

User Manual for Standalone Operation

ONS-C801pi & ONS-C1601pi



Latest Update: July 2020
Revision 1.0

Important Notice

Optigo Networks, Inc. reserves the right to modify the equipment, its specification or this manual without prior notice, in the interest of improving performance, reliability, or servicing. At the time of publication all data is correct for the operation of the equipment at the voltage and/or temperature referred to.

Performance data indicates typical values related to the particular product.

No part of this documentation or information supplied may be divulged to any third party without the express written consent of Optigo Networks Inc. Products offered may contain software which is proprietary to Optigo Networks Inc. The offer or supply of these products and services does not include or infer any transfer of ownership.

Applied Models

This user manual applies to Optigo Networks' ONS-C801pi and ONS-C1601pi industrial managed edge switches.

The model list may be changed, Optigo Networks, Inc. reserves the right to modify the equipment, its specification or this manual without prior notice

Table of Contents

1. About Web Browser Management	6
1.1. Preparing for Web Browser Management.....	6
1.2. System Login	6
1.3 Introduction to the Web Browser Interface	8
2. System.....	9
2.1 System Configuration	10
2.2 System Information	11
2.3 IP Configuration.....	12
2.4 System Time.....	12
2.5 User Accounts.....	15
2.6 SNMP Configuration.....	15
2.6.1 Community.....	16
2.6.2 Trap.....	16
2.6.3 V3 Users	17
2.7 Fault Relay Configuration.....	17
2.8 Digital Input / Digital Output (DIDO)	18
2.9 System Environment Monitoring.....	19
3. DHCP.....	20
3.1 Basic DHCP Server.....	20
3.2 MAC-based DHCP	21
3.3 DHCP Option66	21
3.4 DHCP Option82	22
3.5 Port-based DHCP	22
3.6 DHCP Status.....	23
3.7 DHCP Snooping	23
4. Event & Log.....	24
4.1 View Logs	24
4.2 Events	25
4.3 Actions.....	26
4.3.1 Local Log Action	26
4.3.2 Remote Syslog	26
4.3.3 Email Action.....	27
4.3.4 SNMP Trap Actions.....	28
4.3.5 DOut Action	29
4.4 Event Action Map.....	30
5. Ports.....	33

5.1 Configuration	33
5.2 Status	34
5.3 Statistics	35
5.4 IEC Packet Statistics	35
5.5 Mirroring	36
5.6 Rate Limiting	36
5.7 Loop Protection	38
6. Power over Ethernet.....	39
6.1 Configuration	40
6.2 Status	40
6.3 Detection.....	41
6.4 Scheduling.....	42
7. Topology.....	44
8. QoS.....	45
9. Security.....	48
9.1 MAC Address Tables.....	48
9.1.1 Static MAC Address.....	48
9.1.2 MAC Filtering.....	49
9.1.3 All MAC Addresses.....	49
9.2 Access Control List.....	50
9.3 IEEE 802.1X (Radius Server).....	51
9.4 IP Security	51
10. VLAN.....	53
10.1 Operation Mode	54
10.2 Port-based VLAN Config.....	54
10.3 802.1Q VLAN Config.....	55
10.4 802.1Q VLAN Status.....	56
11. Multicast VLAN Registration (MVR).....	57
12. LLDP.....	58
12.1 LLDP Configuration.....	58
12.2 LLDP Neighbor Information.....	59
12.3 LLDP Statistics	60
13. Cisco Discovery Protocol (CDP).....	61
13.1 CDP Configuration Device Settings	62
13.2 CDP Status	62

13.2.1 Statistics	63
13.2.2 Neighbors.....	63
14. IGMP Snooping.....	64
14.1 IGMP Snooping Configuration	64
14.1.1 Global Configuration	65
14.1.2 Port-Related Configuration	65
14.2 IGMP Snooping Status.....	66
14.2.1 Statistics	66
14.2.2 IGMP Groups	67
14.3 Router Port Status	67
15. MSTP.....	68
15.1 MSTP Global Configuration.....	69
15.2 CIST Settings.....	70
15.2.1 Bridge Configuration	70
15.2.2 Port Configuration	70
15.2.3 How to enable STP/RSTP	71
15.2.4 How to enable MSTP.....	71
15.3 MSTP MSTI Settings.....	72
15.4 MSTP Bridges Status	72
15.5 Bridge Status of all Ports.....	73
16. Link Aggregation.....	74
16.1 Aggregation Configuration.....	74
16.2 LACP Group Status	75
17. G.8032 ERPS.....	76
17.1 Configuration	76
17.2 Status	76
18. Dual Homing	78
18.1 Configuration	78
18.2 Status	78
19. Maintenance.....	79
19.1 Save Configuration.....	79
19.2 Config Backup/Restore	79
19.3 Restart Device (Maintenance Reboot).....	80
19.4 Firmware Upgrade	80
19.5 Diagnostics.....	81
19.5.1 Ping.....	81
19.5.2 ARP Table	81
19.5.3 DDM	82

1. About Web Browser Management

There is a web browser interface on the switch, which offers advanced management features and allows users to manage the switch from anywhere on the network through the latest version of Google's Chrome web browser.

Optigo's ONS-C801pi and ONS-C1601pi switches are designed to be managed using [Optigo OneView™](#). However, they can also be managed directly, as standalone devices, via their web browser interface.

1.1. Preparing for Web Browser Management

Before managing your industrial switch via the web browser interface, connect it to the network with its management port (ONS-C801pi → port 8 / ONS-C1601pi → port 16) and make sure that one of the PCs on that network can connect to it through the web browser. If this switch was previously managed using Optigo's OneView™, reset it to defaults first by holding down the recessed reset button on the front for 30 seconds.

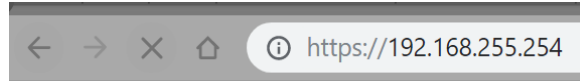
The switch's default management IP address, subnet mask, username and password are listed as below:

- IP Address: **192.168.255.254**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.255.1**
- User Name: **admin**
- Password: **Opt1goat** (*ZERO-pt-ONE-goat*)

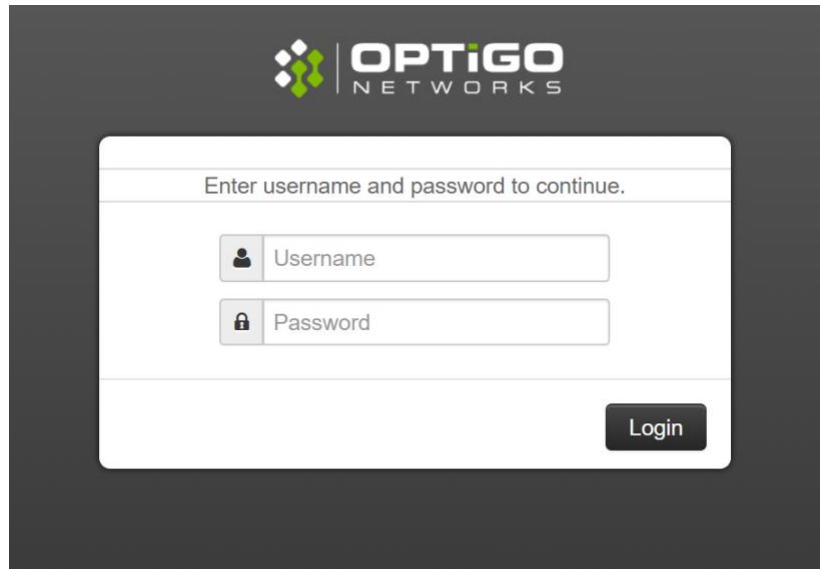
If the switch's management IP has not yet been configured (e.g. via the CLI), configure your PC with an IP address of 192.168.255.100, but with the same Subnet mask and Default Gateway as listed above, and then connect your PC's Ethernet port directly to the switch's management port. You can revert your PC's network settings back to the way they were once the switch's network settings have been configured.

1.2. System Login

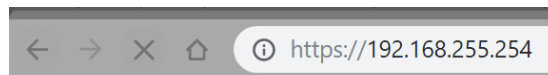
1. Launch Chrome web browser on the computer.
2. Type in http:// followed by the IP address of the switch, and then Press "Enter".



3. The login screen will appear immediately after.

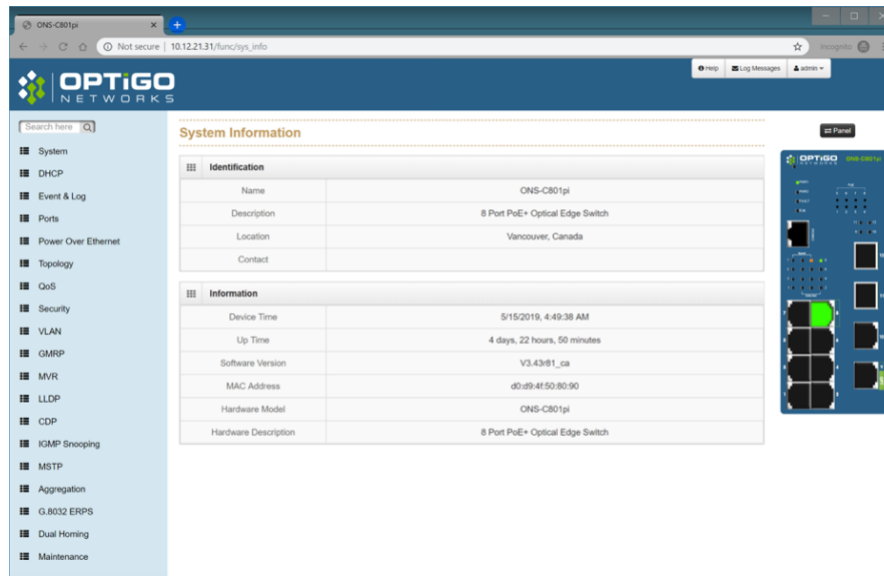


4. Log in with the default credentials (see previous page).
5. Press “Enter” or click the Login Button, and the home screen of the management interface will appear.
6. The switch also supports SSL login, so if you need SSL to protect your switch’s access account, please type in https:// followed by the IP address of the switch, and then press “Enter”.

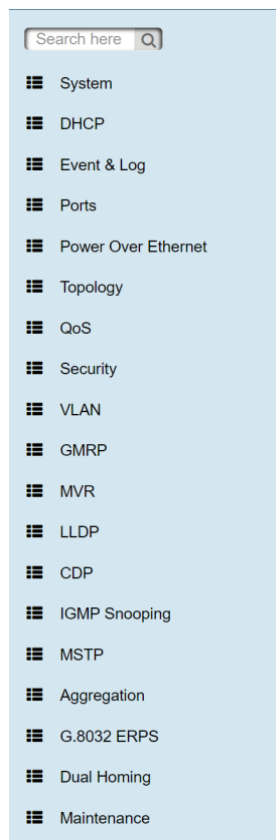


NOTE: The changes you make in the dialogs will be written to the device when you click “Apply”, but in order for these settings to be retained after power cycling or rebooting the switch, you must save them first by going to “Admin” and selecting “Save Configs”.

1.3 Introduction to the Web Browser Interface



From the left menu, left-click on the function you want to modify.



2. System



The “System” submenu consists of the following:

- System Configuration
- System Information
- IP Configuration
- System Time
- User Accounts
- SNMP Configuration
- Fault Relay Alarm
- Digital Input/Output
- Environmental Monitoring

2.1 System Configuration

This section displays the system parameters of the device:

- The system name
- The system description
- The system location
- The name of the contact person for this device
- The value of auto logout time in minutes

System Identification Configuration

1 Name:

2 Description:

3 Location:

4 Contact:

5 Auto Logout Time: minutes

Name	Description
1 Name	This is description of the switch and can't be edited manually.
2 Description	Enter a description of the switch, up to 255 characters long (alphanumeric only).
3 Location	Enter the physical location of the switch (e.g. city name, telephone closet, 3 rd floor, etc.), up to 255 characters long (alphanumeric only).
4 Contact	Enter the contact information (e.g. name and phone number) for the person who is responsible for the switch, up to 255 characters long (alphanumeric only)
5 Auto Logout Time	Enter the duration of user inactivity (in minutes) before the web server ends the session. Choose '0' to disable auto logout.

2.2 System Information

This page displays the switch's basic information.

System Information

Identification	
①	Name: ONS-C801pi
②	Description: 8 Port PoE+ Optical Edge Switch
③	Location: Vancouver, Canada
④	Contact:

Information	
⑤	Device Time: 5/15/2019, 8:00:07 AM
⑥	Up Time: 5 days, 2 hours, 1 minute
⑦	Software Version: V3.43r81_ca
⑧	MAC Address: d0:d9:4f:50:80:90
⑨	Hardware Model: ONS-C801pi
⑩	Hardware Description: 8 Port PoE+ Optical Edge Switch

Identification

Name	Description
① Name	This is the system name of the switch.
② Description	This is the switch's description.
③ Location	This is the switch's geographical location.
④ Contact	This is the contact information for the switch.

Information

Name	Description
⑤ Device Time	This is the time on the switch's system clock.
⑥ Up Time	This is the amount of time that has elapsed since the switch was last powered up or restarted.
⑦ Software Version	This is the version information for the firmware that's currently installed on the switch.
⑧ MAC Address	This is the switch's unique Media Access Control address.
⑨ Hardware Model	This is the switch's model name.
⑩ Hardware Description	This is a description of the switch, containing some basic info about it.

2.3 IP Configuration

The IP settings include the switch's management IP address and subnet mask, as well as the IP address of the default gateway and the DHCP client status.

1 DHCP client:

2 IP Address:

3 IPV6 Address:

4 Network Mask:

5 Default Gateway:

6 DNS Server IP:

Name	Description
1 DHCP Client	Set the switch as a DHCP client to get the IP address from a DHCP server (unchecked → static IP).
2 IP Address	Input the IP address of the switch (IPV4).
3 IPV6 Address	Input the IP address of the switch (IPV6), if applicable.
4 Network Mask	Input the network mask of the IP address.
5 Default Gateway	Input the address of the network gateway (e.g. router address).
6 DNS Server IP	If you need the switch to enable internet service (like SNTP), please input the correct address for the DNS server.

2.4 System Time

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. NTP is intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC). It uses the intersection algorithm, to select accurate time servers and is designed to mitigate the effects of variable network latency. NTP can usually maintain time to within tens of milliseconds over the public Internet and can achieve better than one millisecond accuracy in local area networks under ideal conditions. Asymmetric routes and network congestion can cause errors of 100 ms or more.

Note: This section is taken from the Wiki at https://en.wikipedia.org/wiki/Network_Time_Protocol

① Time Zone:

② Clock Source:

Device Time: 5/15/2019, 8:03:11 AM

③ NTP Server:

Name	Description				
① Time Zone	Universal Time Coordinated. Set the switch location time zone. The following table lists the different location time zone for your reference.				
	<table border="1"> <thead> <tr> <th>Options</th> <th>Default Settings</th> </tr> </thead> <tbody> <tr> <td>Please refer to "Table: Location Time Zone" on the next page.</td> <td>None</td> </tr> </tbody> </table>	Options	Default Settings	Please refer to "Table: Location Time Zone" on the next page.	None
	Options	Default Settings			
Please refer to "Table: Location Time Zone" on the next page.	None				
② Clock Source	You can set the time of the switch manually or set SNTP server to let the switch synch the time with SNTP server via internet.				
	<table border="1"> <thead> <tr> <th>Options</th> <th>Default Settings</th> </tr> </thead> <tbody> <tr> <td>Manual SNTP</td> <td>SNTP</td> </tr> </tbody> </table>	Options	Default Settings	Manual SNTP	SNTP
	Options	Default Settings			
Manual SNTP	SNTP				
③ SNTP	The IP address of the SNTP server.				

Manual Mode: If the switch can't access the internet due to security considerations, you can manually set the switch's clock by pressing "Get Browser Time". The system time of the switch will then be synchronized with your PC via Chrome web browser.

Note: For the most accurate system time synchronization, only use network components (i.e. routers, switches, hubs) which support SNTP in the signal path between the SNTP server and the SNTP client.

Clock Source:

Device Time: 5/15/2019, 8:03:11 AM

Time:

Table: Location Time Zone

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	-1 Hour	11 am
Oscar Time Zone	-2 Hours	10 am
ADT – Atlantic Daylight	-3 Hours	9 am
AST – Atlantic Standard EDT – Eastern Daylight	-4 Hours	8 am
EST- Eastern Standard CDT – Central Daylight	-5 Hours	7 am
CST – Central Standard MDT – Mountain Daylight	-6 Hours	6 am
MST – Mountain Standard PDT – Pacific Daylight	-7 Hours	5 am
PST – Pacific Standard AKDT – Alaskan Daylight	-8 Hours	4 am
AKST – Alaskan Standard	-9 Hours	3 am
HST – Hawaiian Standard	-10 Hours	2 am
CET – Central European FWT – French Winter MET – Middle European SWT – Swedish Winter	+1 Hour	1 pm
EET – Eastern European USSR Zone 1	+2 Hours	2 pm
AST – Arabia Standard Time USSR Zone 2	+3 Hours	3 pm
ZP4 – USSR Zone 3	+4 Hours	4 pm
ZP5 – USSR Zone 4	+5 Hours	5 pm
ZP6 – USSR Zone 5	+6 Hours	6 pm
AWST – West Australian Standard	+8 Hours	8 pm
CST – China Standard USSR Zone 7	+8 Hours	8 pm
JST – Japan Standard	+9 Hours	9 pm

USSR Zone 8		
AEST – East Australian Standard ChST – Chamorro Standard (Guam) USSR Zone 9	+10 Hours	10 pm
IDLE – International Date Line NZT – New Zealand	+12 Hours	Midnight

2.5 User Accounts

This dialog gives you the option of changing the read and read/write passwords that are required for device access. Please note that passwords are case sensitive. Set different passwords for read and read/write privileges.

Name	Description	
① Password:	Enter the password for each account.	
② New User:	Click the 'New User' button to add new account.	
③ Permission:	Set the permission level of each account.	
	Options	Default Setting
	Read-Write, Read-Only	Read-Write

2.6 SNMP Configuration

The ONS-C801pi and ONS-C1601pi both support SNMP V1, V2c, and V3. SNMP V1 and SNMP V2c use a community string match for authentication in which the SNMP servers access all objects with read-only or read/write permissions using the community strings public and private by default. SNMP V3 requires you to select an authentication level of MD5 or SHA, which is the most secure protocol. You can also enable data encryption for enhanced security.

2.6.1 Community

Name	Description				
① Agent Version:	<p>Detected by system automatically.</p> <table border="1"> <thead> <tr> <th>Option</th> <th>Default Setting</th> </tr> </thead> <tbody> <tr> <td>V1 / V2c / V3</td> <td>Detected by system automatically</td> </tr> </tbody> </table>	Option	Default Setting	V1 / V2c / V3	Detected by system automatically
Option	Default Setting				
V1 / V2c / V3	Detected by system automatically				
② String:	Set the community string of SNMP protocol with read only permission or read/write permission.				

2.6.2 Trap

Name	Description				
① IP Address	Enter the IP address of the trap destination (e.g. the PC of the IT manager).				
② String	Enter the community string of the SNMP trap.				
③ Version	<p>Select the SNMP trap version.</p> <table border="1"> <thead> <tr> <th>Options</th> <th>Default Setting</th> </tr> </thead> <tbody> <tr> <td>V1 V2c</td> <td>V2c</td> </tr> </tbody> </table>	Options	Default Setting	V1 V2c	V2c
Options	Default Setting				
V1 V2c	V2c				

2.6.3 V3 Users

Community Trap V3 Users

SNMPV3 Auth/Priv User Accounts

① User Name	② Security Level	③ Authentication Protocol	④ Authentication Password	⑤ Privacy Protocol	⑥ Privacy Password
admin22	NoAuth, NoPriv	N/A	N/A	N/A	N/A

[Apply](#)

Name	Description
① User Name	Set the user name.
② Security Level	Set up the access level. The default is 'NoAuth, NoPriv'.
③ Authentication Protocol	Set the authentication type, the default value is 'N/A'.
④ Authentication Password	Set the authentication password, the default value is 'N/A'.
⑤ Privacy Protocol	Set the privacy protocol, the default value is 'N/A'.
⑥ Privacy Password	Set the privacy password, the default value is 'N/A'.

Note: For security reasons, SNMPv3 encrypts the password. With the “SNMPv1” or “SNMPv2” setting in the dialog, Security: SNMPv1/v2 access, the switch transfers the password unencrypted, meaning it will be shown and readable.

2.7 Fault Relay Configuration

This section allows you to set the conditions (e.g. power failure, port link status, etc.) required to trigger the switch’s Alarm Relay. The alarm relay terminal pins are the middle two pins on the green terminal blocks.

Fault Relay Configuration

Power Failure ①

Power 1 Power 2

Port Link Down/Broken ②

Port 1 Port 2 Port 3 Port 4 Port 5 Port 6 Port 7

Port 8 Port 9 Port 10 Port 11 Port 12

[Apply](#)

Name	Description
❶ Power Failure	If you check 'Power 1' and 'Power 2' in a redundantly powered system, the alarm will be triggered if power is lost on either input.
❷ Port Link Down/Broken	Choose which port(s) will trigger the alarm relay if their connection fails.

2.8 Digital Input / Digital Output (DIDO)

The switch contains two digital input pins, as well as two digital output pins. When enabled, the digital inputs detect transitions in electrical signals (e.g. when a connected device powers off), while the digital outputs allow the switch to output electrical signals to an external device (e.g. provide a signal to a relay).

Digital Input/Output

Digital Input

DIN 1 High -> Low

DIN 2 Low -> High

Digital Output

DOUT 1 Low -> High

DOUT 2 High -> Low

Digital Input: When First/Second Digital Input function is enabled, First Digital Input/Second Digital Input will then be available respectively. Digital Input: Choose the transition type to trigger DI0/DI1.

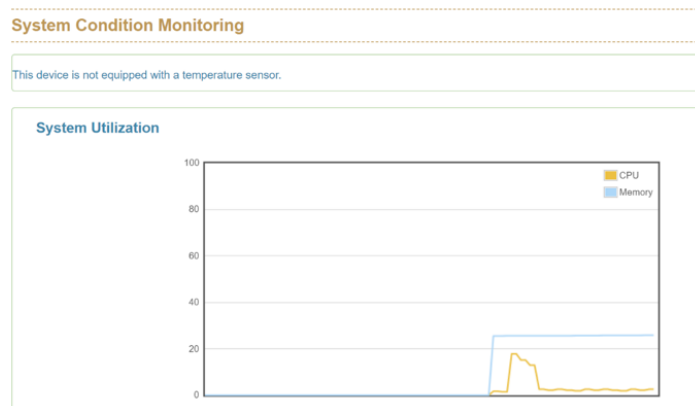
Name	Description
❶ Low → High	Having focused this radio button, DI0/DI1 will only report the status when the external device's voltage changes from low to high.
❷ High → Low	Having focused this radio button, DI0/DI1 will only report the status when the external device's voltage changes from high to low.
❸ Event Description	Please fill in the description for the event.

Digital Output: When First/Second Digital Output function is enabled, First Digital Output/Second Digital Output will then be available respectively.

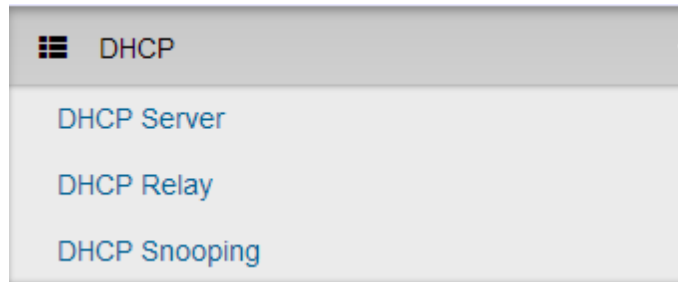
Name	Description
① Action	Choose the output type of electrical signal.
② Low → High	Having focused this radio button, DO0/DO1 will output an electrical signal of Low-to-High when the condition of the ticked checkbox is met (port/power failure occurs).
③ High → Low	Having focused this radio button, DO0/DO1 will output an electrical signal of Low-to-High when the condition of the ticked checkbox is met (port/power failure occurs).

2.9 System Environment Monitoring

This page displays basic information on the system's current condition, including CPU and memory usage. However, temperature monitoring is not currently supported.



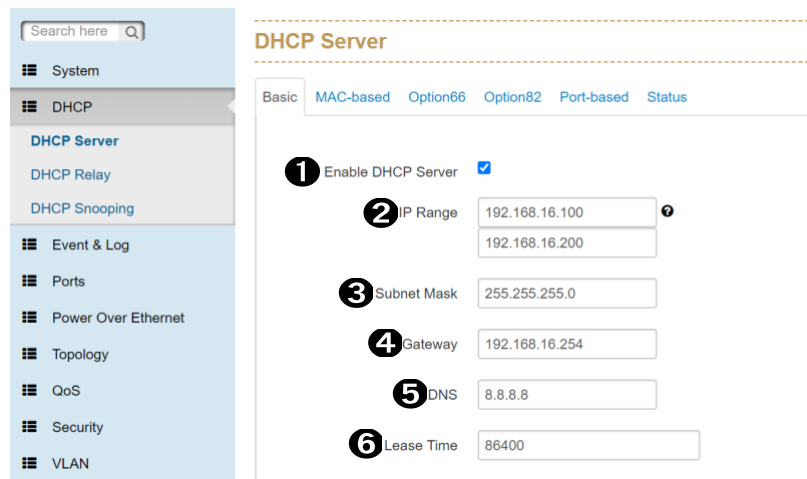
3. DHCP



This section contains the dialogs, displays, and tables for:

- DHCP Server
- DHCP Relay
- DHCP Snooping

3.1 Basic DHCP Server



Name	Description
1 Enable DHCP Server	Enable the switch’s DHCP server (See note below).
2 IP Range	Define the IP range to be assigned to DHCP clients.
3 Subnet Mask	Define the Subnet Mask to be assigned to DHCP clients.
4 Gateway	Define the gateway address to be assigned to DHCP clients.
5 DNS	Define the DNS address to be assigned to DHCP clients.
6 Lease Time	Define the DHCP clients’ lease time.

Note:

Enable DHCP Client: This enables the switch to receive its IP address from a DHCP server. The switch is then considered to be a DHCP client of that DHCP server.

Enable DHCP Server: This enables the switch to act as a DHCP server and issue IP addresses to other devices. The switch is then considered to be a DHCP server, and then the other devices are DHCP clients.

* Before the DHCP Server can be enabled, DHCP client must be disabled. This is because **devices cannot be a server and a client simultaneously**. Therefore, the switch must have a static IP address manually assigned to it.

3.2 MAC-based DHCP

Assign specific IP addresses to clients with specific MAC addresses. This is also known as DHCP reservation by MAC address.

The screenshot shows the 'DHCP Server' configuration page with the 'MAC-based' tab selected. There are two main input fields: 'MAC Address' (labeled with a circled 1) containing '28:60:46:A1:35:2c' and 'IP Address' (labeled with a circled 2) containing '192.168.16.123'. An 'Apply' button is located at the bottom right of the form.

Name	Description
① MAC Address	Enter the MAC address of the device you want to assign a specific IP address.
② IP Address	Enter the IP address that you want to assign to that device.

3.3 DHCP Option66

Assign a dedicated IP address of a TFTP server under the DHCP option66 standard.

The screenshot shows the 'DHCP Server' configuration page with the 'Option66' tab selected. There is one input field labeled 'Server' (labeled with a circled 1) with the placeholder text 'IP or URL'. An 'Apply' button is located at the bottom right of the form.

Name	Description
① Server	Enter the IP address of the TFTP server.

3.4 DHCP Option82

Assign a dedicated IP address under the DHCP option82 standard; you need to assign one Optigo switch as an option82 server and another Optigo switch as a DHCP relay.

Name	Description
❶ Remote ID	Enter the ID of a remote DHCP option82 relay switch.
❷ Circuit ID	Enter the port ID of a remote DHCP option82 relay switch.
❸ IP Range	Enter the IP address range that will be assigned via the current ID.
❹ Netmask	Assign the netmask.
❺ Gateway	Assign the gateway address.
❻ DNS	Assign the DNS address.
❼ Lease Time	Enter the DHCP lease time for the IP address (in seconds).

3.5 Port-based DHCP

Assign dedicated IP address by port that is connected to the device.

Name	Description
❶ Port No.	The switch port number connected to the device.
❷ Desired IP	Enter the dedicated IP address to be assigned to this port.
❸ Do not offer IP	Disable the assignment of IP addresses to the end device.

3.6 DHCP Status

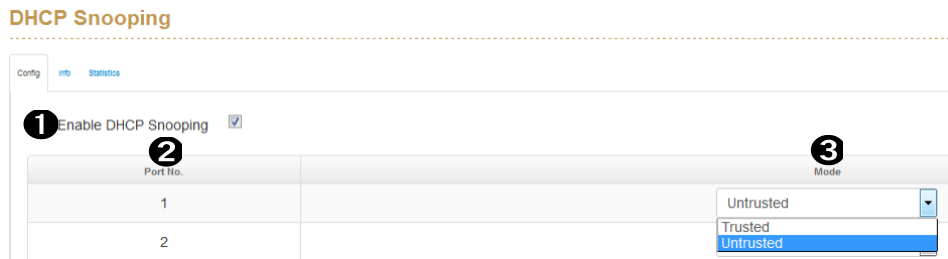
This will show you what IP address have been assigned to the clients.



Name	Description
① Port No.	The switch port number.
② MAC Address	The MAC address of the end device.
③ IP Address	The IP address of the end device.
④ Name	The host name of end device.
⑤ Available Leased Time	The remaining DHCP lease time.

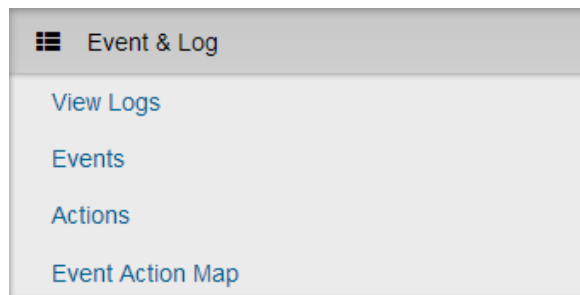
3.7 DHCP Snooping

Configure a dedicated port to forward DHCP packets or block malicious DHCP traffic.



Name	Description	
① Enable DHCP Snooping	Enable the DHCP snooping function.	
② Port No.	The switch port number.	
③ Mode	Trusted: This port will forward DHCP packets. Untrusted: This port will block DHCP packets.	
	Options	Default Setting
	Trusted Untrusted	Untrusted

4. Event & Log



The Event & Log section displays the following information:

- View Logs
- Events
- Actions
- Event Action Map

4.1 View Logs

This section shows the system log entry including the following action types:

Logs

1 Login
 2 Boot
 3 DDM
 4 DIN
 5 Link Change
 6 POE
 7 Power
 8 Ring

✔ Apr 27, 12:14:34	Boot	System Cold Start
✔ Apr 27, 12:14:32	Link Change	Phyport(8).linkChg: up
✔ Apr 27, 12:14:31	Link Change	Phyport(8).linkChg: down
✔ Apr 27, 12:14:30	Link Change	Phyport(8).linkChg: up
✔ Apr 01, 13:07:14	Boot	System Cold Start
✔ Apr 01, 13:07:12	Link Change	Phyport(8).linkChg: up
✔ Apr 01, 13:07:10	Link Change	Phyport(8).linkChg: down
✔ Apr 01, 13:07:09	Link Change	Phyport(8).linkChg: up
✔ Apr 01, 11:04:50	Power	PWR2 is stats: on

Name	Description
1 Login	User Login.
2 Boot	System Boot.
3 DDM	DDM information from SFP module.

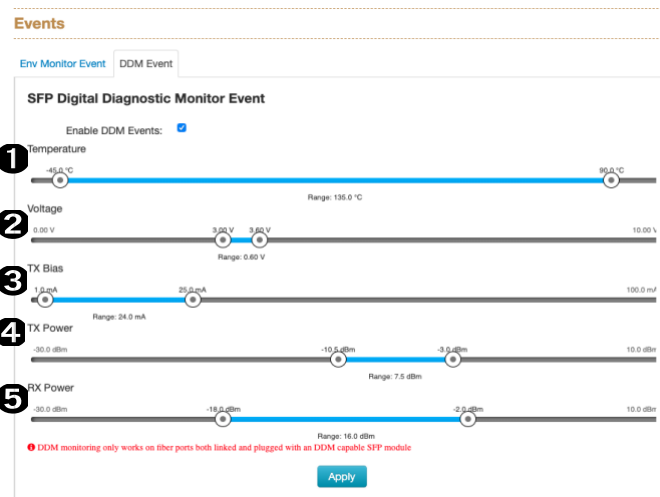
④ DIN	Digital Input Event triggered status.
⑤ Link Change	Port link up or down.
⑥ POE	POE Status.
⑦ Power	Power status.
⑧ Ring	Configuration Change or Save

Note: The maximum log size is 1000 entries. When the log exceeds this size, it will delete the oldest entry.

4.2 Events

This section will help you to monitor the status of SFP Digital Diagnostic Monitor events. (“Environmental monitoring Event” is currently not supported).

You can set the trigger range of each SFP DDM event.



Name	Description
① Temperature	Working temperature of SFP.
② Voltage	Working voltage of SFP.
③ TX Bias	Bias of SFP.
④ TX Power	Tx power of SFP.
⑤ RX Power	Rx power of SFP.

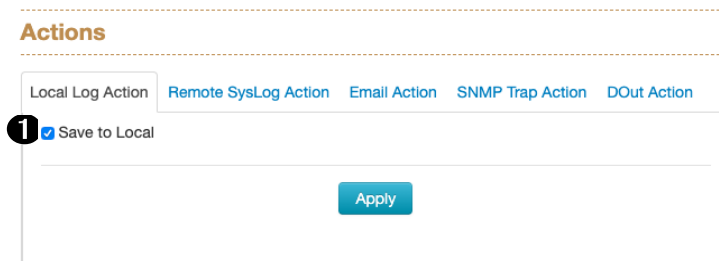
Note: This function only works for SFP modules with the DDM spec.

4.3 Actions

When the switch detects an event, it will trigger one of the pre-configured actions below:

- Local Log Action
- Remote Syslog Action
- Email Action
- SNMP Trap Actions
- DOUT Action

4.3.1 Local Log Action

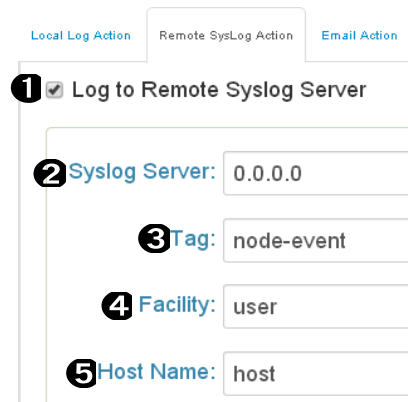


The screenshot shows the 'Actions' configuration interface. At the top, there are tabs for 'Local Log Action', 'Remote SysLog Action', 'Email Action', 'SNMP Trap Action', and 'DOUT Action'. The 'Local Log Action' tab is selected. Below the tabs, there is a checkbox labeled 'Save to Local' which is checked and has a circled '1' next to it. Below the checkbox is an 'Apply' button.

Name	Description
1 Save to Local	Enable saving of the log to the local switch.

4.3.2 Remote Syslog

The “Syslog” dialog enables you to also send events to one or more syslog servers locally or remotely. You can enable or disable this with the check box.



The screenshot shows the 'Remote SysLog Action' configuration interface. At the top, there are tabs for 'Local Log Action', 'Remote SysLog Action', and 'Email Action'. The 'Remote SysLog Action' tab is selected. Below the tabs, there is a checkbox labeled 'Log to Remote Syslog Server' which is checked and has a circled '1' next to it. Below the checkbox are four input fields: 'Syslog Server' with the value '0.0.0.0' (circled '2'), 'Tag' with the value 'node-event' (circled '3'), 'Facility' with the value 'user' (circled '4'), and 'Host Name' with the value 'host' (circled '5').

Name	Description
❶ Log to Remote Syslog Server	Enable to save log to a remote Syslog Server.
❷ Syslog Server	Enter the IP address of the remote Syslog server.
❸ Tag	Tag the event to categorize events into groups.
❹ Facility	This is the machine process that logged the event.
❺ Host Name	Name of the Syslog Server, e.g. Sys-Ser-3.

4.3.3 Email Action

Local Log Action Remote SysLog Action **Email Action** SNMP Trap Action DOut Action

❶ Email Alert

❷ Subject: Event Log

Cloud SMTP:

❸ Sender: some.user@gmail.com

❹ SMTP Server: smtp.gmail.com

❺ Server Port: 465

❻ User ID: some.user

❼ Password:

❽ Enable SSL:

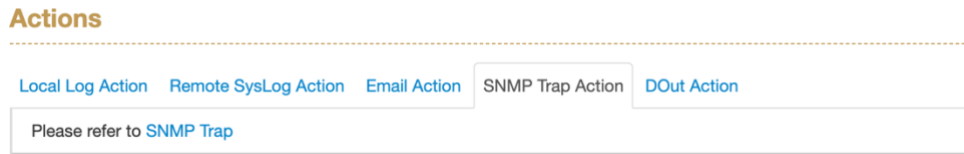
❾ Receivers:

1. some.other.user@gmail.com

Name	Description
❶ Email Alert	Enable log alerts to be sent out via email.
❷ Subject	Enter the subject of the alert email (e.g. link down).
❸ Sender	The email address of the email account used for email notifications.
❹ SMTP Server	The address of the SMTP server.
❺ Server Port	The email server port.
❻ User ID	Login for the sender's email account (not the entire email address).
❼ Password	The password for the sender's email account (Gmail™ may require an app password).
❽ Enable SSL	Check if using Secured Socket Layer (very common).
❾ Receivers	Enter the email address(es) of the alert recipient(s).

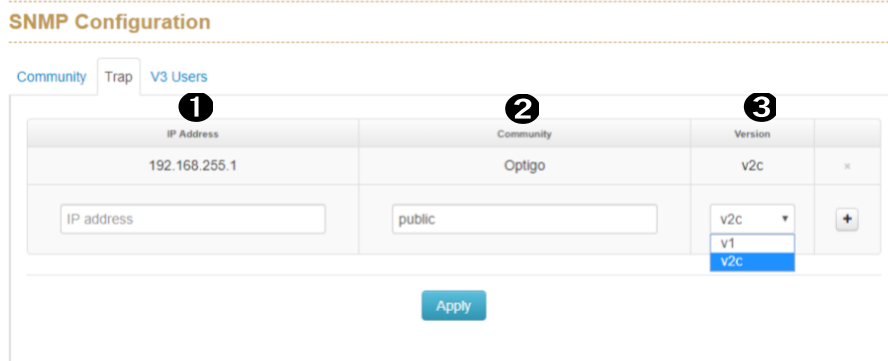
4.3.4 SNMP Trap Actions

Clicking the ‘SNMP Trap Action’ Link will bring you to the following page.



Name	Description
SNMP Trap Action	The user is redirected to the ‘SNMP Trap’ configuration, with a direct link to that page.

Here we can configure the SNMP manager; here we can see an example of an SNMP manager configured named Optigo.



Name	Description
❶ IP Address	Set the IP address of the SNMP Manager.
❷ Community	Set the name of the “community” that will use this SNMP Manager.
❸ Version	Specify what version of software is on the SNMP Manager.

4.3.5 DOut Action

Actions

Local Log Action Remote SysLog Action Email Action SNMP Trap Action **DOut Action**

Please refer to the **Digital OUT** section of [Digital Input/Output](#)

Name	Description
DOut Action	The user is redirected to the 'Digital Input/Output' configuration, with a direct link to that page.

Here we can configure the Digital Input and Digital Output Actions.

Digital Input/Output

Digital Input

1 DIN 1 Low -> High

2 DIN 2

Digital Output

3 DOUT 1 High -> Low

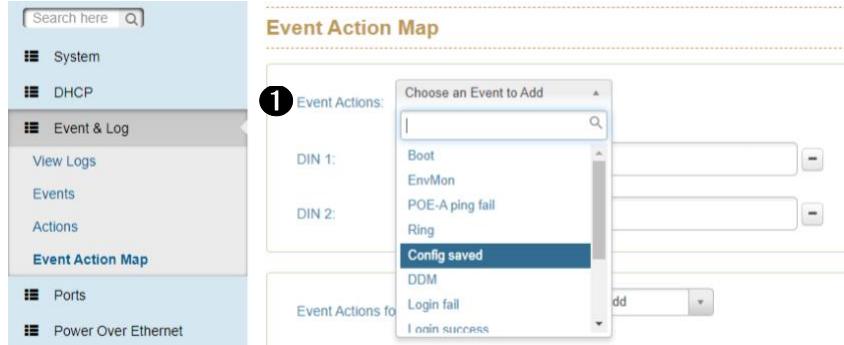
4 DOUT 2 High -> Low

- A digital signal can be high or low (making a binary 0 or 1). We can create actions based on changes from high to low.
- In the screenshot (above) we can see Digital Input 1 has been set to have an action of Low → High. Digital Input 2 is disabled.

Name	Description	Options	Default Setting
1 DIN1	Digital Input 1	LOW → HIGH HIGH → LOW	None
2 DIN2	Digital Input 2	LOW → HIGH HIGH → LOW	None
3 DOUT1	Digital Output 1	LOW → HIGH HIGH → LOW	None
4 DOUT2	Digital Output 2	LOW → HIGH HIGH → LOW	None

4.4 Event Action Map

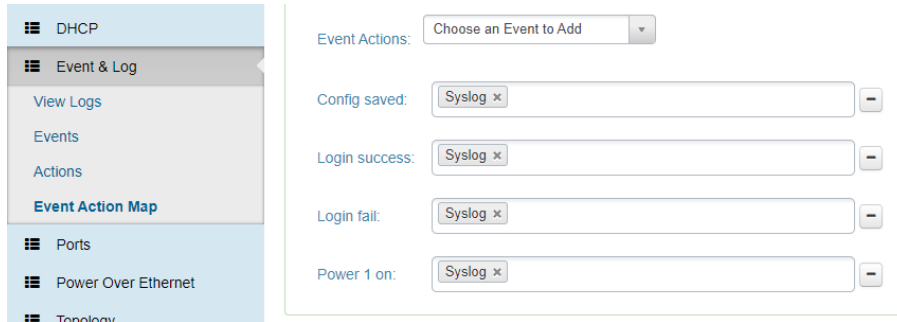
You can combine event and action settings here. The two actions selected in the screenshot are **Digital Input 1** and **Digital Input 2**.



Name	Description
❶ Event Action	Which event will be combined with the desired action.

Event Actions: Please follow the steps below to set the event actions.

A: Choose the event which you want to activate.



Name	Description	Options	Default Setting
❶ Event Actions	Which event will be combined with the desired action.	Boot EnvMon POE-A ping fail Ring Config Saved DDM Login fail Login success Power1 on Power1 off Power2 on Power2	None

B: The selected event will be shown as follows. In the screenshot, the events 'Config Saved', 'Login Success' and 'Login Fail' have been added. Choose your preferred method to forward this event to the manager side.

Name	Description	Options	Default Setting
① Selected Event	Which action will be combined with this event.	Email SMS SNMP Trap DOUT 1 DOUT 2	None

Event Actions for Link Change:

Please follow the steps below to set the event actions:

A: Choose the Port (Link) and Event you want to activate.

Name	Description	Options	Default Setting
① Selected Event	Which action will be combined with this port and event.	Selected Port UP Selected Port DOWN	None

B: The selected event will be shown as follows. In the screenshot, the events 'Port 1 UP', 'Port 3 UP', 'Port 4 DOWN', 'Port 5 UP' and 'Port 5 DOWN' have been added. Choose your preferred method to forward this event to the manager side.

Event Actions for Link Change: Choose a port to Add ▾

Port 1 up SNMP Trap x -

Port 3 up SNMP Trap x -

Port 4 down SNMP Trap x -

Port 5 up SNMP Trap x -

Port 5 down SNMP Trap x -

SNMP Trap x

Syslog

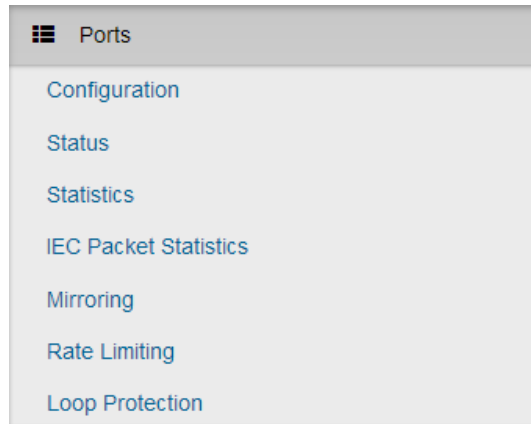
Email

DOUT 1

DOUT 2

Name	Description	Options	Default Setting
① Port Event	Which action will be combined with this event	Email Syslog DOUT 1 DOUT 2	None

5. Ports



This section will show you how to control and manage the switch’s ports.

5.1 Configuration

Port settings are displayed and can be modified on the Device Settings panel.

Device Settings

1 Port No.	2 Type	3 Description	4 Enabled	5 Flow Control	6 Speed
1	100TX	Port 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Auto
2	100TX	Port 2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Auto
3	100TX	Port 3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Auto

Name	Description				
1 Port No.	The port number.				
2 Type	Port type (100Tx/1000T/GSFP/DSFP).				
3 Description	Enter up to 47 alphanumeric characters to describe the port.				
4 Enabled	Enable traffic on the port.				
5 Flow Control	Enable flow control.				
6 Speed	Select the speed of the port from supported options.				
	<table border="1"> <thead> <tr> <th>Options</th> <th>Default Setting</th> </tr> </thead> <tbody> <tr> <td>Disabled: Deactivate the port</td> <td>Auto</td> </tr> </tbody> </table>	Options	Default Setting	Disabled: Deactivate the port	Auto
Options	Default Setting				
Disabled: Deactivate the port	Auto				

	<p>Auto: Let's the port negotiate the speed with the device it's connected to and reach the maximum speed that is possible.</p> <p>10Mbps HDX: Forces the cu port to 10Mbps half duplex mode.</p> <p>10Mbps FDX: Forces the cu port to 10Mbps full duplex mode.</p> <p>100Mbps HDX: Forces the cu port to 100Mbps half duplex mode.</p> <p>100Mbps FDX: Forces the cu port to 100Mbps full duplex mode.</p> <p>1Gbps FDX: Forces the cu port to 1Gbps full duplex mode</p>	
--	--	--

5.2 Status

Port Status

❶ Port No.	❷ Type	❸ Link	❹ State	❺ Speed	❻ Flow Control
1	100TX	up	Enable	100 Full	Disable
2	100TX	down	Enable	N/A	N/A

Name	Description
❶ Port No	Port number.
❷ Type	Port type (100TX/1000T/GSFP/DSFP).
❸ Link	Link status: up or down.
❹ State	Port state: enabled or disabled.
❺ Speed	The port's link speed, which is the capability of the currently connected device (N/A if nothing is connected).
❻ Flow Control	Flow control status. Note: Flow Control is only available when the port's speed is set to 'Auto' and therefore it's efficiency is subject to the negotiation between the port and the device it's connected to.

5.3 Statistics

Port Statistics

Port	Type	Link	State	Tx Good	Tx Bad	Rx Good	Rx Bad	Tx Abort	Collision	Drop	RX BCAST	RX MCAST	TX MCAST
1	100TX	Down	Enable	0	0	0	0	0	0	0	0	0	0
2	100TX	Down	Enable	0	0	0	0	0	0	0	0	0	0
3	100TX	Down	Enable	0	0	0	0	0	0	0	0	0	0
4	100TX	Down	Enable	0	0	0	0	0	0	0	0	0	0

Name	Description
① Port	Number of each port.
② Type	Media type of each port (100TX/1000T/GSFP/DSFP).
③ Link	Link status: Up or Down.
④ State	Port status.
⑤ Tx Good	The number of good packets sent out of this port.
⑥ Tx Bad	The number of bad packets sent out of this port. This includes: undersized (less than 64 octets), oversized, CRC alignment errors, fragments, and jabber packets).
⑦ Rx Good	The number of good packets received by this port.
⑧ Rx Bad	The number of bad packets received by this port. This includes: undersized (less than 64 octets), oversized, CRC alignment errors, fragments, and jabber packets).
⑨ Tx Abort	The number of packets that were aborted during transmission.
⑩ Collision	The number of packet collisions.
⑪ Drop	The number of packets dropped.
⑫ RX BCAST	The number of broadcast packets received by this port.
⑬ RX MCAST	The number of multicast packets received by this port.
⑭ TX MCAST	The number of multicast packets sent out of this port.

5.4 IEC Packet Statistics

Packet counters for common industrial protocols

Port	GOOSE	MMS	PTP	MOBUS	PROFINET
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0

UNIT: packets

5.5 Mirroring

Port Mirroring can be used to monitor network traffic. With port mirroring enabled, the switch sends a copy of all network packets seen on selected ports (Source Port) to another port (Destination Port), where the packets can be analyzed (e.g. by one of Optigo's BACnet Capture Tools).

Source Port: All of a source port's selected traffic (Rx, Tx, or both) will be copied to the Destination Port.

Destination Port: Only a single port can be configured as the Destination Port and all of the source ports' selected traffic will be copied to it.

Port Mirroring

1 Direction	2 Destination	3 Mirror From
RX	Port 1	Choose ports
TX	Port 1	Choose ports

[Apply](#)

Name	Description
1 Direction	Both Tx and Rx traffic can be monitored on Source Ports.
2 Destination Port	Choose the port that will be the mirror port, the one that will receive a copy of the selected traffic (Rx, TX or both) from all monitored ports.
3 Source Port(s)	Select which ports will be monitored by choosing them in the appropriate row. If you want to monitor both Tx and Rx traffic on a particular port, simply choose that port in both rows.

5.6 Rate Limiting

Limiting allows the user to set a limit for each port's ingress/egress data rate.

Ingress control supports data rate limiting and packet type limiting (All, Unicast, Multicast and Broadcast).

Egress control only supports data rate limiting.

Rate Limiting

Port	Ingress	Egress
1	① Packet Type: Unicast, Multicast, Broadcast ② Ingress: 0 kbps 0%	③ Egress: 0 kbps 0%
2	① Packet Type: Unicast, Multicast, Broadcast ② Ingress: 0 kbps	③ Egress: 0 kbps

Name	Description										
① Packet Type	Select which packet types should be rate-limited. All the ports support port ingress and egress rate control. For example, assuming port 1 is rated at 10Mbps, users can set its effective egress rate to 1Mbps and its ingress rate to 500Kbps. The switch references the packet counter value to enforce the specified rate. <table border="1" style="width: 100%; margin-top: 10px;"> <thead> <tr> <th>Packet Types</th> <th>Default Setting</th> </tr> </thead> <tbody> <tr> <td>All</td> <td>All</td> </tr> <tr> <td>Unicast</td> <td></td> </tr> <tr> <td>Multicast</td> <td></td> </tr> <tr> <td>Broadcast</td> <td></td> </tr> </tbody> </table>	Packet Types	Default Setting	All	All	Unicast		Multicast		Broadcast	
Packet Types	Default Setting										
All	All										
Unicast											
Multicast											
Broadcast											
② Ingress	Enter the ingress rate limit (The default value is "0").										
③ Egress	Enter the egress rate limit (The default value is "0").										

Note: Rate Limiting works exclusively on layer 2 to limit the impact of flooding packets. Therefore, this function ignores any protocol information present in higher layers (e.g. IP, TCP, etc).

Note: Ports that are included in a Link Aggregation are excluded from the rate limitation, regardless of the entries in the "Rate Limiting" dialog

5.7 Loop Protection

Loop Protection helps to prevent the broadcast storms that are generated when a loop is created in your network.

Loop Protection

The screenshot shows the configuration page for Loop Protection. It has two tabs: 'Config' and 'Status'. Under the 'Config' tab, there are three settings:

- 1 Enable Loop Protection**: A checkbox that is checked.
- 2 Interval**: A dropdown menu set to '1'.
- 3 Shutdown**: A dropdown menu set to '60'.

An 'Apply' button is located at the bottom right of the configuration area.

Name	Description
1 Enable Loop Protection	Enable or disable loop protection.
2 Interval (seconds)	Define how often the switch will check the loop status of each port.
3 Shutdown (seconds)	Define how long the port will be blocked when it is looping.

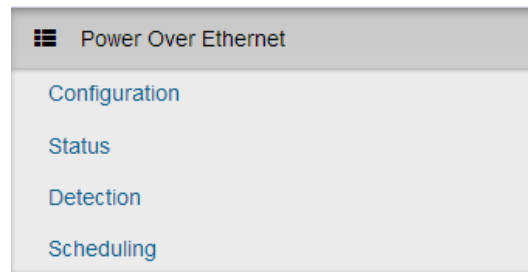
Loop Protection

The screenshot shows the status page for Loop Protection. It has two tabs: 'Config' and 'Status'. Under the 'Status' tab, there is a table with the following columns: 'Port No', 'Looping', 'Loop Counts', and 'Last Loop at'.

Port No	Looping	Loop Counts	Last Loop at
1	1 NO	2 0	3 N/A
2	NO	0	N/A
3	NO	0	N/A
4	NO	0	N/A

Name	Description
1 Looping	Displays the loop status of the port.
2 Loop Counts	Displays how many loops have occurred at the port.
3 Last Loop at	Displays the last time that a loop occurred at the port.

6. Power over Ethernet



Power over Ethernet (PoE) is a way to transmit power over Ethernet cable to PD (Powered devices). The standards are IEEE 802.3at/af with different power output. The IEEE802.3af can transmit max 15.4W per port while IEEE802.3at, also known as PoE+, transmit 30W per port. In the physical connection of PoE technology, please consider power loss over the length of cable. The minimum power available is 12.95 Watts per port over IEEE802.3af and 25.5Watts per port over IEEE802.3at standard.

There are several common techniques for transmitting power over Ethernet cabling. Two of them have been standardized by IEEE 802.3 since 2003. These standards are known as Alternative A and Alternative B. For 10BASE-T and 100BASE-TX, only two of the four data/signal pairs in typical CAT-5 cable are used. Alternative B separates the data and the power conductors, making troubleshooting easier. It also makes full use of all four twisted pair, copper wires. The positive voltage runs along pins 4 and 5, and the negative along pins 7 and 8.

Note: This part is taken from the Wiki at https://en.wikipedia.org/wiki/Power_over_Ethernet

Optigo supports most PoE switches as PSE (power sourcing equipment) using Alternative A technique. Only a couple of models support Alternative B technique.

Optigo PoE models have options with different input ranges including 12/24V \square 48V boost up, 72V \square 48V step down and high voltage 85~265VAC/ 110~300VDC. Furthermore, Optigo managed PoE switches offer PD detection and PoE scheduling for advanced PoE management.

6.1 Configuration

Power over Ethernet Configuration

⚙ **System**

Maximum Power Available: W ①

Legacy Mode: ②

⚙ **Ports**

Port No.	Enabled	Scheduling	Priority	Power Limit(≤ 36000)
1	✓	<input type="checkbox"/>	Low	36000 mW
2	✓	<input type="checkbox"/>	Low	36000 mW
3	✓	<input type="checkbox"/>	Low	36000 mW
4	✓	<input type="checkbox"/>	Low	36000 mW
5	✓	<input type="checkbox"/>	Low	36000 mW
6	✓	<input type="checkbox"/>	Low	36000 mW

Name	Description				
① Maximum Power Available	Set the maximum total power consumption (W).				
② Legacy Mode	Force the switch to supply power to legacy PD.				
③ Port No.	The PoE port number.				
④ Enabled	Enable or Disable the port's PoE functionality.				
⑤ Scheduling	Set the PoE port to be controlled with the PoE scheduling function.				
⑥ Priority	Set the power supply priority. If the total power consumption of all PoE ports exceeds the maximum power limit, then the switch will supply power by priority setting. <table border="1" style="width: 100%; margin-top: 5px;"> <thead> <tr> <th style="width: 60%;">Priority Options</th> <th>Default Setting</th> </tr> </thead> <tbody> <tr> <td>Low / High / Critical</td> <td>Low</td> </tr> </tbody> </table>	Priority Options	Default Setting	Low / High / Critical	Low
Priority Options	Default Setting				
Low / High / Critical	Low				
⑦ Power Limit	Define the maximum power supplied by the PoE port (mW).				

6.2 Status

System

⚡ **System**

① Power Consumption 0W	② Main Voltage 23.5V	③ Main Current 0.000A
--	--	---

Name	Description
① Power Consumption	This is the total power consumption of all PoE ports.
② Main Voltage	This is the output voltage of each PoE port.
③ Main Current	This is the output current of each PoE port.

Ports

Ports	①	②	③	④	⑤	⑥	⑦
Port No.	Link	State	Temperature (°C)	Current (A)	Power (W)	Determined Class	
1	Down	Detecting	49	0.000	0.0	None	
2	Down	Detecting	49	0.000	0.0	None	
3	Down	Detecting	49	0.000	0.0	None	
4	Down	Detecting	49	0.000	0.0	None	
5	Down	Detecting	49	0.000	0.0	None	
6	Down	Detecting	49	0.000	0.0	None	
7	Down	Detecting	49	0.000	0.0	None	
8	Up	Detecting	49	0.000	0.0	None	

Name	Description
① Port No.	The PoE port number.
② Link	The connection status of each PoE port.
③ State	The PoE status of each connected PD (Unknown means that the connected device is non-PD).
④ Temperature (°C)	The temperature of the PoE chipset.
⑤ Current (A)	The output current of each PoE port.
⑥ Power (W)	The power consumption of each PoE port.
⑦ Determined Class	The PoE class of each connected PD.

6.3 Detection

Device Detection							
①	②	③	④	⑤	⑥	⑦	⑧
No.	Enabled	IP address	Interval	Retry Time	Failure Log	Failure Action	Reboot Time
1	<input type="checkbox"/>	0.0.0.0	60 sec(s)	1	error=0, total=0	Nothing ↓	3 sec(s)
2	<input type="checkbox"/>	0.0.0.0	60 sec(s)	1	error=0, total=0	Nothing ↓	3 sec(s)
3	<input type="checkbox"/>	0.0.0.0	60 sec(s)	1	error=0, total=0	Nothing ↓	3 sec(s)
4	<input type="checkbox"/>	0.0.0.0	60 sec(s)	1	error=0, total=0	Nothing ↓	3 sec(s)
5	<input type="checkbox"/>	0.0.0.0	60 sec(s)	1	error=0, total=0	Nothing ↓	3 sec(s)
6	<input type="checkbox"/>	0.0.0.0	60 sec(s)	1	error=0, total=0	Nothing ↓	3 sec(s)
7	<input type="checkbox"/>	0.0.0.0	60 sec(s)	1	error=0, total=0	Nothing ↓	3 sec(s)
8	<input type="checkbox"/>	0.0.0.0	60 sec(s)	1	error=0, total=0	Nothing ↓	3 sec(s)


Name	Description												
① No.	The PoE port number.												
② Enabled	Enable of Disable PoE detection.												
③ IP address	The IP address of the connected PD (Powered Device).												
④ Interval	Define how often to ping the connected PD.												
⑤ Retry Time	Define how many ping failures are allowed before the PD is considered as failed (min = 1, max = 5).												
⑥ Failure Log	The record of PD detection failures.												
⑦ Failure Action	<p>The action to be taken when a PD fails.</p> <table border="1"> <thead> <tr> <th>Action</th> <th>Default Setting</th> </tr> </thead> <tbody> <tr> <td>Nothing: No action.</td> <td>Nothing</td> </tr> <tr> <td>Power Down: Shut down power on PoE port.</td> <td></td> </tr> <tr> <td>Power On: Keep PoE port powered ON.</td> <td></td> </tr> <tr> <td>Restart Forever: Continuously power cycle the PoE port.</td> <td></td> </tr> <tr> <td>Restart Once: Reset the PoE port just once.</td> <td></td> </tr> </tbody> </table>	Action	Default Setting	Nothing: No action.	Nothing	Power Down: Shut down power on PoE port.		Power On: Keep PoE port powered ON.		Restart Forever: Continuously power cycle the PoE port.		Restart Once: Reset the PoE port just once.	
Action	Default Setting												
Nothing: No action.	Nothing												
Power Down: Shut down power on PoE port.													
Power On: Keep PoE port powered ON.													
Restart Forever: Continuously power cycle the PoE port.													
Restart Once: Reset the PoE port just once.													
⑧ Reboot Time	If the action is set to 'Restart Forever', then Reboot Time defines the time between restarts (min = 3 secs, max = 120 secs).												

6.4 Scheduling

Power Schedule																								
Hour	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sunday	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>
Monday	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>
Tuesday	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>
Wednesday	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>
Thursday	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>
Friday	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>
Saturday	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>

Set the weekly PoE power-on schedule.

Power over Ethernet Configuration

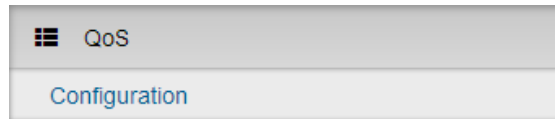
 Power Schedule												
Hour	00	01	02	03	04	05	06	07	08	09	10	11
Sunday	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Monday	<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"/>

In this example (see screenshot above), the PD is set to power on at 10:00 am on Sunday, and then power off again one hour later, at 11:00 am.

7. Topology

The Topology feature is currently not supported.

8. QoS



Quality of service (QoS) is the description or measurement of the overall performance of a service, such as a telephony or computer network or a Cloud computing service, particularly the performance seen by the users of the network. To quantitatively measure quality of service, several related aspects of the network service are often considered, such as error rates, bit rate, throughput, transmission delay, availability, jitter, etc.

In the field of computer networking and other packet-switched telecommunication networks, quality of service refers to traffic prioritization and resource reservation control mechanisms rather than the achieved service quality. Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

Quality of service is particularly important for the transport of traffic with special requirements. In particular, developers have introduced technology to allow computer networks to become as useful as telephone networks for audio conversations, as well as supporting new applications with even stricter service demands.

Note: This section is taken from the Wiki at https://en.wikipedia.org/wiki/Quality_of_service

QoS Policy: Optigo's ONS-C801pi/ONS-C1601pi switches have multiple traffic queues that allow packet prioritization to occur. Higher priority traffic can pass through the switch without being delayed by lower priority traffic. As each packet arrives, it is processed and then sorted into the appropriate queue. The switch then forwards packets from each queue.

Optigo's ONS-C801pi/ONS-C1601pi switches support two different queuing mechanisms:

- **Weighted Fair Queue Ratio:** This method services all the traffic queues, giving priority to the higher priority queues. Under most circumstances, the Weighted Fair Queue Ratio gives high priority precedence over low priority, but in the event that high priority traffic does not reach the link capacity, lower priority traffic is allowed, though.

- Strict: This method services high traffic queues; low priority queues are delayed until no more high priority data needs to be sent. The Strict method always gives precedence to high priority over low priority.

QoS Configuration

QoS Policy:

1 Use weighted fair queuing scheme

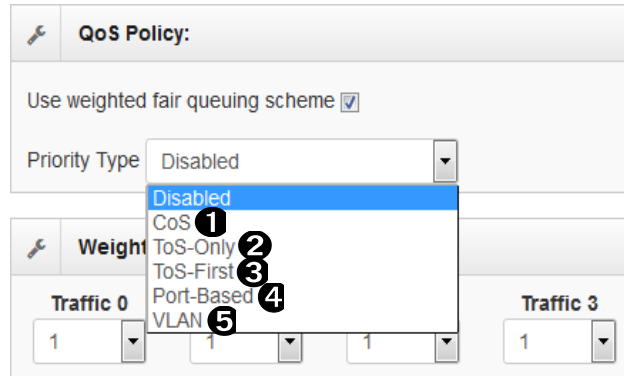
2 Priority Type: Disabled

Weighted Fair Queue Ratio

Traffic 0	Traffic 1	Traffic 2	Traffic 3	Traffic 4	Traffic 5	Traffic 6	Traffic 7
1	1	1	1	1	1	1	1

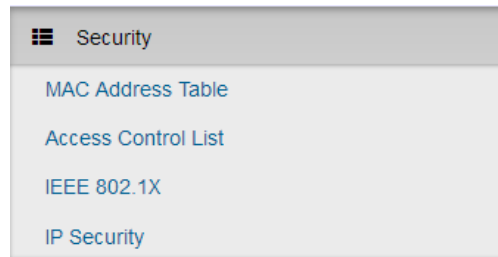
Apply

Name	Description
1 Use the weighted fair queuing scheme	The switch will follow 8:7:6:5:4:3:2:1 rate to process priority queue from the Highest to lowest queue.
2 Priority Type	<p>Port-base: the port priority will follow the default port priority that you have assigned - high, center, low, or lowest.</p> <p>CoS: the port priority will only follow the CoS priority that you have assigned.</p> <p>ToS only: the port priority will only follow the ToS priority that you have assigned.</p> <p>ToS first: the port priority will follow the ToS priority first, and then the other priority rule.</p> <p>Port-based: Set the priority of traffic per port.</p> <p>VLAN: Set the priority of traffic by VLAN.</p>



Name	Description
① CoS	Set the CoS priority level (0 to 7).
② ToS Only	System provides 0~63 ToS Priority level.
③ ToS First	System provides 0~63 ToS priority level. Each level has 8 types of priority - 0~7. The default value is "1" priority for each level. When the IP packet is received, the system will check the ToS level value in the IP packet it has received. For example, the user sets the ToS level 25 is 7. The port 1 is following the ToS priority policy only. When the packet received by port 1, the system will check the ToS value of the received IP packet. If the ToS value of received IP packet is 25 (priority = 7), and then the packet priority will have highest priority.
④ Port Based	Define the priority by switch port.
⑤ VLAN Based	Define the priority by VLAN tag.

9. Security



The “Security” menu contains the dialogs, displays, and tables for configuring the security settings:

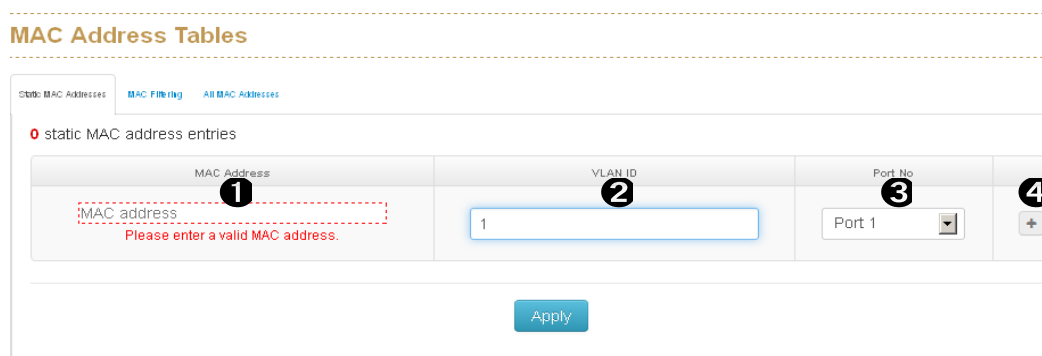
- MAC Address Table
- Access Control List
- IEEE Security 802.1X (Radius Server)
- IP Security

9.1 MAC Address Tables

Use the MAC address table to manage port security.

9.1.1 Static MAC Address

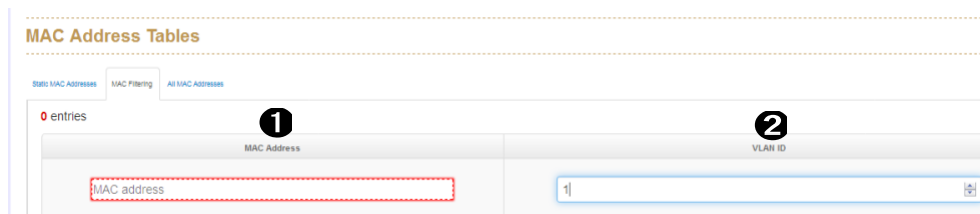
You can add a static MAC address, which will remain in the switch’s MAC address table, regardless of whether the device is physically connected to the switch or not. This saves the switch from having to re-learn a device’s MAC address if it is disconnected or powered off. You can add, modify, or delete a static MAC address.



Name	Description
❶ MAC Address	Enter the MAC address of the device that is allowed on the specified port.
❷ VLAN ID	Enter the corresponding VLAN ID.
❸ Port No.	Specify the port by selecting it from the drop-down list.
❹ +	Add a new entry to the table of static MAC addresses.

9.1.2 MAC Filtering

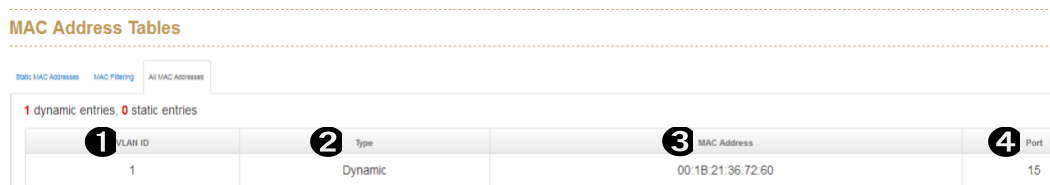
MAC Filtering helps to filter pre-configured MAC addresses, which enhances safety. You can add and delete MAC addresses from the list to be filtered.



Name	Description
❶ MAC Address	Enter the MAC address to be filtered.
❷ VLAN ID	Enter the corresponding VLAN ID.

9.1.3 All MAC Addresses

This panel shows the source MAC address and its corresponding port for all of the packets passing through.



Name	Description
❶ VLAN ID	Displays the VLAN ID.
❷ Type	Dynamic or Static.

③ MAC Address	The MAC address of a connected device or other network equipment.
④ Port	This is the port corresponding to the MAC address.

9.2 Access Control List

This Access Control List (ACL) can be used to deny access to devices with specific IP addresses or MAC addresses.

Access Control List Configuration

Port 1

Port 2

Port 3

Port 4

Port 1

Index	Ingress/Egress	Direction	Type	Address	Mask	Action
1	Ingress	Destination	IP	192.168.13.0	255.255.255.0	Permit
2	Ingress	Destination	IP	192.168.13.0	255.255.255.0	Permit
3	Ingress	Destination	IP	192.168.13.0	255.255.255.0	Permit

Name	Description			
① Index	The index number of the ACL rule.			
② Ingress/Egress	Select whether to apply the ACL rule to Ingress of Egress traffic.			
	<table border="1"> <tr> <td>Options</td> <td>Default Setting</td> </tr> <tr> <td>Ingress Egress</td> <td>Ingress</td> </tr> </table>	Options	Default Setting	Ingress Egress
Options	Default Setting			
Ingress Egress	Ingress			
③ Direction	Apply the ACL rule to either the Source or the Destination address of the packets.			
	<table border="1"> <tr> <td>Options</td> <td>Default Settings</td> </tr> <tr> <td>Source Destination</td> <td>Destination</td> </tr> </table>	Options	Default Settings	Source Destination
Options	Default Settings			
Source Destination	Destination			
④ Type	Apply the ACL rule to either the IP address or the MAC address of the packets.			
	<table border="1"> <tr> <td>Options</td> <td>Default Setting</td> </tr> <tr> <td>IP MAC</td> <td>IP</td> </tr> </table>	Options	Default Setting	IP MAC
Options	Default Setting			
IP MAC	IP			
⑤ Address	Set the address (MAC or IP) to be processed by the ACL rule.			

6 Mask	Set the Subnet Mask.	
7 Action	Select the action to be taken by the ACL rule.	
	Actions	Default Setting
	Deny Permit	Permit

9.3 IEEE 802.1X (Radius Server)

IEEE 802.1X defines a protocol for client/server-based access control and authentication. The protocol restricts unauthorized clients from connecting to a LAN through ports that are open to the Internet, and which otherwise would be readily accessible. The purpose of the authentication server is to check each client that requests access to the port. The client is only allowed access to the port if the client's permission is authenticated.

Radius Server

1 Server IP: 192.168.12.142

2 Server Port: 1812

3 Shared Key: testing123

4 NAS Identifier: superswix

5 Enable on Ports: Select Some Options

9.4 IP Security

The IP security function allows users to assign 20 specific IP addresses that have permission to access the switch through the web browser for switch management.

IP Security

Allowed admin services

1 Web

2 Telnet

3 SSH

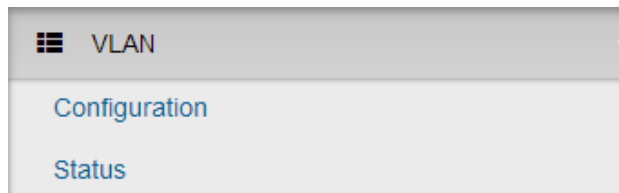
4 Admin Access Restriction Policy: Allow All

5 Denial IPs/Ranges: +

[Input Examples](#)

Name	Description						
① Web	Check this option to make web access available for switch management.						
② Telnet	Check this option to make Telnet access available for switch management.						
③ SSH	Check this option to make SSH access available for switch management.						
④ Admin Access Restriction Policy	Following the IP list should be allowed or denied with web/Telnet/SSH access.						
	<table border="1"> <thead> <tr> <th data-bbox="488 569 959 621">Options</th> <th data-bbox="959 569 1432 621">Default Setting</th> </tr> </thead> <tbody> <tr> <td data-bbox="488 621 959 663">Allow All</td> <td data-bbox="959 621 1432 663">Allow All</td> </tr> <tr> <td data-bbox="488 663 959 705">Deny All</td> <td data-bbox="959 663 1432 705"></td> </tr> </tbody> </table>	Options	Default Setting	Allow All	Allow All	Deny All	
	Options	Default Setting					
Allow All	Allow All						
Deny All							
⑤ IPs/Ranges	Assign up to 20 specific IP addresses to be allowed or denied access to the admin service(s).						

10. VLAN



A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). LAN is the abbreviation for local area network and in this context 'virtual' refers to a physical object recreated and altered by additional logic. VLANs work through tags within network packets and tag handling in networking systems - recreating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks. In this way, VLANs can keep networks separate despite being connected to the same network, and without requiring multiple sets of cabling and networking devices to be deployed.

VLANs allow network administrators to group hosts together, even if the hosts are not on the same network switch. This can greatly simplify network design and deployment, because VLAN membership can be configured through software. Without VLANs, grouping hosts according to their resource needs necessitates the labor of relocating nodes or rewiring data links. It also has benefits in allowing networks and devices that must be kept separate to share the same physical cabling without interacting, for reasons of simplicity, security, traffic management, or economy. For example, a VLAN could be used to separate traffic within a business for different users or between types of traffic, so that users or low priority traffic cannot directly affect the rest of the network. Many Internet hosting services use VLANs to separate their customers' private zones from each other, allowing each customer's servers to be grouped together in a single network segment while being located anywhere in their datacenter. Some precautions are needed to prevent traffic "escaping" from a given VLAN, an exploit known as VLAN hopping.

The VLAN membership configuration for the switch can be monitored and modified here. Up to 4094 VLANs are supported. This panel allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

Note: This section is taken from the Wiki at https://en.wikipedia.org/wiki/Virtual_LAN

10.1 Operation Mode

VLAN Config

Operation Mode: 802.1Q VLAN

802.1Q VLAN Config

1 Management VLAN ID: 0

Port No.	Link Type	VLAN ID	Tagged VLANs
1	Access	1	
2	Access	1	
3	Access	1	
4	Access	1	
5	Access	1	
6	Access	1	

Set Port based VLAN or 802.1Q VLAN

VLAN Config

Operation Mode:

- 1 802.1Q VLAN
- 2 Port based VLAN
- 802.1Q VLAN

Name	Description
1 Port based VLAN	Set an isolated VLAN group by port.
2 802.1Q VLAN	Set an isolated VLAN group by VLAN tag (Default).

10.2 Port-based VLAN Config

Port-based VLAN Config

Group ID	Port Members
1	Port 2 x Port 3 x

Apply

Name	Description
1 Group ID	The ID number for a VLAN Group.
2 Port Members	Select the switch ports to be members of that VLAN group.

10.3 802.1Q VLAN Config

Name	Description
① Management VLAN ID	Define which VLAN group members can access the switch (0 = all VLAN groups).
② Link Type	<p>There are 3 different link types:</p> <p>Access Link: A segment which provides the link path for one or more stations to a VLAN-aware device. An Access Port (untagged port), connected to the access link, has an untagged VID (also called PVID). After an untagged frame arrives at the access port, the switch will insert a four-byte tag in the frame. The contents of the last 12-bits of the tag is the untagged VID. When this frame is sent out through any of the access ports with the same PVID, the switch will remove the tag from the frame to recover it to what it was. Those ports of the same untagged VID are regarded as the same VLAN group members.</p> <p>Trunk Link: A segment which provides the link path for one or more VLAN-aware devices (switches). A Trunk Port, connected to the trunk link, understands tagged frames, which are used for communication among VLANs across switches. Which VID's frames will be forwarded depends on the values filled in the Tagged VID column field. Please insert a comma between each VID.</p> <p>Hybrid Link: A segment which consists of Access and Trunk links. Hybrid ports have the features of both access and trunk ports. A hybrid port has a PVID belonging to a particular VLAN, and it also forwards the specified tagged frames for the purpose of VLAN communication across switches.</p>
③ PVID	Indicates the VLAN ID(s) for each port.
④ Tagged VID	This column is editable when the Link Type is set to Trunk Link or Hybrid Link. Assign a number between 1 and 4094.

10.4 802.1Q VLAN Status

Display the status of each VLAN group.

802.1Q VLAN Status

VLAN ID	Port Members
1	Port 1 U Port 2 U Port 3 U Port 4 U Port 5 U Port 6 U Port 7 U Port 8 U Port 9 U Port 10 U Port 11 T Port 12 T
2	Port 1 U Port 2 U Port 11 T Port 12 T
3	Port 1 U Port 11 T Port 12 T

Icon	Description
U	Untagged (Access) VLAN port.
T	Tagged (Trunk) VLAN port.

11. Multicast VLAN Registration (MVR)

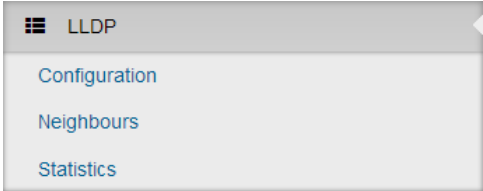


MVR allows the static multicast forwarding table to process the multicast stream from legacy devices that don't support IGMP protocol.



Name	Description
1 VLAN ID	Specify the Multicast VLAN ID.
2 Multicast Addresses	The address of the multicast stream that will be forwarded to the Port Members.
3 Port Members	The list of ports that will receive the specified multicast stream.

12. LLDP



The Link Layer Discovery Protocol (LLDP) is a protocol in the Internet Protocol Suite used by switches to propagate their identity, capabilities, and neighbors on a wired Ethernet network. It is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery Protocol and is specified in IEEE 802.1AB and IEEE 802.3-2012 section 6 clause 79.

12.1 LLDP Configuration

LLDP Configuration

1 Enabled

2 TX Interval(secs)

3 Port NO	4 Mode
1	Both
2	Both

Name	Description
1 Enabled	Enable the switch to send out LLDP information and analyze LLDP information received from neighbors.
2 TX interval (secs)	Enter the interval (5 to 3600 seconds) that the switch will periodically transmit LLDP frames to its neighbors to ensure that the network discovery information is up to date.
3 Port NO	The switch port number for LLDP mode.
4 Mode	Select the LLDP mode: Rx only: The switch port will only get LLDP information from neighbors. Tx only: The switch port will only send out LLDP information to neighbors.

	<p>Disabled: The switch port will not send out LLDP information and will drop LLDP information received from neighbors.</p> <p>Both: The switch port will send out LLDP information, and will analyze LLDP information received from neighbors.</p>
--	---

12.2 LLDP Neighbor Information

This page displays the status of all LLDP neighbors.



Name	Description
1 Local Port	The port which the LLDP frame was received.
2 Chassis ID	The identification of the neighbor's LLDP frames.
3 Port ID	The identification number of the neighbor port.
4 Port Description	The description that is advertised by the neighbor unit.
5 System Name	The name advertised by the neighbor unit.
6 System Capability	<p>This describes the capabilities supported by the neighbor unit, including the following:</p> <ul style="list-style-type: none"> Other Repeater Bridge WLAN Access Point Router Telephone DOCSIS cable device Station only Reserved <p>If a capability is enabled, the capability is shown (+). If the capability is disabled, the capability is shown (-).</p>
7 Management Address	The Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could, for instance, hold the neighbor's IP address.

12.3 LLDP Statistics

This page provides an overview of all LLDP traffic.

LLDP Statistics

Ports	1	2	3	4	5	6	7	8	9	10
Port Number	Neighbors Aged Out	Neighbors Add	Neighbors Delete	Frames Discarded	Frames Received In Error	Frames In	Frames Out	TLVs Discarded	TLVs Unrecognized	
Total										

Name	Description
1 Port Number	The port at which LLDP frames are received or transmitted.
2 Neighbors Aged Out	This displays the number of entries deleted due to Time-To-Live expiration.
3 Neighbors Add	This displays the number of new entries added since a switch reboot.
4 Neighbors Delete	This displays the number of new entries deleted since a switch reboot.
5 Frames Discarded	If an LLDP frame is received on a port, and the switch's internal table is full, the LLDP frame is counted and will be discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.
6 Frames Received in Error	This displays the number of LLDP frames received that contain some kind of error.
7 Frames In	This displays the number of LLDP frames received on the port.
8 Frames Out	This displays the number of LLDP frames transmitted on the port.
9 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.
10 TLVs Unrecognized	This displays the number of TLVs that are well-formed, but have an unknown type value.

13. Cisco Discovery Protocol (CDP)

Cisco Discovery Protocol (CDP) is a proprietary Data Link Layer protocol developed by Cisco Systems. It is used to share information about other directly connected Cisco devices, such as the operating system version and IP address. CDP can also be used for On-Demand Routing, which is a method of including routing information in CDP announcements so that dynamic routing protocols do not need to be used in simple networks.

Cisco devices send CDP announcements out each connected network interface to the multicast destination address 01-00-0C-CC-CC-CC. These multicast frames may be received by Cisco switches and other networking devices that support CDP. This multicast destination is also used in other Cisco protocols such as Virtual Local Area Network (VLAN) Trunking Protocol (VTP). By default, CDP announcements are sent every 60 seconds on interfaces that support Subnetwork Access Protocol (SNAP) headers, including Ethernet, Frame Relay and Asynchronous Transfer Mode (ATM). Each Cisco device that supports CDP stores the information received from other devices in a table that can be viewed using the 'show cdp neighbors' command. This table is also accessible via Simple Network Management Protocol (SNMP). The CDP table information is refreshed each time an announcement is received, and the holdtime for that entry is reinitialized. The holdtime specifies the lifetime of an entry in the table. If no announcements are received from a device for a period in excess of the holdtime, the device information is discarded (default 180 seconds). The information contained in CDP announcements varies by the type of device and the version of the operating system running on it. This information may include the operating system version, hostname, every address (i.e. IP address) from all protocol(s) configured on the port where the CDP frame is sent, the port identifier from which the announcement was sent, device type and model, duplex setting, VTP domain, native VLAN, power draw (for PoE devices), and other device specific information. The details contained in these announcements are easily extended due to the use of the type-length-value (TLV) frame format.

Note: Cisco is a registered trademark of Cisco Systems in the United States and/or other countries.

The above information is taken from the Wiki at https://en.wikipedia.org/wiki/Cisco_Discovery_Protocol

13.1 CDP Configuration Device Settings

CDP Configuration Device Settings

① CDP Enable:

② CDP timer(secs)

③ CDP holdtime(secs)

Port	Enabled
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>

Name	Description
① CDP Enable	Enable the switch to send out CDP information and to analyze CDP information received from neighbors.
② CDP Timer (secs)	Enter the interval (5 to 3600 seconds) that the switch should periodically transmit CDP frames to its neighbors to update network discovery information.
③ CDP Holdtime (secs)	Enter the hold-time value (5 to 3600 seconds) to determine how long the information in the CDP frame shall be considered valid.

13.2 CDP Status

CDP Status

①

Total Packets Output

0

②

Total Packets Input

0

③

Local Port NO

④

CDP Version

⑤

Ageout TTL

⑥

Device ID

⑦

Platform

⑧

Software Version

⑨

Addresses

13.2.1 Statistics

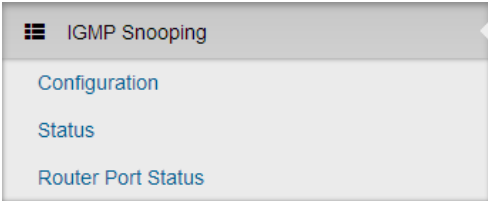
Name	Description
① Total Packets Output	The number of CDP frames transmitted on the switch.
② Total Packets Input	The number of CDP frames received on the switch.

13.2.2 Neighbors

This page provides a status of all CDP neighbors.

Name	Description
③ Local Port NO	The port on which the CDP frame was received.
④ CDP Version	The CDP version advertised by the neighbor unit.
⑤ Ageout TTL	The ageout Time-TOLive advertised by the neighbor device.
⑥ Device ID	The identification number of the neighbor's CDP frames.
⑦ Platform	The description advertised by the neighbor unit.
⑧ Software Version	The software version advertised by the neighbor unit.
⑨ Addresses	The neighbor unit's address (e.g. IP address) that is used by higher layer entities to assist discovery by network management.

14. IGMP Snooping



By default, all Multicast traffic is blocked until requested by a Multicast group member (NOTE: default behavior depends on switch manufacturer). The IGMP filter list is managed by the IGMP Querier - a router or switch configured to send out IGMP group membership queries, retrieve IGMP membership reports, and to allow updating of the group membership tables.

Without IGMP Querying/Snooping, Multicast traffic is treated in the same manner as a Broadcast transmission, which forwards packets to all ports on the network. With IGMP Querying/Snooping, Multicast traffic is only forwarded to ports that are members of that Multicast group. IGMP Snooping generates no additional network traffic, which significantly reduces the Multicast traffic passing through your switch.

Optigo's ONS-C801pi/ONS-C1601pi switches support IGMP and the IGMP snooping function is able to check IGMP packets passing through the network and generate the table holding the member ports for each a multicast group.

14.1 IGMP Snooping Configuration

IGMP Snooping Configuration

Global Configuration

- 1 Enable Querier
- 2 Enable Snooping
- 3 Enable Unregister Flooding
- 4 Flood Well-known Multicast Traffic

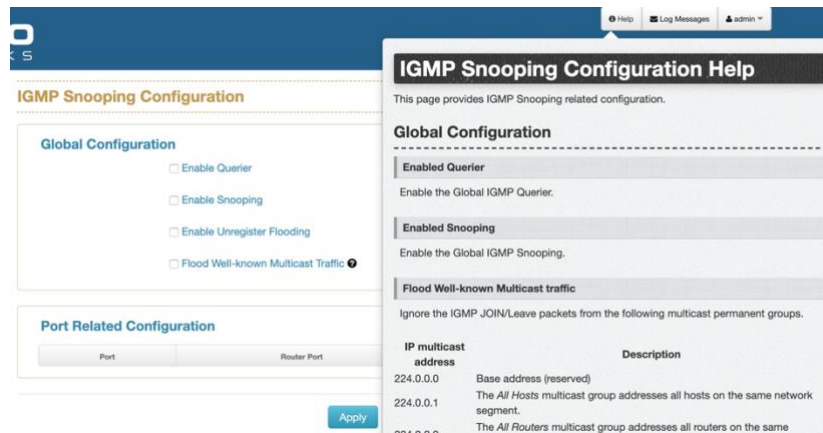
Port Related Configuration

Port	Router Port	Fast Leave
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>

14.1.1 Global Configuration

Name	Description
① Enabled Querier	Enable IGMP Querier.
② Enabled Snooping	Enable IGMP Snooping.
③ Enable Unregister Flooding	Configure the switch to flood all unregistered Multicast data.
④ Flood Well-known Multicast Traffic	Configure the switch to flood all dedicated Multicast data. See help file for more details.

Help File for IGMP Snooping Configuration



14.1.2 Port-Related Configuration

Name	Description
⑤ Port	The switch port number.
⑥ Router Port	Enable the forwarding of all Multicast streams to the router port.
⑦ Fast Leave	Enable fast leave* on the port.

* A device sends an IGMP leave packet (IGMP v2) to a switch, the switch then sends a group query to confirm if any device (host) is left without a response.

14.2 IGMP Snooping Status

This page provides IGMP Snooping status.

14.2.1 Statistics

Statistics							
① VLAN ID	② Status Querier	③ Querier Transmitted	④ Querier Received	⑤ V1 Reports Received	⑥ V2 Leave Received	⑦ V2 Reports Receive Count	⑧ V3 Reports Received
1	IDLE	0	0	0	0	0	12
4093	IDLE	0	0	0	0	0	51

[Clear](#)

Name	Description
① VLAN ID	The VLAN ID of the entry.
② Status Querier	Shows the Querier status is “ACTIVE” or “IDLE”.
③ Querier Transmitted	The number of Transmitted Queries.
④ Querier Received	The number of Received Queries.
⑤ V1 Reports Received	The number of Received IGMP V1 Reports.
⑥ V2 Leave Received	The number of Received IGMP V2 Leaves.
⑦ V2 Reports Received	The number of Received IGMP V2 Reports.
⑧ V3 Reports Received	The number of Received IGMP V3 Reports.

14.2.2 IGMP Groups

The screenshot shows the 'IGMP Groups' configuration page. At the top, there are four input fields labeled 1 through 4: 'VLAN ID', 'Multicast Address', 'Port Members', and 'Membership Interval'. Below these fields is a red 'Clear' button.

Name	Description
① VLAN ID	This is the VLAN ID of the IGMP group.
② Multicast Addresses	This is the Multicast address of the IGMP group.
③ Port Members	These are the ports that are members of the IGMP group.
④ Membership Interval	This is the IGMP table refresh interval (default is 260 seconds).

14.3 Router Port Status

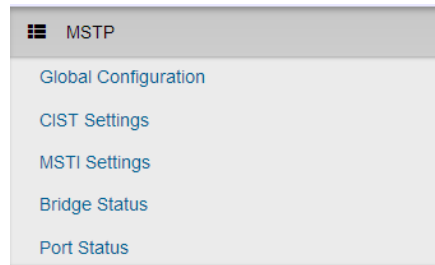
IGMP Router Port Status

The screenshot shows a table titled 'Router Ports'. The table has two columns: 'Port No.' (labeled 1) and 'Status' (labeled 2). The data rows show port 1 with status 'none' and port 2 with status 'none'.

Port No.	Status
1	none
2	none

Name	Description
① Port No.	Port Number.
② Status	Up/Down

15. MSTP



The Spanning Tree Protocol (STP) is a network protocol that builds a logical loop-free topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails. This is done without the danger of bridge loops, or the need for manual enabling or disabling of these backup links.

STP creates a spanning tree within a network of connected layer-2 bridges, and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes.

Within STP, the detection and reconfiguration of network topology (e.g. lost connection, addition of a new switch, etc) takes some time – approximately 30 to 50 seconds. However, many time-sensitive applications cannot tolerate such network down-time. Rapid Spanning Tree Protocol (RSTP) was created to overcome this problem (RSTP takes approximately 5 to 6 seconds to update and re-configure the new network topology/routes).

In RSTP, the link status of each port is monitored pro-actively (instead of waiting for the BPDUs messages) to detect network topology changes quickly, which allows for a faster response. RSTP is backward compatible with STP switches.

MSTP (Multiple Spanning Tree Protocol) can map a group of VLAN's into a single Multiple Spanning Tree instance (MSTI). With MSTP, Spanning Tree Protocol is applied separately for a set of VLAN's instead of the whole network. Different root switches and different STP parameters can be individually configured for each MSTI, so one link can be active for one MSTI and the other link active for the second MSTI, this enables some degree of load-balancing. In general, two MSTI's are used in the network for easier implementation.

Note: This section is taken from the Wiki at https://en.wikipedia.org/wiki/Spanning_Tree_Protocol

15.1 MSTP Global Configuration

MSTP Global Configuration

1 Mode:

2 Name:

3 Revision:

4 Max Age:

5 Forward Delay:

6 Max Hops:

Name	Description						
1 Mode	<p>Select STP, RSTP, or MSTP redundancy protocol for the network.</p> <table border="1"> <thead> <tr> <th>Options</th> <th>Default Setting</th> </tr> </thead> <tbody> <tr> <td>STP</td> <td rowspan="3">MSTP</td> </tr> <tr> <td>RSTP</td> </tr> <tr> <td>MSTP</td> </tr> </tbody> </table>	Options	Default Setting	STP	MSTP	RSTP	MSTP
Options	Default Setting						
STP	MSTP						
RSTP							
MSTP							
2 Name	This is the MSTP name which identifies VLAN to MSTI mapping. Bridges must match the name and revision, as well as the VLAN-to-MSTI mapping configuration, in order to share spanning trees for MSTI's (Intra-region). The name column is up to 32 characters.						
3 Revision	This is the revision of the MSTP configuration named above. This must be an integer between 65535.						
4 Max Age	This is 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. Max Age must be less than or equal to: $(FwdDelay - 1) * 2$.						
5 Forward Delay	This is the delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the 4 to 30 second range.						
6 Max Hops	This is 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.						

15.2 CIST Settings

15.2.1 Bridge Configuration

CIST Settings

Bridge Configuration

① VLANs

② Priority

Port Configuration

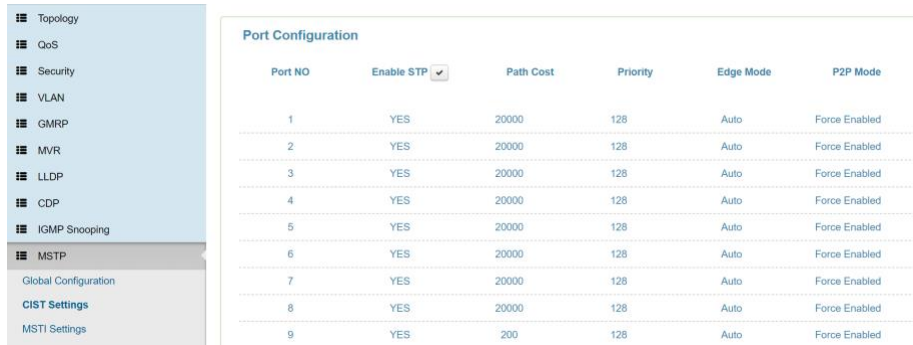
③ Port NO	④ Enable STP	⑤ Path Cost	⑥ Priority	⑦ Edge Mode	⑧ P2P Mode
1	NO	0	128	Auto	Force Enabled
2	NO	0	128	Auto	Force Enabled

Name	Description
① VLANs	This is the list of VLANs mapped to the MSTI. The VLANs must be separated with commas and/or spaces. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty (i.e. with no VLANs mapped to it). Unmapped VLANs are mapped to the CIST (The default bridge instance).
② Priority	Enter the bridge priority here. Lower numeric values have the greatest priority. The bridge priority, plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, forms a Bridge Identifier.

15.2.2 Port Configuration

Name	Description
③ Port No	This is the STP switch port number.
④ Enable STP	Controls whether STP is enabled with this switch port (See Below).
⑤ Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost appropriate by the physical link speed, using the 802.1D recommended values.
⑥ Priority	Controls the port priority. This can be used to control priority of ports having identical path cost (See Above).
⑦ Edge Mode	The port which connects with ending device.
⑧ P2P Mode	The port which connects with another switch.

15.2.3 How to enable STP/RSTP



The screenshot shows a configuration menu on the left with 'MSTP' selected. The main area displays a 'Port Configuration' table with the following data:

Port NO	Enable STP <input checked="" type="checkbox"/>	Path Cost	Priority	Edge Mode	P2P Mode
1	YES	20000	128	Auto	Force Enabled
2	YES	20000	128	Auto	Force Enabled
3	YES	20000	128	Auto	Force Enabled
4	YES	20000	128	Auto	Force Enabled
5	YES	20000	128	Auto	Force Enabled
6	YES	20000	128	Auto	Force Enabled
7	YES	20000	128	Auto	Force Enabled
8	YES	20000	128	Auto	Force Enabled
9	YES	200	128	Auto	Force Enabled

How to enable STP/RSSTP

A: Select STP or RSTP in MSTP Global Configuration (see section 16.1).

B: Press icon to enable STP under CIST Settings.

Note: The default is enabled for all ports.

15.2.4 How to enable MSTP

A: Select MSTP in MSTP Global Configuration (see section 16.1).

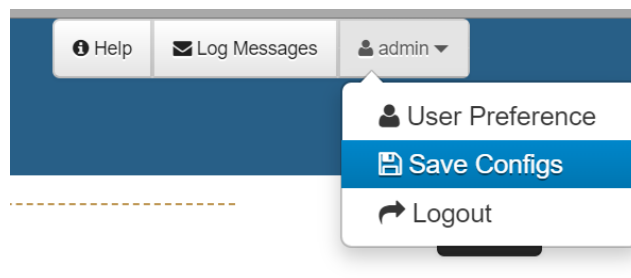
B: Enable STP under CIST Settings.

C: Check the status under 'Enable STP'. All ports should change to 'YES'.

D: Remember to press 'Apply'.



E: Save the new setting.



15.3 MSTP MSTI Settings

MSTP MSTI Settings

① Instance NO
② Enabled
③ VLANs
④ Priority
+

Apply

Name	Description
① Instance NO	This is the index number of the MSTP instance.
② Enabled	This particular instance is enabled.
③ VLANs.	This is the list of VLANs mapped to the MSTI. A VLAN can only be mapped to one MSTI at a time. Unmapped VLANs are mapped to the CIST (the default bridge instance).
④ Priority	Controls the bridge priority. Lower numeric values have better priority.

15.4 MSTP Bridges Status

MSTP Bridges Status

① NO	② Bridge ID	③ Root ID	④ Root Port	⑤ Root Cost	⑥ Topology State
CIST 0	32768-286046ff00ff	32768-286046ff00ff	0	0	Stable

Name	Description
① NO	This is the number of the MSTP instance.
② Bridge ID	This is the ID of this Bridge instance.
③ Root ID	This is the ID of the currently elected root bridge.
④ Root Port	This is the port number of the root port.
⑤ 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 costly path to the Root Bridge.
⑥ Topology State	The current state of the Topology.

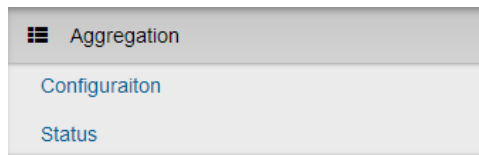
15.5 Bridge Status of all Ports

Bridge status of all ports

1 Port 1 as Designated/FORWARDING in CIST	Port 2 as Disabled/BLOCKING in CIST	Port 3 as Disabled/BLOCKING in CIST
2 Port 4 as Disabled/BLOCKING in CIST	Port 5 as Disabled/BLOCKING in CIST	Port 6 as Disabled/BLOCKING in CIST
Port 7 as Designated/FORWARDING in CIST	Port 8 as Disabled/BLOCKING in CIST	Port 9 as Disabled/BLOCKING in CIST
Port 10 as Disabled/BLOCKING in CIST	Port 11 as Disabled/BLOCKING in CIST	Port 12 as Disabled/BLOCKING in CIST

Name	Description				
1 Port	This is the switch port number of the STP port.				
2 Role	<p>This is the current STP port role of the port. The port role can be one of the following variants:</p> <table border="1"> <thead> <tr> <th>Options</th> <th>Default Setting</th> </tr> </thead> <tbody> <tr> <td>Alternate Port Backup Port Root Port Designated Port Disabled</td> <td>The current setting</td> </tr> </tbody> </table>	Options	Default Setting	Alternate Port Backup Port Root Port Designated Port Disabled	The current setting
Options	Default Setting				
Alternate Port Backup Port Root Port Designated Port Disabled	The current setting				
3 State	<p>The current STP port state of the port. The port state can be one of the following variants:</p> <table border="1"> <thead> <tr> <th>Options</th> <th>Default Setting</th> </tr> </thead> <tbody> <tr> <td>Discarding Learning Forwarding Blocking</td> <td>The current setting</td> </tr> </tbody> </table>	Options	Default Setting	Discarding Learning Forwarding Blocking	The current setting
Options	Default Setting				
Discarding Learning Forwarding Blocking	The current setting				

16. Link Aggregation



In computer networking, the term link aggregation applies to various methods of combining (aggregating) multiple network connections in parallel in order to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links should fail. A Link Aggregation Group (LAG) combines a number of physical ports together to make a single high-bandwidth data path, so as to implement traffic load sharing among the member ports in the group and to enhance connection reliability.

Other umbrella terms used to describe the method include port trunking, link bundling, Ethernet/network/NIC bonding, or NIC teaming. These umbrella terms encompass not only vendor-independent standards such as Link Aggregation Control Protocol (LACP) for Ethernet defined in IEEE 802.3ad standard, but also various proprietary solutions.

Note: This section is taken from the Wiki at https://en.wikipedia.org/wiki/Link_aggregation

16.1 Aggregation Configuration

Group Configuration

Aggregation Configuration

Group Configuration:

Ports must have the same VLAN/trunk settings before they can be dynamically combined into a port channel/aggregation port/trunking group.

1 Trunking Group	2 Enable LACP Dynamic Trunking	3 Port Members
1	<input type="checkbox"/>	Choose ports...
2	<input type="checkbox"/>	Choose ports...

Name	Description
① Trunking Group	This is the number of the trunk group.
② Enable LACP Dynamic Trunking	Enable the LACP Dynamic Trunk function by checking the box.
③ Port Members	Select which ports you want to aggregate with.

16.2 LACP Group Status

LACP Group Status



Name	Description
① Group ID	Number of trunk group (1 to 8 max).
② Type	LACP (enabled) or Static (not enabled).
③ Trunk Members	Switch ports which bind the trunk group (Type → Static).

17. G.8032 ERPS

☰
G.8032 ERPS

Configuration

Status

17.1 Configuration

ID
1

Enabled
2

Role
3

Type
4

VLAN
5

Ring Port 0
6

Ring Port 1
7

Node Failure Protection
8

Detect Miswiring
9

+
10

Name	Description
1 ID	Identifying number.
2 Enabled	Yes / No .
3 Role	Role in Ring (Neighbor / Owner).
4 Type	Type of Ring (Major / Sub).
5 VLAN	VLAN ID.
6 Ring Port 0	Which port will Port0 connect to the ethernet ring.
7 Ring Port 1	Which port will Port1 connect to the ethernet ring.
8 Node Failure Protection	Node Fail Detection Enabled?
9 Detect Miswiring	Miswiring Detection Enabled?
10 +	Add a new ring.

17.2 Status

Ring Status

1
ID

2
State

3
Role

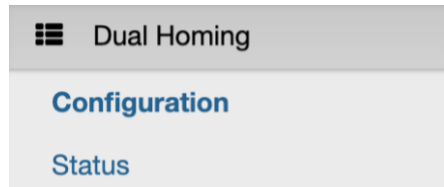
4
Ring Port 0

5
Ring Port 1

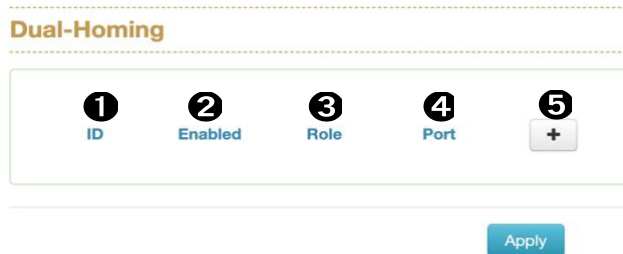
Name	Description
1 ID	Identifying number.

② State	Enabled / Disabled .
③ Role	Neighbor / Owner .
④ Ring Port 0	Which port will Port0 connect to the ethernet ring.
⑤ Ring Port 1	Which port will port1 connect to the ethernet ring.

18. Dual Homing



18.1 Configuration



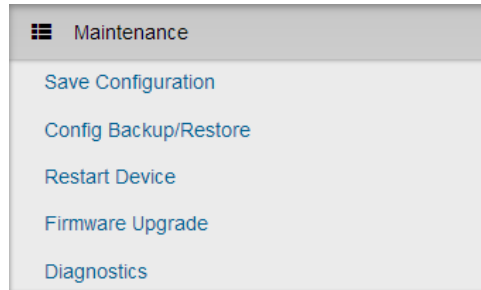
Name	Description
① ID	Identifying number.
② Enabled	Yes / No .
③ Role	Primary or Secondary.
④ Port	Port that this will be configured on.
⑤ +	Add new Dual-Homing.

18.2 Status



Name	Description
① ID	Identifying Number.
② Port	Yes / No .
③ Role	Primary or Secondary.
④ Blocking	Passing / Blocking Traffic .
⑤ State	UP / Down .

19. Maintenance



19.1 Save Configuration

System Config Save



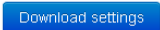
Click to save the settings

19.2 Config Backup/Restore

Config Backup/Restore

1 Settings Backup

Click button to download current settings



2 Settings Restore

Select the file previously backup to restore



3 Reset to default

Click button to reset to default settings



Name	Description							
❶ Settings Backup	Download/export the configuration from switch for back up.							
❷ Settings Restore	Upload/import a previous configuration to startup.							
❸ Reset to default	Reset the switch with four resetting options.							
	<table border="1"> <thead> <tr> <th>Resetting Options</th> <th>Default Setting</th> </tr> </thead> <tbody> <tr> <td>Keep IP & Account</td> <td rowspan="4">Keep IP & Account</td> </tr> <tr> <td>Keep User Accounts</td> </tr> <tr> <td>Keep Network Configs</td> </tr> <tr> <td>Restore Everything</td> </tr> </tbody> </table>	Resetting Options	Default Setting	Keep IP & Account	Keep IP & Account	Keep User Accounts	Keep Network Configs	Restore Everything
	Resetting Options	Default Setting						
Keep IP & Account	Keep IP & Account							
Keep User Accounts								
Keep Network Configs								
Restore Everything								

19.3 Restart Device (Maintenance Reboot)

Click the 'Restart Device' button to manually reboot the switch.

Maintenance Reboot

Restart Device

19.4 Firmware Upgrade

Update the switch's firmware by pressing "Select File" to select the proper firmware on the computer and then perform the firmware upgrade. This will take from 60 to 90 seconds to complete.

Firmware Upgrade

Select the firmwire file to upload

Select File

19.5 Diagnostics

The diagnostic panel contains two troubleshooting tools:

- Ping
- ARP Table
- DDM

19.5.1 Ping

Diagnostics

Ping **ARP Table** **DDM**

➊ Address

➋ Count

➌ Packet Size

```
PING 10.2.100.121 (10.2.100.121): 64 data bytes
72 bytes from 10.2.100.121: seq=0 ttl=64 time=0.325 ms
72 bytes from 10.2.100.121: seq=1 ttl=64 time=0.203 ms
72 bytes from 10.2.100.121: seq=2 ttl=64 time=0.180 ms
72 bytes from 10.2.100.121: seq=3 ttl=64 time=0.192 ms
--- 10.2.100.121 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.180/0.225/0.325 ms
```

Name	Description
➊ Address	Enter the IP address to ping.
➋ Count	Enter how many times to ping the address.
➌ Packet Size	Enter the size of the ping packet.

19.5.2 ARP Table

Address Resolution Protocol (ARP) helps to map an IP address to a MAC address that is recognized on the local network and the ARP Table shows the list of pinged MAC addresses and their corresponding IP addresses.

Ping ARP Table

ARP Table	
00:1f:c6:3d:7e:be	192.168.9.47
00:50:7f:5a:3e:b8	192.168.9.1

19.5.3 DDM

Digital Diagnostics Monitoring for SFP.

Diagnostics

Ping ARP Table DDM

SFP Digital Diagnostic Monitor

Show threshold values stored on SFP transceivers Event Setup

Port 9 Link Down						
Type	Temperature	Vcc	Bias	TX Power	RX Power	
Current Value	0.0 °C	0.0 V	0.0 mA	-∞ dBm	-∞ dBm	

Port 10 Link Down						
Type	Temperature	Vcc	Bias	TX Power	RX Power	
Current Value	0.0 °C	0.0 V	0.0 mA	-∞ dBm	-∞ dBm	

Name	Description
① Type	Current Value/Last Known Value.
② Temperature	Internal Temperature of the SFP.
③ Vcc	Internal supply voltage.
④ Bias	Bias current of the transmitter.
⑤ TX Power	Launch Power (TSSI).
⑥ RX Power	Receive Power (RSSI).