYSTEMS DESIGN

TIME ZONE CONFIGURATION

Configuration → System → Time

Time Zone Configuration

Time Zone Configuration	
Time Zone	None ▼
Acronym	<input type="text"/> (0 - 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled ▼

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

Time Zone

This page allows you to configure the Time Zone.

Time Zone Configuration

- **Time Zone** - Lists various Time Zones world wide. Select appropriate Time Zone from the drop down and click Save to set.
- **Acronym** - User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range : Up to 16 characters)

Daylight Saving Time

This page is used to setup Daylight Saving Time Configuration.

Daylight Saving Time Configuration

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

Recurring Configurations

Start time settings

- **Week** - Select the starting week number.
- **Day** - Select the starting day.
- **Month** - Select the starting month.
- **Hours** - Select the starting hour.
- **Minutes** - Select the starting minute.

End time settings

- **Week** - Select the ending week number.
- **Day** - Select the ending day.
- **Month** - Select the ending month.
- **Hours** - Select the ending hour.
- **Minutes** - Select the ending minute.

Offset settings

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

Non Recurring Configurations

Start time settings

- **Month** - Select the starting month.
- **Date** - Select the starting date.
- **Year** - Select the starting year.
- **Hours** - Select the starting hour.
- **Minutes** - Select the starting minute.

OPTICAL SYSTEMS DESIGN


End time settings


- **Month** - Select the ending month.
- **Date** - Select the ending date.
- **Year** - Select the ending year.
- **Hours** - Select the ending hour.
- **Minutes** - Select the ending minute.

Offset settings

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

Buttons

 : Click to save changes.

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

SYSTEM LOG CONFIGURATION

Configuration → System → Log

System Log Configuration

Server Mode	Disabled
Server Address	
Syslog Level	Informational

Save Reset

Configure System Log on this page.

Server Mode

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

Enabled: Enable server mode operation.

Disabled: Disable server mode operation.

Server Address

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

Syslog Level

Indicates what kind of message will send to syslog server. Possible modes are:

Error: Send the specific messages which severity code is less or equal than Error (3).

Warning: Send the specific messages which severity code is less or equal than Warning (4).

Notice: Send the specific messages which severity code is less or equal than Notice (5).

Informational: Send the specific messages which severity code is less or equal than Informational (6).

Buttons

Save : Click to save changes.

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

GREEN ETHERNET

- ▼ Green Ethernet
 - Fan
 - LED
 - Port Power Savings

FAN CONFIGURATION

[Configuration](#) → [Green Ethernet](#) → [Fan](#)

Fan Configuration

Max Temperature	100	°C
On Temperature	75	°C

This page allows the user to inspect and configure the current settings for controlling the fan. If the system contains multiple temperature sensor the highest temperature is used for controlling the fan

Max Temperature

The temperature at which the fan will be set to run at full speed. The value accepted is within the range of -127 to 127.

On Temperature

The temperature at which the fan will be turn on (at the lowest possible fan speed). The value accepted is within the range of -127 to 127.

Buttons

: Click to save changes.

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

OPTICAL SYSTEMS DESIGN

LED POWER REDUCTION CONFIGURATION

Configuration → Green Ethernet → LED

LED Power Reduction Configuration

LED Intensity Timers

Delete	Start Time	End Time	Intensity
<input type="checkbox"/>	00:00 ▾	00:00 ▾	20 ▾ %

Add Time

Maintenance

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

Save

Reset

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.

LEDS INTENSITY

The LEDs power consumption can be reduced by lowering the LEDs intensity. LEDs intensity could for example be lowered during night time, or they could be turn completely off. It is possible to configure 24 different hours of the day, at where the LEDs intensity should be set.

Start Time

The time at which the LEDs intensity shall be set to the corresponding intensity.

End Time

The time at which the LEDs intensity shall be set to a new intensity. If no intensity is specified for the next hour, the intensity is set to default intensity.

Intensity

The LEDs intensity (100% = Full power, 0% = LED off).

MAINTENANCE


On time at link change

When a network administrator does maintenance of the switch (e.g. adding or moving users) he might want to have full LED intensity during the maintenance period. Therefore it is possible to specify that the LEDs shall use full intensity a specific period of time. **Maintenance Time** is the number of seconds that the LEDs will have full intensity after either a port has changed link state, or the LED pushbutton has been pushed. Valid range is from 0 to 65535 seconds.

On at errors

In the case where maximum power saving is enabled by turning the LEDs completely off, it might be convenient to indicate to the network administrator that an error has been recorded in the system log. By checking the "On at errors" the LEDs will be turned on at 100% in the case that errors are logged in the system log.

Buttons

 : Click to save changes.

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

OPTICAL SYSTEMS DESIGN

PORT POWER SAVINGS CONFIGURATION

Configuration → Green Ethernet → Port Power Savings

Port Power Savings Configuration

Optimize EEE for Latency

Port Configuration

Port	ActiPHY	PerfectReach	EEE	EEE Urgent Queues								
				1	2	3	4	5	6	7	8	
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save

Reset

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

WHAT IS EEE

EEE is a power saving 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.

OPTICAL SYSTEMS DESIGN

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

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.

OPTIMIZE EEE FOR

The switch can be set to optimize EEE for either best power saving or least traffic latency.

PORT CONFIGURATION

Port

The switch port number of the logical port.

ActiPHY

Link down power savings enabled.

ActiPHY works by lowering the power for a port when there is no link. The port is power up for short moment in order to determine if cable is inserted.

PerfectReach

Cable length power savings enabled.

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

EEE

Controls whether EEE is enabled for this switch port.


For maximizing power savings, the circuit isn't started at once transmit data is ready for a port, but is instead queued until a burst of data is ready to be transmitted. This will give some traffic latency.

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

EEE Urgent Queues

Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

Buttons

 : Click to save changes.

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

OPTICAL SYSTEMS DESIGN

PORT CONFIGURATION

Configuration → Ports

Ports

Port Configuration

Port	Description	Link	Speed		Adv Duplex		Adv speed			Flow Control			PFC		Maximum Frame Size	Frame Length Check	
			Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority			
-			<>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
1		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
2		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
3		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
4		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
5		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
6		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
7		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
8		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
9		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
10		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
11		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
12		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
13		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
14		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
15		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
16		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
17		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
18		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
19		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
20		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
21		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
22		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
23		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
24		● 100fdx (Cu SFP)	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
25		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
26		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
27		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>
28		● Down	Auto	▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7	10240	<input type="checkbox"/>

Save Reset

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

Port

This is the logical port number for this row.

Description

The description of the port. It is an ASCII string no longer than 256 characters.

Link

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

Current Link Speed

Provides the current link speed of the port.

OPTICAL SYSTEMS DESIGN

Configured Link Speed

Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are:

`Disabled` - Disables the 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

`SFP_Auto_AMS` - Automatically determines the speed of the SFP. Note: There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect some SFPs might not be detectable. The port is set in AMS mode. Cu port is set in **Auto** mode.

`100-FX` - SFP port in 100-FX speed. Cu port disabled.

`1000-X` - SFP port in 1000-X speed. Cu port disabled.

Ports in AMS mode with 1000-X speed has Cu port preferred.

Ports in AMS mode with 1000-X speed has fiber port preferred.

Ports in AMS mode with 100-FX speed has fiber port preferred.

Advertise Duplex

When duplex is set as auto i.e auto negotiation, the port will only advertise the specified duplex as either `Fdx` or `Hdx` to the link partner. By default port will advertise all the supported duplexes if the Duplex is Auto.

Advertise Speed

When Speed is set as auto i.e auto negotiation, the port will only advertise the specified speeds (10M 100M 1G) to the link partner. By default port will advertise all the supported speeds if speed is set as Auto.

Flow Control

When `Auto Speed` is selected on a port, this section indicates the flow control capability that is advertised to the link partner.

When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto Negotiation.

Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.

NOTICE: The 100FX standard doesn't support Auto Negotiation, so when in 100FX mode the flow control capabilities will always be shown as "disabled".

PFC

When PFC (802.1Qbb Priority Flow Control) is enabled on a port then flow control on a priority level is enabled. Through the `Priority` field, range (one or more) of priorities can be configured, e.g. '0-3,7' which equals '0,1,2,3,7'. PFC is not supported through auto negotiation. PFC and Flowcontrol cannot both be enabled on the same port.

Maximum Frame Size

Enter the maximum frame size allowed for the switch port, including FCS. The range is 1518-10240 bytes.

OPTICAL SYSTEMS DESIGN

Frame Length Check

Configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If "frame length check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actual payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch. Note: No drop counters count frames dropped due to frame length mismatch

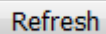
Buttons

 Save

: Click to save changes.

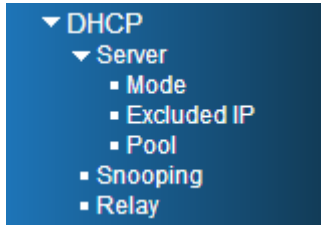
 Reset

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

 Refresh

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

DHCP



SERVER

DHCP Server Mode Configuration

Configuration → DHCP → Server → Mode

DHCP Server Mode Configuration

Global Mode

Mode Disabled ▾

VLAN Mode

Delete	VLAN Range	Mode
--------	------------	------

Add VLAN Range

Save Reset

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

OPTICAL SYSTEMS DESIGN

GLOBAL MODE

Configure operation mode to enable/disable DHCP server per system.

Mode

Configure the operation mode per system. Possible modes are:

Enabled: Enable DHCP server per system.

Disabled: Disable DHCP server per system.

VLAN MODE

Configure operation mode to enable/disable DHCP server per VLAN.

VLAN Range

Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. BUT, if the VLAN range contains only 1 VLAN ID, then you can just input it into either one of the first and second VLAN ID or both.

On the other hand, if you want to disable existed VLAN range, then you can follow the steps.

1. Press to add a new VLAN range.
2. Input the VLAN range that you want to disable.
3. Choose Mode to be Disabled.
4. Press to apply the change.

Then, you will see the disabled VLAN range is removed from the DHCP Server mode configuration page.

Mode

Indicate the operation mode per VLAN. Possible modes are:

Enabled: Enable DHCP server per VLAN.

Disabled: Disable DHCP server per VLAN.

Buttons

: Click to add a new VLAN range

: Click to save changes.

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

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

DHCP Server Excluded IP Configuration

Configuration → DHCP → Server → Excluded IP

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

EXCLUDED IP ADDRESS

Configure excluded IP addresses.

IP Range

Define the IP range to be excluded IP addresses. The first excluded IP must be smaller than or equal to the second excluded IP. BUT, if the IP range contains only 1 excluded IP, then you can just input it to either one of the first and second excluded IP or both.

Buttons

Add IP Range

: Click to add a new excluded IP range.

Save

: Click to save changes.

Reset

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

DHCP Server Pool Configuration

Configuration → DHCP → Server → Pool

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

POOL SETTING

Add or delete pools.

Adding a pool and giving a name is to create a new pool with "default" configuration. If you want to configure all settings including type, IP subnet mask and lease time, you can click the pool name to go into the configuration page.

Name

Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page.

Type

Display which type of the pool is.

Network: the pool defines a pool of IP addresses to service more than one DHCP client.

Host: the pool services for a specific DHCP client identified by client identifier or hardware address.

If "-" is displayed, it means not defined.

IP

Display network number of the DHCP address pool.

If "-" is displayed, it means not defined.

Subnet Mask

Display subnet mask of the DHCP address pool.

If "-" is displayed, it means not defined.

Lease Time

Display lease time of the pool.

Buttons

Add New Pool

: Click to add a new DHCP pool.

Save

: Click to save changes.

Reset

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

DHCP SNOOPING CONFIGURATION

Configuration → *DHCP* → *Snooping*

DHCP Snooping Configuration

Snooping Mode

Port Mode Configuration

Port	Mode
*	<>
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted
6	Trusted
7	Trusted
8	Trusted
9	Trusted
10	Trusted
11	Trusted
12	Trusted
13	Trusted
14	Trusted

Configure DHCP Snooping on this page.

Snooping Mode

Indicates the DHCP snooping mode operation. Possible modes are:

Enabled: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

Disabled: Disable DHCP snooping mode operation.

OPTICAL SYSTEMS DESIGN


Port Mode Configuration

Indicates the DHCP snooping port mode. Possible port modes are:

Trusted: Configures the port as trusted source of the DHCP messages.

Untrusted: Configures the port as untrusted source of the DHCP messages.

Buttons

: Click to save changes.

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

DHCP RELAY CONFIGURATION

Configuration → DHCP → Relay

DHCP Relay Configuration

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

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

Relay Mode

Indicates the DHCP relay mode operation.

Possible modes are:

Enabled: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.

Disabled: Disable DHCP relay mode operation.

Relay Server

Indicates the DHCP relay server IP address.

Relay Information Mode

Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID (in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.

Possible modes are:

Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.

Disabled: Disable DHCP relay information mode operation.

OPTICAL SYSTEMS DESIGN

Relay Information Policy


Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are:


Replace: Replace the original relay information when a DHCP message that already contains it is received.

Keep: Keep the original relay information when a DHCP message that already contains it is received.

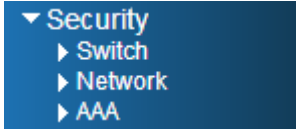
Drop: Drop the package when a DHCP message that already contains relay information is received.

Buttons

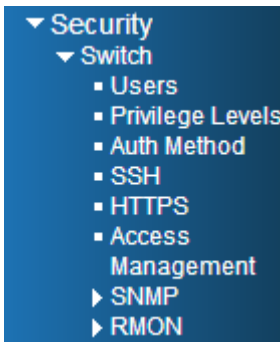
 : Click to save changes.

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

SECURITY



SWITCH



Users Configuration

Configuration → Security → Switch → Users

Users Configuration

User Name	Privilege Level
admin	15

Add New User

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

The displayed values for each user are:

User Name

The name identifying the user. This is also a link to Add/Edit User.


Privilege Level

The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15.

OPTICAL SYSTEMS DESIGN

Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

A rectangular button with a light gray background and a thin black border. The text "Add New User" is centered on the button in a dark gray font.

: Click to add a new user.

OPTICAL SYSTEMS DESIGN

Privilege Level Configuration

Configuration → Security → Switch → Privilege Levels

Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5 ▼	10 ▼	5 ▼	10 ▼
Debug	15 ▼	15 ▼	15 ▼	15 ▼
DHCP	5 ▼	10 ▼	5 ▼	10 ▼
DHCPv6_Client	5 ▼	10 ▼	5 ▼	10 ▼
Diagnostics	5 ▼	10 ▼	5 ▼	10 ▼
EPS	5 ▼	10 ▼	5 ▼	10 ▼
ERPS	5 ▼	10 ▼	5 ▼	10 ▼
ETH_LINK_OAM	5 ▼	10 ▼	5 ▼	10 ▼
EVC	5 ▼	10 ▼	5 ▼	10 ▼
Green_Ethernet	5 ▼	10 ▼	5 ▼	10 ▼
IP	5 ▼	10 ▼	5 ▼	10 ▼
IPMC_Snooping	5 ▼	10 ▼	5 ▼	10 ▼
JSON_RPC	5 ▼	10 ▼	5 ▼	10 ▼
JSON_RPC_Notification	5 ▼	10 ▼	5 ▼	10 ▼
LACP	5 ▼	10 ▼	5 ▼	10 ▼
LLDP	5 ▼	10 ▼	5 ▼	10 ▼
Loop_Protect	5 ▼	10 ▼	5 ▼	10 ▼
MAC_Table	5 ▼	10 ▼	5 ▼	10 ▼
Maintenance	15 ▼	15 ▼	15 ▼	15 ▼
MEP	5 ▼	10 ▼	5 ▼	10 ▼
MVR	5 ▼	10 ▼	5 ▼	10 ▼
NTP	5 ▼	10 ▼	5 ▼	10 ▼
POE	5 ▼	10 ▼	5 ▼	10 ▼
Ports	5 ▼	10 ▼	1 ▼	10 ▼
Private_VLANs	5 ▼	10 ▼	5 ▼	10 ▼
PTP	5 ▼	10 ▼	5 ▼	10 ▼
QoS	5 ▼	10 ▼	5 ▼	10 ▼
RMirror	5 ▼	10 ▼	5 ▼	10 ▼
Security	5 ▼	10 ▼	5 ▼	10 ▼
sFlow	5 ▼	10 ▼	5 ▼	10 ▼
Spanning_Tree	5 ▼	10 ▼	5 ▼	10 ▼
System	5 ▼	10 ▼	1 ▼	10 ▼
UDLD	5 ▼	10 ▼	5 ▼	10 ▼
UPnP	5 ▼	10 ▼	5 ▼	10 ▼
VCL	5 ▼	10 ▼	5 ▼	10 ▼
VLAN_Translation	5 ▼	10 ▼	5 ▼	10 ▼
VLANs	5 ▼	10 ▼	5 ▼	10 ▼
Voice_VLAN	5 ▼	10 ▼	5 ▼	10 ▼
XXRP	5 ▼	10 ▼	5 ▼	10 ▼

Save Reset

OPTICAL SYSTEMS DESIGN

This page provides an overview of the privilege levels.

Group Name

The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:

System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.

Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.

IP: Everything except 'ping'.

Port: Everything except 'VeriPHY'.

Diagnostics: 'ping' and 'VeriPHY'.

Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.


Debug: Only present in CLI.

Privilege Levels

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

Notes that some web pages (for example, MPLS-TP and MEP BFD pages) are based on JSON to transmit dynamic data between the web server and application. These pages require the configuration Read/Write privilege of JSON_RPC group before any operations. This requirement must be met first, then it will evaluate the current privilege level against the required privilege level for the given method. For example, assumes the MPLS-TP page only allows Read-Only attribute under privilege level 5, the privilege configuration should be set as JSON_RPC:[5,5,5,5] and MPLS_TP:[5,10,5,10].

Buttons

 : Click to save changes.

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

Authentication Method Configuration

Configuration → Security → Switch → Auth Method

Authentication Method Configuration

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

Command Authorization Method Configuration

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

Accounting Method Configuration

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

Save Reset

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

The table has one row for each client type and a number of columns, which are:

Client

The management client for which the configuration below applies.

Methods

Method can be set to one of the following values:

- No: Authentication is disabled and login is not possible.
- Local: Use the local user database on the switch for authentication.
- Radius: Use remote RADIUS server(s) for authentication.
- Tacacs: Use remote TACACS+ server(s) for authentication.

OPTICAL SYSTEMS DESIGN

Methods that involves 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.

COMMAND AUTHORIZATION METHOD CONFIGURATION HELP

The command authorization section allows you to limit the CLI commands available to a user.

The table has one row for each client type and a number of columns, which are:

Client

The management client for which the configuration below applies.

Method

Method can be set to one of the following values:

- No: Command authorization is disabled. User is granted access to CLI commands according to his privilege level.
- Tacacs: Use remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.

Cmd Lvl

Authorize all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15.

Cfg Cmd

Also authorize configuration commands.

ACCOUNTING METHOD CONFIGURATION HELP

The accounting section allows you to configure command and exec (login) accounting.

The table has one row for each client type and a number of columns, which are:

Client

The management client for which the configuration below applies.

Method

Method can be set to one of the following values:

- No: Accounting is disabled.
- Tacacs: Use remote TACACS+ server(s) for accounting.

Cmd Lvl


Enable accounting of all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15. Leave the field empty to disable command accounting.


OPTICAL SYSTEMS DESIGN

Exec

Enable exec (login) accounting.

Buttons

: Click to save changes.

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

OPTICAL SYSTEMS DESIGN

SSH Configuration

[Configuration](#) → [Security](#) → [Switch](#) → [SSH](#)

SSH Configuration

Mode Enabled ▾

Configure SSH on this page.

Mode

Indicates the SSH mode operation. Possible modes are:

Enabled: Enable SSH mode operation.

Disabled: Disable SSH mode operation.

Buttons

: Click to save changes.

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

OPTICAL SYSTEMS DESIGN

HTTPS Configuration

Configuration → Security → Switch → HTTPS

HTTPS Configuration

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

This page allows you to configure the HTTPS settings and maintain the current certificate on the switch.

Mode

Indicate the HTTPS mode operation.

Possible modes are:

Enabled: Enable HTTPS mode operation.

Disabled: Disable HTTPS mode operation.

Automatic Redirect

Indicate the HTTPS redirect mode operation. It is only significant when "HTTPS Mode Enabled" is selected. When the redirect mode is enabled, the HTTP connection will be redirected to HTTPS connection automatically.

Notice that the browser may not allow the redirect operation due to the security consideration unless the switch certificate is trusted to the browser. You need to initialize the HTTPS connection manually for this case.

Possible modes are:

Enabled: Enable HTTPS redirect mode operation.

Disabled: Disable HTTPS redirect mode operation.

Certificate Maintain

The operation of certificate maintenance.

Possible operations are:

None: No operation.

Delete: Delete the current certificate.

Upload: Upload a certificate PEM file. Possible methods are: Web Browser or URL.

Generate: Generate a new self-signed RSA certificate.

Certificate Pass Phrase

Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.

OPTICAL SYSTEMS DESIGN

Certificate Upload

Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem
Notice that the RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificate, e.g. Firefox v37 and Chrome v39.

Possible methods are:

Web Browser: Upload a certificate via Web browser.

URL: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP.

The URL format is <protocol>://[<username>[:<password>]@<

host>[:<port>][/<path>]/<file_name>. For example,

tftp://10.10.10.10/new_image_path/new_image.dat,

http://username:password@10.10.10.10:80/new_image_path/new_image.dat. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score (_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '!' is not allowed.

Certificate Status

Display the current status of certificate on the switch.

Possible statuses are:

Switch secure HTTP certificate is presented.

Switch secure HTTP certificate is not presented.

Switch secure HTTP certificate is generating

Buttons

Save

: Click to save changes.

Reset

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

Refresh

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

OPTICAL SYSTEMS DESIGN

Access Management Configuration

[Configuration](#) → [Security](#) → [Switch](#) → [Access Management](#)

Access Management Configuration

Mode

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

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

Mode

Indicates the access management mode operation. Possible modes are:
Enabled: Enable access management mode operation.
Disabled: Disable access management mode operation.

Delete

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

VLAN ID

Indicates the VLAN ID for the access management entry.

Start IP address

Indicates the start IP address for the access management entry.

End IP address

Indicates the end IP address for the access management entry.

HTTP/HTTPS

Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

SNMP


Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.


TELNET/SSH

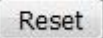
Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

OPTICAL SYSTEMS DESIGN

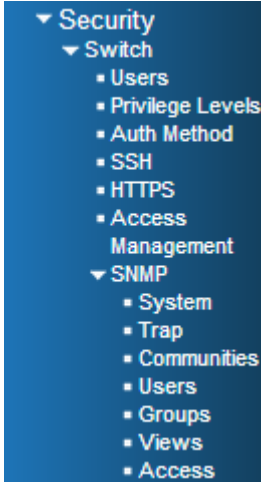
Buttons

: Click to add a new access management entry.

: Click to save changes.

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

SNMP Configuration



SNMP System Configuration

Configuration → Security → Switch → SNMP → System

SNMP System Configuration

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

Save Reset

Configure SNMP on this page.

Mode

Indicates the SNMP mode operation. Possible modes are:
Enabled: Enable SNMP mode operation.
Disabled: Disable SNMP mode operation.

Version

Indicates the SNMP supported version. Possible versions are:
SNMP v1: Set SNMP supported version 1.
SNMP v2c: Set SNMP supported version 2c.
SNMP v3: Set SNMP supported version 3.

OPTICAL SYSTEMS DESIGN

Read Community

Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

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

Write Community


Indicates the community 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.

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

Engine ID

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

Buttons

 : Click to save changes.

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

Trap Configuration

SNMPv3 Configuration → Security → Switch → SNMP → Trap

Trap Configuration

Global Settings

Mode

Trap Destination Configurations

Delete	Name	Enable	Version	Destination Address	Destination Port
--------	------	--------	---------	---------------------	------------------

Configure SNMP trap on this page.

GLOBAL SETTINGS

Configure SNMP trap on this page.

Mode

Indicates the trap mode operation. Possible modes are:

Enabled: Enable SNMP trap mode operation.

Disabled: Disable SNMP trap mode operation.

TRAP DESTINATION CONFIGURATIONS

Configure trap destinations on this page.

Name

Indicates the trap Configuration's name. Indicates the trap destination's name.

Enable

Indicates the trap destination mode operation. Possible modes are:

Enabled: Enable SNMP trap mode operation.

Disabled: Disable SNMP trap mode operation.

Version

Indicates the SNMP trap supported version. Possible versions are:

SNMPv1: Set SNMP trap supported version 1.

SNMPv2c: Set SNMP trap supported version 2c.

SNMPv3: Set SNMP trap supported version 3.

OPTICAL SYSTEMS DESIGN

Destination Address

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

And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.

Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Destination port

Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

Buttons

: Click to add a new access management entry.

: Click to save changes.

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

OPTICAL SYSTEMS DESIGN

Community Configuration

Configuration → Security → Switch → SNMP → Communities

SNMPv3 Community Configuration

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

Add New Entry

Save

Reset

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

Delete

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

Community

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

Source IP

Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.

Source Mask

Indicates the SNMP access source address mask.

Buttons

Add New Entry

: Click to add a new access management entry.

Save

: Click to save changes.

Reset

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

OPTICAL SYSTEMS DESIGN

SNMPv3 User Configuration

[Configuration](#) → [Security](#) → [Switch](#) → [SNMP](#) → [Users](#)

SNMPv3 User Configuration

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

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

Delete

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

Engine ID

An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the `usmUserEngineID` and `usmUserName` are the entry's keys. In a simple agent, `usmUserEngineID` is always that agent's own `snmpEngineID` value. The value can also take the value of the `snmpEngineID` of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.

User Name

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

Security Level

Indicates the security model that this entry should belong to. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.

Authentication Protocol

Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

None: No authentication protocol.

MD5: An optional flag to indicate that this user uses MD5 authentication protocol.

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

The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.

OPTICAL SYSTEMS DESIGN

Authentication Password

A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.

Privacy Protocol

Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

None: No privacy protocol.

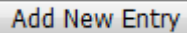
DES: An optional flag to indicate that this user uses DES authentication protocol.

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

Privacy Password

A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons



: Click to add a new access management entry.



: Click to save changes.



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

OPTICAL SYSTEMS DESIGN

SNMPv3 Group Configuration

Configuration → Security → Switch → SNMP → Groups

SNMPv3 Group Configuration

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

Add New Entry

Save

Reset

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

Delete

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

Security Model

Indicates the security model that this entry should belong to. Possible security models are:

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

Security Name

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

Group Name

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

Buttons

Add New Entry

: Click to add a new access management entry.

Save

: Click to save changes.

Reset

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

OPTICAL SYSTEMS DESIGN

SNMPv3 View Configuration

Configuration → Security → Switch → SNMP → Views

SNMPv3 View Configuration

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

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

Delete

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

View Name

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

View Type

Indicates the view type that this entry should belong to. Possible view types are:

included: An optional flag to indicate that this view subtree should be included.

excluded: An optional flag to indicate that this view subtree should be excluded.

In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.

OID Subtree

The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Buttons

: Click to add a new access management entry.

: Click to save changes.

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

OPTICAL SYSTEMS DESIGN

SNMPv3 Access Configuration

Configuration → Security → Switch → SNMP → Access

SNMPv3 Access Configuration

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

Add New Entry

Save

Reset

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

Delete

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

Group Name

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

Security Model

Indicates the view type that this entry should belong to. Possible view types are:

any: Any security model accepted(v1/v2clusm).

v1: Reserved for SNMPv1.

V2c: Reserved for SNMPv2c.

Usm: User-based Security Model (USM).

Security Level

Indicates the security model that this entry should belong to. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

Read View Name

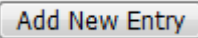
The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.


Write View Name

The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

OPTICAL SYSTEMS DESIGN

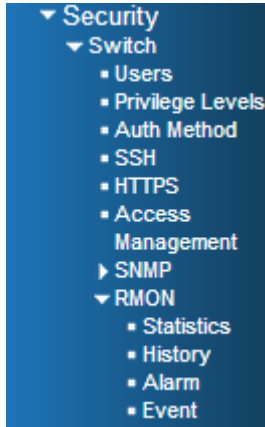
Buttons

: Click to add a new access management entry.

: Click to save changes.

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

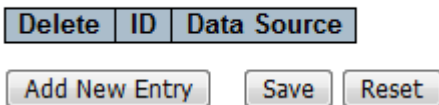
RMON Configuration



RMON Statistics Configuration

Configuration → Security → Switch → RMON → Statistics

RMON Statistics Configuration



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

Delete

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

ID

Indicates the index of the entry. The range is from 1 to 65535.

Data Source

Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.

Buttons

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

Save: Click to save changes.

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

OPTICAL SYSTEMS DESIGN

RMON History Configuration

[Configuration](#) → [Security](#) → [Switch](#) → [RMON](#) → [History](#)

RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
--------	----	-------------	----------	---------	-----------------

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

Delete

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

ID

Indicates the index of the entry. The range is from 1 to 65535.

Data Source

Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.

Interval

Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.

Buckets

Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.

Buckets Granted

The number of data shall be saved in the RMON.

Buttons

: Click to add a new access management entry.

: Click to save changes.

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

OPTICAL SYSTEMS DESIGN

RMON Alarm Configuration

Configuration → Security → Switch → RMON → Alarm

RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
--------	----	----------	----------	-------------	-------	---------------	------------------	--------------	-------------------	---------------

Add New Entry

Save

Reset

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

Delete

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

ID

Indicates the index of the entry. The range is from 1 to 65535.

Interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to $2^{31}-1$.

Variable

Indicates the particular variable to be sampled, the possible variables are:

InOctets: The total number of octets received on the interface, including framing characters.

InUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol.

InNUcastPkts: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.

InDiscards: The number of inbound packets that are discarded even the packets are normal.

InErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

InUnknownProtos: the number of the inbound packets that were discarded because of the unknown or un-support protocol.

OutOctets: The number of octets transmitted out of the interface , including framing characters.

OutUcastPkts: The number of uni-cast packets that request to transmit.

OutNUcastPkts: The number of broad-cast and multi-cast packets that request to transmit.

OutDiscards: The number of outbound packets that are discarded event the packets is normal.

OutErrors: The The number of outbound packets that could not be transmitted because of errors.

OutQLen: The length of the output packet queue (in packets).

Sample Type

The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

Absolute: Get the sample directly.

Delta: Calculate the difference between samples (default).

Value

The value of the statistic during the last sampling period.

OPTICAL SYSTEMS DESIGN

Startup Alarm

The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

`Rising` Trigger alarm when the first value is larger than the rising threshold.

`Falling` Trigger alarm when the first value is less than the falling threshold.

`RisingOrFalling` Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).

Rising Threshold

Rising threshold value (-2147483648-2147483647).

Rising Index

Rising event index (1-65535).

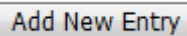
Falling Threshold

Falling threshold value (-2147483648-2147483647)

Falling Index

Falling event index (1-65535).

Buttons



: Click to add a new access management entry.



: Click to save changes.



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

OPTICAL SYSTEMS DESIGN

RMON Event Configuration

[Configuration](#) → [Security](#) → [Switch](#) → [RMON](#) → [Event](#)

RMON Event Configuration

Delete	ID	Desc	Type	Community	Event Last Time
<input type="button" value="Add New Entry"/>	<input type="button" value="Save"/>	<input type="button" value="Reset"/>			

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

Delete

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

ID

Indicates the index of the entry. The range is from 1 to 65535.

Desc

Indicates this event, the string length is from 0 to 127, default is a null string.

Type

Indicates the notification of the event, the possible types are:

none: No SNMP log is created, no SNMP trap is sent.

log: Create SNMP log entry when the event is triggered.

snmptrap: Send SNMP trap when the event is triggered.

logandtrap: Create SNMP log entry and sent SNMP trap when the event is triggered.

Community

Specify the community when trap is sent, the string length is from 0 to 127, default is "public".

Event Last Time

Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons

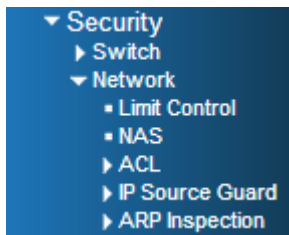
: Click to add a new access management entry.

: Click to save changes.

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

OPTICAL SYSTEMS DESIGN

NETWORK CONFIGURATION



Port Security Limit Control Configuration

Configuration → Security → Network → Limit Control

Port Security Limit Control Configuration

System Configuration

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

Port Configuration

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

Save Reset

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

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

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

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

SYSTEM CONFIGURATION

Mode

Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

Aging Enabled

If checked, secured MAC addresses are subject to aging as discussed under Aging Period.

Aging Period

If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

The Aging Period can be set to a number between 10 and 10,000,000 seconds.

To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured.

When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

PORT CONFIGURATION

The table has one row for each port on the switch and a number of columns, which are:

Port

The port number to which the configuration below applies.

Mode

Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

OPTICAL SYSTEMS DESIGN

Limit

The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

Action

If Limit is reached, the switch can take one of the following actions:

None: Do not allow more than Limit MAC addresses on the port, but take no further action.

Trap: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.

Shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:

- 1) Boot the switch,
- 2) Disable and re-enable Limit Control on the port or the switch,
- 3) Click the Reopen button.

Trap & Shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

State

This column shows the current state of the port as seen from the Limit Control's point of view.

The state takes one of four values:

Disabled: Limit Control is either globally disabled or disabled on the port.

Ready: The limit is not yet reached. This can be shown for all actions.

Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap.


Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.

Re-open Button

If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to *Shutdown* in the Action section.

Note that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.

Buttons

 : Click to save changes.

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

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

OPTICAL SYSTEMS DESIGN

Network Access Server Configuration

Configuration → Security → Network → NAS

Network Access Server Configuration

System Configuration

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

Port Configuration

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

Save Reset

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

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

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

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

SYSTEM CONFIGURATION

Mode

Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.

Reauthentication Enabled

If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).

Reauthentication Period

Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.

EAPOL Timeout

Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.

Aging Period

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.

When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.

If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port 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

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) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.

In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.

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

RADIUS-Assigned QoS Enabled

RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description).

The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

RADIUS-Assigned VLAN Enabled

RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description).

The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

Guest VLAN Enabled

A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

Guest VLAN ID

This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled.

Valid values are in the range [1; 4095].

Max. Reauth. Count

The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled.
Valid values are in the range [1; 255].

Allow Guest VLAN if EAPOL Seen

The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port.
The value can only be changed if the Guest VLAN option is globally enabled.

PORT CONFIGURATION

The table has one row for each port on the switch and a number of columns, which are:

Port

The port number for which the configuration below applies.

Admin State

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

FORCE AUTHORIZED

In this mode, the 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.

PORT-BASED 802.1X

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are

OPTICAL SYSTEMS DESIGN

using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

SINGLE 802.1X

In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant.

Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

MULTI 802.1X

Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.

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

MAC-BASED AUTH.

Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

RADIUS-Assigned QoS Enabled

When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

RADIUS attributes used in identifying a QoS Class:

The `User-Priority-Table` attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

- All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].

RADIUS-Assigned VLAN Enabled

When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the

OPTICAL SYSTEMS DESIGN

meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

RADIUS attributes used in identifying a VLAN ID:

RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

- The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.
- The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):
 - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).
 - Value of Tunnel-Type must be set to "VLAN" (ordinal 13).
 - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

Guest VLAN Enabled

When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.

This option is only available for EAPOL-based modes, i.e.:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

Guest VLAN Operation:

When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

Port State

The current state of the port. It can undertake one of the following values:

Globally Disabled: NAS is globally disabled.

OPTICAL SYSTEMS DESIGN

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.

Buttons

Save

: Click to save changes.

Reset

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

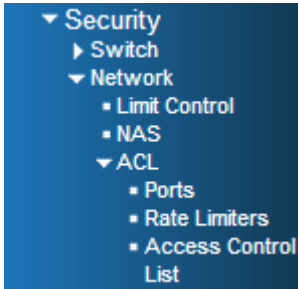
Refresh

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

OPTICAL SYSTEMS DESIGN

ACL Configuration

Configuration → Security → Network → ACL



ACL Port Configuration

Configuration → Security → Network → ACL → Ports

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	0
2	0	Permit	Disabled	Port 3 Port 4 Port 5	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
9	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
11	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
12	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

OPTICAL SYSTEMS DESIGN

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

Port

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

Policy ID

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

Action

Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".

Rate Limiter ID

Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled".

Port Redirect

Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".

Mirror

Specify the mirror operation of this port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored.

The default value is "Disabled".

Logging

Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC. The allowed values are:

Enabled: Frames received on the port are stored in the System Log.

Disabled: Frames received on the port are not logged.

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

Shutdown

Specify the port shut down operation of this port. The allowed values are:

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

Disabled: Port shut down is disabled.

The default value is "Disabled".

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

State

Specify the port state of this port. The allowed values are:

Enabled: To reopen ports by changing the volatile port configuration of the ACL user module.

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


The default value is "Enabled".


Counter

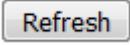
Counts the number of frames that match this ACE.


OPTICAL SYSTEMS DESIGN

Buttons

 : Click to save changes.

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

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

 : Click to clear the counters.

ACL Rate Limiter Configuration

Configuration → Security → Network → ACL → Rate Limiters

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

Configure the rate limiter for the ACL of the switch.

Rate Limiter ID

The rate limiter ID for the settings contained in the same row and its range is 1 to 16.

Rate

The valid rate is 0–35000000 in pps.
or 0, 100, 200, 300, . . . , 10000000 in kbps.

Unit

Specify the rate unit. The allowed values are:
pps: packets per second.
kbps: Kbits per second.

Buttons

: Click to save changes.

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

OPTICAL SYSTEMS DESIGN

Access Control List Configuration

[Configuration](#) → [Security](#) → [Network](#) → [ACL](#) → [Access Control List](#)

Access Control List Configuration

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

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 512 on each switch.

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

ACE

Indicates the ACE ID.

Ingress Port

Indicates the ingress port of the ACE. Possible values are:

All: The ACE will match all ingress port.

Port: The ACE will match a specific ingress port.

Policy / Bitmask

Indicates the policy number and bitmask of the ACE.

Frame Type

Indicates the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

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

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

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

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

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

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

IPv6: The ACE will match all IPv6 standard frames.

Action

Indicates the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Filter: Frames matching the ACE are filtered.

OPTICAL SYSTEMS DESIGN

Rate Limiter

Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When `Disabled` is displayed, the rate limiter operation is disabled.

Port Redirect

Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are `Disabled` or a specific port number. When `Disabled` is displayed, the port redirect operation is disabled.

Mirror

Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:

`Enabled`: Frames received on the port are mirrored.

`Disabled`: Frames received on the port are not mirrored.


The default value is "Disabled".

Counter


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


Modification Buttons


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


: Inserts a new ACE before the current row.

: Edits the ACE row.

: Moves the ACE up the list.

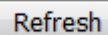
: Moves the ACE down the list.

: Deletes the ACE.

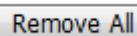
: The lowest plus sign adds a new entry at the bottom of the ACE listings.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

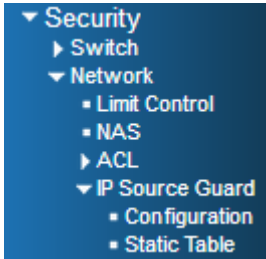
: Click to refresh the page; any changes made locally will be undone.

: Click to clear the counters.

: Click to remove all ACEs.

IP Source Guard Configuration

Configuration → Security → Network → IP Source Guard



IP Source Guard Configuration

Configuration → Security → Network → IP Source Guard → Configuration

IP Source Guard Configuration

Mode

Port Mode Configuration

Port	Mode	Max Dynamic Clients
*	<>	<>
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited
8	Disabled	Unlimited
9	Disabled	Unlimited
10	Disabled	Unlimited
11	Disabled	Unlimited
12	Disabled	Unlimited
13	Disabled	Unlimited
14	Disabled	Unlimited

OPTICAL SYSTEMS DESIGN

This page provides IP Source Guard related configuration.

Mode of IP Source Guard Configuration

Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

Port Mode Configuration

Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

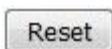
Max Dynamic Clients

Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Buttons



: Click to save changes.



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

OPTICAL SYSTEMS DESIGN

Static IP Source Guard Table

Configuration → Security → Network → IP Source Guard → Static Table

Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC address
--------	------	---------	------------	-------------

Add New Entry

Save

Reset

This page shows the static IP Source Guard rules. The maximum number of rules is 112 on the switch.

Delete

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

Port

The logical port for the settings.

VLAN ID

The vlan id for the settings.

IP Address

Allowed Source IP address.

MAC address

Allowed Source MAC address.

Buttons

Add New Entry

: Click to add a new entry to the Static IP Source Guard table.

Save

: Click to save changes.

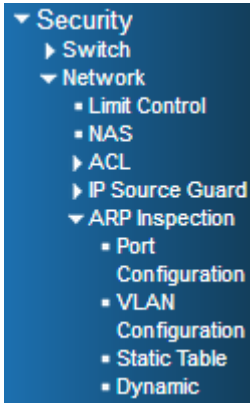
Reset

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

OPTICAL SYSTEMS DESIGN

ARP Inspection Configuration

Configuration → Security → Network → ARP Inspection



ARP Inspection Configuration

Configuration → Security → Network → ARP Inspection → Port Configuration

ARP Inspection Configuration

Mode Disabled ▼

Translate dynamic to static

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
*	<> ▼	<> ▼	<> ▼
1	Disabled ▼	Disabled ▼	None ▼
2	Disabled ▼	Disabled ▼	None ▼
3	Disabled ▼	Disabled ▼	None ▼
4	Disabled ▼	Disabled ▼	None ▼
5	Disabled ▼	Disabled ▼	None ▼
6	Disabled ▼	Disabled ▼	None ▼
7	Disabled ▼	Disabled ▼	None ▼
8	Disabled ▼	Disabled ▼	None ▼
9	Disabled ▼	Disabled ▼	None ▼
10	Disabled ▼	Disabled ▼	None ▼
11	Disabled ▼	Disabled ▼	None ▼
12	Disabled ▼	Disabled ▼	None ▼
13	Disabled ▼	Disabled ▼	None ▼
14	Disabled ▼	Disabled ▼	None ▼

Save Reset

OPTICAL SYSTEMS DESIGN

This page provides ARP Inspection related configuration.

Mode of ARP Inspection Configuration

Enable the Global ARP Inspection or disable the Global ARP Inspection.

Port Mode Configuration

Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:

Enabled: Enable ARP Inspection operation.

Disabled: Disable ARP Inspection operation.

If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are:

Enabled: Enable check VLAN operation.

Disabled: Disable check VLAN operation.

Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

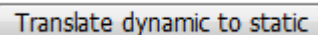
Buttons

 Save

: Click to save changes.

 Reset

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

 Translate dynamic to static

: Click to translate all dynamic entries to static entries.

VLAN Mode Configuration

[Configuration](#) → [Security](#) → [Network](#) → [ARP Inspection](#) → [VLAN Configuration](#)

VLAN Mode Configuration

Start from VLAN with entries per page.

Delete	VLAN ID	Log Type
--------	---------	----------

This page provides ARP Inspection related configuration.

NAVIGATING THE VLAN CONFIGURATION

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

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

Clicking the button will update the displayed table starting from that or the closest next VLAN Table match. The will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the warning message is shown in the displayed table. Use the button to start over.

VLAN Mode Configuration

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

Possible types are:

None: Log nothing.

Deny: Log denied entries.


Permit: Log permitted entries.

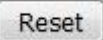
ALL: Log all entries.

OPTICAL SYSTEMS DESIGN

Buttons

 : Click to add a new entry to the Static IP Source Guard table.

 : Click to save changes.

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

Static ARP Inspection Table

Configuration → Security → Network → ARP Inspection → Static Table

Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address
--------	------	---------	-------------	------------

Add New Entry

Save Reset

This page shows the static ARP Inspection rules. The maximum number of rules is 256 on the switch.

Delete

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

Port

The logical port for the settings.

VLAN ID

The vlan id for the settings.

MAC Address

Allowed Source MAC address in ARP request packets.

IP Address

Allowed Source IP address in ARP request packets.

Buttons

Add New Entry : Click to add a new entry to the Static IP Source Guard table.

Save : Click to save changes.

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

OPTICAL SYSTEMS DESIGN

Dynamic ARP Inspection Table

[Configuration](#) → [Security](#) → [Network](#) → [ARP Inspection](#) → [Dynamic Table](#)

Dynamic ARP Inspection Table

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

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

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

NAVIGATING THE ARP INSPECTION TABLE

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

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to

select the starting point in the Dynamic ARP Inspection Table. Clicking the button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition,

the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

ARP INSPECTION TABLE COLUMNS

Port

Switch Port Number for which the entries are displayed.

VLAN ID

VLAN-ID in which the ARP traffic is permitted.

MAC Address

User MAC address of the entry.

OPTICAL SYSTEMS DESIGN

IP Address

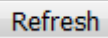
User IP address of the entry.

Translate to static

Select the checkbox to translate the entry to static entry

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

 Refresh

: Refreshes the displayed table starting from the input fields

 Save

: Click to save changes.

 Reset

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

 |<<

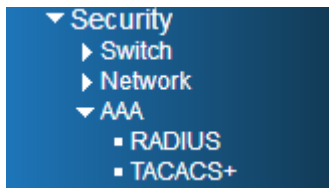
: Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

 >>

: Updates the table, starting with the entry after the last entry currently displayed.

OPTICAL SYSTEMS DESIGN

AAA CONFIGURATION



Configuration → Security → AAA

RADIUS Server Configuration

Configuration → Security → AAA → RADIUS

RADIUS Server Configuration

Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Key	<input type="text"/>	
NAS-IP-Address	<input type="text"/>	
NAS-IPv6-Address	<input type="text"/>	
NAS-Identifier	<input type="text"/>	

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
--------	----------	-----------	-----------	---------	------------	-----

This page allows you to configure the RADIUS servers.

OPTICAL SYSTEMS DESIGN

GLOBAL CONFIGURATION

These settings are common for all of the RADIUS servers.

Timeout

Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.

Retransmit

Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.

Deadtime

Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

Key

The secret key - up to 63 characters long - shared between the RADIUS server and the switch.

NAS-IP-Address (Attribute 4)

The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS-IPv6-Address (Attribute 95)

The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS-Identifier (Attribute 32)

The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

SERVER CONFIGURATION

The table has one row for each RADIUS server and a number of columns, which are:

Delete

To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.

Hostname

The IP address or hostname of the RADIUS server.

Auth Port

The UDP port to use on the RADIUS server for authentication. Set to 0 to disable authentication.

Acct Port

The UDP port to use on the RADIUS server for accounting. Set to 0 to disable accounting.

OPTICAL SYSTEMS DESIGN

Timeout

This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.


Retransmit

This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.

Key

This optional setting overrides the global key. Leaving it blank will use the global key.

ADDING A NEW SERVER

Click  to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported. The delete button can be used to undo the addition of the new server.

Buttons



: Click to add a new RADIUS server.



: Click to save changes.



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

TACACS+ Server Configuration

[Configuration](#) → [Security](#) → [AAA](#) → [TACACS+](#)

TACACS+ Server Configuration

Global Configuration

Timeout	5	seconds
Deadtime	0	minutes
Key	<input type="text"/>	

Server Configuration

Delete	Hostname	Port	Timeout	Key
--------	----------	------	---------	-----

This page allows you to configure the TACACS+ servers.

GLOBAL CONFIGURATION

These settings are common for all of the TACACS+ servers.

Timeout

Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.

Deadtime

Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

Key

The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

OPTICAL SYSTEMS DESIGN

SERVER CONFIGURATION

The table has one row for each TACACS+ server and a number of columns, which are:

Delete

To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.

Hostname

The IP address or hostname of the TACACS+ server.

Port

The TCP port to use on the TACACS+ server for authentication.


Timeout

This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Key

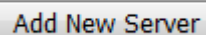
This optional setting overrides the global key. Leaving it blank will use the global key.

ADDING A NEW SERVER

Click  to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported.

The delete button can be used to undo the addition of the new server.

Buttons



: Click to add a new RADIUS server.



: Click to save changes.



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

AGGREGATION

- ▼ Aggregation
 - Static
 - LACP

AGGREGATION MODE AND GROUP CONFIGURATION

Configuration → Aggregation → Static

Aggregation Mode Configuration

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

Aggregation Group Configuration

Group ID	Port Members													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Normal	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Save Reset

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

HASH CODE CONTRIBUTORS

Source MAC Address

The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.

OPTICAL SYSTEMS DESIGN

Destination MAC Address

The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.

IP Address

The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.

TCP/UDP Port Number

The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.

AGGREGATION GROUP CONFIGURATION


Group ID

Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.

Port Members

Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

Buttons

 : Click to save changes.

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

OPTICAL SYSTEMS DESIGN

LACP PORT CONFIGURATION

Configuration → Aggregation → LACP

LACP Port Configuration

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

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

Port

The switch port number.

LACP Enabled

Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner.

OPTICAL SYSTEMS DESIGN

Key

The `Key` value incurred by the port, range 1-65535. The `Auto` setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the `Specific` setting, a user-defined value can be entered. Ports with the same `Key` value can participate in the same aggregation group, while ports with different keys cannot.

Role

The `Role` shows the LACP activity status. The `Active` will transmit LACP packets each second, while `Passive` will wait for a LACP packet from a partner (speak if spoken to).

Timeout

The `Timeout` controls the period between BPDU transmissions. `Fast` will transmit LACP packets each second, while `Slow` will wait for 30 seconds before sending a LACP packet.

Prio

The `Prio` controls the priority of the port, range 1-65535. 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.

Buttons

A rectangular button with rounded corners and a light gray background, containing the word "Save" in a dark gray font.

: Click to save changes.

A rectangular button with rounded corners and a light gray background, containing the word "Reset" in a dark gray font.

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

OPTICAL SYSTEMS DESIGN

LINK OAM CONFIGURATION

- ▼ Link OAM
 - Port Settings
 - Event Settings

PORT SETTINGS

Configuration → Link OAM → Port Settings

Link OAM Port Configuration

Port	OAM Enabled	OAM Mode	Loopback Support	Link Monitor Support	MIB Retrieval Support	Loopback Operation
*	<input type="checkbox"/>	<>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

This page allows the user to inspect the current Link OAM port configurations, and change them as well.

Port

The switch port number.

OAM Enabled

Controls whether Link OAM is enabled on this switch port. Enabling Link OAM provides the network operators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions.

OAM Mode

Configures the OAM Mode as Active or Passive. The default mode is Passive.

ACTIVE MODE

DTE's configured in Active mode initiate the exchange of Information OAMPDUs as defined by the Discovery process. Once the Discovery process completes, Active DTE's are permitted to send any OAMPDU while connected to a remote OAM peer entity in Active mode. Active DTE's operate in a limited respect if the remote OAM entity is operating in Passive mode. Active devices should not respond to OAM remote loopback commands and variable requests from a Passive peer.

PASSIVE MODE

DTE's configured in Passive mode do not initiate the Discovery process. Passive DTE's react to the initiation of the Discovery process by the remote DTE. This eliminates the possibility of passive to passive links. Passive DTE's shall not send Variable Request or Loopback Control OAMPDU's.

Loopback Support

Controls whether the loopback support is enabled for the switch port. Link OAM remote loopback can be used for fault localization and link performance testing. Enabling the loopback support will allow the DTE to execute the remote loopback command that helps in the fault detection.

Link Monitor Support

Controls whether the Link Monitor support is enabled for the switch port. On enabling the Link Monitor support, the DTE supports event notification that permits the inclusion of diagnostic information.


MIB Retrieval Support


Controls whether the MIB Retrieval Support is enabled for the switch port. On enabling the MIB retrieval support, the DTE supports polling of various Link OAM based MIB variables' contents.

Loopback Operation

If the Loopback support is enabled, enabling this field will start a loopback operation for the port.

Buttons

 : Click to save changes.

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

OPTICAL SYSTEMS DESIGN

LINK EVENT CONFIGURATION

Configuration → Link OAM → Event Settings

Link Event Configuration for Port 1

Port 1 ▼

Event Name	Error Window	Error Threshold
Error Frame Event	1	1
Symbol Period Error Event	1	1
Seconds Summary Event	60	1

Save

Reset

This page allows the user to inspect the current Link OAM Link Event configurations, and change them as well.

Port

The switch port number.

Event Name

Name of the Link Event which is being configured.

Error Window

Represents the window period in the order of 1 sec for the observation of various link events.

Error Threshold

Represents the threshold value for the window period for the appropriate Link event so as to notify the peer of this error.

Error Frame Event

The Errored Frame Event counts the number of errored frames detected during the specified period. The period is specified by a time interval (Window in order of 1 sec). This event is generated if the errored frame count is equal to or greater than the specified threshold for that period (Period Threshold). Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Error Frame Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-4294967295 and its default value is '0'.

Symbol Period Error Event


The Errored Symbol Period Event counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period. Error Window for 'Symbol Period Error Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-4294967295 and its default value is '0'.

OPTICAL SYSTEMS DESIGN

Seconds Summary Event

The Errored Frame Seconds Summary Event TLV counts the number of errored frame seconds that occurred during the specified period. The period is specified by a time interval. This event is generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period. An errored frame second is a one second interval wherein at least one frame error was detected. Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Seconds Summary Event' must be an integer value between 10-900 and its default value is '60'. Whereas Error Threshold must be between 0-65535 and its default value is '1'.

Buttons

 : Click to save changes.

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

LOOP PROTECTION

Configuration → *Loop Protection*

Loop Protection Configuration

General Settings

Global Configuration

Enable Loop Protection	Disable ▾
Transmission Time	5 seconds
Shutdown Time	180 seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	<input checked="" type="checkbox"/>	<> ▾	<> ▾
1	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
2	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
3	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
4	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
5	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
6	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
7	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
8	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
9	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
10	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
11	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
12	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
13	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
14	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾

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

OPTICAL SYSTEMS DESIGN

General Settings

Enable Loop Protection

Controls whether loop protections is enabled (as a whole).

Transmission Time

The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds. Default value is 5 seconds.

Shutdown Time

The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart). Default value is 180 seconds.

Port Configuration

Port

The switch port number of the port.

Enable

Controls whether loop protection is enabled on this switch port.

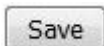
Action

Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log or Log Only.

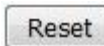
Tx Mode

Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

Buttons



: Click to save changes.



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

SPANNING TREE

- ▼ Spanning Tree
 - Bridge Settings
 - MSTI Mapping
 - MSTI Priorities
 - CIST Ports
 - MSTI Ports

STP BRIDGE CONFIGURATION

Configuration → *Spanning Tree* → *Bridge Settings*

STP Bridge Configuration

Basic Settings

Protocol Version	MSTP ▼
Bridge Priority	128 ▼
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	<input style="width: 100%;" type="text"/>

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

Basic Settings

Protocol Version

The MSTP / RSTP / STP protocol version setting. Valid values are STP, RSTP and MSTP.

Bridge Priority

Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a *Bridge Identifier*.

For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

Hello Time

The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds, default is 2 seconds.

Note: Changing this parameter from the default value is not recommended, and may have adverse effects on your network.

Forward Delay

The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Max Age

The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, *and* MaxAge must be $\leq (\text{FwdDelay}-1)*2$.

Maximum Hop Count

This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Transmit Hold Count

The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Advanced Settings

Edge Port BPDU Filtering

Control whether a port *explicitly* configured as Edge will transmit and receive BPDUs.

Edge Port BPDU Guard

Control whether a port *explicitly* configured as Edge will disable itself upon reception of a BPDU. The port will enter the *error-disabled* state, and will be removed from the active topology.

Port Error Recovery


Control whether a port in the *error-disabled* state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.


Port Error Recovery Timeout

The time to pass before a port in the *error-disabled* state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

OPTICAL SYSTEMS DESIGN

Buttons

 : Click to save changes.

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

OPTICAL SYSTEMS DESIGN

MSTI CONFIGURATION

Configuration → Spanning Tree → MSTI Mapping

MSTI Configuration

Add VLANs separated by spaces or comma.

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

Configuration Identification

Configuration Name	00-26-dc-00-07-61
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

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

Configuration Identification

Configuration Name

The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

OPTICAL SYSTEMS DESIGN

Configuration Revision

The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping


MSTI

The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

VLANs Mapped

The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to *one* MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Example: 2, 5, 20-40.

Buttons

 : Click to save changes.

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

MSTI PRIORITY CONFIGURATION

Configuration → Spanning Tree → MSTI Priorities

MSTI Configuration

MSTI Priority Configuration

MSTI	Priority
*	<> ▼
CIST	128 ▼
MSTI1	128 ▼
MSTI2	128 ▼
MSTI3	128 ▼
MSTI4	128 ▼
MSTI5	128 ▼
MSTI6	128 ▼
MSTI7	128 ▼

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

MSTI

The bridge instance. The CIST is the *default* instance, which is always active.

Priority

Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a *Bridge Identifier*.

Buttons

: Click to save changes.

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

OPTICAL SYSTEMS DESIGN

STP CIST PORT CONFIGURATION

Configuration → Spanning Tree → CIST 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		
-	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True

CIST Normal Port Configuration

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

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

This page contains settings for physical and aggregated ports.

Port

The switch port number of the logical STP port.

STP Enabled

Controls whether STP is enabled on this switch port.

Path Cost

Controls the path cost incurred by the port. The `Auto` setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the `Specific` setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority

Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

OPTICAL SYSTEMS DESIGN

operEdge (state flag)

Operational flag describing whether the port is connecting directly to edge devices. (*No Bridges attached*). Transition to the forwarding state is faster for edge ports (having *operEdge true*) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.

AdminEdge

Controls whether the *operEdge* flag should start as set or cleared. (The initial *operEdge* state when a port is initialized).

AutoEdge

Controls whether the bridge should enable automatic edge detection on the bridge port. This allows *operEdge* to be derived from whether BPDU's are received on the port or not.

Restricted Role

If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as **Root Guard**.

Restricted TCN

If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard


If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting.

A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

Point-to-Point

Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

 : Click to save changes.

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

MSTI PORT CONFIGURATION

[Configuration](#) → [Spanning Tree](#) → [MSTI Ports](#)

MSTI Port Configuration



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

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

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

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

Port

The switch port number of the corresponding STP CIST (and MSTI) port.


Path Cost

Controls the path cost incurred by the port. The `Auto` setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the `Specific` setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.


Priority

Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

Buttons

 : Click to retrieve settings for a specific MSTI.

 : Click to save changes.

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

IPMC PROFILE CONFIGURATIONS

- ▼ IPMC Profile
 - Profile Table
 - Address Entry

IPMC PROFILE TABLE SETTING

[Configurations](#) → [IPMC Profile](#) → [Profile Table](#)

IPMC Profile Configurations

Global Profile Mode

IPMC Profile Table Setting

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

This page provides IPMC Profile related configurations.

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

Global Profile Mode

Enable/Disable the Global IPMC Profile.

System starts to do filtering based on profile settings only when the global profile mode is enabled.

Delete

Check to delete the entry.

The designated entry will be deleted during the next save.

Profile Name

The name used for indexing the profile table.

Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.

OPTICAL SYSTEMS DESIGN


Profile Description


Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile.

No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.

Rule


When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons:

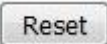
: List the rules associated with the designated profile.

: Adjust the rules associated with the designated profile.

Buttons

: Click to add new IPMC profile. Specify the name and configure the new entry. Click "Save".

: Click to save changes.

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

OPTICAL SYSTEMS DESIGN

IPMC PROFILE ADDRESS CONFIGURATION

[Configurations](#) → [IPMC Profile](#) → [Address Entry](#)

IPMC Profile Address Configuration

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

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

This page provides address range settings used in IPMC profile.

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

Delete

Check to delete the entry.
The designated entry will be deleted during the next save.

Entry Name

The name used for indexing the address entry table.
Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.

Start Address

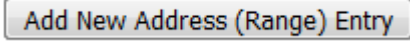
The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.


End Address

The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

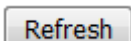
OPTICAL SYSTEMS DESIGN


Buttons


 : Click to add new address range. Specify the name and configure the addresses. Click "Save"

 : Click to save changes.

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

 : Refreshes the displayed table starting from the input fields.

 : Updates the table starting from the first entry in the IPMC Profile Address Configuration.

 : Updates the table, starting with the entry after the last entry currently displayed.

OPTICAL SYSTEMS DESIGN

MVR CONFIGURATIONS

• MVR

MVR CONFIGURATIONS

Configurations → MVR

MVR Configurations

MVR Mode Disabled ▾

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

Delete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile
--------	---------	----------	--------------	------	---------	----------	------	---------------------------

Add New MVR VLAN

Immediate Leave Setting

Port	Immediate Leave
*	<> ▾
1	Disabled ▾
2	Disabled ▾
3	Disabled ▾
4	Disabled ▾
5	Disabled ▾
6	Disabled ▾
7	Disabled ▾
8	Disabled ▾
9	Disabled ▾
10	Disabled ▾
11	Disabled ▾
12	Disabled ▾
13	Disabled ▾
14	Disabled ▾

Save Reset

This page provides MVR related configurations.

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

OPTICAL SYSTEMS DESIGN

It is allowed to create at maximum 4 MVR VLANs with corresponding channel profile for each Multicast VLAN.

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

MVR Mode

Enable/Disable the Global MVR.

The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping.

It is suggested to enable Unregistered Flooding control when the MVR group table is full.

Delete

Check to delete the entry. The designated entry will be deleted during the next save.

MVR VID

Specify the Multicast VLAN ID.

Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

MVR Name

MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 16. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.

IGMP Address

Define the IPv4 address as source address used in IP header for IGMP control frames.

The default IGMP address is not set (0.0.0.0).

When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.

When the IPv4 management address is not set, system uses the first available IPv4 management address.

Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

Mode

Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.

Tagging

Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.

Priority

Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.

OPTICAL SYSTEMS DESIGN

LLQI


Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.

Interface Channel Profile

When the MVR VLAN is created, select the IPMC Profile as the channel filtering condition for the specific MVR VLAN. Summary about the Interface Channel Profiling (of the MVR VLAN) will be shown by clicking the view button. Profile selected for designated interface channel is not allowed to have overlapped permit group address.

Profile Management Button

You can inspect the rules of the designated profile by using the following button:

: List the rules associated with the designated profile.

Port

The logical port for the settings.

Port Role

Configure an MVR port of the designated MVR VLAN as one of the following roles.

Inactive: The designated port does not participate MVR operations.

Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.

Receiver: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.

Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

Select the port role by clicking the Role symbol to switch the setting.

I indicates Inactive; S indicates Source; R indicates Receiver


The default Role is Inactive.


Immediate Leave

Enable the fast leave on the port.

Buttons

: Click to add new MVR VLAN. Specify the VID and configure the new entry. Click "Save".

: Click to save changes.

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

IPMC

- ▼ IPMC
 - ▼ IGMP Snooping
 - Basic Configuration
 - VLAN Configuration
 - Port Filtering Profile
 - ▼ MLD Snooping
 - Basic Configuration
 - VLAN Configuration
 - Port Filtering Profile

IGMP SNOOPING

Basic Configuration

Configuration → IPMC → IGMP Snooping → Basic Configuration

IGMP Snooping Configuration

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

Port Related Configuration

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

This page provides IGMP Snooping related configuration.

Snooping Enabled

Enable the Global IGMP Snooping.

Unregistered IPMCv4 Flooding Enabled

Enable unregistered IPMCv4 traffic flooding.

The flooding control takes effect only when IGMP Snooping is enabled.

When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.

OPTICAL SYSTEMS DESIGN

IGMP SSM Range

SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

Assign valid IPv4 multicast address as prefix with a prefix length (from 4 to 32) for the range.

Leave Proxy Enabled

Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled

Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Router Port

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave

Enable the fast leave on the port.

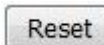
Throttling

Enable to limit the number of multicast groups to which a switch port can belong.

Buttons



: Click to save changes.



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

VLAN Configuration

Configuration → IPMC → IGMP Snooping → VLAN Configuration

IGMP Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
--------	---------	------------------	------------------	-----------------	---------------	-----	----	----------	---------------	----------------	-----------

Add New IGMP VLAN

Save Reset

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 >> 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 << button to start over.

IGMP SNOOPING VLAN TABLE COLUMNS

Delete

Check to delete the entry. The designated entry will be deleted during the next save.

VLAN ID

The VLAN ID of the entry.

IGMP Snooping Enabled

Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.

Querier Election

Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

Querier Address

Define the IPv4 address as source address used in IP header for IGMP Querier election.

When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.

When the IPv4 management address is not set, system uses the first available IPv4 management address.

Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

OPTICAL SYSTEMS DESIGN

Compatibility

Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network.

The allowed selection is `IGMP-Auto`, `Forced IGMPv1`, `Forced IGMPv2`, `Forced IGMPv3`, default compatibility value is `IGMP-Auto`.

PRI

Priority of Interface.

It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.

The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.

RV

Robustness Variable.

The Robustness Variable allows tuning for the expected packet loss on a network.

The allowed range is 1 to 255, default robustness variable value is 2.

QI

Query Interval.

The Query Interval is the interval between General Queries sent by the Querier.

The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.

QRI

Query Response Interval.

The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.

The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP)

Last Member Query Interval.

The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count.

The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).


URI


Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group.

The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

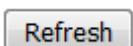
OPTICAL SYSTEMS DESIGN


Buttons


 : Click to add new IGMP VLAN. Specify the VID and configure the new entry. Click "Save". The specific IGMP VLAN starts working after the corresponding static VLAN is also created.

 : Click to save changes.

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

 : Refreshes the displayed table starting from the input fields.















 : Updates the table starting from the first entry in the IPMC Profile Address Configuration.

 : Updates the table, starting with the entry after the last entry currently displayed.

IGMP Snooping Port Filtering Profile Configuration

Configuration → IPMC → IGMP Snooping → Port Filtering Profile

IGMP Snooping Port Filtering Profile Configuration

Port	Filtering Profile
1	 - ▼
2	 - ▼
3	 - ▼
4	 - ▼
5	 - ▼
6	 - ▼
7	 - ▼
8	 - ▼
9	 - ▼
10	 - ▼
11	 - ▼
12	 - ▼
13	 - ▼
14	 - ▼

Port


The logical port for the settings.

Filtering Profile

Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

Profile Management Button

You can inspect the rules of the designated profile by using the following button:

: List the rules associated with the designated profile.

Buttons

: Click to save changes.

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

MLD SNOOPING

MLD Snooping Configuration

Configuration → IPMC → MLD Snooping → Basic Configuration

MLD Snooping Configuration

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

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<> ▾
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
11	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
12	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
13	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
14	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾

Save Reset

This page provides MLD Snooping related configuration.

Snooping Enabled

Enable the Global MLD Snooping.

OPTICAL SYSTEMS DESIGN

Unregistered IPMCv6 Flooding Enabled

Enable unregistered IPMCv6 traffic flooding.

The flooding control takes effect only when MLD Snooping is enabled.

When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

MLD SSM Range

SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

Assign valid IPv6 multicast address as prefix with a prefix length (from 8 to 128) for the range.

Leave Proxy Enabled

Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled

Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Router Port

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave

Enable the fast leave on the port.

Throttling

Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

 Save

: Click to save changes.

 Reset

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

OPTICAL SYSTEMS DESIGN

MLD Snooping VLAN Configuration

Configuration → IPMC → MLD Snooping → VLAN Configuration

MLD Snooping VLAN Configuration

Start from VLAN with entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
--------	---------	------------------	------------------	---------------	-----	----	----------	---------------	----------------	-----------

NAVIGATING THE MLD 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 button will update the displayed table starting from that or the next closest VLAN Table match. The 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 button to start over.

MLD SNOOPING VLAN TABLE COLUMNS

Delete

Check to delete the entry. The designated entry will be deleted during the next save.

VLAN ID

The VLAN ID of the entry.

MLD Snooping Enabled

Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.

Querier Election

Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.

Compatibility

Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network.

The allowed selection is MLD-Auto, Forced MLDv1, Forced MLDv2, default compatibility value is MLD-Auto.

PRI

Priority of Interface.

It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.

The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.

OPTICAL SYSTEMS DESIGN

RV

Robustness Variable.

The Robustness Variable allows tuning for the expected packet loss on a link.

The allowed range is 1 to 255, default robustness variable value is 2.

QI

Query Interval.

The Query Interval is the interval between General Queries sent by the Querier.

The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.

QRI

Query Response Interval.

The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.

The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).

LLQI

Last Listener Query Interval.

The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages.

The allowed range is 0 to 31744 in tenths of seconds, default last listener query interval is 10 in tenths of seconds (1 second).


URI

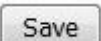
Unsolicited Report Interval.

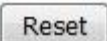
The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address.

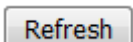
The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.


Buttons


 : Click to add new MLD VLAN. Specify the VID and configure the new entry. Click "Save". The specific MLD VLAN starts working after the corresponding static VLAN is also created.

 : Click to save changes.

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

 : Refreshes the displayed table starting from the input fields.















 : Updates the table starting from the first entry in the IPMC Profile Address Configuration.

 : Updates the table, starting with the entry after the last entry currently displayed.

MLD Snooping Port Filtering Profile Configuration

Configuration → IPMC → MLD Snooping → Port Filtering Profile

MLD Snooping Port Filtering Profile Configuration

Port	Filtering Profile
1	 - ▼
2	 - ▼
3	 - ▼
4	 - ▼
5	 - ▼
6	 - ▼
7	 - ▼
8	 - ▼
9	 - ▼
10	 - ▼
11	 - ▼
12	 - ▼
13	 - ▼
14	 - ▼

Port


The logical port for the settings.

Filtering Profile

Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

Profile Management Button

You can inspect the rules of the designated profile by using the following button:

: List the rules associated with the designated profile.

Buttons

: Click to save changes.

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

OPTICAL SYSTEMS DESIGN

LLDP

- ▼ LLDP
 - LLDP
 - LLDP-MED

LLDP CONFIGURATION

Configuration → LLDP

LLDP Configuration

LLDP Parameters

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

LLDP Interface Configuration

Interface	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/1	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/2	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/3	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/4	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/5	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/6	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/7	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/8	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/9	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/10	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/11	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/12	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/13	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2.5GigabitEthernet 1/1	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

This page allows the user to inspect and configure the current LLDP interface settings.

LLDP PARAMETERS

Tx Interval

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

Tx Hold

Each LLDP frame contains information about how long time the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to **Tx Hold** multiplied by **Tx Interval** seconds. Valid values are restricted to 2 - 10 times.

Tx Delay

If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Tx Delay** seconds. **Tx Delay** cannot be larger than 1/4 of the **Tx Interval** value. Valid values are restricted to 1 - 8192 seconds.

Tx Reinit

When an interface is disabled, LLDP is disabled or the switch is rebooted, a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. **Tx Reinit** controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP INTERFACE CONFIGURATION

Interface

The switch interface name of the logical LLDP interface.

Mode

Select 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.

CDP Aware

Select CDP awareness.

The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the interface is enabled.

Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.

CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.

CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table.

CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.

OPTICAL SYSTEMS DESIGN

CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field. Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.

If all interfaces have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one interface has CDP awareness enabled all CDP frames are terminated by the switch.

Note: When CDP awareness on an interface is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.

Port Descr

Optional TLV: When checked the "port description" is included in LLDP information transmitted.

Sys Name

Optional TLV: When checked the "system name" is included in LLDP information transmitted.

Sys Descr

Optional TLV: When checked the "system description" is included in LLDP information transmitted.


Sys Capa

Optional TLV: When checked the "system capability" is included in LLDP information transmitted.

Mgmt Addr

Optional TLV: When checked the "management address" is included in LLDP information transmitted.

Buttons

 : Click to save changes.

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

OPTICAL SYSTEMS DESIGN

LLDP-MED CONFIGURATION

Configuration → LLDP-MED

LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count

Transmit TLVs

Interface	Capabilities	Policies	Location	PoE
-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/12	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/13	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2.5GigabitEthernet 1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Coordinates Location

Latitude * North Longitude * East Altitude Meters Map Datum

Civic Address Location

Country code	<input type="text"/>	State	<input type="text"/>	County	<input type="text"/>
City	<input type="text"/>	City district	<input type="text"/>	Block (Neighborhood)	<input type="text"/>
Street	<input type="text"/>	Leading street direction	<input type="text"/>	Trailing street suffix	<input type="text"/>
Street suffix	<input type="text"/>	House no.	<input type="text"/>	House no. suffix	<input type="text"/>
Landmark	<input type="text"/>	Additional location info	<input type="text"/>	Name	<input type="text"/>
Zip code	<input type="text"/>	Building	<input type="text"/>	Apartment	<input type="text"/>
Floor	<input type="text"/>	Room no.	<input type="text"/>	Place type	<input type="text"/>
Postal community name	<input type="text"/>	P.O. Box	<input type="text"/>	Additional code	<input type="text"/>

Emergency Call Service

Emergency Call Service

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
No entries present						

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

FAST START REPEAT COUNT

Fast start repeat count

Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPDU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated interface. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbour has been detected in order share LLDP-MED information as fast as possible to new neighbours.

Because there is a risk of an LLDP frame being lost during transmission between neighbours, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbours receiving the LLDP frame. With **Fast start repeat count** it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.

It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

TRANSMIT TLVS

It is possible to select which LLDP-MED information that shall be transmitted to the neighbors. When the checkbox is checked the information is included in the frame transmitted to the neighbor.

Interface

The interface name to which the configuration applies.

Capabilities

When checked the switch's capabilities is included in LLDP-MED information transmitted.

Policies

When checked the configured policies for the interface is included in LLDP-MED information transmitted.

OPTICAL SYSTEMS DESIGN

Location

When checked the configured location information for the switch is included in LLDP-MED information transmitted.

PoE

When checked the configured PoE (Power Over Ethernet) information for the interface is included in LLDP-MED information transmitted.

COORDINATES LOCATION

Latitude

Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits.

It is possible to specify the direction to either **North** of the equator or **South** of the equator.

Longitude

Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits.

It is possible to specify the direction to either **East** of the prime meridian or **West** of the prime meridian.

Altitude

Altitude SHOULD be normalized to within -2097151.9 to 2097151.9 with a maximum of 1 digits.

It is possible to select between two altitude types (floors or meters).

Meters: Representing meters of Altitude defined by the vertical datum specified.

Floors: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

Map Datum

The **Map Datum** is used for the coordinates given in these options:

WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.

NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).

NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

CIVIC ADDRESS LOCATION

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). The total number of characters for the combined civic address information must not exceed 250 characters.

A couple of notes to the limitation of 250 characters.

- 1) A non empty civic address location will use 2 extra characters in addition to the civic address location text.
- 2) The 2 letter country code is not part of the 250 characters limitation.

Country code

The two-letter ISO 3166 country code in capital ASCII letters - Example: AU, DE or US.

State

National subdivisions (state, region, province, prefecture).

County

County, parish, gun (Japan), district.

City

City, township, shi (Japan) - Example: Sydney.

City district

City division, borough, city district, ward, chou (Japan).

Block (Neighborhood)

Neighbourhood, block.

Street

Street - Example: Vuko.

Leading street direction

Leading street direction - Example: N.

Trailing street suffix

Trailing street suffix - Example: SW.

Street suffix

Street suffix - Example: Ave, Pl.

House no.

House number - Example: 21.

House no. suffix

House number suffix - Example: A, 7/1.

Landmark

Landmark or vanity address - Example: University of Sydney.

OPTICAL SYSTEMS DESIGN

Additional location info

Additional location info - Example: South Wing.

Name

Name (residence and office occupant) - Example: Smith John.

Zip code

Postal/zip code - Example: 2102.

Building

Building (structure) - Example: Low Library.

Apartment

Unit (Apartment, suite) - Example: Apt 42.

Floor

Floor - Example: 4.

Room no.

Room number - Example: 450F.

Place type

Place type - Example: Office.

Postal community name

Postal community name - Example: Lucas.

P.O. Box

Post office box (P.O. BOX) - Example: 12345.

Additional code

Additional code - Example: 1320300003.

EMERGENCY CALL SERVICE

Emergency Call Service (e.g. 000, 911 and others), such as defined by TIA or NENA.

Emergency Call Service

Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

OPTICAL SYSTEMS DESIGN

POLICIES

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signalling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Delete

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

Policy ID

ID for the policy. This is auto generated and shall be used when selecting the policies that shall be mapped to the specific interfaces.

OPTICAL SYSTEMS DESIGN

Application Type

Intended use of the application types:

1. **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. **Voice Signalling** (conditional) - for use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the **Voice** application policy.
3. **Guest Voice** - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
4. **Guest Voice Signalling** (conditional) - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the **Guest Voice** application policy.
5. **Softphone Voice** - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.
6. **Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. **Streaming Video** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. **Video Signalling** (conditional) - for use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the **Video Conferencing** application policy.

Tag

Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN.

Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.

Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.

VLAN ID

VLAN identifier (VID) for the interface as defined in IEEE 802.1Q-2003.

OPTICAL SYSTEMS DESIGN


L2 Priority

L2 Priority is the Layer 2 priority to be used for the specified application type. **L2 Priority** may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.

DSCP

DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. **DSCP** may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

Adding a new policy

Click  to add a new policy. Specify the **Application type**, **Tag**, **VLAN ID**, **L2 Priority** and **DSCP** for the new policy. Click "Save".

The number of policies supported is 32

POLICIES INTERFACE CONFIGURATION

Every interface may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or interface configuration.

Interface


The interface name to which the configuration applies.

Policy Id

The set of policies that shall apply to a given interface. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

Buttons

 : Click to add new Policy

 : Click to save changes.

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

MAC ADDRESS TABLE CONFIGURATION

MAC Table

Configuration → MAC Table

MAC Address Table Configuration

Aging Configuration

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

MAC Table Learning

	Port Members													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Auto	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Disable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Static MAC Table Configuration

			Port Members													
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14

Add New Static Entry

Save Reset

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

AGING CONFIGURATION

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds; for example, Age time seconds. The allowed range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by checking **Disable automatic aging.**

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:

Auto

Learning is done automatically as soon as a frame with unknown SMAC is received.

Disable

No learning is done.

Secure

Only static MAC entries are learned, all other frames are dropped.

Note: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

STATIC MAC TABLE CONFIGURATION

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The MAC table is sorted first by VLAN ID and then by MAC address.

Delete

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

VLAN ID

The VLAN ID of the entry.

MAC Address

The MAC address of the entry.

Port Members

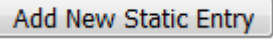
Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.


Adding a New Static Entry

Click 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".


OPTICAL SYSTEMS DESIGN

Buttons

 : Click to add a new entry to the static MAC table.

 : Click to save changes.

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

 : Refreshes the displayed table starting from the input fields.

OPTICAL SYSTEMS DESIGN

GLOBAL VLAN CONFIGURATION

VLANs

Configuration → VLANs

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	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
11	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
12	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
13	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
14	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Save Reset

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

GLOBAL VLAN CONFIGURATION

Allowed Access VLANs

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

The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1, 10-13, 200, 300. Spaces are allowed in between the delimiters.

Ethertype for Custom S-ports

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

OPTICAL SYSTEMS DESIGN

PORT VLAN CONFIGURATION

Port

This is the logical port number of this row.

Mode

The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below.

Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question.

Grayed out fields show the value that the port will get when the mode is applied.

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 not classified to the Access VLAN
- On egress all frames are transmitted untagged

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 member of all VLANs (1-4095)
- The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs
- Frames classified to a VLAN that the port is not a member of are discarded
- By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress
- Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress

Hybrid:

Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:

- Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware
- Ingress filtering can be controlled
- Ingress acceptance of frames and configuration of egress tagging can be configured independently

Port VLAN

Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1.

On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).

On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.

The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.

Port Type

Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.

Unaware:

On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.

C-Port:

On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag.

If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN.

If frames must be tagged on egress, they will be tagged with a C-tag.

S-Port:

On egress, if frames must be tagged, they will be tagged with an S-tag.

On ingress, frames with a VLAN tag with TPID = 0x88A8 get classified to the VLAN ID embedded in the tag.

Priority-tagged frames are classified to the Port VLAN.

If the port is configured to accept **Tagged Only** frames (see Ingress Acceptance below), frames without this TPID are dropped.

Notice:

*If the S-port is configured to accept **Tagged and Untagged** frames (see Ingress Acceptance below), frames with a C-tag are treated like frames with an S-tag.*

*If the S-port is configured to accept **Untagged Only** frames, S-tagged frames will be discarded (except for priority S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID.*

S-Custom-Port:

On egress, if frames must be tagged, they will be tagged with the custom S-tag.

On ingress, frames with a VLAN tag with a TPID equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag.

Priority-tagged frames are classified to the Port VLAN.

If the port is configured to accept **Tagged Only** frames (see Ingress Acceptance below), frames without this TPID are dropped.

Notice:

If the custom S-port is configured to accept **Tagged and Untagged** frames (see Ingress Acceptance below), frames with a C-tag are treated like frames with a custom S-tag.

If the Custom S-port is configured to accept **Untagged Only** frames, custom S-tagged frames will be discarded (except for priority custom S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID.

Ingress Filtering

Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.

If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.

If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.

Ingress Acceptance

Hybrid ports allow for changing the type of frames that are accepted on ingress.

Tagged and Untagged

Both tagged and untagged frames are accepted. See Port Type for a description of when a frame is considered tagged.

Tagged Only

Only frames tagged with the corresponding Port Type tag are accepted on ingress.

Untagged Only

Only untagged frames are accepted on ingress. See Port Type for a description of when a frame is considered untagged.

Egress Tagging

Ports in Trunk and Hybrid mode may control the tagging of frames on egress.

Untag Port VLAN

Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.

Tag All

All frames, whether classified to the Port VLAN or not, are transmitted with a tag.

Untag All

All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.

Allowed VLANs

Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN.

The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to 1-4095.

The field may be left empty, which means that the port will not become member of any VLANs.

OPTICAL SYSTEMS DESIGN

Forbidden VLANs

A port may be configured to never become member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs.

The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field.

By default, the field is left blank, which means that the port may become a member of all possible VLANs.

Buttons

 Save

: Click to save changes.

 Reset

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

VLAN TRANSLATION

- ▼ VLAN Translation
 - Port to Group Configuration
 - VLAN Translation Mappings

VLAN TRANSLATION PORT CONFIGURATION

Configuration → VLAN Translation → Port to Group Configuration

VLAN Translation Port Configuration

Port	Group Configuration	
	Default	Group ID
*	<input type="checkbox"/>	<> ▼
1	<input type="checkbox"/>	1 ▼
2	<input type="checkbox"/>	2 ▼
3	<input type="checkbox"/>	3 ▼
4	<input type="checkbox"/>	4 ▼
5	<input type="checkbox"/>	5 ▼
6	<input type="checkbox"/>	6 ▼
7	<input type="checkbox"/>	7 ▼
8	<input type="checkbox"/>	8 ▼
9	<input type="checkbox"/>	9 ▼
10	<input type="checkbox"/>	10 ▼
11	<input type="checkbox"/>	11 ▼
12	<input type="checkbox"/>	12 ▼
13	<input type="checkbox"/>	13 ▼
14	<input type="checkbox"/>	14 ▼

Save Reset

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

The displayed settings are:

Port

The Port column shows the list of ports for which you can configure the VLAN Translation Mapping Group.

OPTICAL SYSTEMS DESIGN

Default

To set the switch port to use the default VLAN Translation Group click the checkbox and press Save.

Group ID

The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 14.

Note: By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Save

: Click to save changes.


Refresh

: Refreshes the displayed table starting from the input fields.

VLAN TRANSLATION MAPPING TABLE

Configuration → VLAN Translation → VLAN Translation Mappings

VLAN Translation Mapping Table

Group ID	VID	TVID	
			

This page allows you to create mappings of VLANs -> Translated VLANs and organize these mappings into global Groups.

Group ID

The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 14.

Note: By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.

VID




Indicates the VLAN of the mapping (i.e. 'source' VLAN). A valid VLAN ID ranges from 1 to 4095.

TVID

Indicates the VLAN ID to which VLAN ID of an ingress frame will be translated to (granted that the mapping is enabled on the ingress port that the frame arrived at). A valid VLAN ID ranges from 1 to 4095.

Modification Buttons

You can modify each VLAN Translation mapping in the table using the following buttons:

- : Edits the mapping row.
- : Deletes the mapping.
- : Adds a new mapping.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Refreshes the displayed table starting from the input fields.

: Click to remove all VLAN Translation mappings.

PRIVATE VLANS

- ▼ Private VLANs
 - Membership
 - Port Isolation

PRIVATE VLAN MEMBERSHIP CONFIGURATION

Configuration → Private VLANs → Membership

Private VLAN Membership Configuration

		Port Members													
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add New Private VLAN

Save Reset

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

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

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

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

Delete

To delete a private VLAN entry, check this box. The entry will be deleted during the next save.

Private VLAN ID


Indicates the ID of this particular private VLAN.

Port Members


A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

OPTICAL SYSTEMS DESIGN

Adding 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.


The Private VLAN is enabled when you click "Save".

The  button can be used to undo the addition of new Private VLANs.

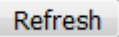
Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

 : Click to add a new entry to the static MAC table.

 : Click to save changes.

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

 : Refreshes the displayed table starting from the input fields.

OPTICAL SYSTEMS DESIGN

PORT ISOLATION CONFIGURATION

[Configuration](#) → [Private VLANs](#) → [Port Isolation](#)

Port Isolation Configuration

Port Number													
1	2	3	4	5	6	7	8	9	10	11	12	13	14
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OVERVIEW

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

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

CONFIGURATION

Port Members

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

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to save changes.

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

: Refreshes the displayed table starting from the input fields.

VCL

- ▼ VCL
 - MAC-based VLAN
 - ▼ Protocol-based VLAN
 - Protocol to Group
 - Group to VLAN
 - IP Subnet-based VLAN

MAC-BASED VLAN MEMBERSHIP CONFIGURATION

Configuration → VCL → MAC-based VLAN

MAC-based VLAN Membership Configuration

			Port Members													
Delete	MAC Address	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Currently no entries present																

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

Delete

To delete a MAC to VLAN ID mapping entry, check this box and press save. The entry will be deleted in the stack.

MAC Address

Indicates the MAC address of the mapping.

VLAN ID

Indicates the VLAN ID the above MAC will be mapped to.

Port Members

A row of check boxes for each port is displayed for each MAC to VLAN ID mapping entry. To include a port in the mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

OPTICAL SYSTEMS DESIGN

Adding a New MAC to VLAN ID mapping entry

Click to add a new MAC to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any unicast MAC address can be used to configure the mapping. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095.

The MAC to VLAN ID entry is enabled when you click on "Save". A mapping without any port members will not be added when you click "Save".

The button can be used to undo the addition of new mappings. The maximum possible MAC to VLAN ID mapping entries are limited to 256.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to save changes.

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

: Refreshes the displayed table starting from the input fields.

PROTOCOL-BASED VLAN

Protocol to Group

[Configuration](#) → [VCL](#) → [Protocol-based VLAN](#) → [Protocol to Group](#)

Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
No Group entry found!			

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

The displayed settings are:

Delete

To delete a Protocol to Group Name map entry, check this box. The entry will be deleted from the switch during the next Save.

Frame Type

Frame Type can have one of the following values:

1. Ethernet
2. LLC
3. SNAP

Note: When changing the Frame type field, the valid value of the following text field will vary depending on the new frame type you selected.

Value

Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu.

Below are the criteria for the three different Frame Types:

1. **Ethernet** : Value in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype range between 0x0600 and 0xffff
2. **LLC** : Valid value in this case is comprised of two different sub-values.
 - a. **DSAP** : 1-byte long string (0x00-0xff)
 - b. **SSAP** : 1-byte long string (0x00-0xff)

OPTICAL SYSTEMS DESIGN

3. SNAP: Valid value in this case is also comprised of two different sub-values.
 - a. OUI: OUI (Organizationally Unique Identifier) is a parameter in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value ranging between 0x00 and 0xff.
 - b. PID: PID (Protocol ID). If OUI is hexadecimal 000000, then the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.
In other words, if the value of OUI field is 00-00-00 then the value of PID will be etype (0x0600-0xffff) and if the value of OUI is other than 00-00-00 then valid values of PID will be any value between 0x0000 and 0xffff.

Group Name

A valid Group Name is a 16-character long string, unique for every entry, which consists of a combination of alphabets (a-z or A-Z) and integers(0-9).

Note: Special characters and underscores (_) are not allowed.

Adding a New Group to VLAN mapping entry

Click to add a new entry in the mapping table. An empty row is added to the table, where Frame Type, Value and the Group Name can be configured as needed.

The button can be used to undo the addition of new entry. The maximum possible Protocol to Group mappings are limited to 128.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to save changes.

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

: Refreshes the displayed table starting from the input fields.

OPTICAL SYSTEMS DESIGN

Protocol to Group

Configuration → VCL → Protocol-based VLAN → Group to VLAN

Group Name to VLAN mapping Table

			Port Members													
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Currently no entries present in the switch																

Add New Entry

Save

Reset

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

The displayed settings are:

Delete

To delete a Group Name to VLAN mapping, check this box. The entry will be deleted from the switch during the next Save.

Group Name

A valid Group Name is a string, at the most 16 characters long, which consists of a combination of alphabets (a-z or A-Z) and integers (0-9) with no special characters allowed. You may either use a Group that already includes one or more protocols (see Protocol to Group mappings), or create a Group to VLAN ID mapping that will become active the moment you add one or more protocols inside that Group. Furthermore, the Group to VLAN ID mapping is not unique, as long as the port lists of these mappings are mutually exclusive (e.g. Group1 can be mapped to VID 1 on port#1 and to VID 2 on port#2).

VLAN ID

Indicates the VLAN ID to which the Group Name will be mapped. A valid VLAN ID ranges from 1 to 4095.

Port Members

A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in the mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a new Group to VLAN mapping entry

Click to add a new entry in the mapping table. An empty row is added to the table and the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095.

The button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings are limited to 256.

OPTICAL SYSTEMS DESIGN

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to save changes.

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

: Refreshes the displayed table starting from the input fields.

OPTICAL SYSTEMS DESIGN

IP SUBNET-BASED VLAN MEMBERSHIP CONFIGURATION

Configuration → VCL → IP Subnet-based VLAN

IP Subnet-based VLAN Membership Configuration

				Port Members													
Delete	IP Address	Mask Length	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Currently no entries present																	

Add New Entry

Save

Reset

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

Delete

To delete a mapping, check this box and press save. The entry will be deleted in the stack.

IP Address

Indicates the subnet's IP address (Any of the subnet's host addresses can be also provided here, the application will convert it automatically).

Mask Length

Indicates the subnet's mask length.

VLAN ID

Indicates the VLAN ID the subnet will be mapped to. IP Subnet to VLAN ID is a unique matching.

Port Members

A row of check boxes for each port is displayed for each IP subnet to VLAN ID mapping entry. To include a port in a mapping, simply check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members and all boxes are unchecked.

Adding a New IP subnet-based VLAN

Click to add a new IP subnet to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any IP address/mask can be configured for the mapping. Legal values for the VLAN ID are 1 to 4095.

The IP subnet to VLAN ID mapping entry is enabled when you click on "Save". The button can be used to undo the addition of new mappings. The maximum possible IP subnet to VLAN ID mappings are limited to 128.

OPTICAL SYSTEMS DESIGN

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to save changes.

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

: Refreshes the displayed table starting from the input fields.

OPTICAL SYSTEMS DESIGN

VOICE VLAN CONFIGURATION

- ▼ Voice VLAN
 - Configuration
 - OUI

VOICE VLAN CONFIGURATION

Configuration → *Voice VLAN* → *Configuration*

Voice VLAN Configuration

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

Port Configuration

Port	Mode	Security	Discovery Protocol
*	<>	<>	<>
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
3	Disabled	Disabled	OUI
4	Disabled	Disabled	OUI
5	Disabled	Disabled	OUI
6	Disabled	Disabled	OUI
7	Disabled	Disabled	OUI
8	Disabled	Disabled	OUI
9	Disabled	Disabled	OUI
10	Disabled	Disabled	OUI
11	Disabled	Disabled	OUI
12	Disabled	Disabled	OUI
13	Disabled	Disabled	OUI
14	Disabled	Disabled	OUI

Save

Reset

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

Mode

Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are:

Enabled: Enable Voice VLAN mode operation.

Disabled: Disable Voice VLAN mode operation.

VLAN ID

Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.

Aging Time

Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.

Traffic Class

Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.

Port Mode

Indicates the Voice VLAN port mode. Possible port modes are:

Disabled: Disjoin from Voice VLAN.

Auto: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.

Forced: Force join to Voice VLAN.

Port Security

Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are:

Enabled: Enable Voice VLAN security mode operation.

Disabled: Disable Voice VLAN security mode operation.

Port Discovery Protocol

Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process.

Possible discovery protocols are:


OUI: Detect telephony device by OUI address.


LLDP: Detect telephony device by LLDP.

Both: Both OUI and LLDP.

OPTICAL SYSTEMS DESIGN

Buttons

 : Click to save changes.

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

OPTICAL SYSTEMS DESIGN

VOICE VLAN OUI TABLE

Configuration → Voice VLAN → OUI

Voice VLAN OUI Table

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

Add New Entry

Save

Reset

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

Delete

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

Telephony OUI

A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).

Description

The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

Buttons

Add New Entry

: Click to add a new access management entry.

Save

: Click to save changes.

Reset

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

QoS

- ▼ QoS
 - Port Classification
 - Port Policing
 - Queue Policing
 - Port Scheduler
 - Port Shaping
 - Port Tag Remarking
 - Port DSCP
 - DSCP-Based QoS
 - DSCP Translation
 - DSCP Classification
 - QoS Control List
 - Storm Policing
 - WRED

QoS INGRESS PORT CLASSIFICATION

Configuration → QoS → Port Classification

QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	WRED Group
*	<> ▼	<> ▼	<> ▼	<> ▼		<input type="checkbox"/>	<> ▼
1	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	1 ▼
2	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	1 ▼
3	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	1 ▼
4	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	1 ▼
5	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	1 ▼
6	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	1 ▼
7	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	1 ▼
8	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	1 ▼
9	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	1 ▼
10	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	1 ▼
11	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	1 ▼
12	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	1 ▼
13	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	1 ▼
14	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	1 ▼
15	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	1 ▼

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

OPTICAL SYSTEMS DESIGN

The displayed settings are:

Port

The port number for which the configuration below applies.

CoS

Controls the default class of service.

All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS.

The classified CoS can be overruled by a QCL entry.

Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.

DPL

Controls the default drop precedence level.

All frames are classified to a drop precedence level.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL.

The classified DPL can be overruled by a QCL entry.

PCP

Controls the default PCP value.

All frames are classified to a PCP value.

If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.

DEI

Controls the default DEI value.

All frames are classified to a DEI value.

If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.

OPTICAL SYSTEMS DESIGN

Tag Class.

Shows the classification mode for tagged frames on this port.

Disabled: Use default CoS and DPL for tagged frames.

Enabled: Use mapped versions of PCP and DEI for tagged frames.

Click on the mode in order to configure the mode and/or mapping.

Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.


DSCP Based

Click to Enable DSCP Based QoS Ingress Port Classification.

WRED Group

Controls the WRED group membership.

Buttons

 : Click to save changes.

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

OPTICAL SYSTEMS DESIGN

QOS INGRESS PORT POLICERS

Configuration → QoS → Port Policing

QoS Ingress Port Policers

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

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

The displayed settings are:

Port

The port number for which the configuration below applies.

Enable

Enable or disable the port policer for this switch port.

Rate

Controls the rate for the port policer. This value is restricted to 100-3276700 when "Unit" is kbps or fps, and 1-3276 when "Unit" is Mbps or kfps. The rate is internally rounded up to the nearest value supported by the port policer.

Unit


Controls the unit of measure for the port policer rate as kbps, Mbps, fps or kfps.

Flow Control

If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

OPTICAL SYSTEMS DESIGN

Buttons

 : Click to save changes.

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

OPTICAL SYSTEMS DESIGN

QOS INGRESS QUEUE POLICERS

Configuration → QoS → Queue Policing

QoS Ingress Queue Policers

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

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

The displayed settings are:

Port

The port number for which the configuration below applies.

Enable (E)

Enable or disable the port policer for this switch port.

Rate

Controls the rate for the port policer. This value is restricted to 25-13128147 when "Unit" is kbps or fps, and 1-13128 when "Unit" is Mbps or kfps. The rate is internally rounded up to the nearest value supported by the port policer. This field is only shown if at least one of the queue policers are enabled.

Unit

Controls the unit of measure for the queue policer rate as kbps or Mbps.
This field is only shown if at least one of the queue policers are enabled.

Buttons

: Click to save changes.

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

OPTICAL SYSTEMS DESIGN

QOS EGRESS PORT SCHEDULERS

[Configuration](#) → [QoS](#) → [Port Scheduler](#)

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	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-
11	Strict Priority	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-
13	Strict Priority	-	-	-	-	-	-
14	Strict Priority	-	-	-	-	-	-

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

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.

Mode

Shows the scheduling mode for this port.

Qn

Shows the weight for this queue and port.

OPTICAL SYSTEMS DESIGN

QoS Egress Port Scheduler and Shapers Port 7

Scheduler Mode:

Queue Shaper		
Enable	Rate	Unit
<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="kbps"/>
<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="kbps"/>
<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="kbps"/>
<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="kbps"/>
<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="kbps"/>
<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="kbps"/>
<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="kbps"/>
<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="kbps"/>

Port Shaper		
Enable	Rate	Unit
<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="kbps"/>

Buttons

: Click to save changes.

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

OPTICAL SYSTEMS DESIGN

QOS EGRESS PORT SHAPERS

[Configuration](#) → [QoS](#) → [Port Shaping](#)

QoS Egress Port Shapers

Port	Shapers								Port
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-	-
14	-	-	-	-	-	-	-	-	-

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

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 shapers.

Qn

Shows "-" for disabled or actual queue shaper rate - e.g. "800 Mbps".

Port

Shows "-" for disabled or actual port shaper rate - e.g. "800 Mbps".

QOS EGRESS PORT TAG REMARKING

Configuration → QoS → Port Tag Remarking

QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified
13	Classified
14	Classified

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

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 tag remarking.

Mode

Shows the tag remarking mode for this port.
Classified: Use classified PCP/DEI values.
Default: Use default PCP/DEI values.
Mapped: Use mapped versions of QoS class and DP level.

OPTICAL SYSTEMS DESIGN

QOS PORT DSCP CONFIGURATION

Configuration → QoS → Port DSCP

QoS Port DSCP Configuration

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

Save

Reset

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

The displayed settings are:

Port

The Port column shows the list of ports for which you can configure dscp ingress and egress settings.

Ingress

In Ingress settings you can change ingress translation and classification settings for individual ports.

There are two configuration parameters available in Ingress:

1. Translate
2. Classify

1. Translate

To Enable the Ingress Translation click the checkbox.

OPTICAL SYSTEMS DESIGN

2. Classify

Classification for a port have 4 different values.


- **Disable:** No Ingress DSCP Classification.
- **DSCP=0:** Classify if incoming (or translated if enabled) DSCP is 0.
- **Selected:** Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.
- **All:** Classify all DSCP.

Egress

Port Egress Rewriting can be one of -

- **Disable:** No Egress rewrite.
- **Enable:** Rewrite enabled without remapping.
- **Remap DP Unaware:** DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

Buttons

 : Click to save changes.

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

OPTICAL SYSTEMS DESIGN

DSCP-BASED QOS INGRESS CLASSIFICATION

Configuration → QoS → DSCP-Based QoS

DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
*	<input type="checkbox"/>	<>	<>
0 (BE)	<input type="checkbox"/>	0	0
1	<input type="checkbox"/>	0	0
2	<input type="checkbox"/>	0	0
3	<input type="checkbox"/>	0	0
4	<input type="checkbox"/>	0	0
5	<input type="checkbox"/>	0	0
6	<input type="checkbox"/>	0	0
7	<input type="checkbox"/>	0	0
8 (CS1)	<input type="checkbox"/>	0	0
9	<input type="checkbox"/>	0	0
10 (AF11)	<input type="checkbox"/>	0	0
11	<input type="checkbox"/>	0	0
12 (AF12)	<input type="checkbox"/>	0	0
13	<input type="checkbox"/>	0	0
14 (AF13)	<input type="checkbox"/>	0	0
15	<input type="checkbox"/>	0	0
16 (CS2)	<input type="checkbox"/>	0	0
17	<input type="checkbox"/>	0	0
18 (AF21)	<input type="checkbox"/>	0	0
19	<input type="checkbox"/>	0	0
20 (AF22)	<input type="checkbox"/>	0	0
21	<input type="checkbox"/>	0	0
22 (AF23)	<input type="checkbox"/>	0	0
23	<input type="checkbox"/>	0	0
24 (CS3)	<input type="checkbox"/>	0	0
25	<input type="checkbox"/>	0	0
26 (AF31)	<input type="checkbox"/>	0	0
27	<input type="checkbox"/>	0	0

35	<input type="checkbox"/>	0	0
36 (AF42)	<input type="checkbox"/>	0	0
37	<input type="checkbox"/>	0	0
38 (AF43)	<input type="checkbox"/>	0	0
39	<input type="checkbox"/>	0	0
40 (CS5)	<input type="checkbox"/>	0	0
41	<input type="checkbox"/>	0	0
42	<input type="checkbox"/>	0	0
43	<input type="checkbox"/>	0	0
44	<input type="checkbox"/>	0	0
45	<input type="checkbox"/>	0	0
46 (EF)	<input type="checkbox"/>	0	0
47	<input type="checkbox"/>	0	0
48 (CS6)	<input type="checkbox"/>	0	0
49	<input type="checkbox"/>	0	0
50	<input type="checkbox"/>	0	0
51	<input type="checkbox"/>	0	0
52	<input type="checkbox"/>	0	0
53	<input type="checkbox"/>	0	0
54	<input type="checkbox"/>	0	0
55	<input type="checkbox"/>	0	0
56 (CS7)	<input type="checkbox"/>	0	0
57	<input type="checkbox"/>	0	0
58	<input type="checkbox"/>	0	0
59	<input type="checkbox"/>	0	0
60	<input type="checkbox"/>	0	0
61	<input type="checkbox"/>	0	0
62	<input type="checkbox"/>	0	0
63	<input type="checkbox"/>	0	0

Save

Reset

OPTICAL SYSTEMS DESIGN

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

The displayed settings are:

DSCP

Maximum number of supported DSCP values are 64.

Trust

Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.

QoS Class

QoS class value can be any of (0-7)

DPL

Drop Precedence Level (0-1)

Buttons

: Click to save changes.

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

OPTICAL SYSTEMS DESIGN

DSCP TRANSLATION

Configuration → QoS → DSCP Translation

DSCP Translation

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

OPTICAL SYSTEMS DESIGN

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

The displayed settings are:

DSCP

Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.

Ingress

Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.

There are two configuration parameters for DSCP Translation -

1. Translate
2. Classify

1. Translate

DSCP at Ingress side can be translated to any of (0-63) DSCP values.

2. Classify

Click to enable Classification at Ingress side.

Egress


There are the following configurable parameters for Egress side -

1. Remap DP0 Controls the remapping for frames with DP level 0.
2. Remap DP1 Controls the remapping for frames with DP level 1.

Remap

Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

Buttons

 : Click to save changes.

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

OPTICAL SYSTEMS DESIGN

DSCP CLASSIFICATION

Configuration → QoS → DSCP Classification

DSCP Classification

QoS Class	DSCP DP0	DSCP DP1	DSCP DP2	DSCP DP3
*	<> ▾	<> ▾	<> ▾	<> ▾
0	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾
1	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾
2	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾
3	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾
4	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾
5	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾
6	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾
7	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾	0 (BE) ▾

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

The displayed settings are:

QoS Class

Actual QoS class.

DSCP DP0

Select the classified DSCP value (0-63) for Drop Precedence Level 0.

DSCP DP1

Select the classified DSCP value (0-63) for Drop Precedence Level 1.

DSCP DP2

Select the classified DSCP value (0-63) for Drop Precedence Level 2.

DSCP DP3

Select the classified DSCP value (0-63) for Drop Precedence Level 3.

Buttons

: Click to save changes.

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

OPTICAL SYSTEMS DESIGN

QOS CONTROL LIST CONFIGURATION

Configuration → QoS → QoS Control List

QoS Control List Configuration

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

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

QCE

Indicates the QCE id.

Port

Indicates the list of ports configured with the QCE or 'Any'.

DMAC

Indicates the destination MAC address. Possible values are:

Any: Match any DMAC.

Unicast: Match unicast DMAC.

Multicast: Match multicast DMAC.

Broadcast: Match broadcast DMAC.

The default value is 'Any'.

SMAC

Match specific source MAC address or 'Any'.

If a port is configured to match on destination addresses, this field indicates the DMAC.

Tag Type

Indicates tag type. Possible values are:

Any: Match tagged and untagged frames.

Untagged: Match untagged frames.

Tagged: Match tagged frames.

The default value is 'Any'.

VID

Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'

PCP

Priority Code Point: Valid values of PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

OPTICAL SYSTEMS DESIGN

DEI

Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.

Frame Type

Indicates the type of frame. Possible values are:

Any: Match any frame type.

Ethernet: Match EtherType frames.

LLC: Match (LLC) frames.

SNAP: Match (SNAP) frames.

IPv4: Match IPv4 frames.

IPv6: Match IPv6 frames.

Action

Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.

Possible actions are:

CoS: Classify Class of Service.

DPL: Classify Drop Precedence Level.

DSCP: Classify DSCP value.


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.

OPTICAL SYSTEMS DESIGN

GLOBAL STORM POLICER CONFIGURATION

Configuration → QoS → Storm Policing

Global Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unicast	<input type="checkbox"/>	10	fps ▾
Multicast	<input type="checkbox"/>	10	fps ▾
Broadcast	<input type="checkbox"/>	10	fps ▾

Port Storm Policer Configuration

Port	Unicast Frames			Broadcast Frames			Unknown Frames		
	Enable	Rate	Unit	Enable	Rate	Unit	Enable	Rate	Unit
*	<input type="checkbox"/>	500	<> ▾	<input type="checkbox"/>	500	<> ▾	<input type="checkbox"/>	500	<> ▾
1	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
2	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
3	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
4	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
5	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
6	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
7	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
8	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
9	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
10	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
11	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
12	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
13	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
14	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
15	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
16	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
17	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
18	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
19	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
20	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
21	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
22	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
23	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
24	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
25	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
26	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
27	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
28	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾

Save Reset

OPTICAL SYSTEMS DESIGN

GLOBAL STORM POLICER CONFIGURATION

Global storm policers for the switch are configured on this page.

There is a unicast storm policer, multicast storm policer, and a broadcast storm policer. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table. The displayed settings are:

Frame Type

The frame type for which the configuration below applies.

Enable

Enable or disable the global storm policer for the given frame type.

Rate

Controls the rate for the global storm policer. This value is restricted to 1-1024000 when "Unit" is fps, and 1-1024 when "Unit" is kfps. The rate is internally rounded up to the nearest value supported by the global storm policer.

Unit

Controls the unit of measure for the global storm policer rate as fps or kfps.

PORT STORM POLICER CONFIGURATION

Port storm policers for all switch ports are configured on this page.

There is a storm policer for unicast frames, broadcast frames and unknown (flooded) frames. The displayed settings are:

Port

The port number for which the configuration below applies.

Enable

Enable or disable the storm policer for this switch port.


Rate

Controls the rate for the port storm policer. This value is restricted to 10-13128147 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the port storm policer.

Unit

Controls the unit of measure for the port storm policer rate as fps, kfps, kbps or Mbps.

Buttons

 : Click to save changes.

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

OPTICAL SYSTEMS DESIGN

WRED – WEIGHTED RANDOM EARLY DETECTION HELP

Configuration → QoS → WRED

Weighted Random Early Detection Configuration

Group	Queue	DPL	Enable	Min	Max	Max Unit
1	0	1	<input type="checkbox"/>	0	50	Drop Probability ▼
1	0	2	<input type="checkbox"/>	0	50	Drop Probability ▼
1	0	3	<input type="checkbox"/>	0	50	Drop Probability ▼
1	1	1	<input type="checkbox"/>	0	50	Drop Probability ▼
1	1	2	<input type="checkbox"/>	0	50	Drop Probability ▼
1	1	3	<input type="checkbox"/>	0	50	Drop Probability ▼
1	2	1	<input type="checkbox"/>	0	50	Drop Probability ▼
1	2	2	<input type="checkbox"/>	0	50	Drop Probability ▼
1	2	3	<input type="checkbox"/>	0	50	Drop Probability ▼
1	3	1	<input type="checkbox"/>	0	50	Drop Probability ▼
1	3	2	<input type="checkbox"/>	0	50	Drop Probability ▼
1	3	3	<input type="checkbox"/>	0	50	Drop Probability ▼
1	4	1	<input type="checkbox"/>	0	50	Drop Probability ▼
1	4	2	<input type="checkbox"/>	0	50	Drop Probability ▼
1	4	3	<input type="checkbox"/>	0	50	Drop Probability ▼
1	5	1	<input type="checkbox"/>	0	50	Drop Probability ▼
1	5	2	<input type="checkbox"/>	0	50	Drop Probability ▼
1	5	3	<input type="checkbox"/>	0	50	Drop Probability ▼
1	6	1	<input type="checkbox"/>	0	50	Drop Probability ▼
1	6	2	<input type="checkbox"/>	0	50	Drop Probability ▼
1	6	3	<input type="checkbox"/>	0	50	Drop Probability ▼
1	7	1	<input type="checkbox"/>	0	50	Drop Probability ▼
1	7	2	<input type="checkbox"/>	0	50	Drop Probability ▼
1	7	3	<input type="checkbox"/>	0	50	Drop Probability ▼
2	0	1	<input type="checkbox"/>	0	50	Drop Probability ▼
2	0	2	<input type="checkbox"/>	0	50	Drop Probability ▼
2	0	3	<input type="checkbox"/>	0	50	Drop Probability ▼
2	1	1	<input type="checkbox"/>	0	50	Drop Probability ▼

OPTICAL SYSTEMS DESIGN

This page allows you to configure the Random Early Detection (RED) settings.

Through different RED configuration for the queues (QoS classes) it is possible to obtain Weighted Random Early Detection (WRED) operation between queues.

The settings are global for all ports in the switch.

The displayed settings are:

Group

The WRED group number for which the configuration below applies.

Queue

The queue number (QoS class) for which the configuration below applies.

DPL

The Drop Precedence Level for which the configuration below applies.

Enable

Controls whether RED is enabled for this entry.

Min

Controls the lower RED fill level threshold. If the queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100%.

Max

Controls the upper RED drop probability or fill level threshold for frames marked with Drop Precedence Level > 0 (yellow frames). This value is restricted to 1-100%.

Max Unit

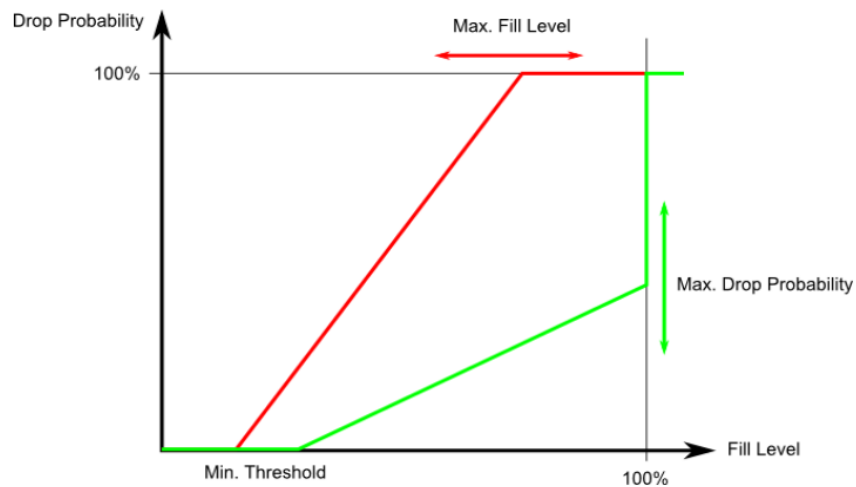
Selects the unit for Max. Possible values are:

Drop Probability: Max controls the drop probability just below 100% fill level.

Fill Level: Max controls the fill level where drop probability reaches 100%.

RED DROP PROBABILITY FUNCTION

The following illustration shows the drop probability versus fill level function with associated parameters.



OPTICAL SYSTEMS DESIGN

Min is the fill level where the queue randomly start dropping frames marked with Drop Precedence Level > 0 (yellow frames).

If Max Unit is 'Drop Probability' (the green line), Max controls the drop probability when the fill level is just below 100%.

If Max Unit is 'Fill Level' (the red line), Max controls the fill level where drop probability reaches 100%. This configuration makes it possible to reserve a portion of the queue exclusively for frames marked with Drop Precedence Level 0 (green frames). The reserved portion is calculated as $(100 - \text{Max}) \%$.

Frames marked with Drop Precedence Level 0 (green frames) are never dropped.

The drop probability for frames increases linearly from zero (at Min average queue filling level) to Max Drop Probability or Fill Level.

Buttons

: Click to save changes.

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

UPNP CONFIGURATION

UPnP

Configuration → UPNP

UPnP Configuration

Mode	Disabled
TTL	4
Advertising Duration	100

Save

Reset

Configure UPnP on this page.

Mode

Indicates the UPnP operation mode. Possible modes are:

Enabled: Enable UPnP mode operation.

Disabled: Disable UPnP mode operation.

When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled.

TTL

The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255.

Advertising Duration

The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.

Buttons

Save

: Click to save changes.

Reset

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

PTP EXTERNAL CLOCK MODE

▪ PTP

Configuration → PTP

PTP External Clock Mode

One_PPS_Mode	Disable
External Enable	False
Adjust Method	LTC frequency
Clock Frequency	1

PTP Clock Configuration

Delete	Clock Instance	Device Type	Profile
No Clock Instances Present			

This page allows the user to configure and inspect the current PTP clock settings.

PTP EXTERNAL CLOCK CONFIGURATION

One_PPS_Mode

This Selection box will allow you to select the One_pps_mode configuration.

The following values are possible:

1. Output: Enable the 1 pps clock output
2. Input: Enable the 1 pps clock input
3. Disable: Disable the 1 pps clock in/out-put

External Enable

This Selection box will allow you to configure the External Clock output.

The following values are possible:

1. True: Enable the external clock output
2. False: Disable the external clock output

Adjust Method

This Selection box will allow you to configure the Frequency adjustment configuration.

1. LTC frequency: Select Local Time Counter (LTC) frequency control
2. SyncE-DPLL: Select SyncE DPLL frequency control, if allowed by SyncE
3. Oscillator: Select an oscillator independent of SyncE for frequency control, if supported by the HW
4. LTC phase: Select Local Time Counter (LTC) phase control (assumes that the frequency is locked by means of SyncE)

OPTICAL SYSTEMS DESIGN

Clock Frequency

This will allow to set the Clock Frequency.

The possible range of values are 1 - 25000000 (1 - 25MHz)

PTP CLOCK CONFIGURATION

Delete

Check this box and click on 'Save' to delete the clock instance.

Inst

Indicates the Instance of a particular Clock Instance [0..3].

Click on the Clock Instance number to edit the Clock details.

ClkDom

Indicates the Clock domain used by the Instance of a particular Clock Instance [0..3]. More instances may use the same clock domain, e.g. a Boundary clock and a Transparent clock. Only one Slave or Boundary clock is allowed within the same Clock domain.

Device Type

Indicates the Type of the Clock Instance. There are five Device Types.

1. Ord-Bound - clock's Device Type is Ordinary-Boundary Clock.
2. P2p Transp - clock's Device Type is Peer to Peer Transparent Clock.
3. E2e Transp - clock's Device Type is End to End Transparent Clock.
4. Master Only - clock's Device Type is Master Only.
5. Slave Only - clock's Device Type is Slave Only.

Profile

Indicates the profile used by the clock.

Port List

Set check mark for each port configured for this Clock Instance. One port can only be active within one Clock domain. I.e. enabling a port which is already active in an other Clock domain is rejected.

2 Step Flag

Static member: defined by the system, true if two-step Sync events and Pdelay_Resp events are used

Clock Identity

It shows unique clock identifier

One Way

If true, one-way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.

OPTICAL SYSTEMS DESIGN

Protocol

Transport protocol used by the PTP protocol engine

Ethernet PTP over Ethernet multicast

EthernetMixed PTP using a combination of Ethernet multicast and unicast

IPv4Multi PTP over IPv4 multicast

IPv4Mixed PTP using a combination of IPv4 multicast and unicast

IPv4Uni PTP over IPv4 unicast

Note : IPv4 unicast protocol only works in Master only and Slave only clocks

See parameter Device Type

In a unicast Slave only clock you also need configure which master clocks to request Announce and Sync messages from. See: Unicast Slave Configuration

VID


VLAN Identifier used for tagging the PTP frames.


Note: Packets are tagged if the port is configured for vlan tagging for the configured VID.

PCP

Priority Code Point value used for PTP frames.

Buttons

 : Click to create a new clock instance.

 : Click to save changes.

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

GVRP CONFIGURATION

- ▼ GVRP
 - Global config
 - Port config

GVRP CONFIGURATION

Configuration → GVRP → Global config

GVRP Configuration

Enable GVRP

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

This page allows you to configure the global GVRP configuration settings that are commonly applied to all GVRP enabled ports.

Enable GVRP globally

The GVRP feature is globally enabled by setting the check mark in the checkbox named Enable GVRP and pressing the Save button.

GVRP protocol timers

Join-time is a value in the range of 1-20cs, i.e. in units of one hundredth of a second. The default value is 20cs.

Leave-time is a value in the range of 60-300cs, i.e. in units of one hundredth of a second. The default is 60cs.

LeaveAll-time is a value in the range of 1000-5000cs, i.e. in units of one hundredth of a second. The default is 1000cs.

Max number of VLANs

When GVRP is enabled, a maximum number of VLANs supported by GVRP is specified. By default this number is 20. This number can only be changed when GVRP is turned off.

Buttons

: Click to save changes.

GVRP PORT CONFIGURATION

Configuration → *GVRP* → *Port config*

GVRP Port Configuration

Port	Mode
*	<> ▼
1	Disabled ▼
2	Disabled ▼
3	Disabled ▼
4	Disabled ▼
5	Disabled ▼
6	Disabled ▼
7	Disabled ▼
8	Disabled ▼
9	Disabled ▼
10	Disabled ▼
11	Disabled ▼
12	Disabled ▼
13	Disabled ▼
14	Disabled ▼

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

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

Port

The logical port that is to be configured.

Mode

Mode can be either 'Disabled' or 'GVRP enabled'. These values turn the GVRP feature off or on respectively for the port in question.

Buttons

: Click to save changes.

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

OPTICAL SYSTEMS DESIGN

SFLOW CONFIGURATION

▪ sFlow

Configuration → sFlow

sFlow Configuration

Agent Configuration

IP Address

Receiver Configuration

Owner	<none>	<input type="button" value="Release"/>
IP Address/Hostname	0.0.0.0	
UDP Port	6343	
Timeout	0	seconds
Max. Datagram Size	1400	bytes

Port Configuration

Port	Flow Sampler			Counter Poller	
	Enabled	Sampling Rate	Max. Header	Enabled	Interval
*	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
1	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
2	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
3	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
4	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
5	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
6	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
7	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
8	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
9	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
10	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
11	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
12	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
13	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
14	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0

OPTICAL SYSTEMS DESIGN

This page allows for configuring sFlow. The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.

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

AGENT CONFIGURATION

IP Address

The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time.

Both IPv4 and IPv6 addresses are supported.

RECEIVER CONFIGURATION

Owner

Basically, sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains `<none>`.
- If sFlow is currently configured through Web or CLI, Owner contains `<Configured through local management>`.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.

If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.

The button allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).

IP Address/Hostname

The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.

UDP Port

The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.

Timeout

The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings. Valid range is 0 to 2147483647 seconds.

Max. Datagram Size

The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

OPTICAL SYSTEMS DESIGN

PORT CONFIGURATION

Port

The port number for which the configuration below applies.

Flow Sampler Enabled

Enables/disables flow sampling on this port.

Flow Sampler Sampling Rate

The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port.

Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field. Valid range is 1 to 4294967295.

Flow Sampler Max. Header

The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes.

If the maximum datagram size does not take into account the maximum header size, samples may be dropped.

Counter Poller Enabled

Enables/disables counter polling on this port.

Counter Poller Interval

With counter polling enabled, this specifies the interval - in seconds - between counter poller samples. Valid range is 1 to 3600 seconds.

Buttons

Release

: See description under Owner.

Refresh

: Click to refresh the page. Note that unsaved changes will be lost.

Save

: Click to save changes. Note that sFlow configuration is not persisted to non-volatile memory.

Reset

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

UDLD PORT CONFIGURATION

UDLD

Configuration → UDLD

UDLD Port Configuration

Port	UDLD mode	Message Interval
*	<>	7
1	Disable	7
2	Disable	7
3	Disable	7
4	Disable	7
5	Disable	7
6	Disable	7
7	Disable	7
8	Disable	7
9	Disable	7
10	Disable	7
11	Disable	7
12	Disable	7
13	Disable	7
14	Disable	7

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

Port

Port number of the switch.

UDLD Mode

Configures the UDLD mode on a port. Valid values are *Disable*, *Normal* and *Aggressive*. Default mode is *Disable*.

- ***Disable***
In disabled mode, UDLD functionality doesn't exist on port.
- ***Normal***
In normal mode, if the link state of the port was determined to be unidirectional, it will not affect the port state.

OPTICAL SYSTEMS DESIGN

- **Aggressive**
In aggressive mode, unidirectional detected ports will get shutdown. To bring back the ports up, need to disable UDLD on that port.

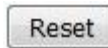
Message Interval

Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is from 7 to 90 seconds (Default value is 7 seconds) (Currently default time interval is supported, due to lack of detailed information in RFC 5171).

Buttons



: Click to save changes.



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

OPTICAL SYSTEMS DESIGN

PROGRAMMABLE ALARM

Alarm

Configuration → Alarm

Programmable Alarm

Alarm Reset Option

Automatic Reset	<input type="checkbox"/>
Alarm Reset(Seconds)	5

Alarm Selection

Alarm	Alarm1 ▼
-------	----------

Port Link Alarm Configuration

Port	Link Alarm	Enable
1	Link_down ▼	Disable ▼
2	Link_down ▼	Disable ▼
3	Link_down ▼	Disable ▼
4	Link_down ▼	Disable ▼
5	Link_down ▼	Disable ▼
6	Link_down ▼	Disable ▼
7	Link_down ▼	Disable ▼
8	Link_down ▼	Disable ▼
9	Link_down ▼	Disable ▼
10	Link_down ▼	Disable ▼
11	Link_down ▼	Disable ▼
12	Link_down ▼	Disable ▼
13	Link_down ▼	Disable ▼
14	Link_down ▼	Disable ▼
15	Link_down ▼	Disable ▼
16	Link_down ▼	Disable ▼
17	Link_down ▼	Disable ▼
18	Link_down ▼	Disable ▼
19	Link_down ▼	Disable ▼
20	Link_down ▼	Disable ▼
21	Link_down ▼	Disable ▼
22	Link_down ▼	Disable ▼
23	Link_down ▼	Disable ▼
24	Link_down ▼	Disable ▼
25	Link_down ▼	Disable ▼
26	Link_down ▼	Disable ▼
27	Link_down ▼	Disable ▼
28	Link_down ▼	Disable ▼

Temperature Alarm Configuration

ID	Temperature	Enable
1	80	Disable ▼

Save	Reset
------	-------

OPTICAL SYSTEMS DESIGN

This page allows the user to configure the programmable alarm.

ALARM RESET OPTION

The alarm automatically resets after the specified duration (1 — in the valid entry, it is 1-3600 seconds), when automatic reset is selected. Otherwise, the alarm has to be reset manually from the status page.

Automatic Reset: Enable/Disable automatic alarm reset.

Alarm Reset (Seconds): Duration of alarm time when the automatic reset option selected.

ALARM SELECTION

There are two alarms. Select which alarm is to be configured from the dropdown list.

PORT LINK ALARM CONFIGURATION


Alarms can be triggered by link down, link up, link change event.


Disable/Enable option enables the specified alarm.

TEMPERATURE ALARM SETTING

If the temperature goes above the specified temperature the alarm will be triggered. Temperature value saved only when the temperature alarm is enabled.

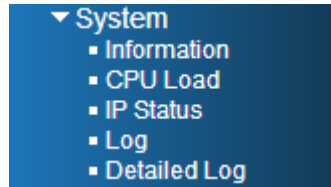
Buttons

 : Click to save changes.

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

5.3 MONITOR

SYSTEM



SYSTEM INFORMATION

[Monitor](#) → [System](#) → [Information](#)

System Information

System	
Contact	
Name	
Location	
Hardware	
MAC Address	00-26-dc-00-07-61
Chip ID	VSC7429
Time	
System Date	1970-01-05T08:01:18+00:00
System Uptime	4d 08:01:18
Software	
Software Version	60007801
Software Date	2017-12-15T16:10:23+11:00
Acknowledgments	Details

The switch system information is provided here.

Contact

The system contact configured in Configuration | System | Information | System Contact.

Name

The system name configured in Configuration | System | Information | System Name.

Location

The system location configured in Configuration | System | Information | System Location.

MAC Address

The MAC Address of this switch.

Chip ID

The Chip ID of this switch.

OPTICAL SYSTEMS DESIGN

System Date

The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.

System Uptime

The period of time the device has been operational.

Software Version

The software version of this switch.

Software Date

The date when the switch software was produced.

Buttons

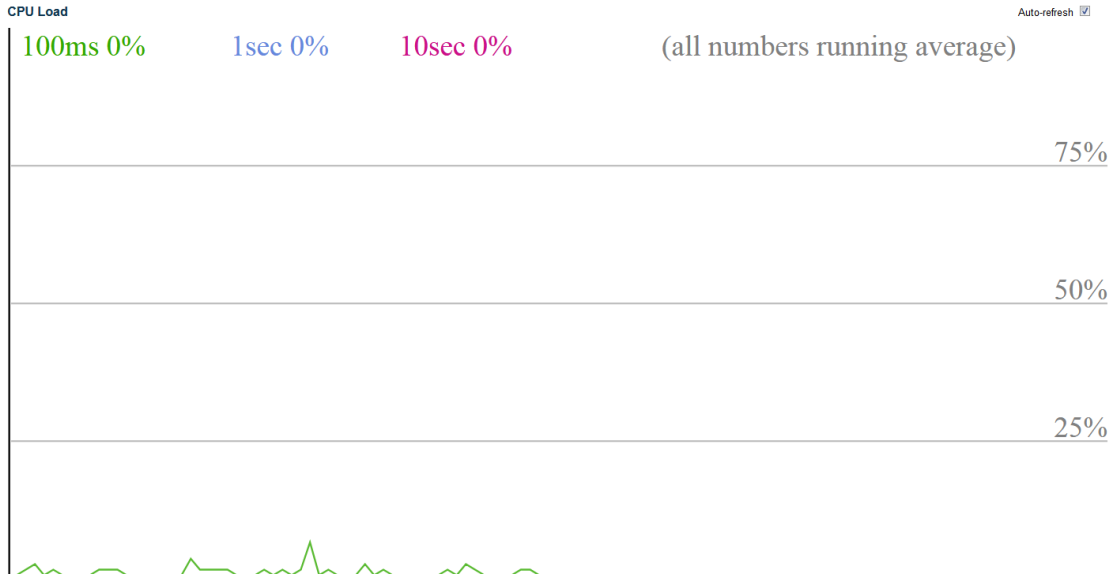
Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

OPTICAL SYSTEMS DESIGN

CPU LOAD

Monitor → System → CPU Load



This page displays the CPU load, using an 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.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

OPTICAL SYSTEMS DESIGN

IP INTERFACES

Monitor → System → IP 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	
OS:lo	IPv6	fe80::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	00-26-dc-00-07-61	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.99/24	
VLAN1	IPv6	fe80::226:dcff:fe00:761/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.0.27	VLAN1:90-60-f1-c4-83-29
192.168.0.102	VLAN1:d0-17-c2-8b-9a-cf
192.168.0.111	VLAN1:74-d4-35-83-9f-83
192.168.0.219	VLAN1:30-85-a9-b1-b4-c4
fe80::226:dcff:fe00:761	VLAN1:00-26-dc-00-07-61

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

IP Interfaces

Interface

The name of the interface.

Type

The address type of the entry. This may be LINK or IPv4.

Address

The current address of the interface (of the given type).

Status

The status flags of the interface (and/or address).

IP Routes

Network

The destination IP network or host address of this route.

Gateway

The gateway address of this route.

Status

The status flags of the route.

Neighbour cache

IP Address

The IP address of the entry.

Link Address

The Link (MAC) address for which a binding to the IP address given exist.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

OPTICAL SYSTEMS DESIGN

SYSTEM LOG INFORMATION

Monitor → System → Log

System Log Information

Level	All	▼
Clear Level	All	▼

The total number of entries is 4 for the given level.

Start from ID with entries per page.

ID	Level	Time	Message
1	Informational	1970-01-01T00:00:01+00:00	SYS-BOOTING: Switch just made a cold boot.
2	Notice	1970-01-01T00:00:01+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
3	Notice	1970-01-01T00:00:03+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/8, changed state to up.
4	Notice	1970-01-01T00:00:04+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.

The switch system log information is provided here.

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.

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

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

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

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

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

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

When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

SYSTEM LOG INFORMATION ENTRY COLUMNS

ID

The identification of the system log entry.

Level

The level of the system log entry. Info: The system log entry is belonged information level.

Warning: The system log entry is belonged warning level.

Error: The system log entry is belonged error level.

OPTICAL SYSTEMS DESIGN

Time

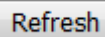
The occurred time of the system log entry.

Message

The detail message of the system log entry.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

 Refresh

: Click to refresh the page immediately

 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.

OPTICAL SYSTEMS DESIGN

DETAILED SYSTEM LOG INFORMATION

[Monitor](#) → [System](#) → [Detailed Log](#)

Detailed System Log Information

ID	1
----	---

Message

Level	Informational
Time	1970-01-01T00:00:01+00:00
Message	SYS-BOOTING: Switch just made a cold boot.

The switch system detailed log information is provided here.

Level

The severity level of the system log entry.

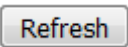
ID


The ID (≥ 1) of the system log entry.


Message


The detailed message of the system log entry.

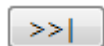
Buttons

 : 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.

OPTICAL SYSTEMS DESIGN

GREEN ETHERNET

- ▼ Green Ethernet
 - Port Power Savings
 - Fan

PORT POWER SAVINGS STATUS

Monitor → Green Ethernet → Port Power Savings

Port Power Savings Status

Port	Link	EEE Cap	EEE Ena	LP EEE Cap	EEE In power save	ActiPhy Savings	PerfectReach Savings
1	●	×	×	×	×	×	×
2	●	×	×	×	×	×	×
3	●	×	×	×	×	×	×
4	●	×	×	×	×	×	×
5	●	×	×	×	×	×	×
6	●	×	×	×	×	×	×
7	●	×	×	×	×	×	×
8	●	×	×	×	×	×	×
9	●	×	×	×	×	×	×
10	●	×	×	×	×	×	×
11	●	×	×	×	×	×	×
12	●	×	×	×	×	×	×
13	●	×	×	×	×	×	×
14	●	×	×	×	×	×	×
15	●	×	×	×	×	×	×
16	●	×	×	×	×	×	×
17	●	×	×	×	×	×	×
18	●	×	×	×	×	×	×
19	●	×	×	×	×	×	×
20	●	×	×	×	×	×	×
21	●	×	×	×	×	×	×
22	●	×	×	×	×	×	×
23	●	×	×	×	×	×	×
24	●	×	×	×	×	×	×
25	●	×	×	×	×	×	×
26	●	×	×	×	×	×	×
27	●	×	×	×	×	×	×
28	●	×	×	×	×	×	×

This page provides the current status for EEE.

Local Port

This is the logical port number for this row.

Link

Shows if the link is up for the port (green = link up, red = link down).

OPTICAL SYSTEMS DESIGN

EEE cap

Shows if the port is EEE capable.

EEE Ena

Shows if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page).

LP EEE cap

Shows if the link partner is EEE capable.

EEE In power save

Shows if the system is currently saving power due to EEE. When EEE is enabled, the system will powered down if no frame has been received or transmitted in 5 uSec.

ActiPhy Savings

Shows if the system is currently saving power due to ActiPhy.

PerfectReach Savings

Shows if the system is currently saving power due to PerfectReach.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

OPTICAL SYSTEMS DESIGN

FAN STATUS

Monitor → **Green Ethernet** → **Fan**

This page provides an overview of information related to the fan control.

FAN STATUS

Fan Speed

Shows the speed that the fan is currently running at in RPM (Rounds Per Minute)

Temperature Sensor

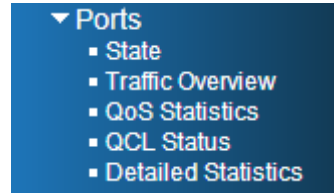
Shows the temperature of the temperature sensor(s) in Celsius degrees.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

PORTS



PORT STATE OVERVIEW

Monitor → Ports → State

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

The port states are illustrated as follows:



Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

 : Click to refresh the page immediately.

OPTICAL SYSTEMS DESIGN

PORT STATISTICS OVERVIEW

[Monitor](#) → [Ports](#) → [Traffic Overview](#)

Port Statistics Overview

Port	Description	Packets		Bytes		Errors		Drops		Filtered
		Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1		0	0	0	0	0	0	0	0	0
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		1946118	213667	295634615	28252572	0	0	0	0	492024
9		0	0	0	0	0	0	0	0	0
10		0	0	0	0	0	0	0	0	0
11		0	0	0	0	0	0	0	0	0
12		0	0	0	0	0	0	0	0	0
13		0	0	0	0	0	0	0	0	0
14		0	0	0	0	0	0	0	0	0

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

The displayed counters are:

Port

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

Description

The description of the port.

Packets

The number of received and transmitted packets per port.

Bytes

The number of received and transmitted bytes per port.

Errors

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

Drops

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

Filtered

The number of received frames filtered by the forwarding process.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Clears the counters for all ports.

: Click to refresh the page immediately.

OPTICAL SYSTEMS DESIGN

QUEUING COUNTERS

Monitor → Ports → QoS Statistics

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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
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	1945922	0	0	0	0	0	0	0	0	0	0	0	0	0	0	213650
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

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

The displayed counters are:

Port

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

Qn

There are 8 QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx

The number of received and transmitted packets per queue.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Clears the counters for all ports.

: Click to refresh the page immediately.

OPTICAL SYSTEMS DESIGN

QOS CONTROL LIST STATUS

Monitor → Ports → QCL Status

QoS Control List Status

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

Combined Auto-refresh

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

User

Indicates the QCL user.

QCE

Indicates the QCE id.

Port

Indicates the list of ports configured with the QCE.

Frame Type

Indicates the type of frame. Possible values are:

Any: Match any frame type.

Ethernet: Match EtherType frames.

LLC: Match (LLC) frames.

SNAP: Match (SNAP) frames.

IPv4: Match IPv4 frames.

IPv6: Match IPv6 frames.

Action

Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.

Possible actions are:

CoS: Classify Class of Service.

DPL: Classify Drop Precedence Level.

DSCP: Classify DSCP value.

PCP: Classify PCP value.

DEI: Classify DEI value.

Policy: Classify ACL Policy number.

Conflict

Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

OPTICAL SYSTEMS DESIGN

Buttons

: Select the QCL status from this drop down list.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.

: Clears the counters for all ports.

: Click to refresh the page immediately.

OPTICAL SYSTEMS DESIGN

DETAILED PORT STATISTICS PORT

Monitor → Ports → Detailed Statistics

Detailed Port Statistics Port 8 Port 8 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	1945194	Tx Packets	213544
Rx Octets	295511298	Tx Octets	28239649
Rx Unicast	96758	Tx Unicast	12142
Rx Multicast	708523	Tx Multicast	201399
Rx Broadcast	1139913	Tx Broadcast	3
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	275456	Tx 64 Bytes	7591
Rx 65-127 Bytes	1434183	Tx 65-127 Bytes	202090
Rx 128-255 Bytes	99620	Tx 128-255 Bytes	943
Rx 256-511 Bytes	36620	Tx 256-511 Bytes	1085
Rx 512-1023 Bytes	39018	Tx 512-1023 Bytes	249
Rx 1024-1526 Bytes	59297	Tx 1024-1526 Bytes	1586
Rx 1527 Bytes	0	Tx 1527 Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	1945194	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	213544
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	491855		

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

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

RECEIVE TOTAL AND TRANSMIT TOTAL

Rx and Tx Packets

The number of received and transmitted (good and bad) packets.

Rx and Tx Octets

The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

Rx and Tx Unicast

The number of received and transmitted (good and bad) unicast packets.

Rx and Tx Multicast

The number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast

The number of received and transmitted (good and bad) broadcast packets.

Rx and Tx Pause

A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

RECEIVE AND TRANSMIT SIZE COUNTERS

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

RECEIVE AND TRANSMIT QUEUE COUNTERS

The number of received and transmitted packets per input and output queue.

RECEIVE ERROR COUNTERS

Rx Drops

The number of frames dropped due to lack of receive buffers or egress congestion.

Rx CRC/Alignment

The number of frames received with CRC or alignment errors.

Rx Undersize

The number of short ¹ frames received with valid CRC.

Rx Oversize

The number of long ² frames received with valid CRC.

Rx Fragments

The number of short ¹ frames received with invalid CRC.

Rx Jabber

The number of long ² frames received with invalid CRC.

Rx Filtered

The number of received frames filtered by the forwarding process.

¹ Short frames are frames that are smaller than 64 bytes.

² Long frames are frames that are longer than the configured maximum frame length for this port.

TRANSMIT ERROR COUNTERS

Tx Drops

The number of frames dropped due to output buffer congestion.

Tx Late/Exc. Coll.

The number of frames dropped due to excessive or late collisions.

OPTICAL SYSTEMS DESIGN

Buttons

The port select box determines which port is affected by clicking the buttons.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Clears the counters for the selected port.

: Click to refresh the page immediately.

OPTICAL SYSTEMS DESIGN

LINK OAM

- ▼ Link OAM
 - Statistics
 - Port Status
 - Event Status

DETAILED LINK OAM STATISTICS FOR PORTS

[Monitor](#) → [Link OAM](#) → [Statistics](#)

Detailed Link OAM Statistics for Port 1

Port 1 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx OAM Information PDU's	0	Tx OAM Information PDU's	0
Rx Unique Error Event Notification	0	Tx Unique Error Event Notification	0
Rx Duplicate Error Event Notification	0	Tx Duplicate Error Event Notification	0
Rx Loopback Control	0	Tx Loopback Control	0
Rx Variable Request	0	Tx Variable Request	0
Rx Variable Response	0	Tx Variable Response	0
Rx Org Specific PDU's	0	Tx Org Specific PDU's	0
Rx Unsupported Codes	0	Tx Unsupported Codes	0
Rx Link Fault PDU's	0	Tx Link Fault PDU's	0
Rx Dying Gasp	0	Tx Dying Gasp	0
Rx Critical Event PDU's	0	Tx Critical Event PDU's	0

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

The displayed counters represent the total number of OAM frames received and transmitted for the selected port. Discontinuities of these counter can occur at re-initialization of the management system.

RECEIVE TOTAL AND TRANSMIT TOTAL

Rx and Tx OAM Information PDU's

The number of received and transmitted OAM Information PDU's. Discontinuities of this counter can occur at re-initialization of the management system.

Rx and Tx Unique Error Event Notification

A count of the number of unique Event OAMPDU's received and transmitted on this interface. Event Notifications may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. Duplicate Event Notification transmissions are counted by Duplicate Event Notification counters for Tx and Rx respectively. A unique Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is distinct from the previously transmitted Event Notification OAMPDU Sequence Number.

Rx and Tx Duplicate Error Event Notification

A count of the number of duplicate Event OAMPDU's received and transmitted on this interface. Event Notification OAMPDU's may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. A duplicate Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is identical to the previously transmitted Event Notification OAMPDU Sequence Number.

OPTICAL SYSTEMS DESIGN

Rx and Tx Loopback Control

A count of the number of Loopback Control OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Request

A count of the number of Variable Request OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Response

A count of the number of Variable Response OAMPDUs received and transmitted on this interface.

Rx and Tx Org Specific PDU's

A count of the number of Organization Specific OAMPDUs transmitted on this interface.

Rx and Tx Unsupported Codes

A count of the number of OAMPDUs transmitted on this interface with an unsupported op-code.

Rx and Tx Link fault PDU's

A count of the number of Link fault PDU's received and transmitted on this interface.

Rx and Tx Dying Gasp

A count of the number of Dying Gasp events received and transmitted on this interface.

Rx and Tx Critical Event PDU's

A count of the number of Critical event PDU's received and transmitted on this interface.

Buttons

The port select box determines which port is affected by clicking the buttons.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Clears the counters for the selected port.

: Click to refresh the page immediately.

OPTICAL SYSTEMS DESIGN

DETAILED LINK OAM STATUS FOR PORTS

Monitor → Link OAM → Port Status

Detailed Link OAM Status for Port 1

Port 1 Auto-refresh Refresh

PDU Permission	Receive only
Discovery State	Fault state
Peer MAC Address	-----

Local		Peer	
Mode	Passive	Mode	-----
Unidirectional Operation Support	Disabled	Unidirectional Operation Support	-----
Remote Loopback Support	Disabled	Remote Loopback Support	-----
Link Monitoring Support	Enabled	Link Monitoring Support	-----
MIB Retrieval Support	Disabled	MIB Retrieval Support	-----
MTU Size	1500	MTU Size	-----
Multiplexer State	Forwarding	Multiplexer State	-----
Parser State	Forwarding	Parser State	-----
Organizational Unique Identification	00-26-dc	Organizational Unique Identification	-----
PDU Revision	0	PDU Revision	-----

This page provides Link OAM configuration operational status.

The displayed fields shows the active configuration status for the selected port.

LOCAL AND PEER

Mode

The Mode in which the Link OAM is operating, Active or Passive.

Unidirectional Operation Support

This feature is not available to be configured by the user. The status of this configuration is retrieved from the PHY.

Remote Loopback Support

If status is enabled, DTE is capable of OAM remote loopback mode.

Link Monitoring Support

If status is enabled, DTE supports interpreting Link Events.

MIB Retrieval Support

If status is enabled DTE supports sending Variable Response OAMPDUs.

MTU Size

It represents the largest OAMPDU, in octets, supported by the DTE. This value is compared to the remotes Maximum PDU Size and the smaller of the two is used.

Multiplexer State

When in forwarding state, the Device is forwarding non-OAMPDUs to the lower sublayer. In case of discarding, the device discards all the non-OAMPDU's.

Parser State

When in forwarding state, Device is forwarding non-OAMPDUs to higher sublayer. When in loopback, Device is looping back non-OAMPDUs to the lower sublayer. When in discarding state, Device is discarding non-OAMPDUs.

Organizational Unique Identification

24-bit Organizationally Unique Identifier of the vendor.

OPTICAL SYSTEMS DESIGN

PDU Revision

It indicates the current revision of the Information TLV. The value of this field shall start at zero and be incremented each time something in the Information TLV changes. Upon reception of an Information TLV from a peer, an OAM client may use this field to decide if it needs to be processed (an Information TLV that is identical to the previous Information TLV doesn't need to be parsed as nothing in it has changed).

PDU Permission

This field is available only for the Local DTE. It displays the current permission rules set for the local DTE. Possible values are "Link fault", "Receive only", "Information exchange only", "ANY".

Discovery State

Displays the current state of the discovery process. Possible states are Fault state, Active state, Passive state, SEND_LOCAL_REMOTE_STATE, SEND_LOCAL_REMOTE_OK_STATE, SEND_ANY_STATE.

Buttons

The port select box determines which port is affected by clicking the buttons.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

OPTICAL SYSTEMS DESIGN

DETAILED LINK OAM LINK STATUS FOR PORTS

Monitor → Link OAM → Event Status

Detailed Link OAM Link Status for Port 1

Port 1 ▾ / Auto-refresh

Local Frame Error Status		Remote Frame Error Status	
Sequence Number	0		
Frame Error Event Timestamp	0	Frame Error Event Timestamp	0
Frame error event window	0	Frame error event window	0
Frame error event threshold	0	Frame error event threshold	0
Frame errors	0	Frame errors	0
Total frame errors	0	Total frame errors	0
Total frame error events	0	Total frame error events	0
Local Frame Period Status		Remote Frame Period Status	
Frame Period Error Event Timestamp	0	Frame Period Error Event Timestamp	0
Frame Period Error Event Window	0	Frame Period Error Event Window	0
Frame Period Error Event Threshold	0	Frame Period Error Event Threshold	0
Frame Period Errors	0	Frame Period Errors	0
Total frame period errors	0	Total frame period errors	0
Total frame period error events	0	Total frame period error events	0
Local Symbol Period Status		Remote Symbol Period Status	
Symbol Period Error Event Timestamp	0	Symbol Period Error Event Timestamp	0
Symbol Period Error Event Window	0	Symbol Period Error Event Window	0
Symbol Period Error Event Threshold	0	Symbol Period Error Event Threshold	0
Symbol Period Errors	0	Symbol Period Errors	0
Symbol frame period errors	0	Symbol frame period errors	0
Symbol frame period error events	0	Symbol frame period error events	0
Local Event Seconds Summary Status		Remote Event Seconds Summary Status	
Event Seconds Summary Time Stamp	0	Event Seconds Summary Time Stamp	0
Event Seconds Summary Window	0	Event Seconds Summary Window	0
Event Seconds Summary Threshold	0	Event Seconds Summary Threshold	0
Event Seconds Summary Events	0	Event Seconds Summary Events	0
Event Seconds Summary Error Total	0	Event Seconds Summary Error Total	0
Event Seconds Summary Event Total	0	Event Seconds Summary Event Total	0

This page allows the user to inspect the current Link OAM Link Event configurations, and change them as well.

The left pane displays the Event status for the Local OAM unit while the right pane displays the status for the Peer for the respective port.

Port

The switch port number.

Sequence Number

This two-octet field indicates the total number of events occurred at the remote end.

Frame Error Event Timestamp

This two-octet field indicates the time reference when the event was generated, in terms of 100ms intervals.

Frame error event window

This two-octet field indicates the duration of the period in terms of 100 ms intervals. 1) The default value is one second. 2) The lower bound is one second. 3) The upper bound is one minute.

Frame error event threshold

This four-octet field indicates the number of detected errored frames in the period is required to be equal to or greater than in order for the event to be generated. 1) The default value is one frame error. 2) The lower bound is zero frame errors. 3) The upper bound is unspecified.

Frame errors

This four-octet field indicates the number of detected errored frames in the period.

OPTICAL SYSTEMS DESIGN

Total frame errors

This eight-octet field indicates the sum of errored frames that have been detected since the OAM sublayer was reset.

Total frame error events

This four-octet field indicates the number of Errored Frame Event TLVs that have been generated since the OAM sublayer was reset.

Frame Period Error Event Timestamp

This two-octet field indicates the time reference when the event was generated, in terms of 100ms intervals.

Frame Period Error Event Window

This four-octet field indicates the duration of period in terms of frames.

Frame Period Error Event Threshold

This four-octet field indicates the number of errored frames in the period is required to be equal to or greater than in order for the event to be generated.

Frame Period Errors

This four-octet field indicates the number of frame errors in the period.

Total frame period errors

This eight-octet field indicates the sum of frame errors that have been detected since the OAM sublayer was reset.

Total frame period error events

This four-octet field indicates the number of Errored Frame Period Event TLVs that have been generated since the OAM sublayer was reset.

Symbol Period Error Event Timestamp

This two-octet field indicates the time reference when the event was generated, in terms of 100ms intervals.

Symbol Period Error Event Window

This eight-octet field indicates the number of symbols in the period.

Symbol Period Error Event Threshold

This eight-octet field indicates the number of errored symbols in the period is required to be equal to or greater than in order for the event to be generated.

Symbol Period Errors

This eight-octet field indicates the number of symbol errors in the period.

Symbol frame period errors

This eight-octet field indicates the sum of symbol errors since the OAM sublayer was reset.

Symbol frame period error events

This four-octet field indicates the number of Errored Symbol Period Event TLVs that have been generated since the OAM sublayer was reset.

Event Seconds Summary Time Stamp

This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

OPTICAL SYSTEMS DESIGN

Event Seconds Summary Window

This two-octet field indicates the duration of the period in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

Event Seconds Summary Threshold

This two-octet field indicates the number of errored frame seconds in the period is required to be equal to or greater than in order for the event to be generated, encoded as a 16-bit unsigned integer.

Event Seconds Summary Events

This two-octet field indicates the number of errored frame seconds in the period, encoded as a 16-bit unsigned integer.

Event Seconds Summary Error Total

This four-octet field indicates the sum of errored frame seconds that have been detected since the OAM sublayer was reset.

Event Seconds Summary Event Total

This four-octet field indicates the number of Errored Frame Seconds Summary Event TLVs that have been generated since the OAM sublayer was reset, encoded as a 32bit unsigned integer.

Buttons

The port select box determines which port is affected by clicking the buttons.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to clear the data.

: Click to refresh the page immediately.

DHCP

- ▼ DHCP
 - ▼ Server
 - Statistics
 - Binding
 - Declined IP
 - Snooping Table
 - Relay Statistics
 - Detailed Statistics

DHCP SERVER

DHCP Server Statistics

Monitor → DHCP → Server → Statistics

DHCP Server Statistics

Database Counters

Pool	Excluded IP Address	Declined IP Address
0	0	0

Binding Counters

Automatic Binding	Manual Binding	Expired Binding
0	0	0

DHCP Message Received Counters

DISCOVER	REQUEST	DECLINE	RELEASE	INFORM
0	0	0	0	0

DHCP Message Sent Counters

OFFER	ACK	NAK
0	0	0

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

DATABASE COUNTERS

Display counters of various databases.

Pool

Number of pools.

Excluded IP Address

Number of excluded IP address ranges.

Declined IP Address

Number of declined IP addresses.

BINDING COUNTERS

Display counters of various databases.

Automatic Binding

Number of bindings with network-type pools.

Manual Binding

Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type.

Expired Binding

Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.

DHCP MESSAGE RECEIVED COUNTERS

Display counters of DHCP messages received by DHCP server.

DISCOVER

Number of DHCP DISCOVER messages received.

REQUEST

Number of DHCP REQUEST messages received.

DECLINE

Number of DHCP DECLINE messages received.

RELEASE

Number of DHCP RELEASE messages received.

INFORM

Number of DHCP INFORM messages received.

OPTICAL SYSTEMS DESIGN

DHCP MESSAGE SENT COUNTERS

Display counters of DHCP messages sent by DHCP server.

OFFER

Number of DHCP OFFER messages sent.

ACK

Number of DHCP ACK messages sent.

NAK

Number of DHCP NAK messages sent.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to clear DHCP Message Received Counters and DHCP Message Sent Counters.

: Click to refresh the page immediately.

DHCP Server Binding IP

[Monitor](#) → [DHCP](#) → [Server](#) → [Binding](#)

DHCP Server Binding IP

Binding IP Address

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

This page displays bindings generated for DHCP clients.

BINDING IP ADDRESS

Display all bindings.

IP

IP address allocated to DHCP client.

Type

Type of binding. Possible types are Automatic, Manual, Expired.

State

State of binding. Possible states are Committed, Allocated, Expired.

Pool Name

The pool that generates the binding.

Server ID

Server IP address to service the binding.

OPTICAL SYSTEMS DESIGN

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh

: Click to refresh the page immediately.

Clear Selected

: Click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to be Expired. If the selected binding is expired, then it is freed.

Clear Automatic

: Click to clear all Automatic bindings and Change them to Expired bindings.

Clear Manual

: Click to clear all Manual bindings and Change them to Expired bindings.

Clear Expired

: Click to clear all Expired bindings and free them.

OPTICAL SYSTEMS DESIGN

DHCP Server Declined IP

[Monitor](#) → [DHCP](#) → [Server](#) → [Declined IP](#)

DHCP Server Declined IP

Declined IP Address

Declined IP

This page displays declined IP addresses.

DECLINED IP ADDRESSES

Display IP addresses declined by DHCP clients.

Declined IP

List of IP addresses declined.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh

: Click to refresh the page immediately.

OPTICAL SYSTEMS DESIGN

DHCP SNOOPING TABLE

Monitor → DHCP → Snooping Table

Dynamic DHCP Snooping Table

Start from MAC address , VLAN with entries per page.

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

This page display the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

NAVIGATING THE DHCP SNOOPING TABLE

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

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

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

DHCP SNOOPING TABLE COLUMNS

MAC Address

User MAC address of the entry..

VLAN ID

VLAN-ID in which the DHCP traffic is permitted.

Source Port

Switch Port Number for which the entries are displayed.

IP Address

User IP address of the entry.

IP Subnet Mask

User IP subnet mask of the entry.

DHCP Server Address


DHCP Server address of the entry.


Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

 : Click to clear HHCP Message Received Counters and DHCP Message Sent Counters.

 : Click to refresh the page immediately.

 : Updates the table starting from the first entry in the Dynamic DHCP snooping Table.

 : Updates the table entries, starting from the last entry currently displayed.

OPTICAL SYSTEMS DESIGN

DHCP RELAY STATISTICS

Monitor → DHCP → Relay Statistics

DHCP Relay Statistics

Server Statistics

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

Client Statistics

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

This page provides statistics for DHCP relay.

SERVER STATISTICS

Transmit To Server

The number of packets that are relayed from client to server.

Transmit Error

The number of packets that resulted in errors while being sent to clients.

Receive from Server

The number of packets received from server.

Receive Missing Agent Option

The number of packets received without agent information options.

Receive Missing Remote ID

The number of packets received with the Remote ID option missing.

Receive Bad Circuit

The number of packets whose Circuit ID option did not match known circuit ID.

Receive Bad Remote ID

The number of packets whose Remote ID option did not match known Remote ID.

SERVER STATISTICS

Transmit To Client

The number of relayed packets from server to client.

Transmit Error

The number of packets that resulted in error while being sent to servers.

OPTICAL SYSTEMS DESIGN

Receive from Client

The number of received packets from server.

Receive Agent Option

The number of received packets with relay agent information option.

Replace Agent Option

The number of packets which were replaced with relay agent information option.

Keep Agent Option

The number of packets whose relay agent information was retained.

Drop Agent Option

The number of packets that were dropped which were received with relay agent information

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

: Clear all statistics

OPTICAL SYSTEMS DESIGN

DHCP DETAILED STATISTICS PORT 1

Monitor → DHCP → Detailed Statistics

DHCP Detailed Statistics Port 1

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

Combined ▼ Port 1 ▼ Auto-refresh Refresh Clear

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

RECEIVE AND TRANSMIT PACKETS

Rx and Tx Discover

The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer

The number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request

The number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline

The number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK

The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK

The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release

The number of release (option 53 with value 7) packets received and transmitted

Rx and Tx Inform

The number of inform (option 53 with value 8) packets received and transmitted.

OPTICAL SYSTEMS DESIGN

Rx and Tx Lease Query

The number of lease query (option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned

The number of lease unassigned (option 53 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown

The number of lease unknown (option 53 with value 12) packets received and transmitted.

Rx and Tx Lease Active

The number of lease active (option 53 with value 13) packets received and transmitted.

Rx Discarded Checksum Error

The number of discard packet that IP/UDP checksum is error.

Rx Discarded from Untrusted

The number of discarded packet that are coming from untrusted port.

Buttons

The DHCP user select box determines which user is affected by clicking the buttons.

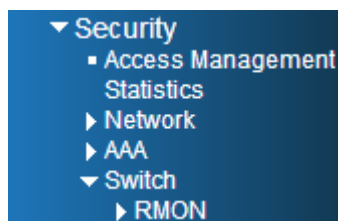
The port select box determines which port is affected by clicking the buttons.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

: Clear all statistics

SECURITY



ACCESS MANAGEMENT STATISTICS

Monitor → **Security** → **Access Management Statistics**

Access Management Statistics

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

This page provides statistics for access management.

Interface

The interface type through which the remote host can access the switch.

Received Packets

Number of received packets from the interface when access management mode is enabled.

Allowed Packets

Number of allowed packets from the interface when access management mode is enabled.

Discarded Packets

Number of discarded packets from the interface when access management mode is enabled.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

: Clear all statistics

OPTICAL SYSTEMS DESIGN

NETWORK

▼ Network
▶ Port Security
▶ NAS
▪ ACL Status
▪ ARP Inspection
▪ IP Source Guard

Port Security

▼ Port Security
▪ Switch
▪ Port

Port Security Switch Status

Monitor → Security → Network → Port Security → Switch

Port Security Switch Status

User Module Legend

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

Port Status

Port	Users	State	MAC Count	
			Current	Limit
<u>1</u>	---	Disabled	-	-
<u>2</u>	---	Disabled	-	-
<u>3</u>	---	Disabled	-	-
<u>4</u>	---	Disabled	-	-
<u>5</u>	---	Disabled	-	-
<u>6</u>	---	Disabled	-	-
<u>7</u>	---	Disabled	-	-
<u>8</u>	---	Disabled	-	-
<u>9</u>	---	Disabled	-	-
<u>10</u>	---	Disabled	-	-
<u>11</u>	---	Disabled	-	-
<u>12</u>	---	Disabled	-	-
<u>13</u>	---	Disabled	-	-
<u>14</u>	---	Disabled	-	-

OPTICAL SYSTEMS DESIGN

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.

USER MODULE LEGEND

The legend shows all user modules that may request Port Security services.

User Module Name

The full name of a module that may request Port Security services.

Abbr

A one-letter abbreviation of the user module. This is used in the Users column in the port status table.

PORT STATUS

The table has one row for each port on the switch and a number of columns, which are:

Port

The port number for which the status applies. Click the port number to see the status for this particular port.

Users

Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.

State

Shows the current state of the port. It can take one of four values:

Disabled: No user modules are currently using the Port Security service.

Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.

Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.

Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

OPTICAL SYSTEMS DESIGN

MAC Count (Current, Limit)

The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

If no user modules are enabled on the port, the Current column will show a dash (-).

If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

Port Security Port Status Ports

Monitor → Security → Network → Port Security → Port

Port Security Port Status Port 1

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

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.

MAC Address & VLAN ID

The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "*No MAC addresses attached*" is displayed.

State

Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition

Shows the date and time when this MAC address was first seen on the port.

Age/Hold

If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

OPTICAL SYSTEMS DESIGN

Buttons

: Use the port select box to select which port to show status for.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

NAS

- ▼ NAS
 - Switch
 - Port
 - ACL Status
 - ARP Inspection
 - IP Source Guard

Network Access Server Switch Status

[Monitor](#) → [Security](#) → [Network](#) → [NAS](#) → [Switch](#)

Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN 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			-	
9	Force Authorized	Globally Disabled			-	
10	Force Authorized	Globally Disabled			-	
11	Force Authorized	Globally Disabled			-	
12	Force Authorized	Globally Disabled			-	
13	Force Authorized	Globally Disabled			-	
14	Force Authorized	Globally Disabled			-	

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

Port

The switch port number. Click to navigate to detailed NAS statistics for this port.

Admin State

The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port State

The current state of the port. Refer to NAS Port State for a description of the individual states.

Last Source

The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

OPTICAL SYSTEMS DESIGN

Last ID

The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

QoS Class

QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID

The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs at Configuration→Security→Network→NAS.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs Configuration→Security→Network→NAS.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

NAS Statistics Ports

[Monitor](#) → [Security](#) → [Network](#) → [NAS](#) → [Port](#)

NAS Statistics Port 1

Port State

Admin State	Force Authorized
Port State	Globally Disabled

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.

PORT STATE

Admin State

The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port State

The current state of the port. Refer to NAS Port State for a description of the individual states.

QoS Class

The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

Port VLAN ID

The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, " (RADIUS-assigned) " is appended to the VLAN ID. Read more about RADIUS-assigned VLANs Configuration→Security→Network→NAS.

If the port is moved to the Guest VLAN, " (Guest) " is appended to the VLAN ID. Read more about Guest VLANs Configuration→Security→Network→NAS.

PORT COUNTERS

EAPOL Counters

These supplicant frame counters are available for the following administrative states:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

OPTICAL SYSTEMS DESIGN

EAPOL Counters			
Direction	Name	IEEE Name	Description
Rx	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	Response ID	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
Rx	Responses	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
Rx	Start	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	Logoff	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
Rx	Invalid Type	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	Invalid Length	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	Total	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	Request ID	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
Tx	Requests	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

Backend Server Counters

These backend (RADIUS) frame counters are available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

OPTICAL SYSTEMS DESIGN

Backend Server Counters			
Direction	Name	IEEE Name	Description
Rx	Access Challenges	dot1xAuthBackendAccessChallenges	<p>802.1X-based: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch.</p> <p>MAC-based: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).</p>
Rx	Other Requests	dot1xAuthBackendOtherRequestsToSupplicant	<p>802.1X-based: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method.</p> <p>MAC-based: Not applicable.</p>
Rx	Auth. Successes	dot1xAuthBackendAuthSuccesses	<p>802.1X- and MAC-based: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.</p>
Rx	Auth. Failures	dot1xAuthBackendAuthFails	<p>802.1X- and MAC-based: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.</p>
Tx	Responses	dot1xAuthBackendResponses	<p>802.1X-based: Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible</p>

OPTICAL SYSTEMS DESIGN

			retransmissions are not counted. MAC-based: Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.
--	--	--	---

Last Supplicant/Client Info

Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

Last Supplicant/Client Info		
Name	IEEE Name	Description
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
VLAN ID	-	The VLAN ID on which the last frame from the last supplicant/client was received.
Version	dot1xAuthLastEapolFrameVersion	802.1X-based: The protocol version number carried in the most recently received EAPOL frame. MAC-based: Not applicable.
Identity	-	802.1X-based: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. MAC-based: Not applicable.

SELECTED COUNTERS

Selected Counters

The Selected Counters table is visible when the port is in one of the following administrative states:

- Multi 802.1X
- MAC-based Auth.

The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.

OPTICAL SYSTEMS DESIGN

ATTACHED MAC ADDRESSES

Identity

Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows *No supplicants attached*. This column is not available for MAC-based Auth.

MAC Address

For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client. Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows *No clients attached*.

VLAN ID

This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.

State

The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.

Last Authentication

Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Buttons

: The port select box determines which port is affected when clicking the buttons.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

: This button is available in the following modes:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X

Click to clear the counters for the selected port.

OPTICAL SYSTEMS DESIGN

Clear All

: This button is available in the following modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however.

Clear This

: This button is available in the following modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear only the currently selected client's counters.

OPTICAL SYSTEMS DESIGN

ACL Status

[Monitor](#) → [Security](#) → [Network](#) → [ACL Status](#)

ACL Status

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

combined ▼ Auto-refresh Refresh

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 512 on each switch.

User

Indicates the ACL user.

ACE

Indicates the ACE ID on local switch.

Frame Type

Indicates the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

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

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

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

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

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

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

IPv6: The ACE will match all IPv6 standard frames.

Action

Indicates the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Filter: Frames matching the ACE are filtered.

Rate Limiter

Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

CPU

Forward packet that matched the specific ACE to CPU.

OPTICAL SYSTEMS DESIGN

Counter

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

Conflict

Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Buttons

: The select box determines which ACL user is affected by clicking the buttons.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

OPTICAL SYSTEMS DESIGN

Dynamic ARP Inspection Table

Monitor → **Security** → **Network** → **ARP Inspection**

Dynamic ARP Inspection Table

Start from Port 1, VLAN 1, MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	MAC Address	IP Address
No more entries			

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

NAVIGATING THE ARP INSPECTION TABLE

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

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

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

ARP INSPECTION TABLE COLUMNS

Port

Switch Port Number for which the entries are displayed.

VLAN ID

VLAN-ID in which the ARP traffic is permitted.

MAC Address

User MAC address of the entry.

IP Address

User IP address of the entry.

OPTICAL SYSTEMS DESIGN

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

: Flushes all dynamic entries

: Updates the table starting from the first entry in the Dynamic ARP Inspection Table

: Updates the table, starting with the entry after the last entry currently displayed.

OPTICAL SYSTEMS DESIGN

Dynamic IP Source Guard Table

[Monitor](#) → [Security](#) → [Network](#) → [IP Source Guard](#)

Dynamic IP Source Guard Table

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

Port	VLAN ID	IP Address	MAC Address
No more entries			

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

NAVIGATING THE IP SOURCE GUARD TABLE

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

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

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

IP SOURCE GUARD TABLE COLUMNS

Port

Switch Port Number for which the entries are displayed.

VLAN ID

VLAN-ID in which the IP traffic is permitted.

IP Address

User IP address of the entry.

MAC Address

Source MAC address.

OPTICAL SYSTEMS DESIGN

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

: Flushes all dynamic entries

: Updates the table starting from the first entry in the Dynamic ARP Inspection Table

: Updates the table, starting with the entry after the last entry currently displayed.

OPTICAL SYSTEMS DESIGN

AAA

- ▼ AAA
 - RADIUS Overview
 - RADIUS Details

RADIUS Server Status Overview

[Monitor](#) → [Security](#) → [AAA](#) → [RADIUS Overview](#)

RADIUS Server Status Overview

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

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

RADIUS SERVERS

#

The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address

The IP address of this server.

Authentication Port

UDP port number for authentication.

Authentication Status

The current status of the server. This field takes one of the following values:

Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but 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.

Accounting Port

UDP port number for accounting.

OPTICAL SYSTEMS DESIGN

Accounting Status

The current status of the server. This field takes one of the following values:

Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but 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.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

OPTICAL SYSTEMS DESIGN

RADIUS Authentication Statistics for Servers

[Monitor](#) → [Security](#) → [AAA](#) → [RADIUS Details](#)

RADIUS Authentication Statistics for Server #1

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

RADIUS Accounting Statistics for Server #1

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

Server #1 ▾ Auto-refresh Refresh Clear

This page provides detailed statistics for a particular RADIUS server.

RADIUS AUTHENTICATION STATISTICS

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS authentication server packet counter. There are seven receive and four transmit counters.

OPTICAL SYSTEMS DESIGN

Direction	Name	RFC4668 Name	Description
Rx	Access Accepts	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	Access Rejects	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	Access Challenges	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	Malformed Access Responses	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
Rx	Bad Authenticators	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	Unknown Types	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Rx	Packets Dropped	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx	Access Requests	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx	Access Retransmissions	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication

OPTICAL SYSTEMS DESIGN

			server.
Tx	Pending Requests	radiusAuthClientExtPendingRequests	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.
Tx	Timeouts	radiusAuthClientExtTimeouts	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.

Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4668 Name	Description
IP Address	-	IP address and UDP port for the authentication server in question.
State	-	Shows 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	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS

OPTICAL SYSTEMS DESIGN

		authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.
--	--	--

RADIUS ACCOUNTING STATISTICS

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB. Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS accounting server packet counter. There are five receive and four transmit counters.

Direction	Name	RFC4670 Name	Description
Rx	Responses	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	Malformed Responses	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.
Rx	Bad Authenticators	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	Unknown Types	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	Packets Dropped	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	Requests	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	Retransmissions	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	Pending Requests	radiusAccClientExtPendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
Tx	Timeouts	radiusAccClientExtTimeouts	The number of accounting

OPTICAL SYSTEMS DESIGN

			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.
--	--	--	--

Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4670 Name	Description
IP Address	-	IP address and UDP port for the accounting server in question.
State	-	Shows 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 accounting attempts. Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but 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	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Buttons

: The server select box determines which server is affected by clicking the buttons.

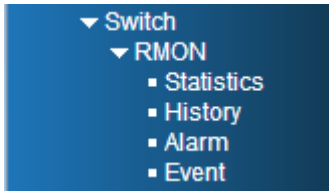
Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

: Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation

OPTICAL SYSTEMS DESIGN

SWITCH



RMON

RMON Statistics Status Overview

[Monitor](#) → [Security](#) → [Switch](#) → [RMON](#) → [Statistics](#)

RMON Statistics Status Overview

Start from Control Index with entries per page.

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

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

The "Start from Control Index" allows the user to select the starting point in the Statistics table. Clicking the button will update the displayed table starting from that or the next closest Statistics table match.

The 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 button to start over.

The displayed counters are:

ID

Indicates the index of Statistics entry.

Data Source(ifIndex)

The port ID which wants to be monitored.

Drop

The total number of events in which packets were dropped by the probe due to lack of resources.

OPTICAL SYSTEMS DESIGN

Octets

The total number of octets of data (including those in bad packets) received on the network.

Pkts

The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broad-cast

The total number of good packets received that were directed to the broadcast address.

Multi-cast

The total number of good packets received that were directed to a multicast address.

CRC Errors

The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Under-size

The total number of packets received that were less than 64 octets.

Over-size

The total number of packets received that were longer than 1518 octets.

Frag.

The number of frames which size is less than 64 octets received with invalid CRC.

Jabb.

The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.

The best estimate of the total number of collisions on this Ethernet segment.

64

The total number of packets (including bad packets) received that were 64 octets in length.

65~127

The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

128~255

The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

256~511

The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

512~1023

The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

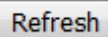
OPTICAL SYSTEMS DESIGN

1024~1588

The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

 Refresh

: Click to refresh the page immediately

 | <<

: Updates the table starting from the first entry in the Statistics Table, i.e. the entry with the lowest ID

 >>

: Updates the table, starting with the entry after the last entry currently displayed.

OPTICAL SYSTEMS DESIGN

RMON History Overview

[Monitor](#) → [Security](#) → [Switch](#) → [RMON](#) → [History](#)

RMON History Overview

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

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

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

The "Start from History Index and Sample Index" allows the user to select the starting point in the History table. Clicking the button will update the displayed table starting from that or the next closest History table match.

The 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 button to start over.

The displayed fields are:

History Index

Indicates the index of History control entry.

Sample Index

Indicates the index of the data entry associated with the control entry.

Sample Start

The value of sysUpTime at the start of the interval over which this sample was measured.

Drop

The total number of events in which packets were dropped by the probe due to lack of resources.

Octets

The total number of octets of data (including those in bad packets) received on the network.

Pkts

The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast

The total number of good packets received that were directed to the broadcast address.

OPTICAL SYSTEMS DESIGN

Multicast

The total number of good packets received that were directed to a multicast address.

CRCErrors

The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Undersize

The total number of packets received that were less than 64 octets.

Oversize

The total number of packets received that were longer than 1518 octets.

Frag.

The number of frames which size is less than 64 octets received with invalid CRC.

Jabb.

The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.

The best estimate of the total number of collisions on this Ethernet segment.

Utilization

The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

: Updates the table starting from the first entry in the Statistics Table, i.e. the entry with the lowest ID

: Updates the table, starting with the entry after the last entry currently displayed.

OPTICAL SYSTEMS DESIGN

RMON Alarm Overview

Monitor → **Security** → **Switch** → **RMON** → **Alarm**

RMON Alarm Overview

Start from Control Index with entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

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

The "Start from Control Index" allows the user to select the starting point in the Alarm table. Clicking the button will update the displayed table starting from that or the next closest Alarm table match.

The 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 button to start over.

The displayed fields are:

ID

Indicates the index of Alarm control entry.

Interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

Variable

Indicates the particular variable to be sampled

Sample Type

The method of sampling the selected variable and calculating the value to be compared against the thresholds.

Value

The value of the statistic during the last sampling period.

Startup Alarm

The alarm that may be sent when this entry is first set to valid.

OPTICAL SYSTEMS DESIGN

Rising Threshold

Rising threshold value.

Rising Index

Rising event index.

Falling Threshold

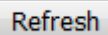
Falling threshold value.

Falling Index

Falling event index.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

 Refresh

: Click to refresh the page immediately

 | <<

: Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID

 >>

: Updates the table, starting with the entry after the last entry currently displayed.

RMON Event Overview

Monitor → Security → Switch → RMON → Event

RMON Event Overview

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

Event Index	LogIndex	LogTime	LogDescription
No more entries			

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

The "Start from Event Index and Log Index" allows the user to select the starting point in the Event table. Clicking the button will update the displayed table starting from that or the next closest Event table match.

The 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 button to start over.

The displayed fields are:

Event Index

Indicates the index of the event entry.

Log Index

Indicates the index of the log entry.

LogTime

Indicates Event log time

LogDescription

Indicates the Event description.

OPTICAL SYSTEMS DESIGN

Buttons

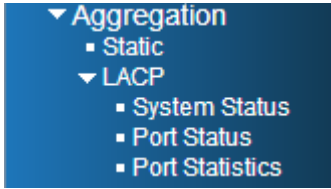
Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

: Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest ID

: Updates the table, starting with the entry after the last entry currently displayed.

AGGREGATION



AGGREGATION STATUS

Monitor → Aggregation → Static

Aggregation Status

Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports
No aggregation groups					

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

AGGREGATION GROUP STATUS

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

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

OPTICAL SYSTEMS DESIGN

LACP

LACP System Status

[Monitor](#) → [Aggregation](#) → [LACP](#) → [System Status](#)

LACP System Status

Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
<i>No ports enabled or no existing partners</i>					

This page provides a status overview for all LACP instances.

Aggr ID

The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'

Partner System ID

The system ID (MAC address) of the aggregation partner.

Partner Key

The Key that the partner has assigned to this aggregation ID.

Last changed

The time since this aggregation changed.

Local Ports

Shows which ports are a part of this aggregation for this switch.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

OPTICAL SYSTEMS DESIGN

LACP Status

Monitor → Aggregation → LACP → Port Status

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	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-
11	No	-	-	-	-	-
12	No	-	-	-	-	-
13	No	-	-	-	-	-
14	No	-	-	-	-	-

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

Port

The switch port number.

LACP

'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile its LACP status is disabled.

Key

The key assigned to this port. Only ports with the same key can aggregate together.

Aggr ID

The Aggregation ID assigned to this aggregation group.

Partner System ID

The partner's System ID (MAC address).

Partner Port

The partner's port number connected to this port.

Partner Prio

The partner's port priority.

OPTICAL SYSTEMS DESIGN

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

OPTICAL SYSTEMS DESIGN

LACP Statistics

Monitor → Aggregation → LACP → Port 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
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0

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

Port

The switch port number.

LACP Received

Shows how many LACP frames have been received at each port.

LACP Transmitted

Shows how many LACP frames have been sent from each port.

Discarded

Shows how many unknown or illegal LACP frames have been discarded at each port.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

: Clears the counters for the selected server. The “Pending Requests” counter will not be cleared by this operation

LOOP PROTECTION STATUS

▪ Loop Protection

Monitor → Loop Protection

Loop Protection Status

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

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

Loop protection port status is:

Port

The switch port number of the logical port.

Action

The currently configured port action.

Transmit

The currently configured port transmit mode.

Loops

The number of loops detected on this port.

Status

The current loop protection status of the port.

Loop

Whether a loop is currently detected on the port.

Time of Last Loop

The time of the last loop event detected.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

OPTICAL SYSTEMS DESIGN

SPANNING TREE

- ▼ Spanning Tree
 - Bridge Status
 - Port Status
 - Port Statistics

STP BRIDGES

[Monitor](#) → [Spanning Tree](#) → [Bridge Status](#)

STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-26-DC-00-07-61	32768.00-26-DC-00-07-61	-	0	Steady	0d 20:19:10

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

The displayed table contains a row for each STP bridge instance, where the column displays the following information:

MSTI

The Bridge Instance. This is also a link to the STP Detailed Bridge Status.

Bridge ID

The Bridge ID of this Bridge instance.

Root ID

The Bridge ID of the currently elected root bridge.

Root Port

The switch port currently assigned the *root* port role.

Root Cost

Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology Flag

The current state of the Topology Change Flag of this Bridge instance.

Topology Change Last

The time since last Topology Change occurred.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

OPTICAL SYSTEMS DESIGN

STP PORT STATUS

Monitor → Spanning Tree → Port Status

STP Port Status

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	DesignatedPort	Forwarding	6d 05:24:07
9	Disabled	Discarding	-
10	Disabled	Discarding	-
11	Disabled	Discarding	-
12	Disabled	Discarding	-
13	Disabled	Discarding	-
14	Disabled	Discarding	-

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

STP port status is:

Port

The switch port number of the logical STP port.

CIST Role

The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort BackupPort RootPort DesignatedPort Disabled.

CIST State

The current STP port state of the CIST port. The port state can be one of the following values: Discarding Learning Forwarding.

Uptime

The time since the bridge port was last initialized.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

OPTICAL SYSTEMS DESIGN

STP STATISTICS

Monitor → Spanning Tree → Port Statistics

STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
8	268905	0	0	0	227920	12489	0	0	0	0

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

The STP port statistics counters are:

Port

The switch port number of the logical STP port.

MSTP

The number of MSTP BPDU's received/transmitted on the port.

RSTP

The number of RSTP BPDU's received/transmitted on the port.

STP

The number of legacy STP Configuration BPDU's received/transmitted on the port.

TCN

The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.

Discarded Unknown

The number of unknown Spanning Tree BPDU's received (and discarded) on the port.

Discarded Illegal

The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

OPTICAL SYSTEMS DESIGN

MVR

- ▼ MVR
 - Statistics
 - MVR Channel Groups
 - MVR SFM Information

MVR STATISTICS

Monitor → MVR → Statistics

MVR Statistics

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

This page provides MVR Statistics information.

VLAN ID

The Multicast VLAN ID.

IGMP/MLD Queries Received

The number of Received Queries for IGMP and MLD, respectively.

IGMP/MLD Queries Transmitted

The number of Transmitted Queries for IGMP and MLD, respectively.

IGMPv1 Joins Received

The number of Received IGMPv1 Join's.

IGMPv2/MLDv1 Report's Received

The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.

IGMPv3/MLDv2 Report's Received

The number of Received IGMPv1 Join's and MLDv2 Report's, respectively.

IGMPv2/MLDv1 Leave's Received

The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

: Clears all Statistics counters

OPTICAL SYSTEMS DESIGN

MVR CHANNELS (GROUPS) INFORMATION

Monitor → **MVR** → **MVR Channel Groups**

MVR Channels (Groups) Information

Start from VLAN and Group Address with entries per page.

		Port Members													
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14
No more entries															

Entries in the MVR Channels (Groups) Information Table are shown on this page. The MVR Channels (Groups) Information Table is sorted first by VLAN ID, and then by group.

NAVIGATING THE MVR CHANNELS (GROUPS) INFORMATION TABLE

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

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

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

MVR CHANNELS (GROUPS) INFORMATION TABLE COLUMNS

VLAN ID

VLAN ID of the group.

Groups

Group ID of the group displayed.

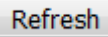
Port Members

Ports under this group.

OPTICAL SYSTEMS DESIGN

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

 Refresh

: Refreshes the displayed table starting from the input fields

 | <<

: Updates the table starting from the first entry in the MVR Channels (Groups) Information Table

 >>

: Updates the table, starting with the entry after the last entry currently displayed.

OPTICAL SYSTEMS DESIGN

MVR SFM INFORMATION

Monitor → MVR → MNV SFM Information

MVR SFM Information

Start from VLAN and Group Address with entries per page.

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

Entries in the MVR SFM Information Table are shown on this page. The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

NAVIGATING THE MVR SFM INFORMATION TABLE

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

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

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

MVR SFM INFORMATION TABLE COLUMNS

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

Port

Switch port number.

Mode

Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

OPTICAL SYSTEMS DESIGN

Source Address

IP Address of the source.

Currently, the maximum number of IP source address for filtering (per group) is 8.

When there is no any source filtering address, the text "None" is shown in the Source Address field.

Type

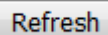
Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch

Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

 Refresh

: Refreshes the displayed table starting from the input fields

 | <<

: Updates the table starting from the first entry in the MVR Channels (Groups) Information Table

 >>

: Updates the table, starting with the entry after the last entry currently displayed.

IPMC



IGMP SNOOPING

IGMP Snooping Status

[Monitor](#) → [IPMC](#) → [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	-
9	-
10	-
11	-
12	-
13	-
14	-

This page provides IGMP Snooping status.

VLAN ID

The VLAN ID of the entry.

Querier Version

Working Querier Version currently.

OPTICAL SYSTEMS DESIGN

Host Version

Working Host Version currently.

Querier Status

Shows the Querier status is "ACTIVE" or "IDLE".
"DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted

The number of Transmitted Queries.

Queries Received

The number of Received Queries.

V1 Reports Received

The number of Received V1 Reports.

V2 Reports Received

The number of Received V2 Reports.

V3 Reports Received

The number of Received V3 Reports.

V2 Leaves Received

The number of Received V2 Leaves.

Router Port

Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

Both denote the specific port is configured or learnt to be a router port.

Port

Switch port number.

Status

Indicate whether specific port is a router port or not.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

: Clears all Statistics counters

IGMP Snooping Group Information

Monitor → IPMC → IGMP Snooping → Groups Information

IGMP Snooping Group Information

Start from VLAN and group address with entries per page.

		Port Members													
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14
No more entries															

Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group.

NAVIGATING THE IGMP GROUP TABLE

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

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

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

IGMP GROUP TABLE COLUMNS

VLAN ID

VLAN ID of the group.

Groups

Group address of the group displayed.

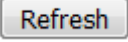
Port Members


Ports under this group.


OPTICAL SYSTEMS DESIGN

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

 : Refreshes the displayed table starting from the input fields

 : Updates the table starting from the first entry in the MVR Channels (Groups) Information Table

 : Updates the table, starting with the entry after the last entry currently displayed

OPTICAL SYSTEMS DESIGN

IGMP SFM Information

[Monitor](#) → [IPMC](#) → [IGMP Snooping](#) → [IP4V SFM Information](#)

IGMP SFM Information

Start from VLAN and Group with entries per page.

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

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

NAVIGATING THE IGMP SFM INFORMATION TABLE

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

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

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

IGMP SFM INFORMATION TABLE COLUMNS

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

Port

Switch port number.

Mode

Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

OPTICAL SYSTEMS DESIGN

Source Address

IP Address of the source.

Currently, the maximum number of IPv4 source address for filtering (per group) is 8.

When there is no any source filtering address, the text "None" is shown in the Source Address field.

Type

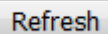
Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch

Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

 Refresh

: Refreshes the displayed table starting from the input fields

 | <<

: Updates the table starting from the first entry in the IGMP SFM Information Table

 >>

: Updates the table, starting with the entry after the last entry currently displayed

OPTICAL SYSTEMS DESIGN

MLD SNOOPING

MLD Snooping Status

Monitor → IPMC → MLD Snooping → Status

MLD Snooping Status

Statistics

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

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-

This page provides MLD Snooping status.

VLAN ID

The VLAN ID of the entry.

Querier Version

Working Querier Version currently.

Host Version

Working Host Version currently.

Querier Status

Shows the Querier status is "ACTIVE" or "IDLE".
"DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted

The number of Transmitted Queries.

Queries Received

The number of Received Queries.

OPTICAL SYSTEMS DESIGN

V1 Reports Received

The number of Received V1 Reports.

V2 Reports Received

The number of Received V2 Reports.

V1 Leaves Received

The number of Received V1 Leaves.

Router Port

Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

Both denote the specific port is configured or learnt to be a router port.

Port

Switch port number.

Status

Indicate whether specific port is a router port or not.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

: Clears all Statistics counters

OPTICAL SYSTEMS DESIGN

MLD Snooping Group Information

Monitor → IPMC → MLD Snooping → Groups Information

MLD Snooping Group Information

Start from VLAN and group address with entries per page.

		Port Members													
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14
No more entries															

Entries in the MLD Group Table are shown on this page. The MLD Group Table is sorted first by VLAN ID, and then by group.

NAVIGATING THE MLD GROUP TABLE

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

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

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

MLD GROUP TABLE COLUMNS

VLAN ID

VLAN ID of the group.

Groups

Group address of the group displayed.

Port Members

Ports under this group.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Refreshes the displayed table starting from the input fields

: Updates the table starting from the first entry in the MLD Group Table

: Updates the table, starting with the entry after the last entry currently displayed

OPTICAL SYSTEMS DESIGN

MLD SFM Information

[Monitor](#) → [IPMC](#) → [MLD Snooping](#) → [IPv6 SFM Information](#)

MLD SFM Information

Start from VLAN and Group with entries per page.

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

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

NAVIGATING THE MLD SFM INFORMATION TABLE

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

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

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

MLD SFM INFORMATION TABLE COLUMNS

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

Port

Switch port number.

Mode

Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

OPTICAL SYSTEMS DESIGN

Source Address

IP Address of the source.

Currently, the maximum number of IPv6 source address for filtering (per group) is 8.

When there is no any source filtering address, the text "None" is shown in the Source Address field.

Type

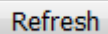
Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch

Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

 Refresh

: Refreshes the displayed table starting from the input fields

 | <<

: Updates the table starting from the first entry in the MLD SFM Table

 >>

: Updates the table, starting with the entry after the last entry currently displayed

OPTICAL SYSTEMS DESIGN

LLDP



LLDP NEIGHBOUR INFORMATION

Monitor → LLDP → Neighbours

LLDP Neighbor Information

LLDP Remote Device Summary						
Local Interface	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
No neighbor information found						

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

Local Interface

The interface on which the LLDP frame was received.

Chassis ID

The identification of the neighbor's LLDP frames.

Port ID

The identification of the neighbor port.

Port Description

The port description advertised by the neighbor unit.

System Name

The name advertised by the neighbor unit.

System Capabilities

Describes the neighbour unit's capabilities. The possible capabilities are:

1. Other
2. Repeater
3. Bridge
4. WLAN Access Point
5. Router

OPTICAL SYSTEMS DESIGN

- 6. Telephone
- 7. DOCSIS cable device
- 8. Station only
- 9. Reserved

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

Management Address

The neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh this page

LLDP-MED NEIGHBOUR INFORMATION

Monitor → LLDP → LLDP-MED Neighbours

LLDP-MED Neighbor Information

Local Interface
No LLDP-MED neighbor information found

This page provides a status overview of all LLDP-MED neighbours. The displayed table contains a row for each interface on which an LLDP neighbour is detected. This function applies to VoIP devices which support LLDP-MED. The columns hold the following information:

Interface

The interface on which the LLDP frame was received.

Device Type

LLDP-MED Devices are comprised of two primary **Device Types**: Network Connectivity Devices and Endpoint Devices.

LLDP-MED Network Connectivity Device Definition

LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

1. LAN Switch/Router
2. IEEE 802.1 Bridge
3. IEEE 802.3 Repeater (included for historical reasons)
4. IEEE 802.11 Wireless Access Point
5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

LLDP-MED Endpoint Device Definition

LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.

Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

LLDP-MED Generic Endpoint (Class I)

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

LLDP-MED Media Endpoint (Class II)

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.

Discovery services defined in this class include media-type-specific network layer policy discovery.

LLDP-MED Communication Endpoint (Class III)

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.

LLDP-MED Capabilities

LLDP-MED Capabilities describes the neighbour unit's LLDP-MED capabilities. The possible capabilities are:

1. LLDP-MED capabilities
2. Network Policy
3. Location Identification
4. Extended Power via MDI - PSE
5. Extended Power via MDI - PD
6. Inventory
7. Reserved

OPTICAL SYSTEMS DESIGN

Application Type

Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.

1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media.
3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.
5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.
6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.

Policy

Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown

Unknown: The network policy for the specified application type is currently unknown.

Defined: The network policy is defined (known).

TAG

TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged.

Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.

Tagged: The device is using the IEEE 802.1Q tagged frame format.

OPTICAL SYSTEMS DESIGN

VLAN ID

VLAN ID is the VLAN identifier (VID) for the interface as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress interface is used instead.

Priority

The Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).

DSCP

The DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

Auto-negotiation

Identifies if MAC/PHY auto-negotiation is supported by the link partner.

Auto-negotiation status

Identifies if auto-negotiation is currently enabled at the link partner. If **Auto-negotiation** is supported and **Auto-negotiation status** is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.

Auto-negotiation Capabilities

Shows the link partners MAC/PHY capabilities.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh this page

OPTICAL SYSTEMS DESIGN

LLDP NEIGHBOURS EEE INFORMATION

Monitor → LLDP → EEE

LLDP Neighbors EEE Information

Local Interface	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								

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

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

LLDP NEIGHBORS EEE INFORMATION

The displayed table contains a row for each interface.

If the interface does not supports EEE, then it displays as "EEE not supported for this interface".

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

If the link partner doesn't supports EEE, then it displays as "Link partner is not EEE capable.

The columns hold the following information:

Local Interface

The interface at which LLDP frames are received or transmitted.

Tx Tw

The link partner's maximum time that transmit path can hold-off sending data after deassertion of LPI.

Rx Tw

The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.

Fallback Receive Tw

The link partner's fallback receive Tw.

A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.

OPTICAL SYSTEMS DESIGN

Echo Tx Tw

The link partner's Echo Tx Tw value.

The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.

Echo Rx Tw

The link partner's Echo Rx Tw value.

Resolved Tx Tw

The resolved Tx Tw for this link. Note : NOT the link partner

The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

Resolved Rx Tw

The resolved Rx Tw for this link. Note : NOT the link partner

The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

EEE in Sync

Shows whether the switch and the link partner have agreed on wake times.

Red - Switch and link partner have not agreed on wakeup times.

Green - Switch and link partner have agreed on wakeup times.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh this page

OPTICAL SYSTEMS DESIGN

LLDP GLOBAL COUNTERS AND STATISTICS LOCAL COUNTERS

Monitor → LLDP → Port Statistics

LLDP Global Counters

Global Counters	
Clear global counters	<input checked="" type="checkbox"/>
Neighbor entries were last changed	1970-01-01T00:00:00+00:00 (551669 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 Interface	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs	Clear
GigabitEthernet 1/1	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/2	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/3	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/4	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/5	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/6	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/7	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/8	18396	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/9	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/10	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/11	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/12	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/13	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
2.5GigabitEthernet 1/1	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>

This page provides an overview of all LLDP traffic.

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

GLOBAL COUNTERS

Clear global counters

If checked the global counters are cleared when is pressed.

Neighbor entries were last changed

Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

Total Neighbors Entries Added

Shows the number of new entries added since switch reboot.

Total Neighbors Entries Deleted

Shows the number of new entries deleted since switch reboot.

Total Neighbors Entries Dropped

Shows the number of LLDP frames dropped due to the entry table being full.

Total Neighbors Entries Aged Out

Shows the number of entries deleted due to Time-To-Live expiring.

LOCAL COUNTERS

The displayed table contains a row for each interface. The columns hold the following information:

Local Interface

The interface on which LLDP frames are received or transmitted.

Tx Frames

The number of LLDP frames transmitted on the interface.

Rx Frames

The number of LLDP frames received on the interface.

Rx Errors

The number of received LLDP frames containing some kind of error.

Frames Discarded

If a LLDP frame is received on a interface, 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 interface's link is down, an LLDP shutdown frame is received, or when the entry ages out.

TLVs Discarded

Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized

The number of well-formed TLVs, but with an unknown type value.

Org. Discarded

If LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted.

Age-Outs

Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the **Age-Out** counter is incremented.

Clear

If checked the counters for the specific interface are cleared when is pressed.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

: Clears all Statistics counters

PTP

• PTP

Monitor → PTP

PTP External Clock Mode

One PPS Mode	Disable
External Enable	False
Adjust Method	LTC frequency
Clock Frequency	1

PTP Clock Configuration

Inst	Device Type	Port List													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
No Clock Instances Present															

This page allows the user to inspect the current PTP clock settings.

PTP EXTERNAL CLOCK DESCRIPTION

One_PPS_Mode

Shows the current One_pps_mode configured.

1. Output : Enable the 1 pps clock output
2. Input : Enable the 1 pps clock input
3. Disable : Disable the 1 pps clock in/out-put

External Enable

Shows the current External clock output configuration.

1. True : Enable the external clock output
2. False : Disable the external clock output

Adjust Method

Shows the current Frequency adjustment configuration.

1. LTC frequency : Local Time Counter (LTC) frequency control
2. SyncE-DPLL : SyncE DPLL frequency control, if allowed by SyncE
3. Oscillator : Oscillator independent of SyncE for frequency control, if supported by the HW
4. LTC phase : Local Time Counter (LTC) phase control (assumes that the frequency is locked by means of SyncE)

Clock Frequency

Shows the current clock frequency used by the External Clock.

The possible range of values are 1 - 25000000 (1 - 25MHz)

PTP CLOCK DESCRIPTION

Inst

Indicates the Instance of a particular Clock Instance [0..3].
Click on the Clock Instance number to monitor the Clock details.

ClkDom

Indicates the Clock domain used by the Instance of a particular Clock Instance [0..3].

Device Type

Indicates the Type of the Clock Instance. There are five Device Types.

1. Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock.
2. P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock.
3. E2e Transp - Clock's Device Type is End to End Transparent Clock.
4. Master Only - Clock's Device Type is Master Only.
5. Slave Only - Clock's Device Type is Slave Only.

Port List

Shows the ports configured for that Clock Instance.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

NAVIGATING THE MAC TABLE

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

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

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

MAC TABLE COLUMNS

Type

Indicates whether the entry is a static or a dynamic entry.

MAC address

The MAC address of the entry.

VLAN

The VLAN ID of the entry.

Port Members

The ports that are members of the entry.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields

: Flushes all dynamic entries

: Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address

: Updates the table, starting with the entry after the last entry currently displayed

OPTICAL SYSTEMS DESIGN

VLANS

- ▼ VLANS
 - Membership
 - Ports

VLAN MEMBERSHIP STATUS FOR COMBINED USERS

Monitor → VLANS → Membership

VLAN Membership Status for Combined users

Start from VLAN with entries per page.

VLAN ID	Port Members													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

This page provides an overview of membership status of VLAN users.

VLAN User

Various internal software modules may use VLAN services to configure VLAN memberships on the fly.

The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.

The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

VLAN ID

VLAN ID for which the Port members are displayed.

Port Members

A row of check boxes for each port is displayed for each VLAN ID.

If a port is included in a VLAN, the following image will be displayed: .

If a port is in the forbidden port list, the following image will be displayed: .

If a port is in the forbidden port list and at the same time attempted included in the VLAN, the following image will be displayed: . The port will not be a member of the VLAN in this case.

NAVIGATING THE VLAN MEMBERSHIP STATUS PAGE

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

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

OPTICAL SYSTEMS DESIGN

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

Buttons

: Select VLAN Users from this drop down list.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

OPTICAL SYSTEMS DESIGN

VLAN PORT STATUS FOR COMBINED USERS

Monitor → VLANs → Ports

VLAN Port Status for Combined users

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

This page provides VLAN Port Status.

VLAN User

Various internal software modules may use VLAN services to configure VLAN port configuration on the fly.

The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.

The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

If a given software modules hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table.

Port

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

Port Type

Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port.) that a given user wants to configure on the port.

The field is empty if not overridden by the selected user.

Ingress Filtering

Shows whether a given user wants ingress filtering enabled or not.

The field is empty if not overridden by the selected user.

Frame Type

Shows the acceptable frame types (All, Taged, Untagged) that a given user wants to configure on the port.

The field is empty if not overridden by the selected user.

OPTICAL SYSTEMS DESIGN

Port VLAN ID

Shows the Port VLAN ID (PVID) that a given user wants the port to have.
The field is empty if not overridden by the selected user.

Tx Tag

Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port.
The field is empty if not overridden by the selected user.

Untagged VLAN ID

If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field will show the VLAN ID the user wants to tag or untag on egress.
The field is empty if not overridden by the selected user.

Conflicts

Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress.

Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list: The higher in the list, the higher priority.

If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module.

The "Combined" user reflects what is actually configured in hardware.

Buttons

: Select VLAN Users from this drop down list.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

OPTICAL SYSTEMS DESIGN

SFLOW

▪ sFlow

SFLOW STATISTICS

Monitor → sFlow

sFlow Statistics

Receiver Statistics

Owner	<none>
IP Address/Hostname	0.0.0.0
Timeout	0
Tx Successes	0
Tx Errors	0
Flow Samples	0
Counter Samples	0

Port Statistics

Port	Flow Samples	Counter Samples
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0

This page shows receiver and per-port sFlow statistics.

RECEIVER STATISTICS

Owner

This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
- If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.

OPTICAL SYSTEMS DESIGN

IP Address/Hostname

The IP address or hostname of the sFlow receiver.

Timeout

The number of seconds remaining before sampling stops and the current sFlow owner is released.

Tx Successes

The number of UDP datagrams successfully sent to the sFlow receiver.

Tx Errors

The number of UDP datagrams that has failed transmission.

The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics → Ping/Ping6).

Flow Samples

The total number of flow samples sent to the sFlow receiver.

Counter Samples

The total number of counter samples sent to the sFlow receiver.

PORT STATISTICS

Port

The port number for which the following statistics applies.

Flow Samples

The number of flow samples sent to the sFlow receiver originating from this port.

Counter Samples

The total number of counter samples sent to the sFlow receiver originating from this port.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh

: Click to refresh the page immediately

Clear Receiver

: Clears the sFlow receiver counters

Clear Ports

: Clears the per-port counters

OPTICAL SYSTEMS DESIGN

UDLD

• UDLD

DETAILED UDLD STATUS FOR PORTS

Monitor → UDLD

Detailed UDLD Status for Port 1

UDLD status	
UDLD Admin state	Disable
Device ID(local)	00-26-DC-00-07-61
Device Name(local)	-
Bidirectional State	Indeterminant

Neighbour Status

Port	Device Id	Link Status	Device Name
<i>No Neighbour ports enabled or no existing partners</i>			

This page displays the UDLD status of the ports

UDLD PORT STATUS

UDLD Admin State

The current port state of the logical port, Enabled if any of state (Normal, Aggressive) is Enabled.

Device ID(local)

The ID of Device.

Device Name(local)

Name of the Device.

Bidirectional State

The current state of the port.

NEIGHBOUR STATUS

Port

The current port of neighbor device.

Device ID

The current ID of neighbor device.

OPTICAL SYSTEMS DESIGN

Link Status

The current link status of neighbor port.

Device Name

Name of the Neighbor Device.

Buttons

: The port select box determines which port is affected by clicking the buttons.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately

OPTICAL SYSTEMS DESIGN

ALARM

▪ Alarm

PROGRAMMABLE ALARM

Monitor → Alarm

Programmable Alarm

Alarm Alarm1 ▾

Alarm Status

Alarm	State
Alarm1	Inactive

Link Alarm Status

Port	Link Alarm Setting	Enable	Status	Active	Alarm Time
1	Link down	Disable	Link down	Inactive	--
2	Link down	Disable	Link down	Inactive	--
3	Link down	Disable	Link down	Inactive	--
4	Link down	Disable	Link down	Inactive	--
5	Link down	Disable	Link down	Inactive	--
6	Link down	Disable	Link down	Inactive	--
7	Link down	Disable	Link down	Inactive	--
8	Link down	Disable	Link down	Inactive	--
9	Link down	Disable	Link down	Inactive	--
10	Link down	Disable	Link down	Inactive	--
11	Link down	Disable	Link down	Inactive	--
12	Link down	Disable	Link down	Inactive	--
13	Link down	Disable	Link down	Inactive	--
14	Link down	Disable	Link down	Inactive	--
15	Link down	Disable	Link down	Inactive	--
16	Link down	Disable	Link down	Inactive	--
17	Link down	Disable	Link down	Inactive	--
18	Link down	Disable	Link down	Inactive	--
19	Link down	Disable	Link down	Inactive	--
20	Link down	Disable	Link down	Inactive	--
21	Link down	Disable	Link down	Inactive	--
22	Link down	Disable	Link down	Inactive	--
23	Link down	Disable	Link down	Inactive	--
24	Link down	Disable	Link up	Inactive	--
25	Link down	Disable	Link down	Inactive	--
26	Link down	Disable	Link down	Inactive	--
27	Link down	Disable	Link down	Inactive	--
28	Link down	Disable	Link down	Inactive	--

Temperature Alarm Status

ID	Alarm Temperature	Enable	Current Temperature	Active	Alarm Time
1	--	Disable	--	Inactive	--

OPTICAL SYSTEMS DESIGN

This page displays the current status of the Alarm

ALARM

Select the Alarm output number to see its status.

ALARM STATUS

Shows the current alarm's state. It will display "Active" when the alarm is triggered.

LINK ALARM STATUS

Port

Port number.

Link Alarm Setting

Shows the current link alarm setting.

Enable

Shows if the triggering state is enabled/disabled.

Status

Current port link status.

Active

Current link alarm trigger status.

Alarm Time

Time when the alarm triggered.

TEMPERATURE ALARM STATUS

Alarm Temperature

Temperature setting for the alarm to trigger.

Enable

Shows if the alarm is Enabled/Disabled.

Current Temperature

Current temperature of the board.

Active

Shows the temperature alarm status.

Alarm Time

Time when the temperature alarm triggered.

OPTICAL SYSTEMS DESIGN

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Refreshes the page

: Clear the Alarm selected

5.4 DIAGNOSTICS

PING

▪ Ping

Diagnostics → Ping

ICMP Ping

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

Start

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

After you press **Start**, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception 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
```

Buttons

Start: Click to start transmitting ICMP packets

New Ping: Click to re-start diagnostics with PING

LINK OAM

- ▼ Link OAM
 - MIB Retrieval

MIB RETRIEVAL

Diagnostics → *Link OAM* → *MIB Retrieval*

Link OAM MIB Retrieval

Local
Peer
Port

LINK OAM MIB RETRIEVAL

This page allows you to retrieve the local or remote OAM MIB variable data on a particular port. Select the appropriate radio button and enter the port number of the switch to retrieve the content of interest. Click on to retrieve the content. Click on to retrieve another content of interest.

Buttons

: Click to start transmitting ICMP packets

: Click to re-start diagnostics with PING

: Retrieves content of interest

PING6 (ICMPV6 PING)

▪ Ping6

Diagnostics → Ping6

ICMPv6 Ping

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

Start

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

After you press , ICMPv6 packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
PING6 server ff02::2, 56 bytes of data.  
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=0, time=10ms  
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=0, time=10ms  
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=1, time=0ms  
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=1, time=0ms  
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=2, time=0ms  
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=2, time=0ms  
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=3, time=0ms  
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=3, time=0ms  
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=4, time=0ms  
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=4, time=0ms  
Sent 5 packets, received 10 OK, 0 bad
```

You can configure the following properties of the issued ICMP packets:

IP Address

The destination IP Address.

Ping Length

The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Ping Count

The count of the ICMP packet. Values range from 1 time to 60 times.

OPTICAL SYSTEMS DESIGN

Ping Interval

The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Egress Interface (Only for IPv6)

The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes.

The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.

When the egress interface is not given, PING6 finds the best match interface for destination.

Do not specify egress interface for loopback address.

Do specify egress interface for link-local or multicast address.

Buttons

Start: Click to start transmitting ICMPv6 packets

New Ping: Click to re-start diagnostics with PING

New Retrieval: Retrieves content of interest

5.5 MAINTENANCE

- ▼ **Maintenance**
 - Restart Device
 - Factory Defaults
 - ▶ Software
 - ▶ Configuration

RESTART DEVICE

Maintenance → Restart Device

Restart Device

Are you sure you want to perform a Restart?

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

Buttons

: Click to restart device.

: Click to return to the Port State page without restarting.

OPTICAL SYSTEMS DESIGN

FACTORY DEFAULTS

Maintenance → Factory Defaults

Factory Defaults

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

Yes

No

You can reset the configuration of the switch on this page. Only the [IP](#) configuration is retained.

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

Buttons

Yes

: Click to reset the configuration to Factory Defaults

No

: Click to return to the Port State page without restarting.

Note: Restoring factory default 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

SOFTWARE

- ▼ Software
 - Upload
 - Image Select

SOFTWARE UPLOAD

Maintenance → **Software** → **Upload**

Software Upload

No file selected.

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

to the location of a software image and click .

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.*

Buttons

: Click to locate file for uploading.

: Click to start upload process.

OPTICAL SYSTEMS DESIGN

SOFTWARE IMAGE SELECTION

[Maintenance](#) → [Software](#) → [Image Select](#)

Software Image Selection

Active Image	
Image	managed
Version	60007801
Date	2017-12-15T16:10:23+11:00

Alternate Image	
Image	managed.bk
Version	60007801
Date	2017-12-15T16:10:23+11:00

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

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

Note:

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

IMAGE INFORMATION

Image

The file name of the firmware image, from when the image was last updated.

Version

The version of the firmware image.

Date

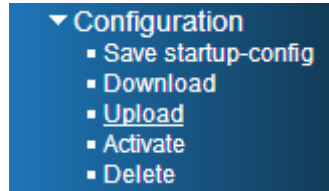
The date where the firmware was produced.

Buttons

: Click to use the alternate image. This button may be disabled depending on system state.

: Cancel activating the backup image. Navigates away from this page.

CONFIGURATION



SAVE RUNNING CONFIGURATION TO STATIP-CONFIG

Maintenance → Configuration → Save Startup-Config

Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

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.

The available files are:

- *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. If this file doesn't exist at boot time, the switch will start up in default configuration.
- *default-config*: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.
- Up to 31 other files, typically used for configuration backups or alternative configurations.

Save startup-config

This copies *running-config* to *startup-config*, thereby ensuring that the currently active configuration will be used at the next reboot.

Buttons

: Click to save the current configuration.

DOWNLOAD CONFIGURATION

Maintenance → Configuration → Download

Download Configuration

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

File Name
<input type="radio"/> running-config
<input type="radio"/> default-config
<input type="radio"/> startup-config

Download Configuration

It is possible to download any of the files on the switch to the web browser. Select the file and click

Download Configuration.

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

Buttons

Download Configuration : Click to download the configuration.

UPLOAD CONFIGURATION

Maintenance → Configuration → Upload

Upload Configuration

File To Upload

No file selected.

Destination File

File Name	Parameters
<input type="radio"/> running-config	<input checked="" type="radio"/> Replace <input type="radio"/> Merge
<input type="radio"/> startup-config	
<input type="radio"/> Create new file	<input type="text"/>

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.

Select the file to upload, select the destination file on the target, then click .

If the destination is *running-config*, the file will be applied to the switch configuration.

This can be done in two ways:

- Replace mode: The current configuration is fully replaced with the configuration in the uploaded file.
- Merge mode: The uploaded file is merged into *running-config*.

If the flash file system is full (i.e. contains *default-config* and 32 other files, usually including *startup-config*), it is not possible to create new files. Instead an existing file must be overwritten or another file must be deleted.

Buttons

: Click to locate file for uploading.

: Click to start upload process.

OPTICAL SYSTEMS DESIGN

ACTIVATE CONFIGURATION

Maintenance → Configuration → Activate

Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will not be saved to startup-config automatically.

File Name
<input type="radio"/> default-config
<input type="radio"/> startup-config

Activate Configuration

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

Select the file to activate and click [Activate Configuration](#). This will initiate the process of completely replacing the existing configuration with that of the selected file.

Buttons

[Activate Configuration](#): Click to activate configuration file.

DELETE CONFIGURATION FILE

Maintenance → Configuration → Delete

Delete Configuration File

Select configuration file to delete.

File Name
<input type="radio"/> startup-config

Delete Configuration File

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.

Buttons

Delete Configuration File

: Click to delete configuration file.

OPTICAL SYSTEMS DESIGN

6 WARRANTY

Thank you for purchasing equipment designed, manufactured and serviced by Optical Systems Design (OSD). OSD warrants that at the time of shipment, its products are free from defects in material and workmanship and conforms to specifications. Our Warranty conditions are outlined below:

6.1 WARRANTY PERIOD

For warranty period, please call your local OSD distributor.

6.2 REPAIRS

Optical Systems Design reserves the right to repair or replace faulty modules/units. Please obtain a "Return Material Authorisation" (RMA) form and number before returning goods.

Goods must be returned in adequate packing material to Optical Systems Design, Warriewood or its nominated authorised representative, for all repairs.

WARRANTY REPAIRS

Return shipments to OSD shall be at customer's expense and freight back to the customer will be at OSD expense.

OUT-OF-WARRANTY REPAIRS

OSD reserves the right to repair or replace any faulty goods. Freight costs and insurance for both journeys are met by the user. All equipment repaired by OSD will have a 3-Month Warranty from the date of dispatch.

SITE REPAIRS

By agreement site repairs may be undertaken for which out of pocket, hotel and travel expenses will be charged.

EXCLUSIONS

This warranty does not apply to defects caused by unauthorized modifications, misuse, abuse or transport damage to the equipment. All modifications to OSD's standard product will need written authorization and will be charged at normal repair rates. All modifications are to be carried out by OSD Technicians. Warranty is void if unauthorized removal and/or tampering with serial number and/or repair labels is evident.

Optical Systems Design Pty. Ltd.
7/1 Vuko Pl. Warriewood 2102
P.O. Box 891 Mona Vale
N.S.W. Australia 2103
Telephone: +61 2 9913 8540
Facsimile: +61 2 9913 8735
Email: sales@osd.com.au
Web Site: www.osd.com.au

OPTICAL
SYSTEMS
DESIGN

PTY LTD

A.B.N. 83 003 020 504

Printed in Australia