VOLKTEK

User Manual

IEN-8648-PN

Managed 8 x 10/100/1000 RJ45 & 4 x GbE SFP
Industrial PROFINET Switch

v.1.1, 02/2020

COPYRIGHT

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photo copying, recording or otherwise, without the prior written permission of the publisher.

FCC WARNING

This equipment has been tested and found to comply with the limits for a class A device, pursuant to part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. Operation of this equipment in a residential area is likely to cause harmful interference, in which case, the user will be required to correct the interference at the user's own expense.

CE

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

HOT& COLD WARNING

The Switch surface will getting very hot or cold depend on the operating environment. Please take special care when touch to the working switch.

Warning

Take special care to read and understand all the content in the warning boxes.

Warning

Do not work on the system or connect or disconnect cables during periods of lightning activity.

⚠ **Warning**

Take special care to read and understand all the content in the warning boxes.

⚠ **Warning**

Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

⚠ **Warning**

Do not stack the chassis on any other equipment. If the chassis falls, it can cause severe bodily injury and equipment damage.

⚠ **Warning**

An exposed wire lead from a DC-input power source can conduct harmful levels of electricity. Be sure that no exposed portion of the DC-input power source wire extends from the terminal block plug.

⚠ **Warning**

Ethernet cables must be shielded when used in a central office environment.

⚠ **Warning**

If a redundant power system (RPS) is not connected to the switch, install an RPS connector cover on the back of the switch.

⚠ **Warning**

Read the wall-mounting instructions carefully before beginning installation. Failure to use the correct hardware or to follow the correct procedures could result in a hazardous situation to people and damage to the system.

⚠ **Warning**

Before performing any of the following procedures, ensure that power is removed from the DC circuit.

Warning

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Warning

This unit might have more than one power supply connection. All connections must be removed to de-energize the unit.

Warning

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Warning

When installing or replacing the unit, the ground connection must always be made first and disconnected last.

Warning

No user-serviceable parts inside. Do not open.

Warning

This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Table of Content

1. About this Manual

1.1. Welcome

The IEN-8648-PN is a Managed Industrial PROFINET Switch perfectly suited for industrial network applications which require managed devices that offer hassle-free fiber deployment and an ideal solution to deploy in automation systems. The switch's rugged IP30 aluminum case and hardened components withstand in operating temperatures from -40℃ to 75℃.

PROFINET has become one of the most important communication standards in the field of automation. Network devices can be configured and monitored using the plug-and-play principle, enabling you to benefit from convenient, system-wide engineering. What's more, our comprehensive product portfolio permits you to build homogeneous PROFINET solutions with end-to-end features such as management, diagnostic and filter functions, and a variety of redundancy protocols, security mechanisms and real-time applications. You obtain by far the most extensive functional scope in the field of automation.

The IEN-8648-PN features with 4-slot Gigabit SFP which immune to moisture, static electricity, power surges and short circuits, plus 8 10/100/1000Base-T ports. Switch is also equipped with a variety of management functions that let you configure communication parameters as you desire and monitor the network behavior in number of different simple ways. In addition, the switch is built with dual redundant power inputs to ensure reliability and maximize network up time. Other integrated features of the switch such as Rate limitation, Port Isolation etc., optimizes your network performance and provide a secure network, offering a cost-effective solution in a small but powerful package.

1.2. Purpose

This guide describes how to install and configure the IEN-8648-PN Industrial Managed PROFINET Switch.

1.3. Terms/ Usage

In this guide, the term "Switch" (first letter upper case) refers to the IEN-8648-PN Switch, and "switch" (first letter lower case) refers to other switches.

2. About the IEN-8648-PN

2.1. Features

Network Functions
Port-based Mirroring
4K Active VLAN
IGMP Snooping v1/v2/v3
IGMP Querier
Link Layer Discovery Protocol
Loop Detection, Auto Recovery Timer
STP/RSTP
PROFINET MRP Slave mode
SFP DDMI Support
RMON Statistics
Loop Detection, Auto Recovery Timer

Network Security
Access Control List (L2/L3/L4)
MAC Limitation

Traffic management & QoS
Port Priority
Rate Limitation
Storm Control
Port Isolation
Auto MDI/MDI-X
802.1Q Tag-based VLAN

Network Management
Command Line Interface, Telnet
Web GUI
SNMP v1/v2c/v3
Management VLAN
System log
Firmware Upgradable
Configuration Upload/Download
LED, SNMP trap

2.2. Specifications

IEEE Standards	
IEEE 802.3	10Base-T
IEEE 802.3u	100Base-TX
IEEE 802.3ab	1000Base-T
IEEE 802.3z	1000Base-SX/LX
IEEE 802.3x	Flow Control
IEEE 802.1d	Spanning Tree Protocol
IEEE 802.1w	Rapid STP
IEEE 802.1q	VLAN Tagging
IEEE 802.1p	Class of Service
IEEE 802.1ab	Link Layer Discovery Protocol
Performance	
Switching fabric	24Gbps
L2 forwarding	17.86Mpps
Packet buffer size	8Mbits
MAC Entries	16 K
Jumbo frame	10 K

Ports

10/100/1000Base-T (RJ45)	8
Gigabit SFP slots	4
Console port (RJ45 to RS232)	1

Power

Input Voltage:

- Primary inputs	12~60VDC at 1.5A
- Redundant inputs	12~60VDC at 1.5A.

Connection:

Removable 6-pin terminal block	one
Overload current protection	Support
Reverse Polarity Protection	Support
Relay output	One with current carrying capacity of 1 A @ 24V DC

Mechanical

Dimension (WxHxD)	50x161.5x122.2mm (1.97x6.36x4.81 inch)
Weight	860g
Mounting	DIN-Rail
Housing	IP30 protection

Operating Requirement

Operating temperature	-40 to 75℃
Storage temperature	-40 to 85℃
Operating humidity	5% to 95% RH (Non Condensing)
Storage humidity	5% to 95% RH (Non Condensing)

DIN RAIL Recommendation

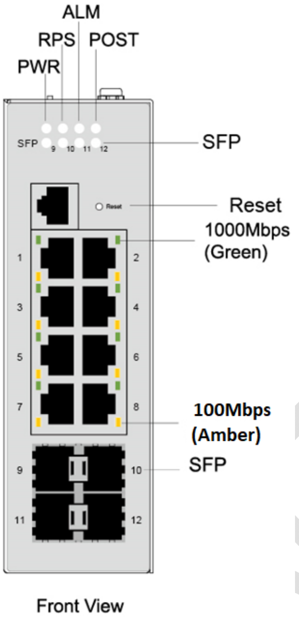
Steel with Electrolytic Zinc Plating

Stand-Off Brackets: 45^0 Angle and Straight

Comply with DIN 50045, 50022 and 50035 Standards

3. Hardware Description

IEN-8648-PN Front Panel



8x10/100/1000Base-Tports + 4xGigabit SFP slots
Managed Industrial Ethernet Switch

3.1. Connectors

The Switch utilizes ports with copper and SFP fiber port connectors functioning under Ethernet/Fast Ethernet/Gigabit Ethernet standards.

10/100/1000Base-T Ports

The 10/100/1000Base-T ports support network speeds of 10Mbps, 100Mbps or 1000Mbps, and can operate in half- and full-duplex transfer modes. These ports also offer automatic MDI/MDI-X crossover detection that gives true “plug-n-play” capability – just plug the network cables into the ports and the ports will adjust according to the end-node devices. The following are recommended cabling for the RJ45 connectors: (1) 10Mbps – Cat 3 or better; (2) 100/1000Mbps – Cat 5e or better.

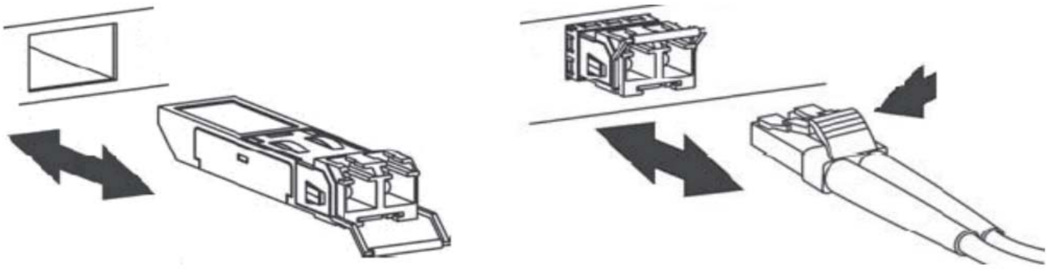
SFP Slots for SFP modules

The four SFP slots are designed to Gigabit SFP modules that support network speed of1000Mbps.

Installing the SFP modules and Fiber Cable

1. Slide the selected SFP module into the selected SFP slot (Make sure the SFP module is aligned correctly with the inside of the slot)
2. Insert and slide the module into the SFP slot until it clicks into place
3. Remove any rubber plugs that may be present in the SFP module’s mouth
4. Align the fiber cable’s connector with the SFP module’s mouth and insert the connector
5. Slide the connector in until a click is heard

6. If you want to pull the connector out, first push down the release clip on top of the connector to release the connector from the SFP module.



To properly connect fiber cabling: Check that the fiber terminators are clean. You can clean the cable plugs by wiping them gently with a clean tissue or cotton ball moistened with a little ethanol. Dirty fiber terminators on fiber optic cables will impair the quality of the light transmitted through the cable and lead to degraded performance on the port.

Note: When inserting the cable, be sure the tab on the plug clicks into position to ensure that it is properly seated.

Check the corresponding port LED on the Switch to be sure that the connection is valid. (Refer to the LED chart).

3.2. Installation

The location chosen for installing the Switch may greatly affect its performance. When selecting, we recommend considering the following rules:

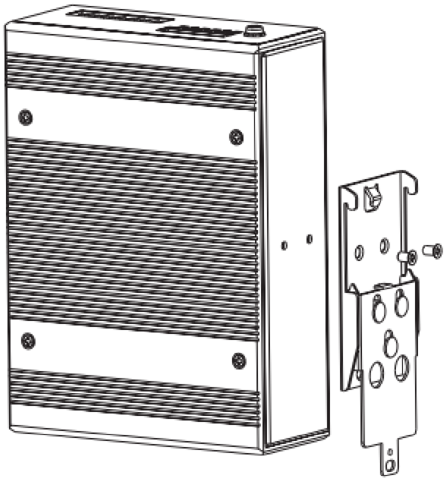
- ✓ Install the Switch in an appropriate place. See Technical Specifications for the acceptable temperature and humidity ranges.
- ✓ Install the Switch in a location that is not affected by strong electromagnetic field generators (such as motors), vibration, dust, and direct sunlight.
- ✓ Leave at least 10cm of space at the front and rear of the unit for ventilation.

ATTENTION

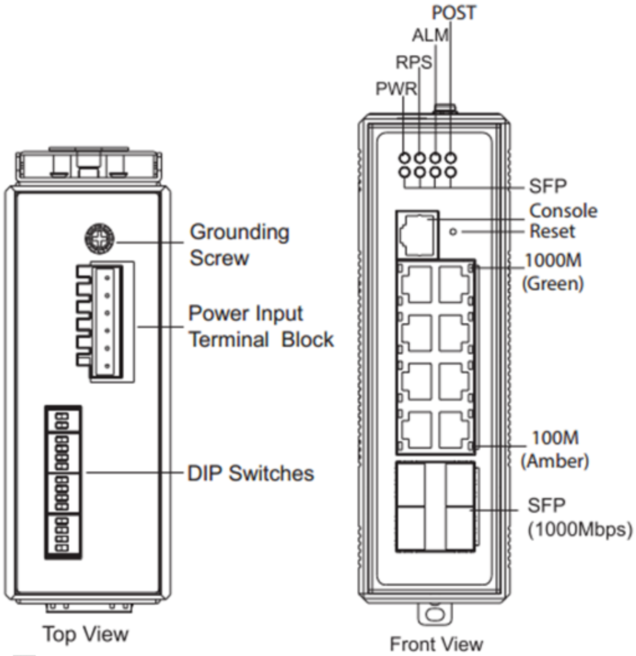
⚠ The IEN-8648-PN is an open type device and IEN-8648-PN shall be DIN-Rail mounted or wall mounted (optional) in cabinet or enclosure

Hardware Installation

- ✓ **Step 1**: Unpack the device and other contents of the package.
- ✓ **Step 2**: Fasten DIN-Rail kit on the rear of the IEN-8648-PN



- ✓ **Step 3:** Connect the 12~60V DC power to the power terminal block.

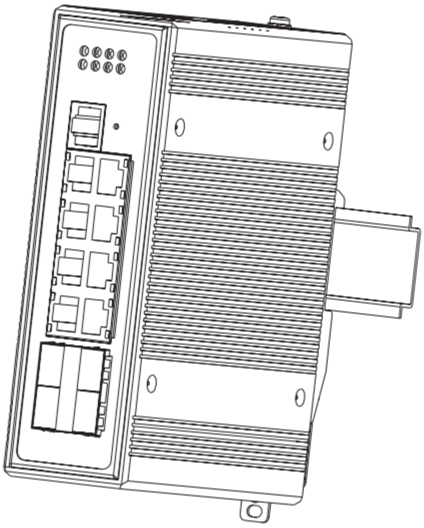


- ✓ **Step 4**: Connect the Ethernet (RJ45) port to the networking device and check the LED status to confirm the connection is established.

DIN rail Installation
The IEN-8648-PN has a DIN rail bracket on the back of the Switch.

Location: The IEN-8648-PN can be DIN-Rail-mounted in cabinet or enclosure.

Mounting the switch:
Place the IEN-8648-PN on the DIN rail from above using the slot and push the front of the switch toward the mounting surface until it snaps into place with a click sound.



Dismounting the switch

Pull out the lower edge of the switch and then remove the switch from the DIN rail.

Ground the Switch:

Before powering on the switch, ground the switch to earth. Ensure the rack on which the switch is to be mounted is properly grounded and incompliance with ETSI ETS 300 253. Verify that there is a good electrical connection to the grounding point on the rack (no paint or isolating surface treatment).

ATTENTION

This product is intended to be mounted to a well-grounded mounting surface such as a metal panel.

CAUTION

The earth connection must not be removed unless all power supply connection has been disconnected.

The device is installed in a restricted-access location it has a separate protective Earthing terminal on the chassis that must be permanently connected to earth ground to adequately ground the chassis and protect the operator from electrical hazards.

ATTENTION

The product should be mounted in an Industrial Control Panel and the ambient temperature should not exceed 75°C.

ATTENTION

A corrosion-free mounting rail is advisable.

When installing, make sure to allow for enough space to properly install the cabling.

Wiring Power Inputs

You can use “Terminal Block (PWR)” for Primary Power input and “Terminal Block (RPS)” for secondary power source for Redundant Power Input.

To insert power wire and connect the 12~60V DC power to the power terminal block, follow the steps below:

- ✓ **Step 1**: Insert the positive/negative DC wires into the V+/V- terminal, respectively.
- ✓ **Step 2**: Use you r finger to press the orange plug on top of terminal block connector to insert power cables.
- ✓ **Step 3**: Insert the terminal block connector which includes "PWR" and "RPS" into the terminal block receptor which is located on the top panel.

WARNING

⚠

- Use **copper** conductors only, **60/75°C**, tighten to **5lb**
- The wire gauge for the terminal block should range between **12~24 AWG**.

Redundant Power Input: Choose "Terminal Block (PWR)" as primary power and "Terminal Block (RPS)" for redundant power option

Connect power cables to terminal block: *Use your finger to press the orange plug on top of terminal block connector to insert power cables*

WARNING

⚠ Safety measures should be taken before connecting the power cable. Turn off the power before connecting modules or wires. The correct power supply voltage is listed on the product label. Check the voltage of your power source to make sure that you are using the correct voltage. DO NOT use a voltage greater than what is specified on the product label. Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size. If current exceeds the maximum rating, the wiring can overheat causing serious damage to your equipment.

Please read and follow these guidelines:

- Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.

NOTE: Do not run signal or communications wiring and power wiring through the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.

- You can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring that shares similar electrical characteristics can be bundled together
- You should separate input wiring from output wiring
- We advise that you label the wiring to all devices in the system.

Wiring the Alarm Contact:

The Alarm Contact consists of the two last contacts of the terminal block on switch's top panel.

ALM: The two last contacts of the 6-contact terminal block connector are used to detect both power faults and port faults. The two wires attached to the ALM contacts form an open circuit when:

1. The Switch has lost power from one of the DC power inputs.
OR
2. One of the ports for which the corresponding PORT ALARM DIP Switch is set to ON is not properly connected.

If neither of these two conditions is satisfied, the Fault circuit will be closed.

WARNING

- Use **copper** conductors only, **60/75°C**, tighten to **5lb**
- The wire gauge for the terminal block should range between **12~24 AWG**.

Powering On the Unit

The Switch accepts the power input voltage from 12~60VDC.

✓ Insert the power cables into the terminal block located on the top of the device.

✓ Check the front-panel LEDs as the device is powered on to verify that the Power LED is lit. If not, check that the power cable is correctly and securely plugged in.

Notice: Turn off the power before connecting modules or wires.

- *The correct power supply voltage is listed on the product label. Check the voltage of your power source to make sure that you are using the correct voltage. Do NOT use a voltage greater than what is specified on the product label.*
- *Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size. If current go above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.*

Reset Button

There is a "Reset" button in front of Switch which helps to manually reboot the device.

3.3. LED Indicators

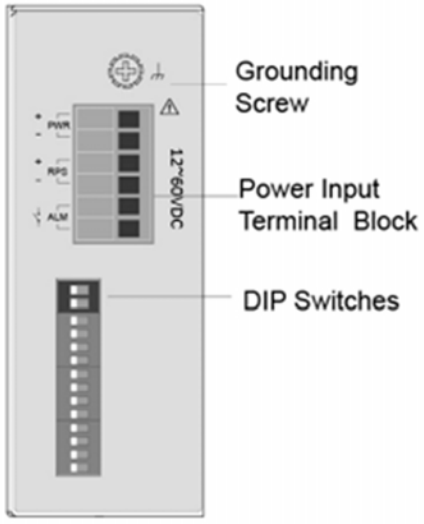
This Switch is equipped with Unit LEDs to enable you to determine the status of the Switch, as well as Port LEDs to display what is happening in all your connections. They are as follows:

LED	Condition	Status
PWR	Illuminated	Primary Power on
	Off	Primary Power off or failure
RPS	Illuminated	Redundant (secondary) Power on
	Off	Redundant Power off or failure
ALM	Illuminated	Alarm for following conditions ✓ Power lost ✓ Link lost ✓ Abnormal voltage input
	Off	Normal operation or DIP function is disabled
POST	Illuminated	System is ready to use

	Blinking	Power on self-test
	Off	Power off or test fail
Port Number 1-8 Copper port LED (10/100/1000Mbps)		
1000M	Illuminated	Link speed is at 1000Mbps
	Blinking	Activity (receiving or transmitting data)
	Off	Port disconnected or link failed
10/100M	Illuminated	Ethernet link-up at 100Mbps or 10Mbps
	Blinking	Activity (receiving or transmitting data)
	Off	Port disconnected or link failed
Port number 9-12 SFP slot LED (1000Mbps)		
SFP	Illuminated	Ethernet link-up
	Blinking	Activity (receiving or transmitting data)
	Off	Port disconnected or link failed

3.4. DIP Switches

- Power: DIP 1 and DIP 2 is for primary power and redundant power supply.
- Alarm Relay output: DIP 3 to DIP 14 control each of ports to trigger the external alarm device.



Top View

No	Name	Description
1	PWR	ON: Master power alarm reporting is enabled OFF: Master power alarm reporting is disabled
2	RPS	ON: Redundant power alarm reporting is enabled OFF: Redundant power alarm reporting is disabled
3	P1	ON: port 1 link alarm reporting is enabled. OFF: port 1 link alarm reporting is disabled.
4	P2	ON: port 2 link alarm reporting is enabled. OFF: port 2 link alarm reporting is disabled.
5	P3	ON: port 3 link alarm reporting is enabled.

		OFF: port 3 link alarm reporting is disabled.
6	P4	ON: port 4 link alarm reporting is enabled. OFF: port 4 link alarm reporting is disabled.
7	P5	ON: port 5 link alarm reporting is enabled. OFF: port 5 link alarm reporting is disabled.
8	P6	ON: port 6 link alarm reporting is enabled. OFF: port 6 link alarm reporting is disabled.
9	P7	ON: port 7 link alarm reporting is enabled. OFF: port 7 link alarm reporting is disabled.
10	P8	ON: port 8 link alarm reporting is enabled. OFF: port 8 link alarm reporting is disabled.
11	P9	ON: port 9 (SFP) link alarm reporting is enabled. OFF: port 9 (SFP) link alarm reporting is disabled.
12	P10	ON: port 10 (SFP) link alarm reporting is enabled. OFF: port 10 (SFP) link alarm reporting is disabled.
13	P11	ON: port 11 (SFP) link alarm reporting is enabled. OFF: port 11 (SFP) link alarm reporting is disabled.
14	P12	ON: port 12 (SFP) link alarm reporting is enabled. OFF: port 12 (SFP) link alarm reporting is disabled.

4. System Status

4.1. Console Port

- Connect your computer to the console port on the Switch using the appropriate cable.
- Use terminal emulation software with the following settings:

Default Settings for the Console Port

Setting	Default Value
Terminal Emulation	VT100
Baud Rate	38400
Parity	None
Number of Data Bits	8
Number of Stop Bits	1
Flow Control	None

- Press [ENTER] to open the login screen.

Setting	Default Value
Default Username	admin
Default Password	admin

4.2. Telnet/SSH

- Connect your computer to one of the Ethernet ports.
- Open a Telnet session to the Switch's IP address. If this is your first login, use the default values.

Default Management IP Address

Setting	Default Value
IP Address	192.168.0.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Management VLAN	1
Default Username	admin
Default Password	admin

- Make sure your computer IP address is in the same subnet, unless you are accessing the Switch through one or more routers.

4.3. How to enter the CLI?

Press [Enter] key to enter the login command prompt when below message is displayed on the screen.

Please press Enter to activate this console

Input "***admin***" to enter the CLI mode when below message is displayed on the screen.

L2SWITCH login:

You can execute a few limited commands when CLI prompt is displayed as below.

L2SWITCH>

If you want to execute more powerful commands, you must enter the privileged mode.

Input command “***enable***”
L2SWITCH>enable

Input a valid username and password when below prompt are displayed.
user:admin
password:admin

L2SWITCH#

4.4. CLI command concept

Node	Command	Description
enable	show hostname	This command displays the system’s network name.
configure	reboot	This command reboots the system.
eth0	ip address A.B.C.D/M	This command configures a static IP and subnet mask for the system.
interface	show	This command displays the current port configurations.
acl	show	This command displays the current access control profile.
vlan	show	This command displays the current VLAN configurations.

The Node type:

- enable
  Its command prompt is “***L2SWITCH#*”.**
  It means these commands can be executed in this command prompt.

- configure
  Its command prompt is “***L2SWITCH(config)#*”.**
  It means these commands can be executed in this command prompt.
  In ***Enable*** code, executing command “***configure terminal***” enter the configure node.
  L2SWITCH#configure terminal

- eth0
  Its command prompt is “***L2SWITCH(config-if)#*”.**
  It means these commands can be executed in this command prompt.
  In ***Configure*** code, executing command “***interface eth0***” enter the eth0 interface node.
  L2SWITCH(config)#interface eth0
  L2SWITCH(config-if)#

- interface
  Its command prompt is “***L2SWITCH(config-if)#*”.**
  It means these commands can be executed in this command prompt.
  In ***Configure*** code, executing command “***interface gigaethernet1/0/5***” enter the interface port 5 node.
  Or

In ***Configure*** code, executing command "***interface fastethernet1/0/5***" enter the interface port 5 node.
Note: depend on your port speed, gigaethernet1/0/5 for gigabit Ethernet ports and fastethernet1/0/5 for fast Ethernet ports.

```
L2SWITCH(config)#interface gigaethernet1/0/5
L2SWITCH(config-if)#
```

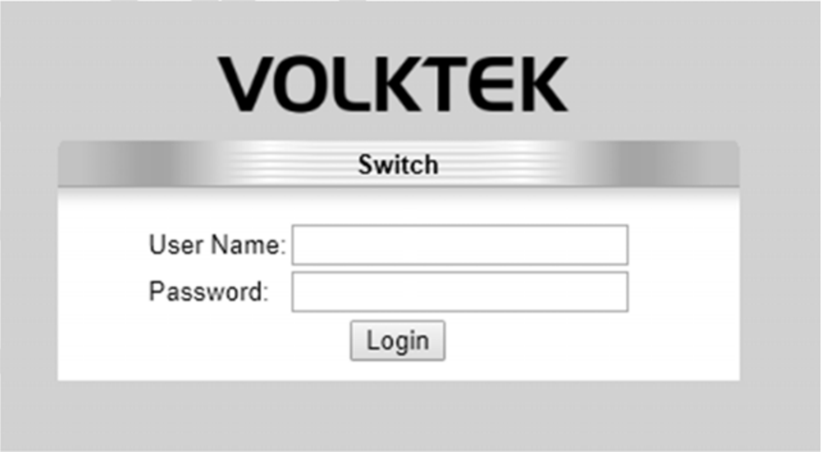
- vlan
  Its command prompt is "***L2SWITCH(config-vlan)#".***
  It means these commands can be executed in this command prompt.
  In ***Configure*** code, executing command "***vlan 2***" enter the vlan 2 node.
  Note: where the "2" is the vlan ID.

```
L2SWITCH(config)#vlan 2
L2SWITCH(config-vlan)#
```

- acl
  Its command prompt is "***L2SWITCH(config-acl)#".***
  It means these commands can be executed in this command prompt.
  In ***Configure*** code, executing command "***access-list test***" enter the access-list test node.
  Note: where the "***test***" is the profile name.

```
L2SWITCH(config)#access-list test
L2SWITCH(config-acl)#
```

4.5. GUI Login



Parameter	**Description**
User ID	Enter the user name.
Password	Enter the password.

Default:

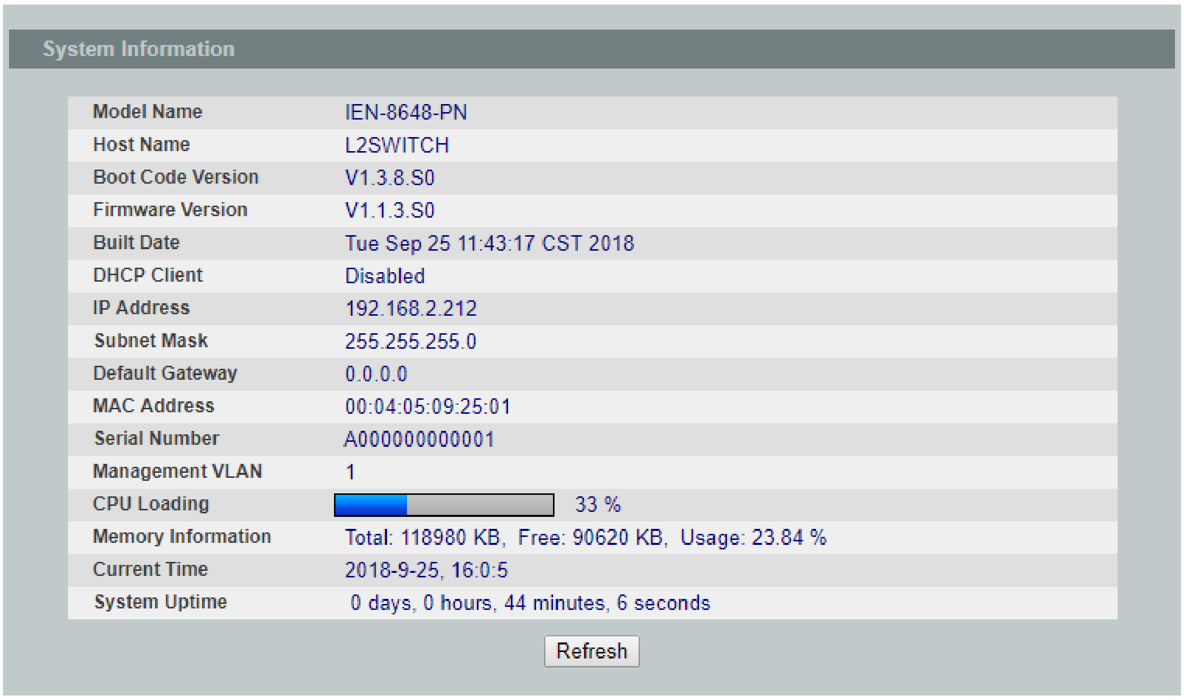
User name: admin,
Password: admin.

4.6. CLI Configuration

Node	Command	Description
enable	show hostname	This command displays the system's network name.
enable	show interface eth0	This command displays the current Eth0 configurations.
enable	show model	This command displays the system information.
enable	show running-config	This command displays the current operating configurations.
enable	show system-info	This command displays the system's CPU loading and memory information.
enable	show uptime	This command displays the system uptime.

4.7. System Information

System Information



System Information

Model Name	IEN-8648-PN
Host Name	L2SWITCH
Boot Code Version	V1.3.8.S0
Firmware Version	V1.1.3.S0
Built Date	Tue Sep 25 11:43:17 CST 2018
DHCP Client	Disabled
IP Address	192.168.2.212
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
MAC Address	00:04:05:09:25:01
Serial Number	A000000000001
Management VLAN	1
CPU Loading	33 %
Memory Information	Total: 118980 KB, Free: 90620 KB, Usage: 23.84 %
Current Time	2018-9-25, 16:0:5
System Uptime	0 days, 0 hours, 44 minutes, 6 seconds

Parameter	Description
Model Name	This field displays the model name of the Switch.
Host name	This field displays the name of the Switch.

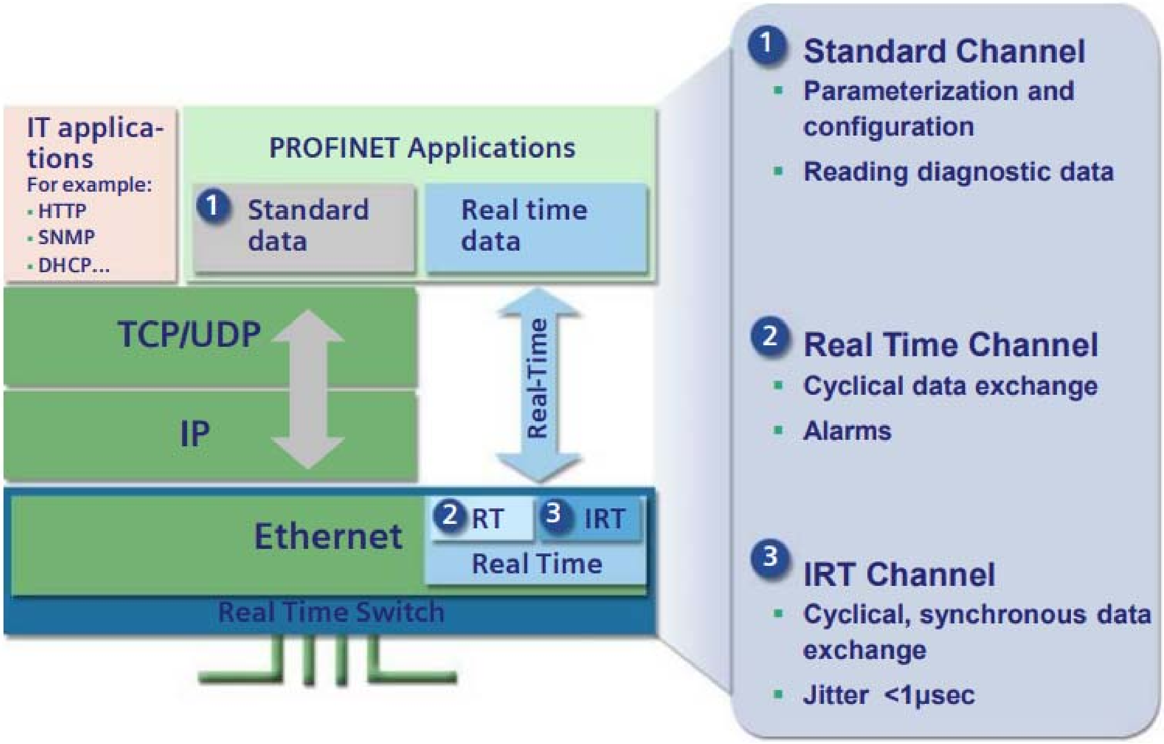
Boot Code Version	This field displays the boot code version.
Firmware Version	This field displays the firmware version.
Built Date	This field displays the built date of the firmware.
DHCP Client	This field displays whether the DHCP client is enabled on the Switch.
IP Address	This field indicates the IP address of the Switch.
Subnet Mask	This field indicates the subnet mask of the Switch.
Default Gateway	This field indicates the default gateway of the Switch.
MAC Address	This field displays the MAC (Media Access Control) address of the Switch.
Serial Number	The serial number assigned by manufacture for identification of the unit.
Management VLAN	This field displays the VLAN ID that is used for the Switch management purposes.
CPU Loading	This field displays the percentage of your Switch's system load.
Memory Information	This field displays the total memory the Switch has and the memory which is currently available (**Free**) and occupied (**Usage**).
Current Time	This field displays current date (yyyy-mm-dd) and time (hh:mm:ss).
System Uptime	This field displays how long the switch is running after it has been powered on. Days, Hours, Minutes and seconds.

5. PROFINET

5.1. Profinet Introduction

PROFINET is the advanced Industrial Ethernet solution for the networking of production equipment such as PLCs, DCS and enterprise-wide IT systems. PROFINET is a communication standard for automation of PROFIBUS & PROFINET International (PI).PROFINET is fully compatible with office Ethernet. However office Ethernet is not capable of the real time performance required by industrial automation.

PROFINET is able to operate in the difficult environments of industry and is capable of delivering the speed and precision required by manufacturing plants. It can also provide additional functions and can be used in combination with the control and monitoring functions.



PROFINET I/O is used for data exchange between I/O controllers (PLC, etc.) and I/O devices (field devices). This specification defines a protocol and an application interface for exchanging I/O data, alarms, and diagnostics. Here are some other advantages of working with PROFINET at the IO level:

- Highly scalable architectures.
- Access to field devices over the network.
- Maintenance and servicing from anywhere (even over the internet).
- Lower costs for production/quality data monitoring.

5.2. Volktek PN Switch capabilities:

Cyclic functions (PROFINET RT):

- Minimum Device Interval **32ms**
- Advanced and Legacy Startup
- Connection configuration supports:
  1x IOC_AR, 1x DA_AR
  1x Input CR
  1x Output CR
  1x Alarm CR

Acyclic functions:

- Connected mode:
  Read diagnostic information (Record) from the IO-Device.
  Multiple Write configuration parameters.
  Output alarms to an IO-Controller.

- Non-connected mode:
  Read diagnostic information (Record) from the IO-Device

General functions:

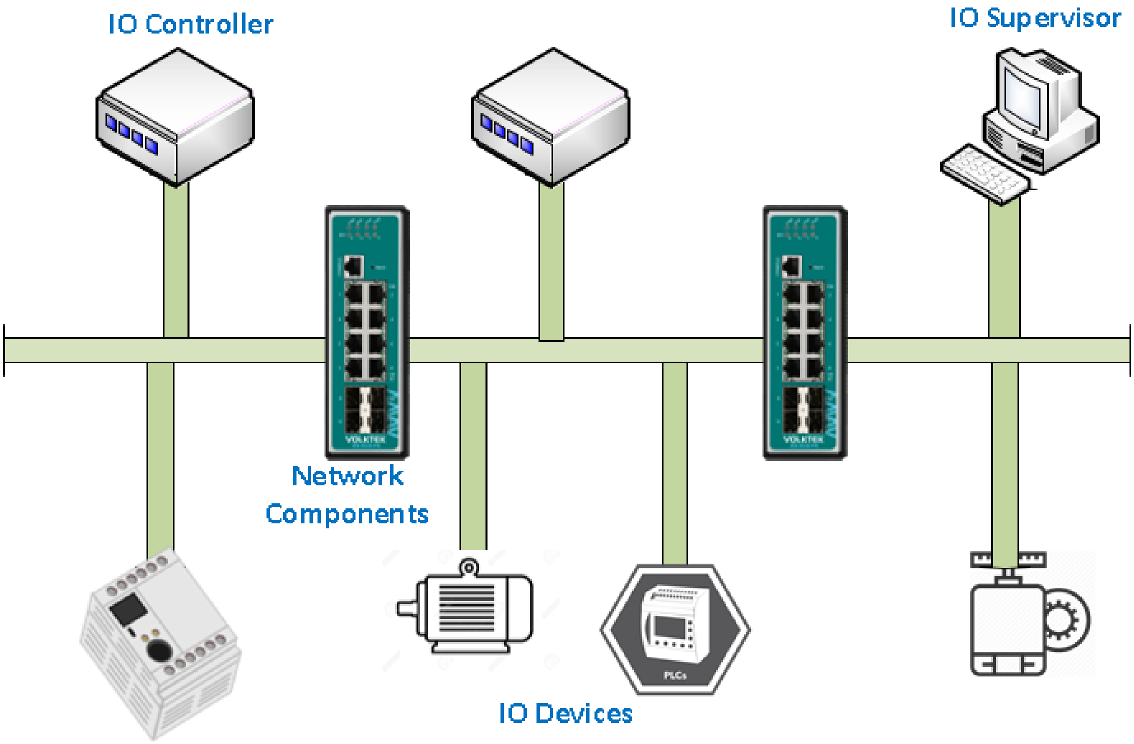
- MRP Client/Manager, Single Instance
- LLDP & LLDP MIB
- Easy Replacement
- Netload II Certified.

Functions Not Supported

- DHCP
- FSU
- Shared Input
- Shared Device
- IOS_AR
- IOS_AR Take Over
- IRT, RT_CLASS_3 Data Exchange
- PROFI energy
- Precision Transparent Clock Protocol (PTCP)

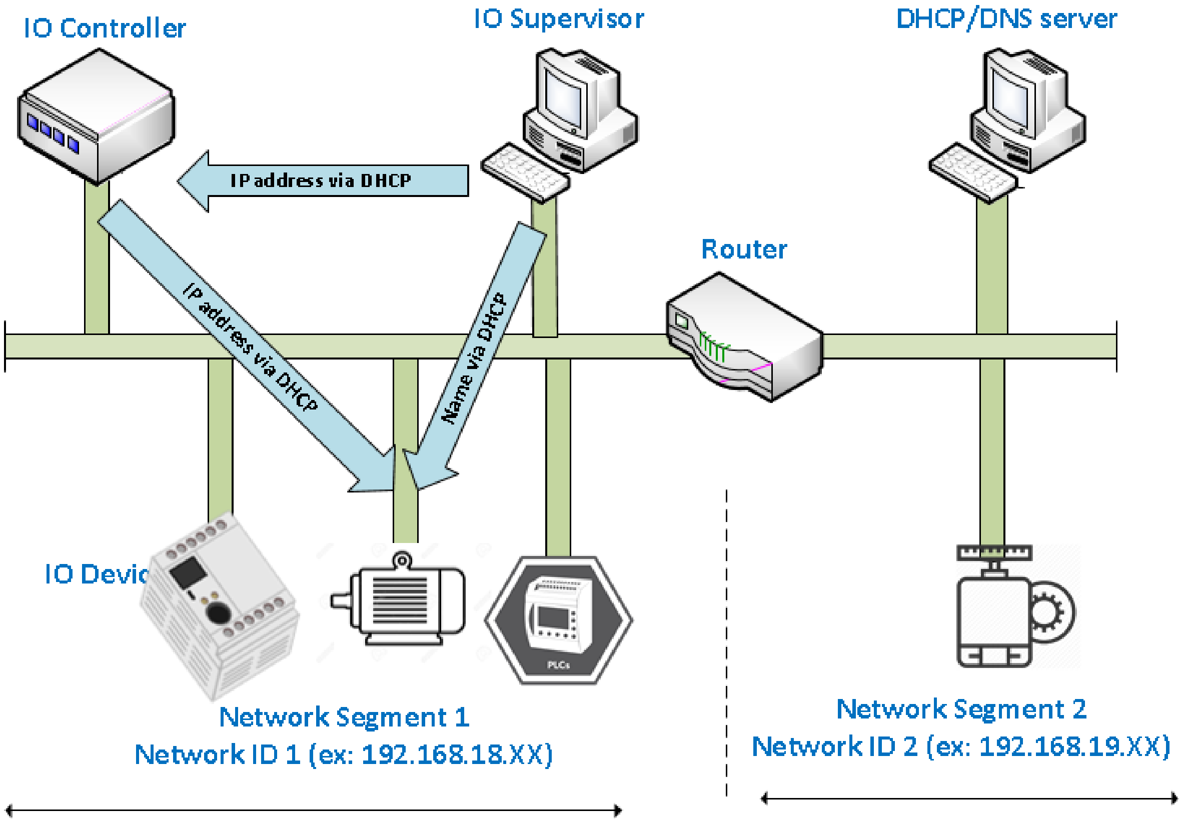
5.3. PROFINET network architecture

PROFINET is designed for fast data exchange between Ethernet-based field devices and follows the provider/consumer model.



The 3 major character types defined by PROFINET I/O include I/O controller, I/O supervisor and I/O devices. These are explained below.

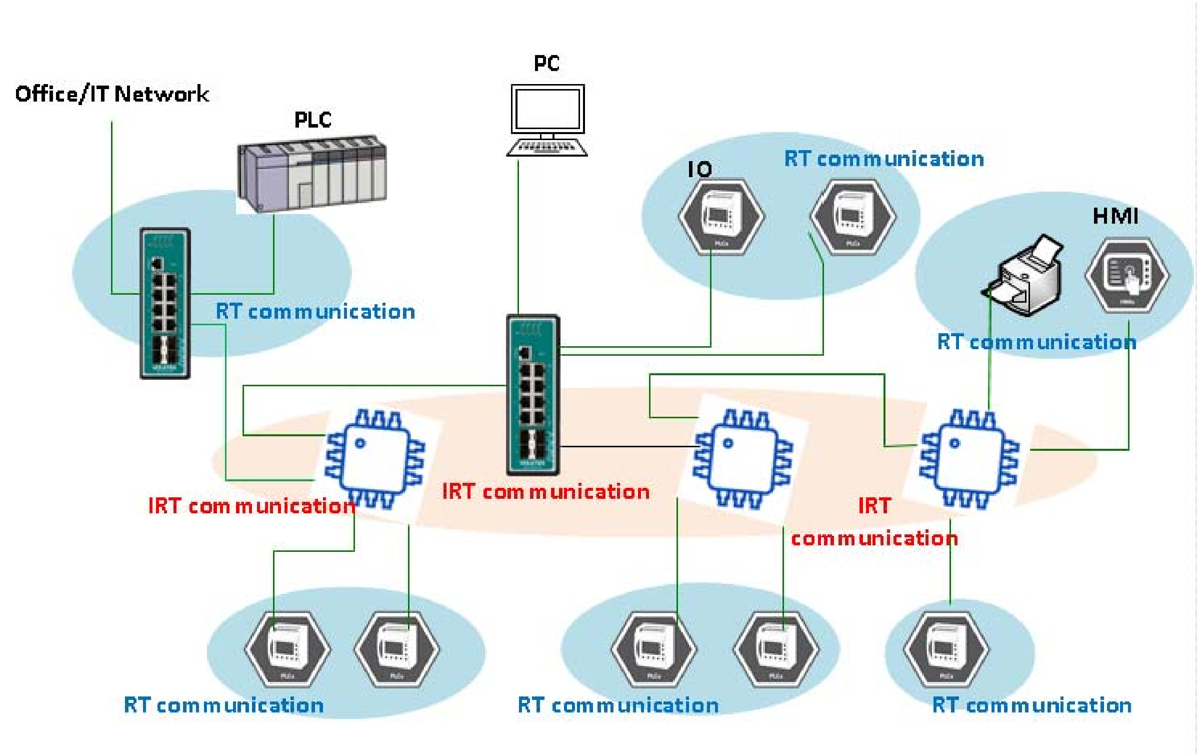
I/O controller: This is typically the programmable logic controller (PLC) on which the automation program runs. The I/O controller provides output data to the configured I/O-devices in its role as provider and is the consumer of input data of I/O devices.



I/O Supervisor: This can be a programming device, personal computer (PC), or human machine interface (HMI) device for commissioning or diagnostic purposes.

I/O Device: An I/O device is a distributed I/O field device that is connected to one or more I/O controllers via PROFINET I/O. The I/O device is the provider of input data and the consumer of output data.

Connection of PROFINET field devices: PROFINET field device are connected exclusively via switches as network components. This takes the form of a star or bus topology. So, it’s better to provide redundancy to ensure high availability of nodes in an automation system.



5.4. PROFINET protocols

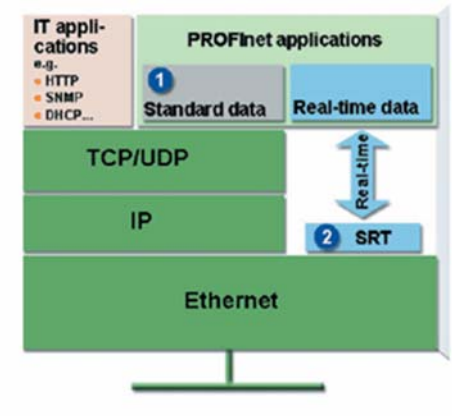
DCP: In PROFNET I/O, each field device has a symbolic name that uniquely identifies the field device within a PROFINET I/O system. This name is used for assigning the IP address and the MAC address. The DCP protocol (Dynamic Configuration Protocol) integrated in every I/O device is used for this purpose.

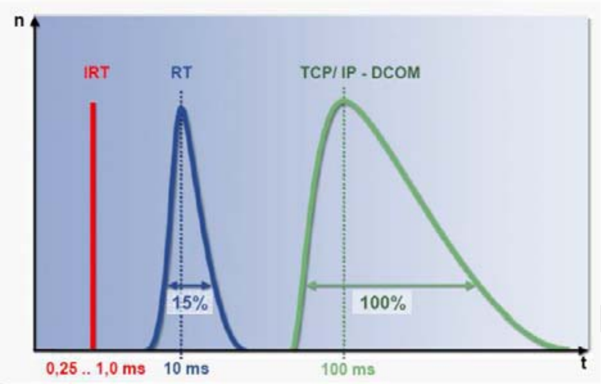
LLDP: Automation systems can be configured flexibly in a line, star, or tree structure. To compare the specified and actual topologies, to determine which field devices are connected to which switch port, and to identify the respective port neighbor, LLDP according to IEEE 802.1AB was applied in PROFINET I/O.
PROFINET filed bus exchange existing addressing information with connected neighbor devices via each switch port. The neighbor devices are thereby unambiguously identified and their physical location is determined.

MRP
Media Redundancy Protocol (MRP) is a data network protocol that allows rings of industrial ethernet switches to overcome any single failure with recovery time much faster than with Spanning Tree Protocol.

RTC
With Real Time technology, TCP/IP layers are bypassed allowing for deterministic performance of applications to reach a speed time of between 1 to 10 milliseconds. This makes PROFINET RT ideal for applications where digital and analog I/O control is critical to production cycles, such as a packaging machine. By skipping TCP/IP and taking data messages from the Ethernet

physical layer to the application layer, PROFINET Real Time provides high-precision determinism.



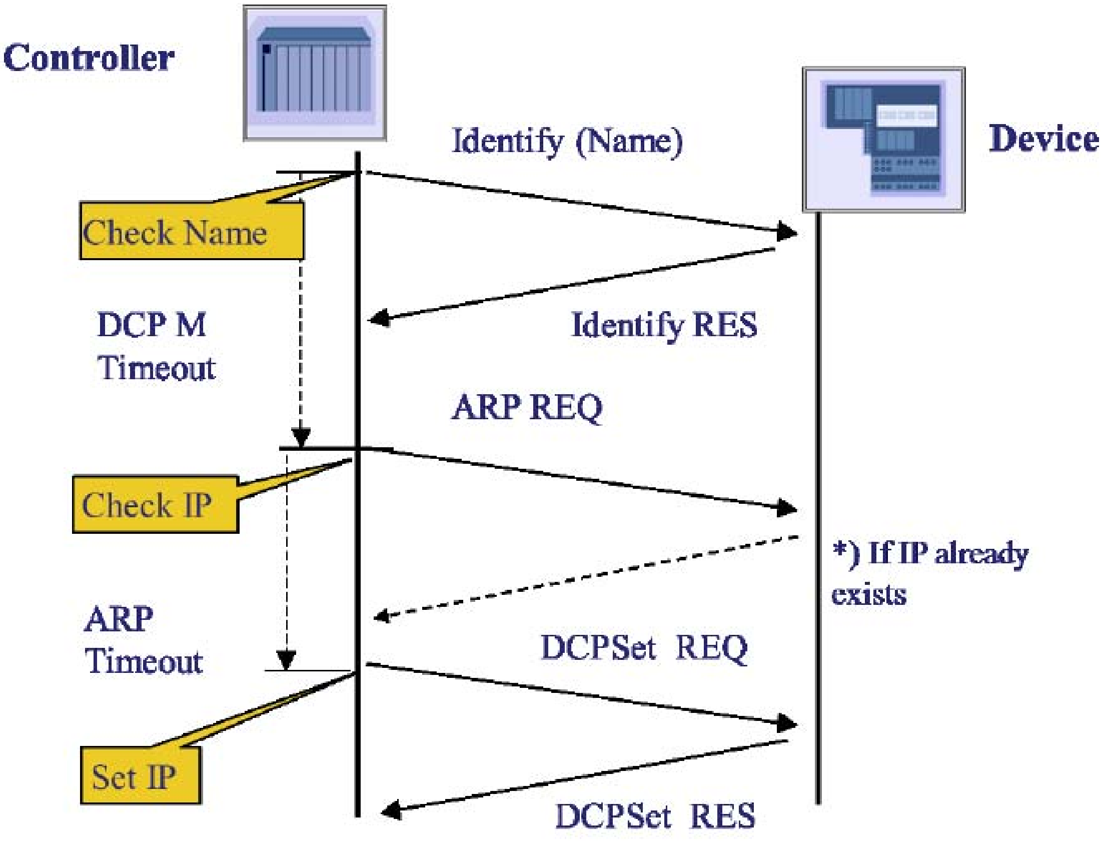


5.4.1. Device descriptions

GSD file: The GSD files (General Station Description) of the field devices to be configured are required for system engineering. This XML-based GSD describes the properties and functions of the PROFINET I/O field devices. It contains all data relevant for engineering as well as for data exchange with the device.

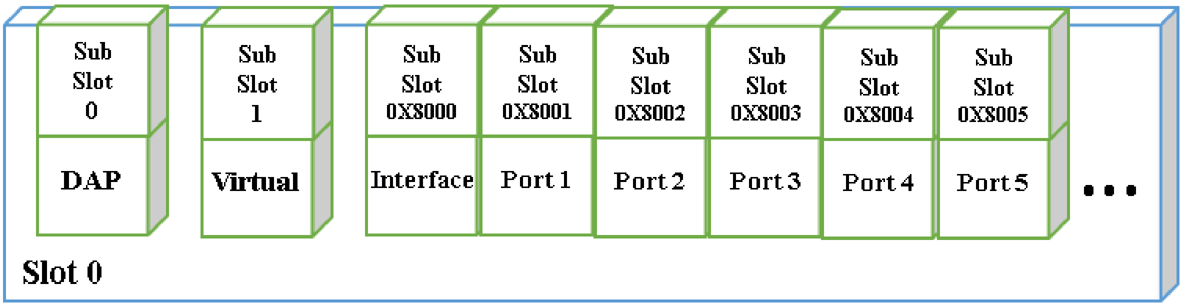
5.5. DCP IP assignment before system startup

The startup of an automation system begins with the address resolution of the configured IO field devices. This is accomplished by using the default DCP protocol integrated in every PROFINET field device, which contains all services for name assignment and address resolution.
Every field device consists of MAC address and system-specific device name that will be discovered and assigned with an IP using DCP before start-up. DCP hand-shaking is shown as below.



5.6. Addressing of I/O Data in PROFINET I/O Based on Slot and Sub-Slots

The concept of the Volktek PROFINET switch with GSD is shown the table below. In this structure, each switch port represents one sub-slot.
We have only one Slot defined in Volktek PN switch, Slot 0.



Sub Slot 0	Sub Slot 1	Sub Slot 0X8000	Sub Slot 0X8001	Sub Slot 0X8002	Sub Slot 0X8003	Sub Slot 0X8004	Sub Slot 0X8005	
DAP	Virtual	Interface	Port 1	Port 2	Port 3	Port 4	Port 5	• • •

5.6.1. PROFINET attributes

The PROFINET I/O connection can be configured for both cyclic I/O data and I/O parameters. I/O parameters are acyclic I/O data. These are major setup and monitor attributes in PROFINET.

• **Cyclic I/O Data** Cyclic I/O data are always sent between the PLC and Switches at the specified periodic time. These data are transmitted almost real time. For example, status information from the Switches, and variables to be written to the Switch would typically be part of the cyclic data.

• **I/O Parameters** PROFINET I/O parameters are defined for device configuration and status monitoring. These data are useful for infrequent data transfers, or for very large data transfers. Only transfer when needed

• **Alarm**

Alarms are mainly PROFINET I/O transmitted high-priority events. Alarm data are exchanged between an I/O device and an I/O controller. Once an event triggers it, the switch will send the alarm to the PLC immediately. Enable or disable these alarms by setting I/O parameters.
The switch supports below listed PROFINET Alarms:

- PWR Under Voltage
- RPS Under Voltage
- PWR Over Voltage
- RPS Over Voltage
- Board Over Heat
- CPU Over Heat
- PHY Over Heat

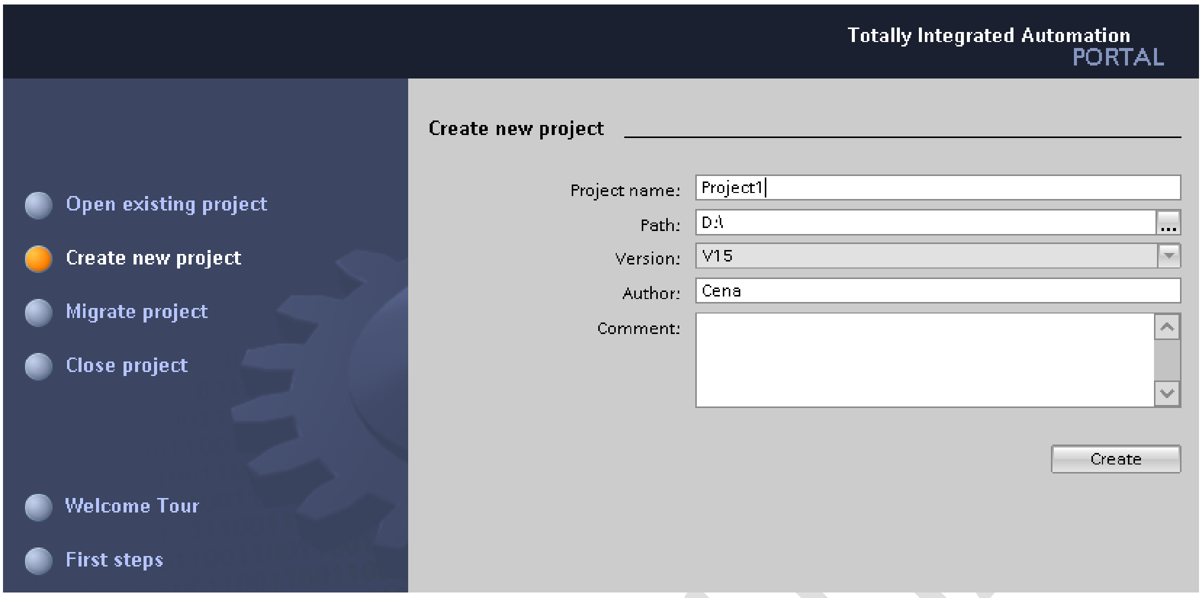
5.7. IEN-8648-PN switches Integration with SEIMEN's TIA.

The following example show how to integrate the IEN-8648-PN switch into a PROFINET network which includes Siemens PLC using Siemens Totally Integrated Automation (TIA) portal.

Components required:

- Siemens SIMATIC S7-1500 PLC
- Volktek PROFINET switch
- Siemens TIA (v15) portal

1. **Create a new PROFINET I/O project in Siemens TIA V15 portal fill in the basic information and enter create.**



Create new project

Project name: Project1

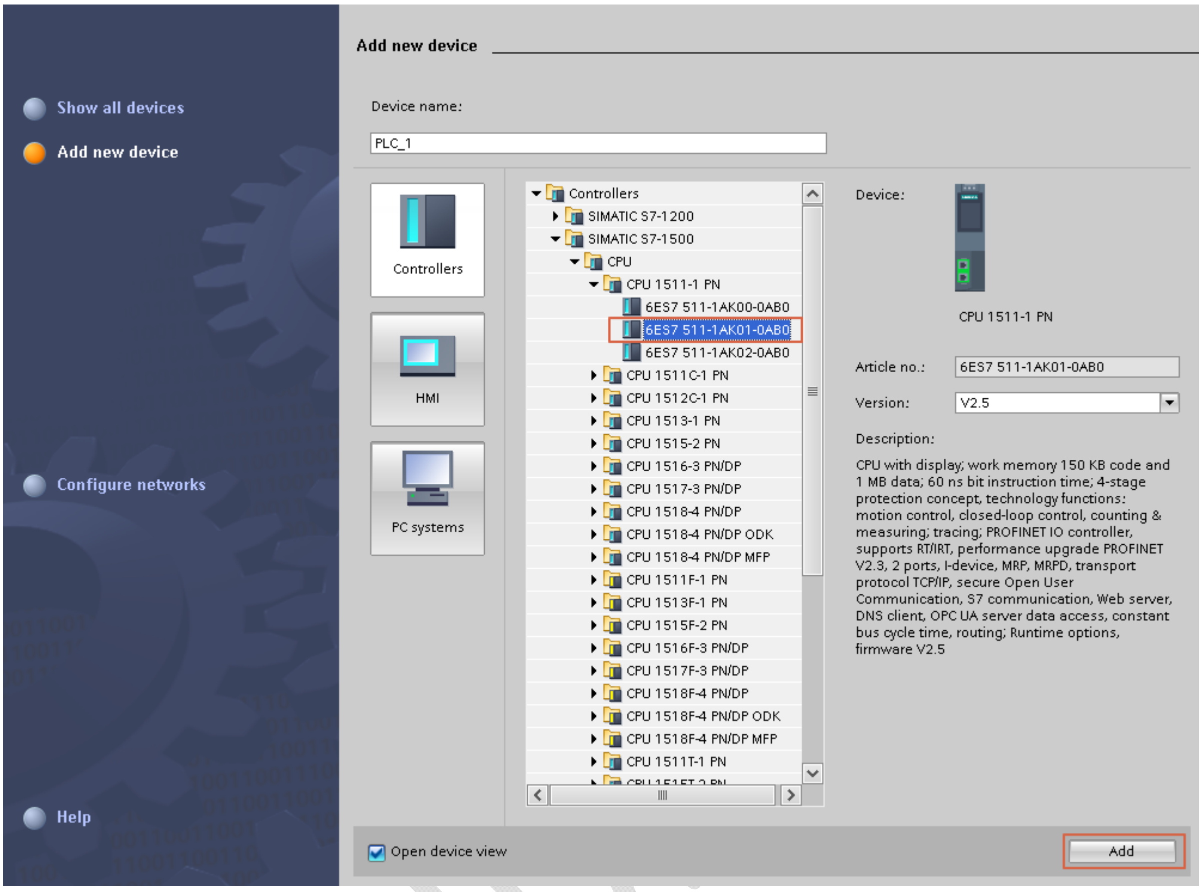
Path: D:\

Version: V15

Author: Cena

Comment:

2. In Device and networks, select add new device. On the right side select appropriate controller you are using and enter add. (in this example we are using Siemens Simatic S7-1500 controller)



Device name: PLC_1

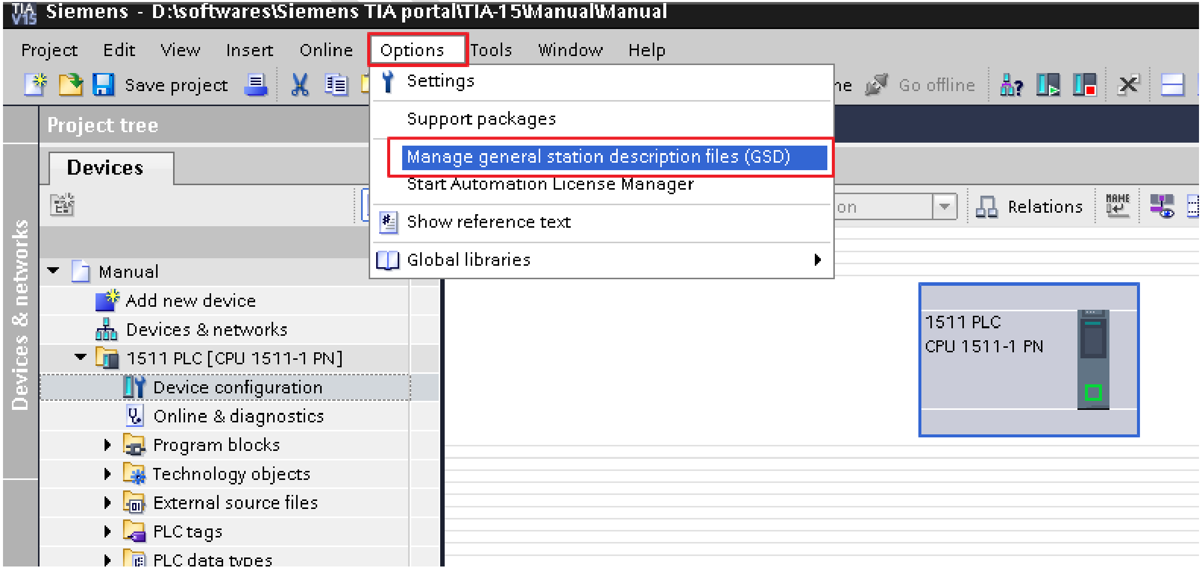
Article no.: 6ES7 511-1AK01-0AB0

Version: V2.5

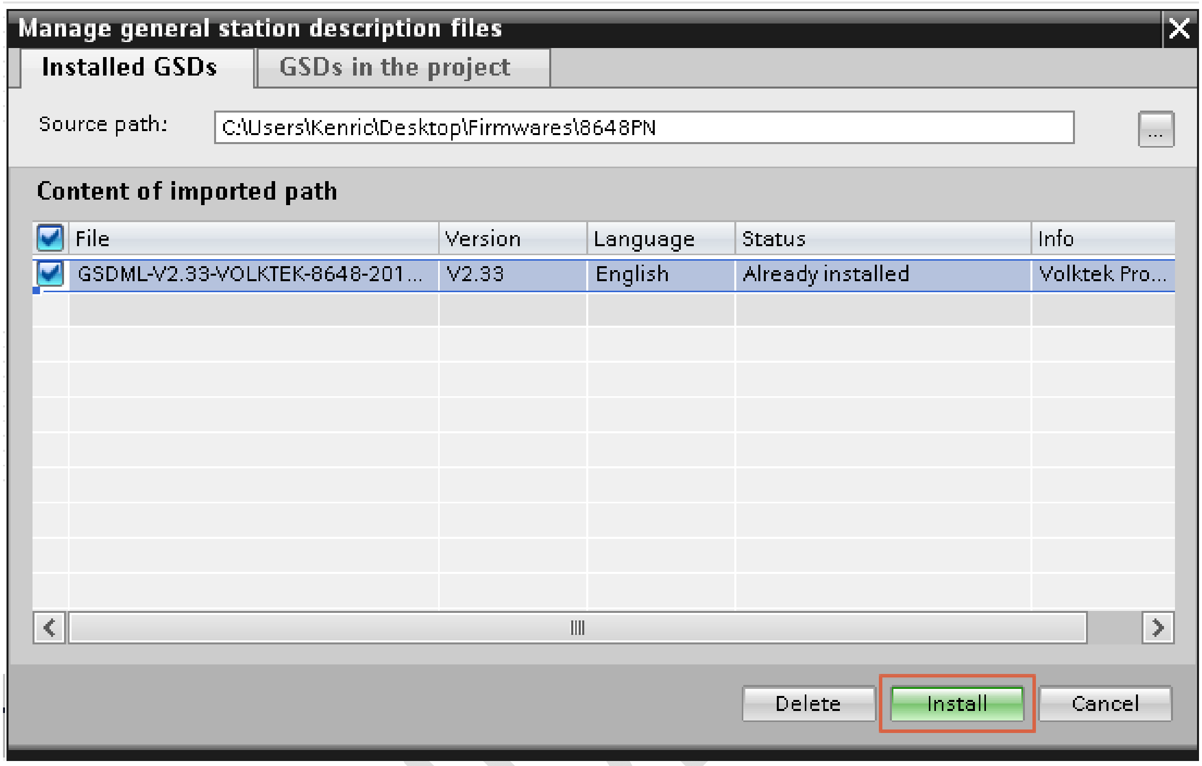
Description:
CPU with display; work memory 150 KB code and 1 MB data; 60 ns bit instruction time; 4-stage protection concept, technology functions: motion control, closed-loop control, counting & measuring; tracing; PROFINET IO controller, supports RT/IRT, performance upgrade PROFINET V2.3, 2 ports, I-device, MRP, MRPD, transport protocol TCP/IP, secure Open User Communication, S7 communication, Web server, DNS client, OPC UA server data access, constant bus cycle time, routing; Runtime options, firmware V2.5

☑ Open device view

3. **GSD file installation:** Import IEN-8648-PN switch GSD to add device into the project Select **Options -> Manage GSD file**



4. Open the folder where the GSD is placed and select the appropriate **GSD** file provided for that **IEN-8648-PN** switch device and click install



Manage general station description files

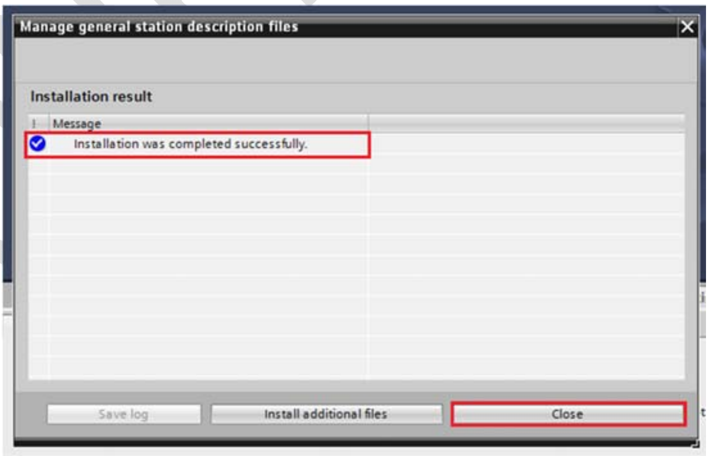
Installed GSDs | GSDs in the project

Source path: C:\Users\Kenric\Desktop\Firmwares\8648PN

Content of imported path

☑	File	Version	Language	Status	Info
☑	GSDML-V2.33-VOLKTEK-8648-201...	V2.33	English	Already installed	Volktek Pro...

After successful install close

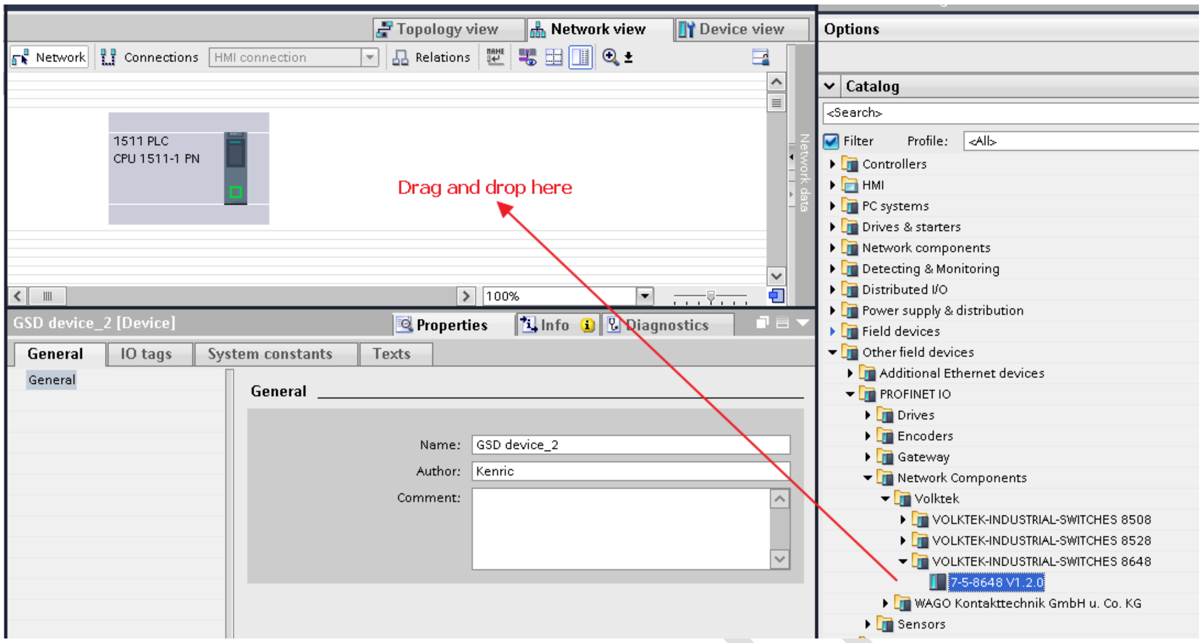


Manage general station description files

Installation result

!	Message
✓	Installation was completed successfully.

5. **Device configuration:** on the right side in Hardware catalog option search and discover the switch IEN-8648-PN. Drag and drop the device.



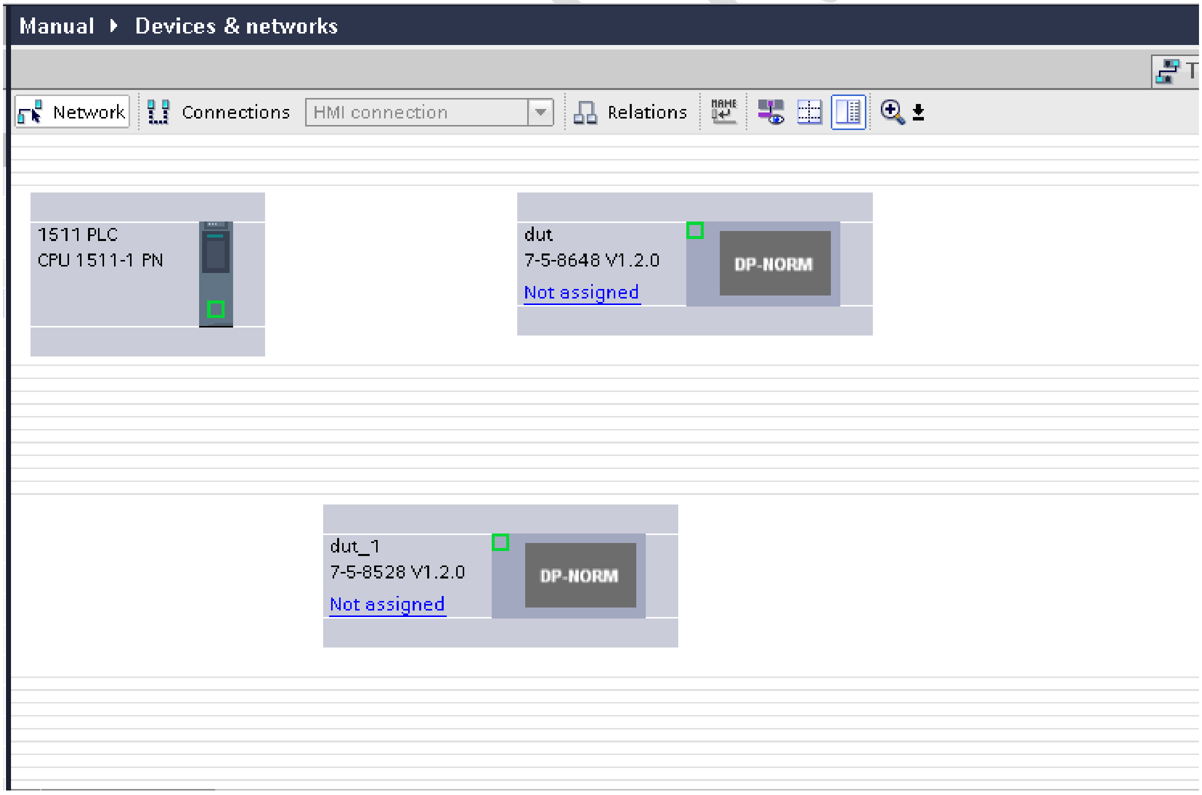
Drag and drop here

Name: GSD device_2

Author: Kenric

Comment:

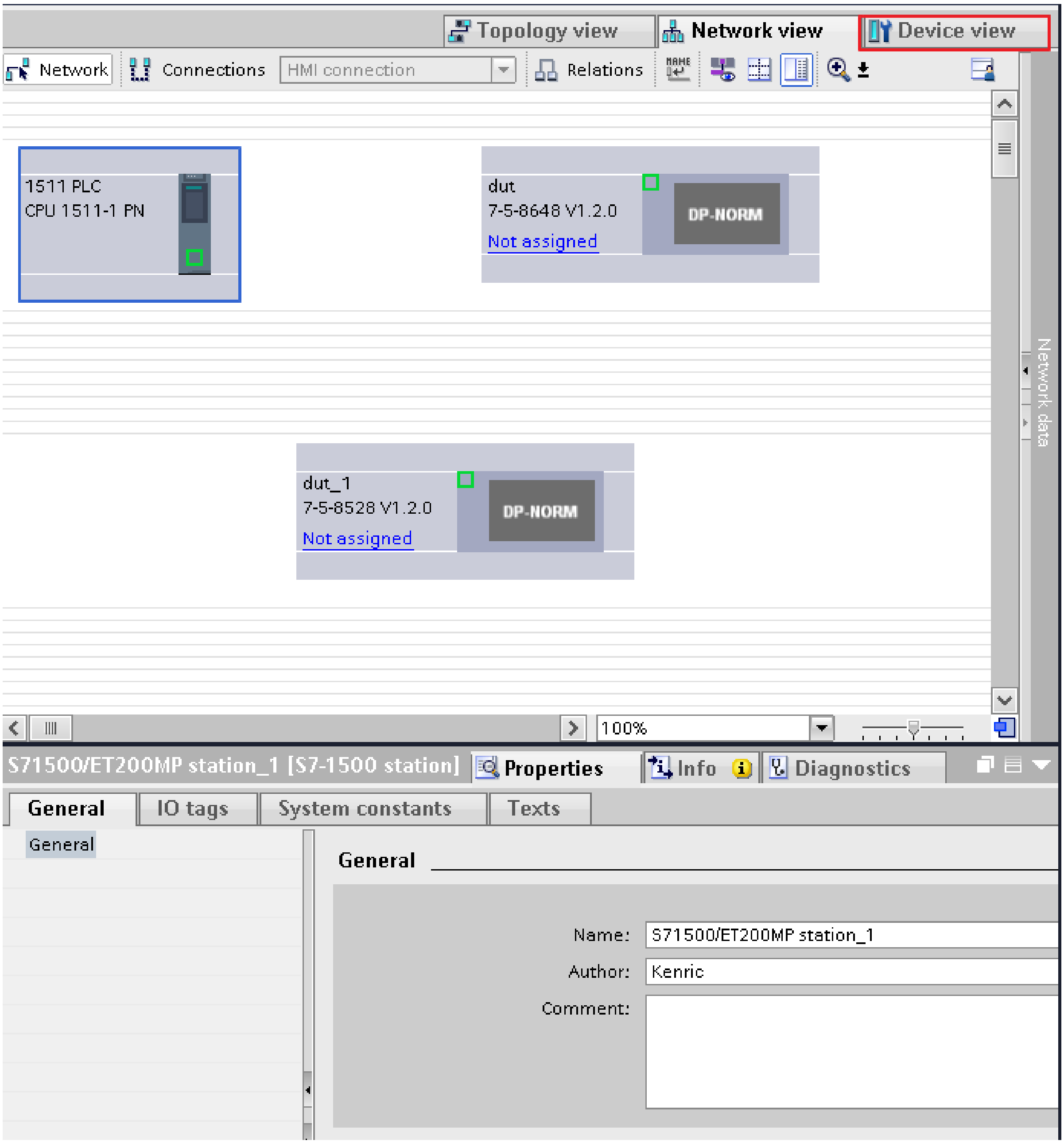
For demo added 2 switches



6. Configure PROFINET attributes such as IP address, device name and I/O parameters.

    1. Click on the particular device that is to be configured, in the properties enter details like

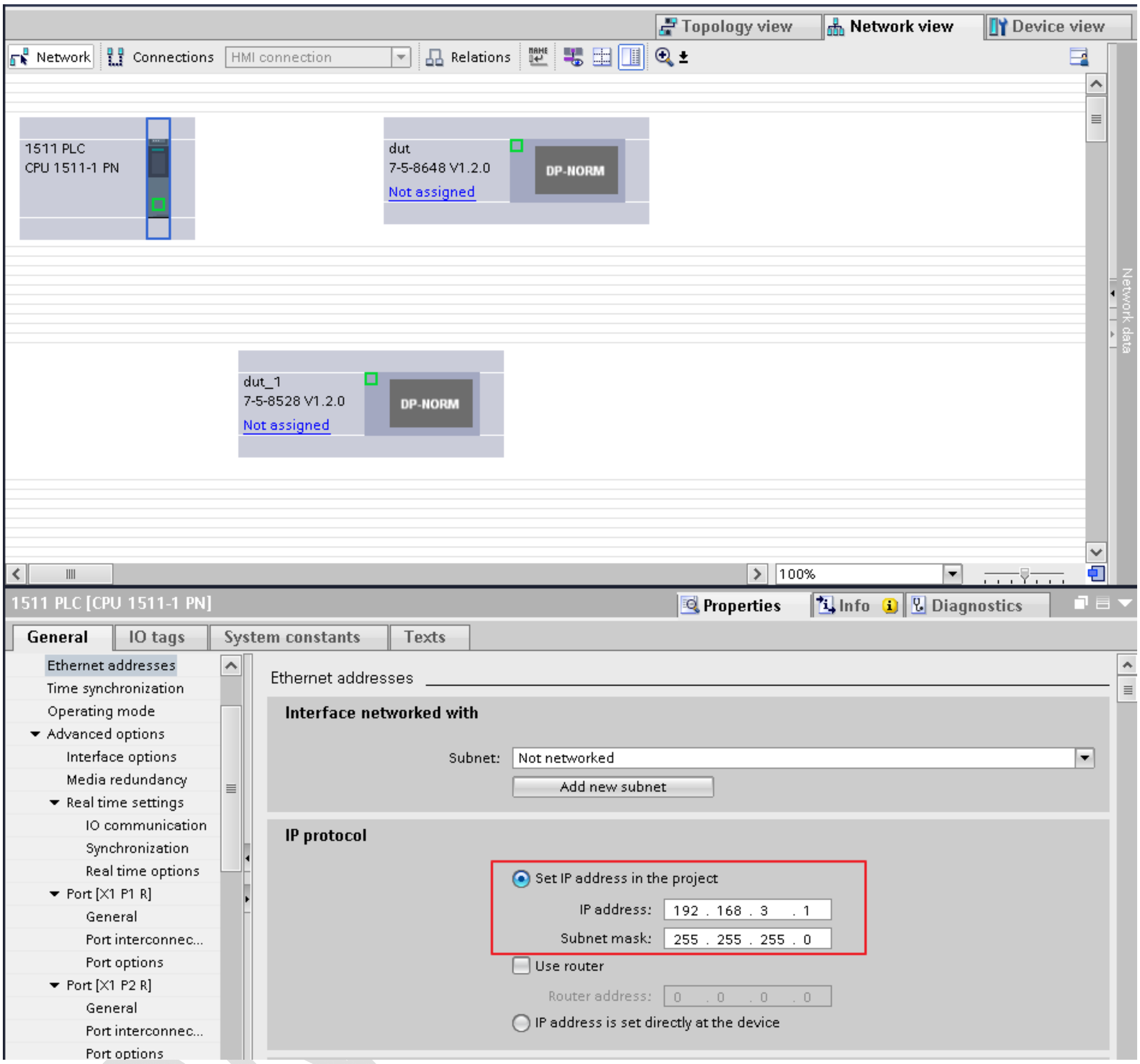
- Device name
- IP address



Name: S71500/ET200MP station_1

Author: Kenric

Comment:



Ethernet addresses

Interface networked with

Subnet: Not networked

Add new subnet

IP protocol

● Set IP address in the project

IP address: 192 . 168 . 3 . 1

Subnet mask: 255 . 255 . 255 . 0

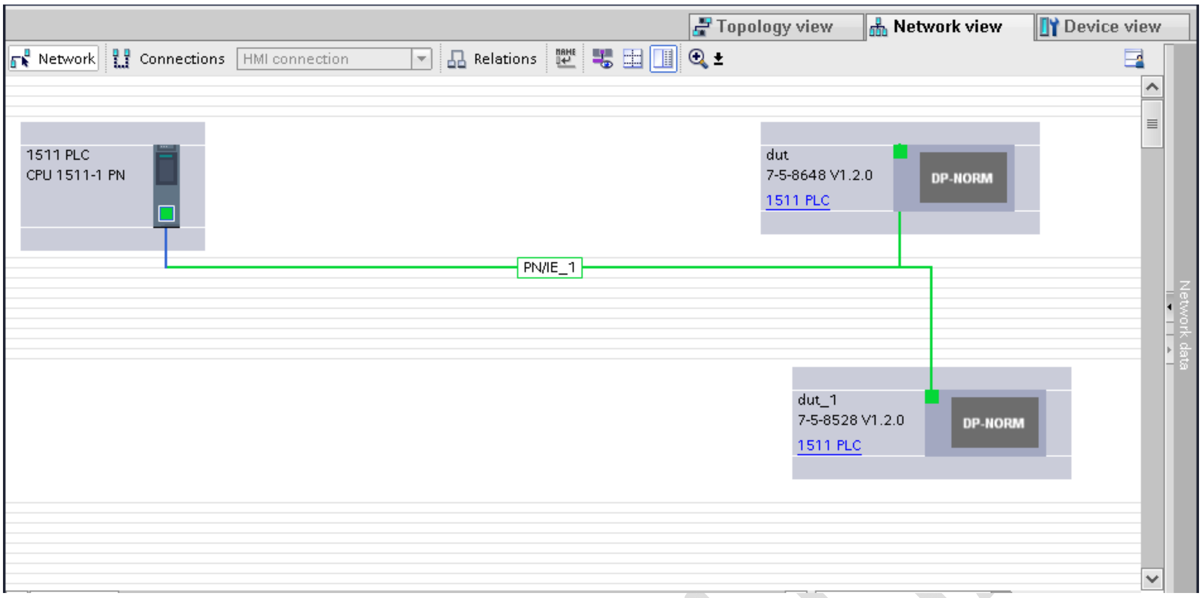
□ Use router

Router address: 0 . 0 . 0 . 0

○ IP address is set directly at the device

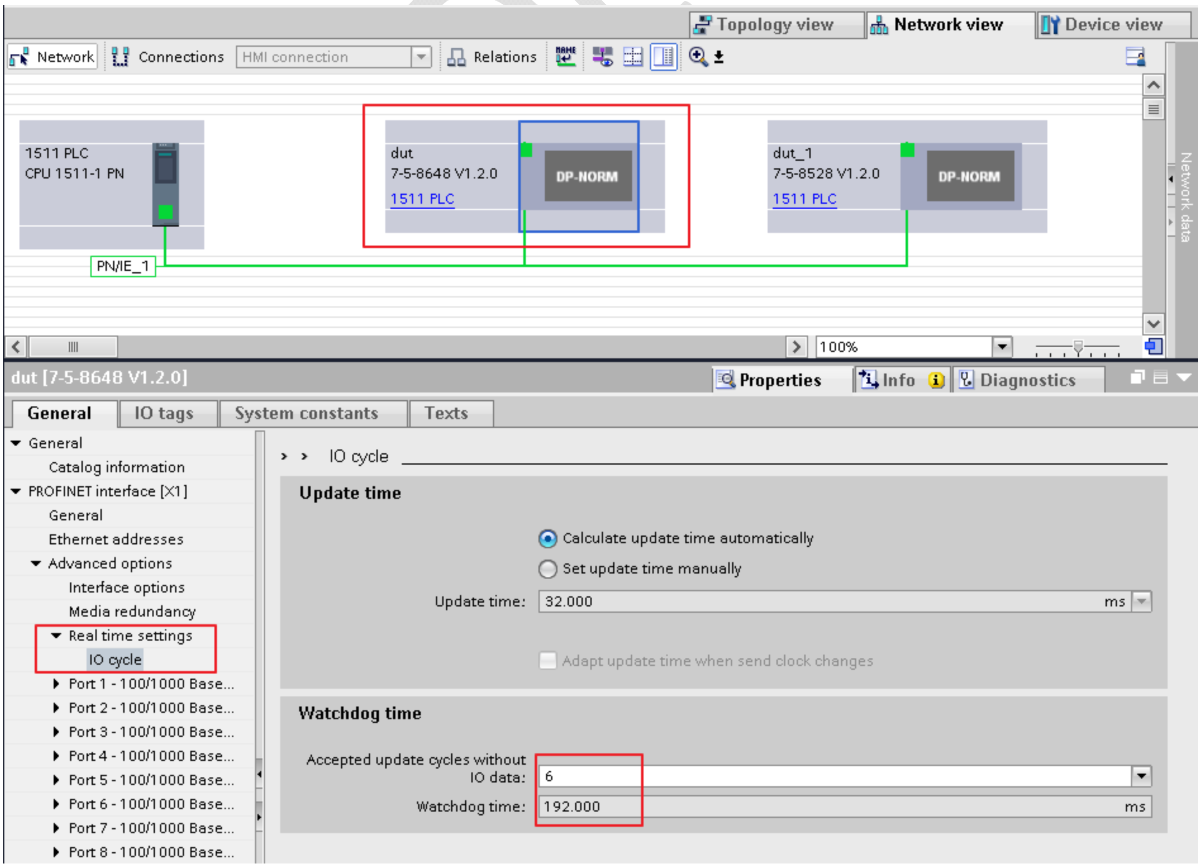
Do the same for other two devices.

7. Connect the devices to create PLC PROFINET IO-system



8. Assign real time settings

- Update time>=64ms
- Watchdog should be >=192ms



dut [7-5-8648 V1.2.0]

IO cycle

Update time

● Calculate update time automatically

○ Set update time manually

Update time: 32.000 ms

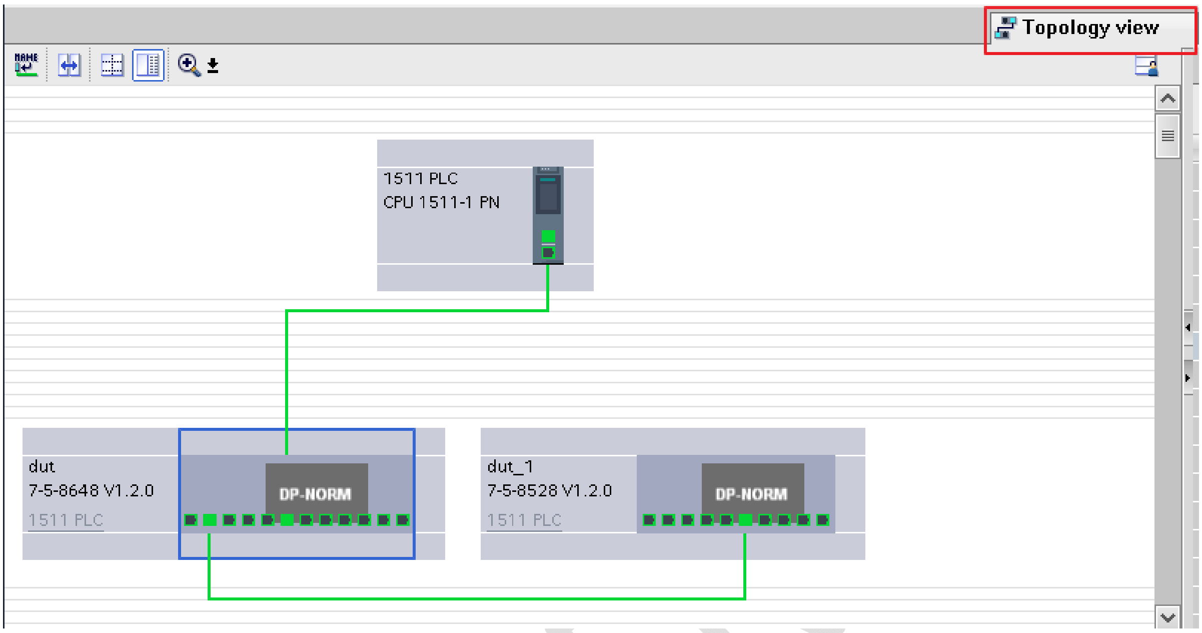
□ Adapt update time when send clock changes

Watchdog time

Accepted update cycles without IO data: 6

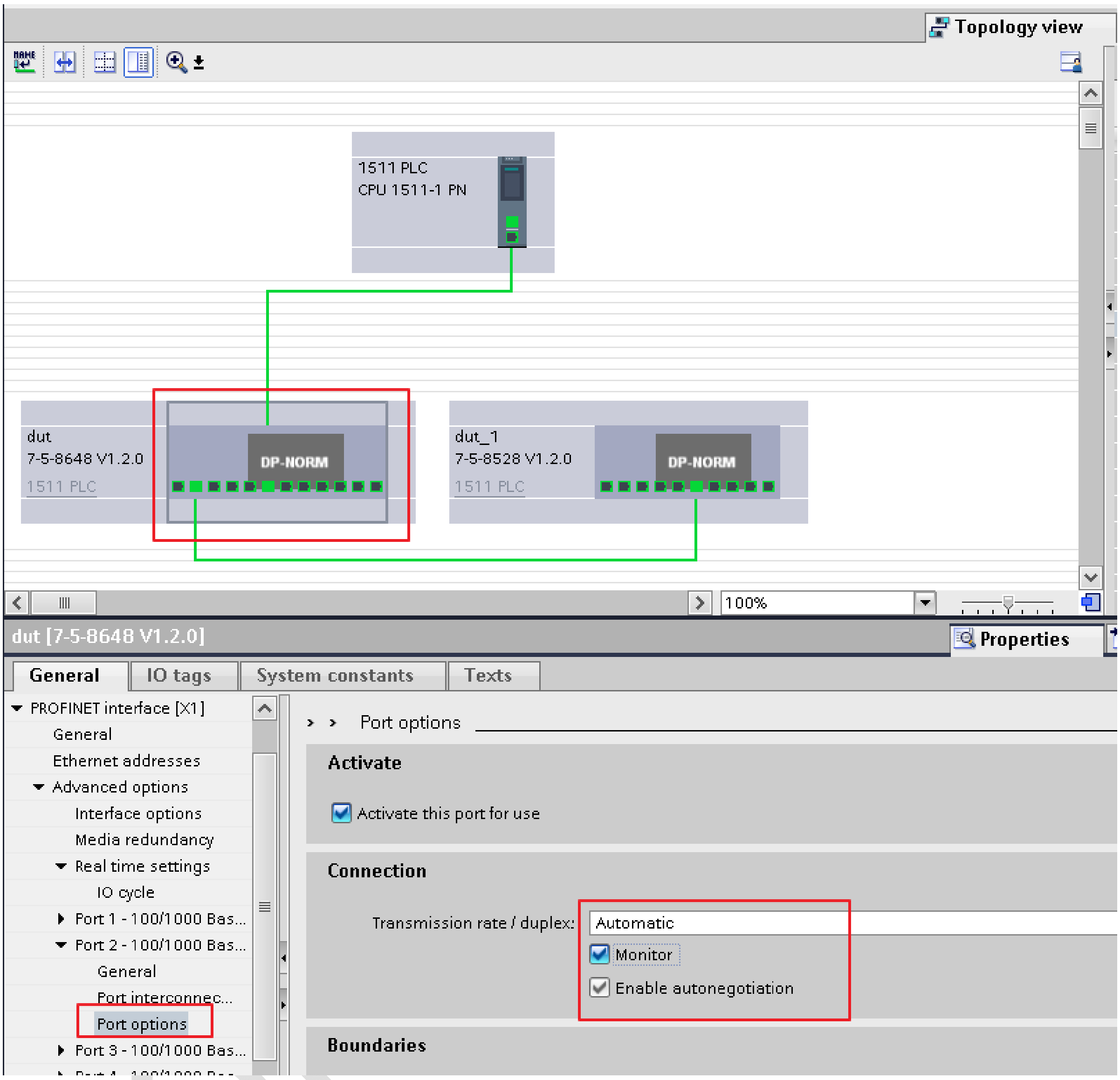
Watchdog time: 192.000 ms

9. Assign topology connection



10. Assign port speed options for all the devices

Port#1 Speed = 100 Mbps , Full Duplex + Monitor + Auto-Negotiation



dut [7-5-8648 V1.2.0]

- PROFINET interface [X1]
  - General
  - Ethernet addresses
  - Advanced options
    - Interface options
    - Media redundancy
    - Real time settings
      - IO cycle
    - Port 1 - 100/1000 Bas...
    - Port 2 - 100/1000 Bas...
      - General
      - Port interconnec...
      - Port options
    - Port 3 - 100/1000 Bas...

> > Port options

Activate

☑ Activate this port for use

Connection

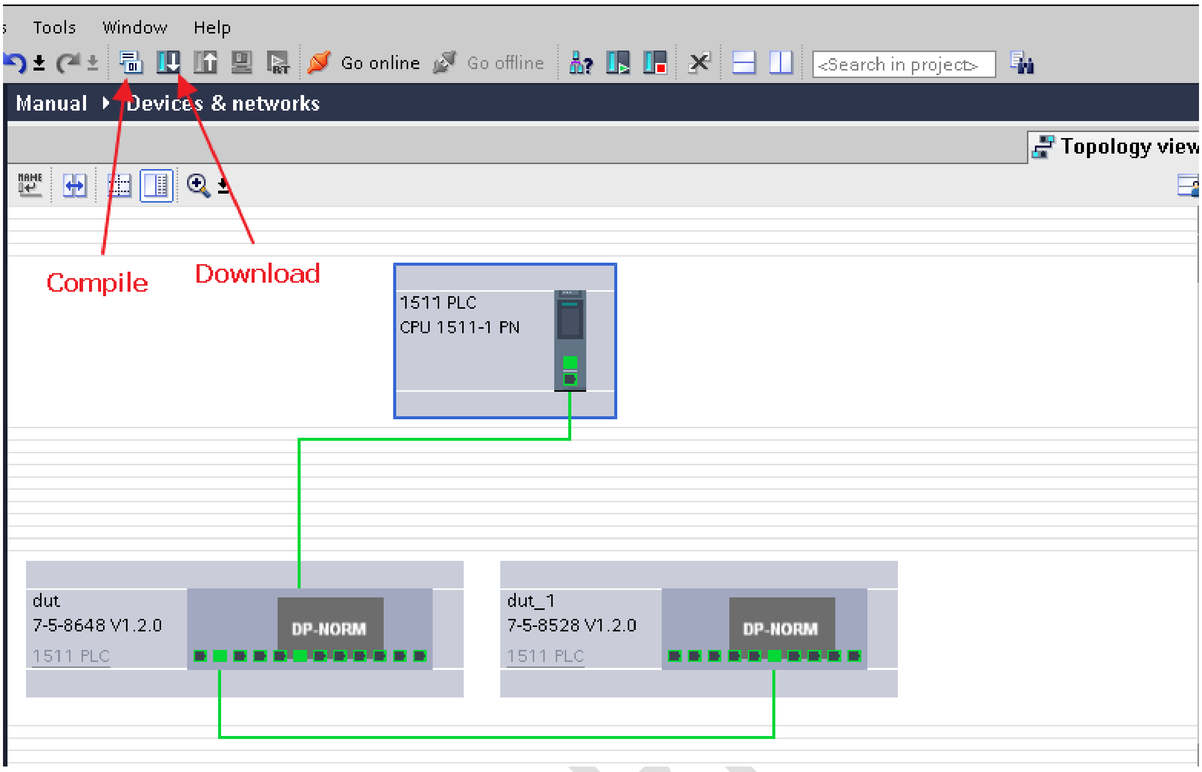
Transmission rate / duplex: Automatic

☑ Monitor

☑ Enable autonegotiation

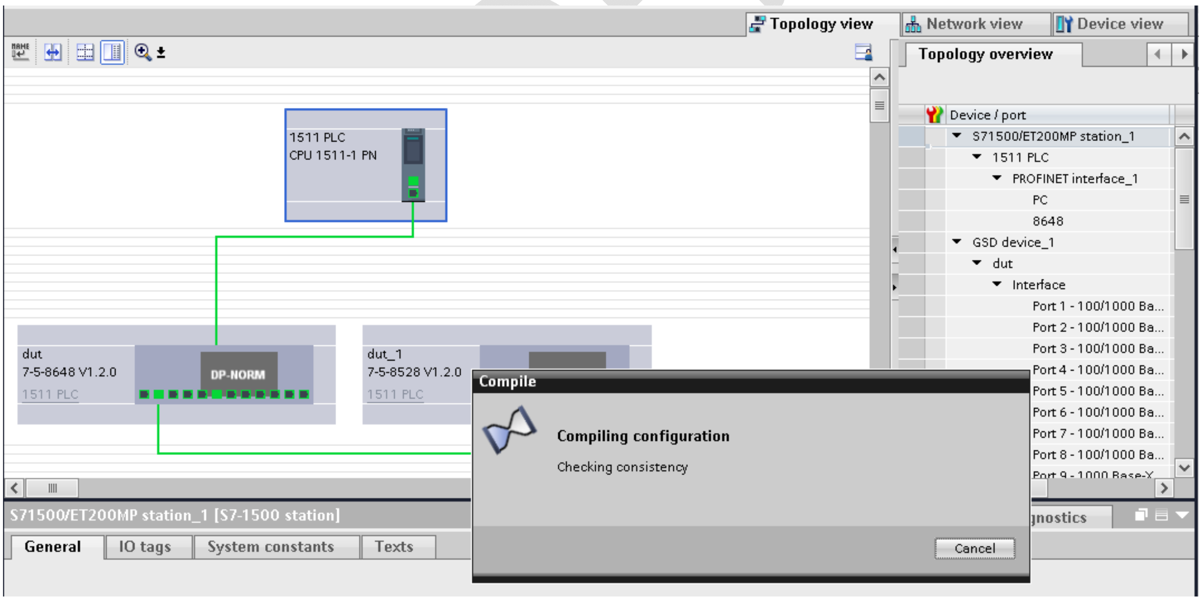
Boundaries

11. Now compile the configuration and download it



Compile

Download

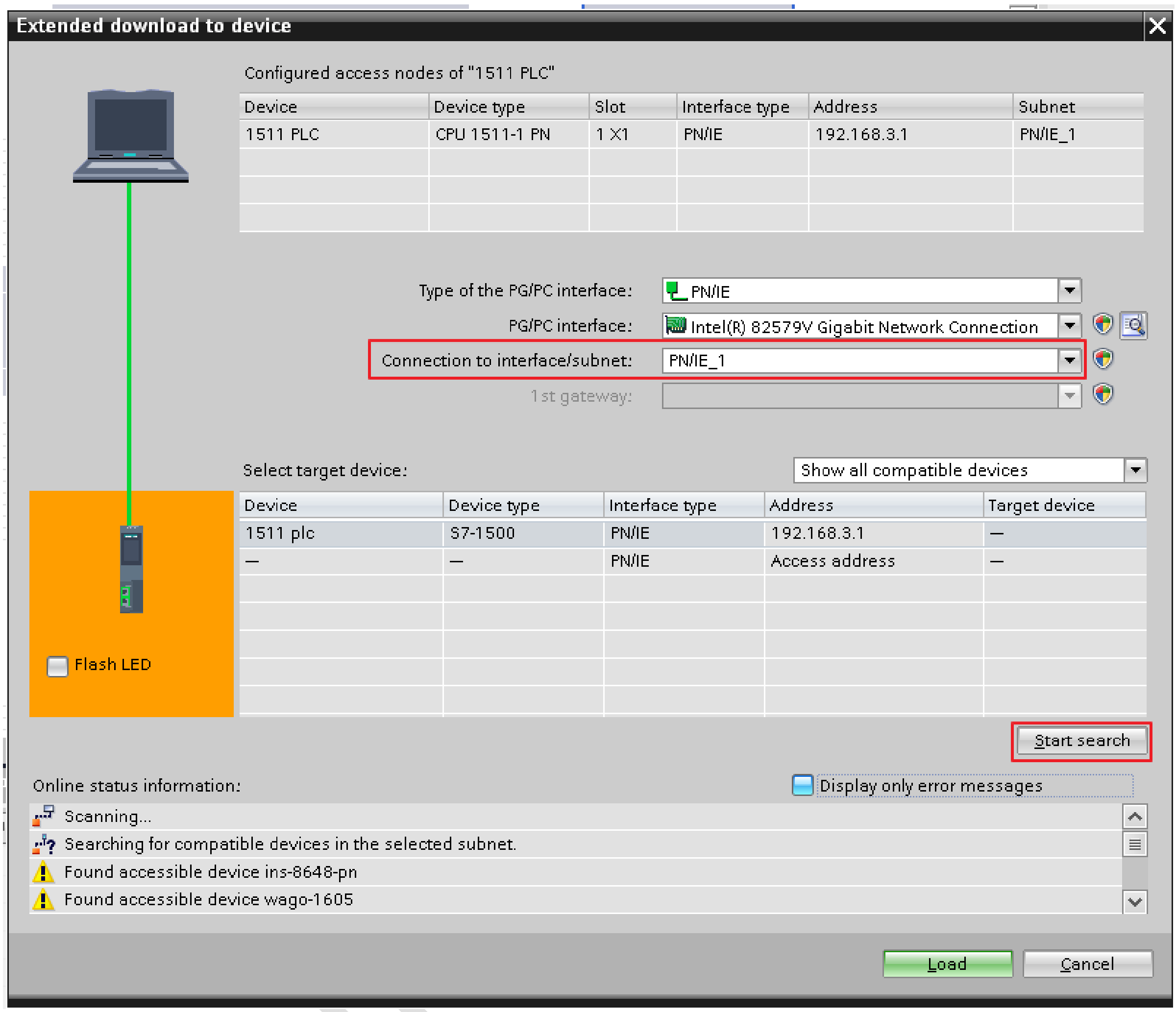


Compile

Compiling configuration

Checking consistency

12. Select the connection interface/subnet as PN/IE_1 and start search



Extended download to device

Configured access nodes of "1511 PLC"

Device	Device type	Slot	Interface type	Address	Subnet
1511 PLC	CPU 1511-1 PN	1 X1	PN/IE	192.168.3.1	PN/IE_1

Type of the PG/PC interface: PN/IE

PG/PC interface: Intel(R) 82579V Gigabit Network Connection

Connection to interface/subnet: PN/IE_1

1st gateway:

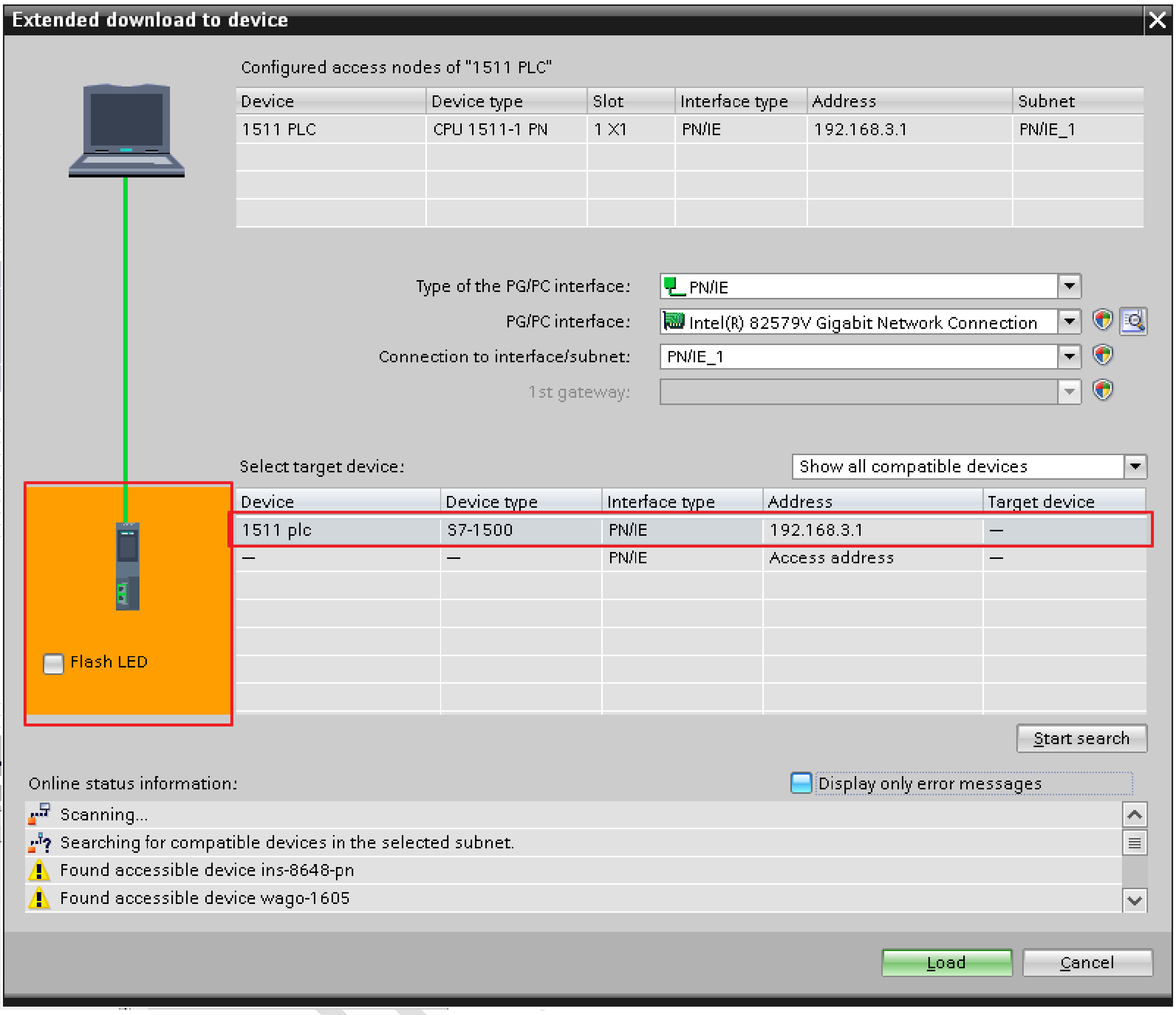
Select target device: Show all compatible devices

Device	Device type	Interface type	Address	Target device
1511 plc	S7-1500	PN/IE	192.168.3.1	—
—	—	PN/IE	Access address	—

Online status information: □ Display only error messages

Scanning...
Searching for compatible devices in the selected subnet.
Found accessible device ins-8648-pn
Found accessible device wago-1605

13. Select the appropriate PLC, you can also see where the PLC is present by using ‘flash LED’ option, when you click it the LED on the PLC will blink to indicate the selected PLC is right one.



Extended download to device

Configured access nodes of "1511 PLC"

Device	Device type	Slot	Interface type	Address	Subnet
1511 PLC	CPU 1511-1 PN	1 X1	PN/IE	192.168.3.1	PN/IE_1

Type of the PG/PC interface: PN/IE

PG/PC interface: Intel(R) 82579V Gigabit Network Connection

Connection to interface/subnet: PN/IE_1

1st gateway:

Select target device: Show all compatible devices

Device	Device type	Interface type	Address	Target device
1511 plc	S7-1500	PN/IE	192.168.3.1	—
—	—	PN/IE	Access address	—

Online status information: □ Display only error messages

Scanning...

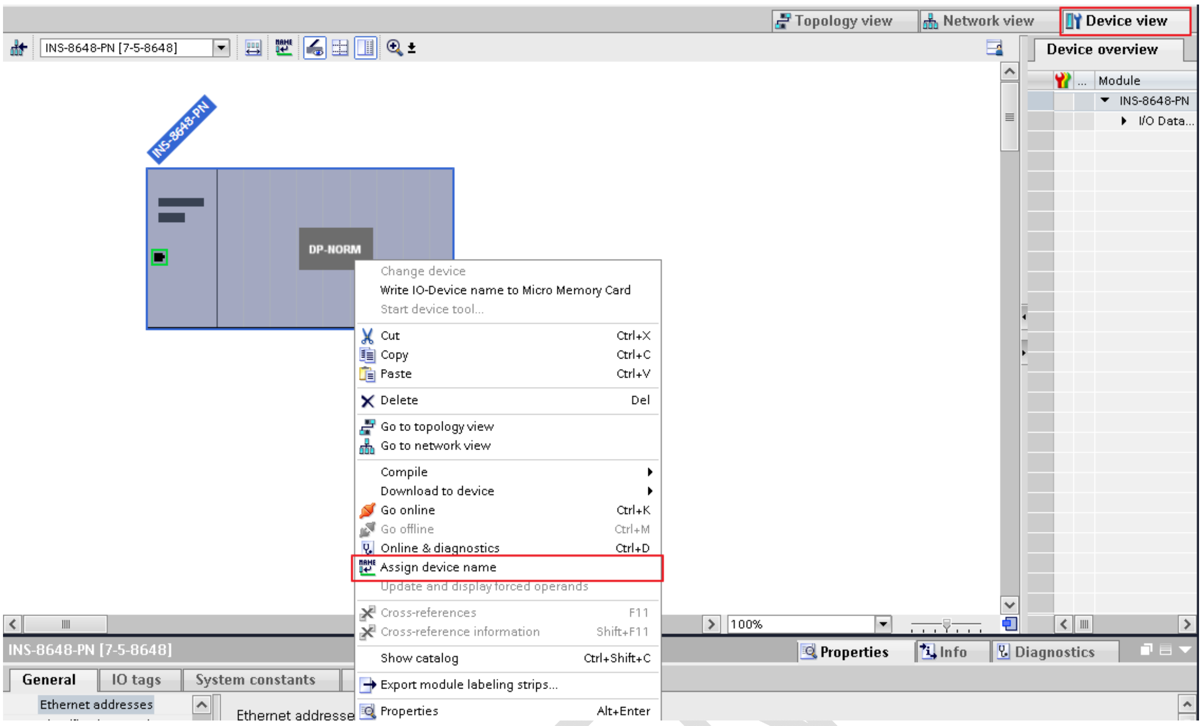
Searching for compatible devices in the selected subnet.

Found accessible device ins-8648-pn

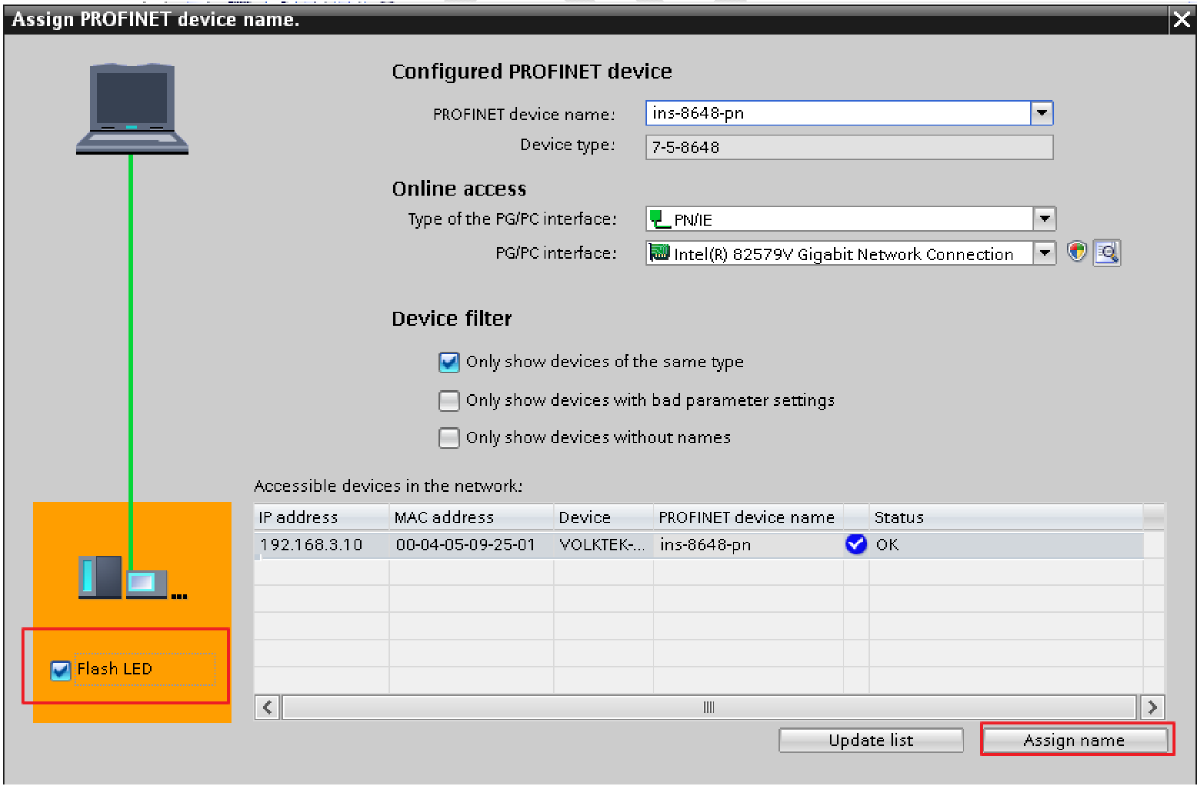
Found accessible device wago-1605

14. You can assign device name as below

- Select the device
- Go to device view on the top right corner
- And then right click on the device
- Select 'assign device name'



15. First update the list and select assign name for that device. The device name in TIA should match the device.


Assign PROFINET device name.

Configured PROFINET device

PROFINET device name: ins-8648-pn

Device type: 7-5-8648

Online access

Type of the PG/PC interface: PN/IE

PG/PC interface: Intel(R) 82579V Gigabit Network Connection

Device filter

☑ Only show devices of the same type

□ Only show devices with bad parameter settings

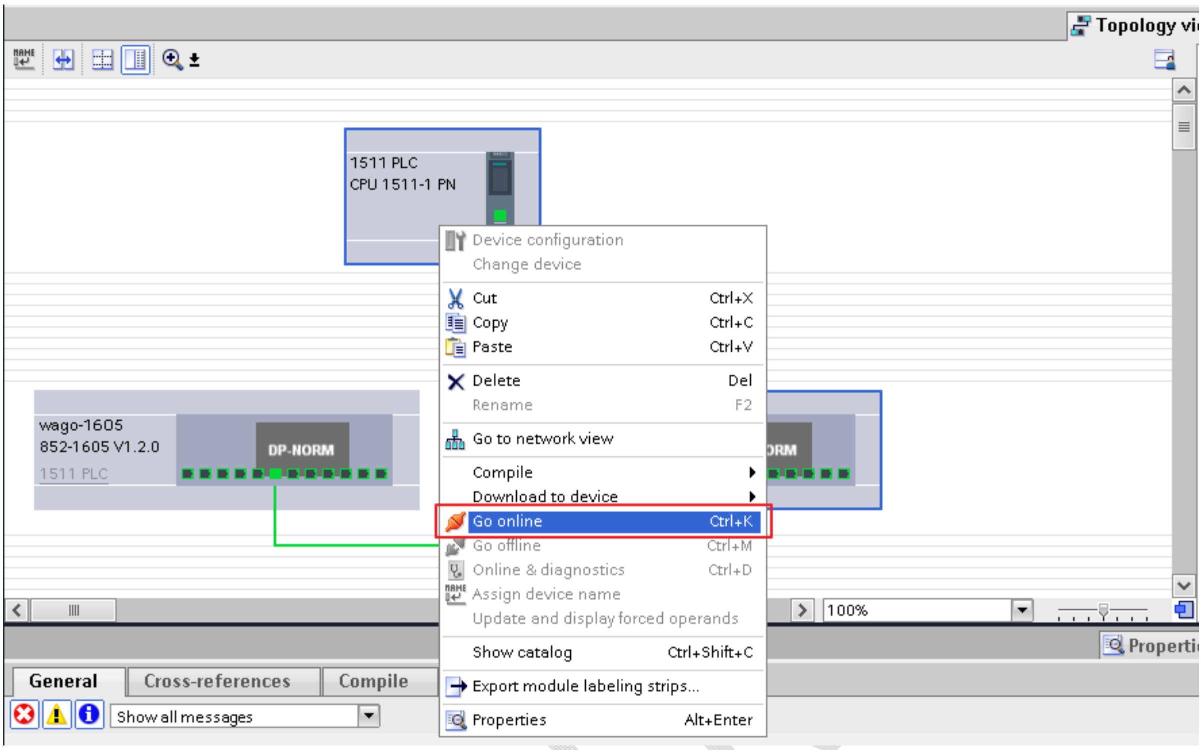
□ Only show devices without names

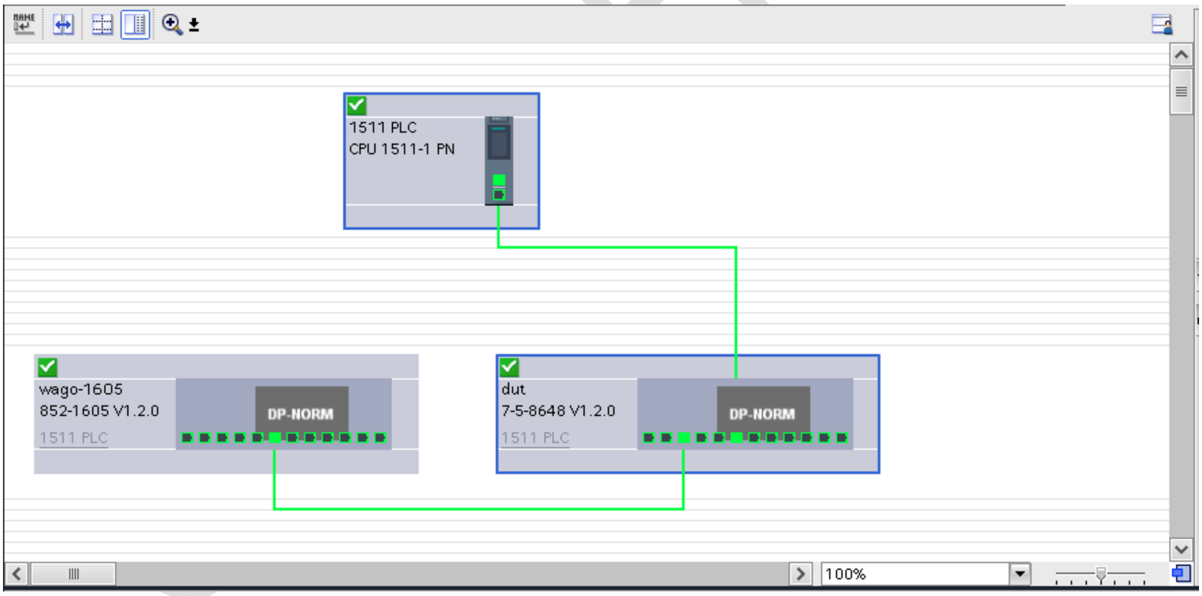
Accessible devices in the network:

IP address	MAC address	Device	PROFINET device name	Status
192.168.3.10	00-04-05-09-25-01	VOLKTEK-...	ins-8648-pn	✓ OK

☑ Flash LED

16. Go online to check whether the connected devices have established connection



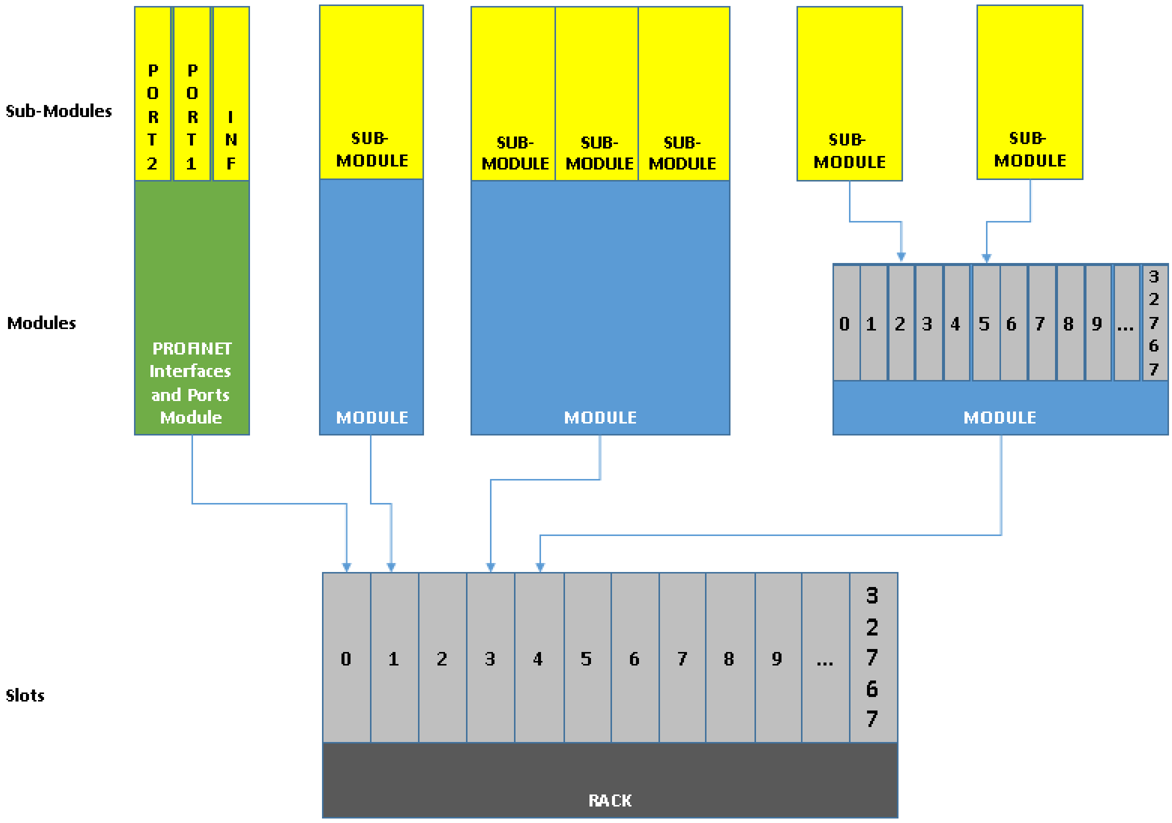


If all are green in color then the connection is successful and all the devices are working normally.

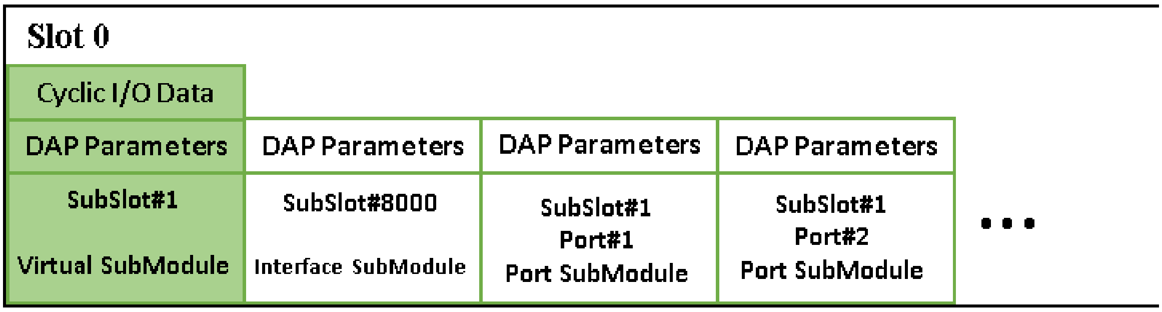
5.8. Cyclic I/O Data

Cyclic I/O data are always sent between the PLC and Switches at the specified periodic time.

These data are transmitted almost real time. For example, status information from the Switches, and variables to be written to the Switch would typically be part of the cyclic data.
Cyclic I/O Data is binding to the Submodule and conventionally, Subslot#0 is not used to I/O submodule.
Profinet has 3 types of submodules - virtual Submodule, interface submodule and port submodule.
All of these submodules are allowed to be binded with an I/O data.
Virtual-Submodule is always inserted into subslot#1.
We defined our cyclic I/O data only on virtual-submodule.



Volktek Profinet Switch defines cyclic I/O data (RTC) only on the Virtual-Submodule associated with Slot#0\SubSlot#1. There is no cyclic I/O data defined on submodules other than Virtual-Submodule.
Since Virtual-Submodule is always placed in subslot#1, Cyclic IO data in Volktek PN switch is addressed with the Slot#0\Subslot#1.



The cyclic I/O data format is listed as below.
There is 26 Bytes of cyclic I/O data. First two bytes of data indicates device's diagnosis information and the other 24 Bytes denotes the Port Status information. 2-Bytes of data for each port information.

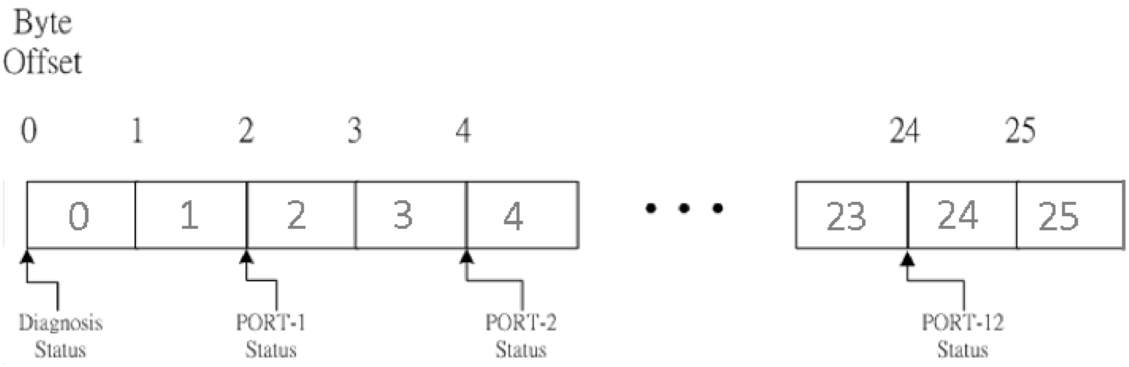
26 Bytes of Cyclic Input on Virtual-submodule addressed with Slot#0/Subslot#1

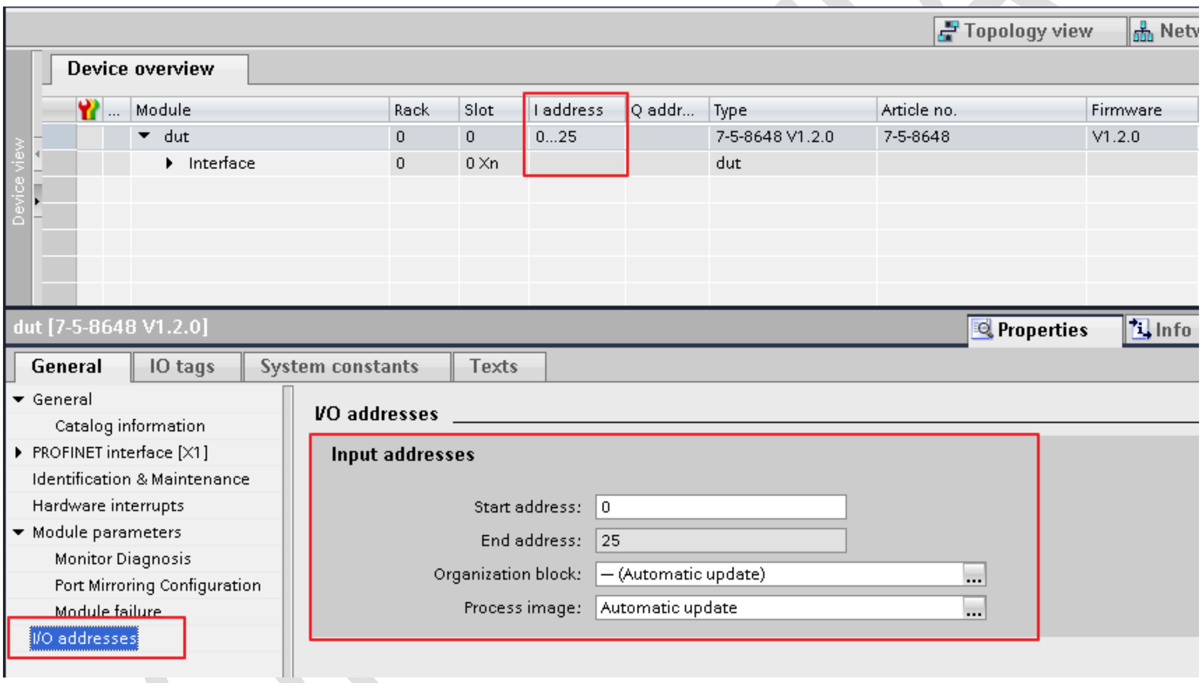
Byte Offset	Description
0	16 bits of data represent device diagnosis status
2	16 bits of data represent PORT-1 status
4	16 bits of data represent PORT-2 status
6	16 bits of data represent PORT-3 status
8	16 bits of data represent PORT-4 status
10	16 bits of data represent PORT-5 status
12	16 bits of data represent PORT-6 status
14	16 bits of data represent PORT-7 status
16	16 bits of data represent PORT-8 status
18	16 bits of data represent PORT-9 status
20	16 bits of data represent PORT-10 status
22	16 bits of data represent PORT-11 status
24	16 bits of data represent PORT-12 status

5.8.1. Cyclic IO example:

For Cyclic IO data addressed with Slot#0\SubSlot#1, the TIA Portal will automatically generate a mapping address for it after it is dragged and dropped into Network View from the Hardware catalog.

Following diagram show the IO addresses that TIA Portal assigned for the 26 bytes of cyclic IO data addressed with Slot#0/Subslot#1. The IO address mapping is from 0 to 25 which is just equal to 26 Bytes.
User can use this mapping address to access each bit of data via the PLC tags.
For example, if you want to access PORT-2 status information embedded in the cyclic IO data then you need to create a PLC tag and bind it with **"%IW4"** address.





...	Module	Rack	Slot	I address	Q addr...	Type	Article no.	Firmware
	dut	0	0	0...25		7-5-8648 V1.2.0	7-5-8648	V1.2.0
	Interface	0	0 Xn			dut		

dut [7-5-8648 V1.2.0]

I/O addresses

Input addresses

Start address: 0

End address: 25

Organization block: — (Automatic update)

Process image: Automatic update

Below is detailed data structure.

Cyclic Input for Device Diagnosis

TAG for Cyclic Input Data	
DIAG.%X0	bit0: pn_diagcode_board_temp Value: 0-NO, 1-YES MainBoard Over Temparature Diag
DIAG.%X1	bit1: pn_diagcode_cpu_temp,

	Value: 0-NO, 1-YES CPU Over Temparature Diag
DIAG.%X2	bit2: pn_diagcode_phy_temp, Value: 0-NO, 1-YES PHY Over Temparature Diag
DIAG.%X3	bit3: pn_diagcode_pwr_ovolt, Value: 0-NO, 1-YES 1st Power Module Over Voltage Diag
DIAG.%X4	bit4: pn_diagcode_rps_ovolt, Value: 0-NO, 1-YES 2nd Power Module Under Voltage Diag
DIAG.%X5	bit5: pn_diagcode_pwr_uvolt, Value: 0-NO, 1-YES 1st Power Module Under Voltage Diag
DIAG.%X6	bit6: pn_diagcode_rps_uvolt, Value: 0-NO, 1-YES 2nd Power Module Under Voltage Diag
DIAG.%X7	bit7: pn_diagcode_pwr_nopwr Value: 0-NO, 1-YES 1st Power Module Not Existed Diag
DIAG.%X8	bit8: pn_diagcode_rps_nopwr Value: 0-NO, 1-YES 2nd Power Module Not Existed Diag
DIAG.%X9	bit9: MRP Ring State Value: 0-Disabled, 1-Enabled
DIAG.%X10	bit10: MRP Ring Running Status Value: 0-Closed, 1-Opened NOTE:

	This bit is meaningful only when DIAG.%X9 = 1
DIAG.%X11- DIAG.%X14	bit11 - bit14 Reserved
DIAG.%X15	bit15: Device Status Value: 0-OK, 1-Failed Device Status is OK, No Alarm is generated from Profinet Stack

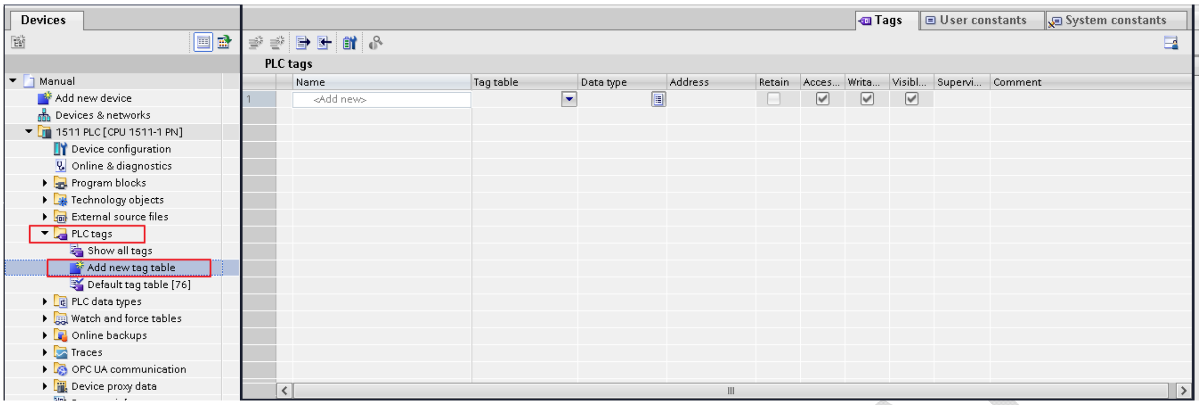
Cyclic Input for P1 – P12 Port Status (Pn: n, 1–12)

TAG for Cyclic Input Data	
Pn.%X0	The Nth Port, bit#0 of a WORD, Port Power Status 0: power down, 1: power up
Pn.%X1	The Nth Port, bit#1 of a WORD Port Duplex Mode 0: Full Duplex, 1: Half Duplex
Pn.%X2	The Nth Port, bit#2 of a WORD Port Link Status 0: Link Down, 1: Link Up
Pn.%X3	The Nth Port, bit#3 of a WORD This bit is combined with Pn.%X4 , Pn.%X5 to represent Port Speed Pn.%X5-Pn.%X4-Pn.%X3 Values 0b000: 10M, 0b001: 100M, 0b010: 1000M, 0b111: Auto
Pn.%X4	The Nth Port, bit#4 of a WORD

Pn.%X5	The Nth Port, bit#5 of a WORD
Pn.%X6	The Nth Port, bit#6 of a WORD This bit is combined with Pn.%X7 , Pn.%X8 to represent Port Current Link Activity Pn.%X8-Pn.%X7-Pn.%X6 Values 1: Disable, 2: Block, 3: Listen, 4: Learn, 5: Foward
Pn.%X7	The Nth Port, bit#7 of a WORD
Pn.%X8	The Nth Port, bit#8 of a WORD
Pn.%X9	The Nth Port, bit#9 of a WORD This bit is combined with Pn.%X10 to represent Port LLDP Admin Status Pn.%X10-Pn.%X9 Values 0: disabled, 1: txonly, 2: rxonly, 3: txrx
Pn.%X10	The Nth Port, bit#10 of a WORD
Pn.%X11 - Pn.%X15	The Nth Port, bit#12-bit#15 of a WORD Reserved

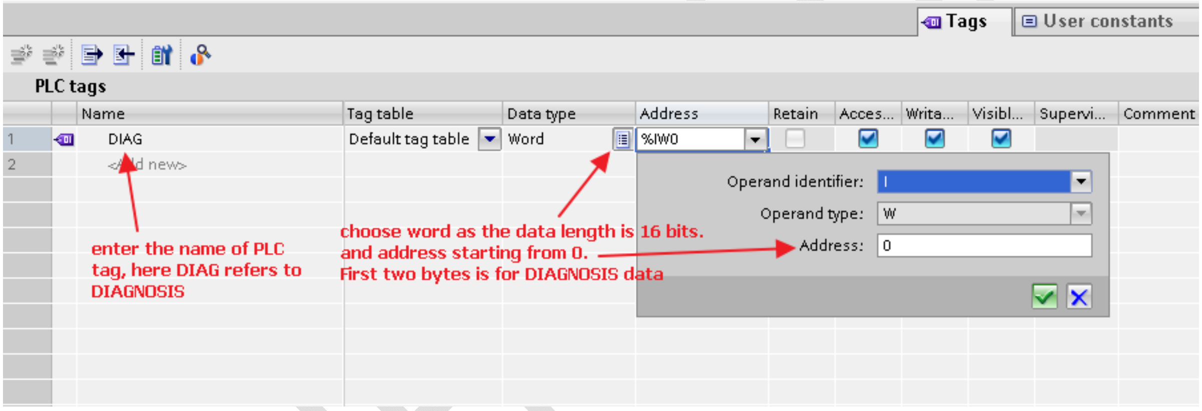
We will show below how to use the TIA Portal to access these cyclic I/O data.

1. In project tree menu select PLC tags and select add new tag table



	Name	Tag table	Data type	Address	Retain	Acces...	Writa...	Visibl...	Supervi...	Comment
1	<Add new>				□	☑	☑	☑		

2. Enter the details of that PLC tag u created, First Two Bytes of Cyclic Input is for Diagnosis data defined in Interface Submodule (Refer to chapter 6.7.10 Cyclic Input in this document)



	Name	Tag table	Data type	Address	Retain	Acces...	Writa...	Visibl...	Supervi...	Comment
1	DIAG	Default tag table	Word	%IW0	□	☑	☑	☑		
2	<Add new>									

Operand identifier: I

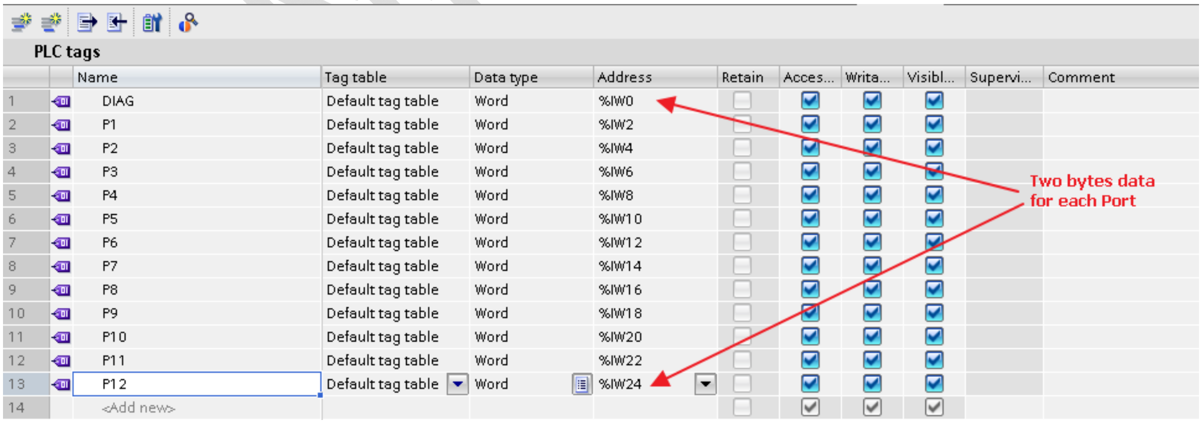
Operand type: W

Address: 0

enter the name of PLC tag, here DIAG refers to DIAGNOSIS

choose word as the data length is 16 bits. and address starting from 0. First two bytes is for DIAGNOSIS data

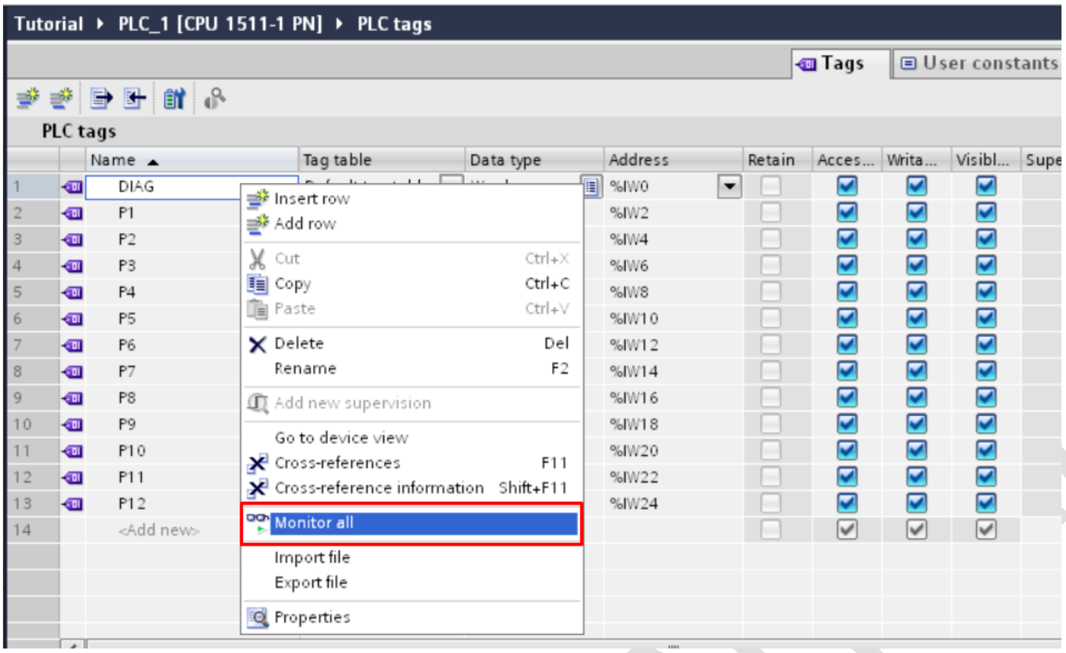
3. Add other tags for port sub-modules, P1 to P12, IO address is from



	Name	Tag table	Data type	Address	Retain	Acces...	Writa...	Visibl...	Supervi...	Comment
1	DIAG	Default tag table	Word	%IW0	□	☑	☑	☑		
2	P1	Default tag table	Word	%IW2	□	☑	☑	☑		
3	P2	Default tag table	Word	%IW4	□	☑	☑	☑		
4	P3	Default tag table	Word	%IW6	□	☑	☑	☑		
5	P4	Default tag table	Word	%IW8	□	☑	☑	☑		
6	P5	Default tag table	Word	%IW10	□	☑	☑	☑		
7	P6	Default tag table	Word	%IW12	□	☑	☑	☑		
8	P7	Default tag table	Word	%IW14	□	☑	☑	☑		
9	P8	Default tag table	Word	%IW16	□	☑	☑	☑		
10	P9	Default tag table	Word	%IW18	□	☑	☑	☑		
11	P10	Default tag table	Word	%IW20	□	☑	☑	☑		
12	P11	Default tag table	Word	%IW22	□	☑	☑	☑		
13	P12	Default tag table	Word	%IW24	□	☑	☑	☑		
14	<Add new>				□	☑	☑	☑		

Two bytes data for each Port

4. After Re-Compile & Download program to PLC, Right click on the tag name and select “Monitor all” to Monitor device cyclic input data.

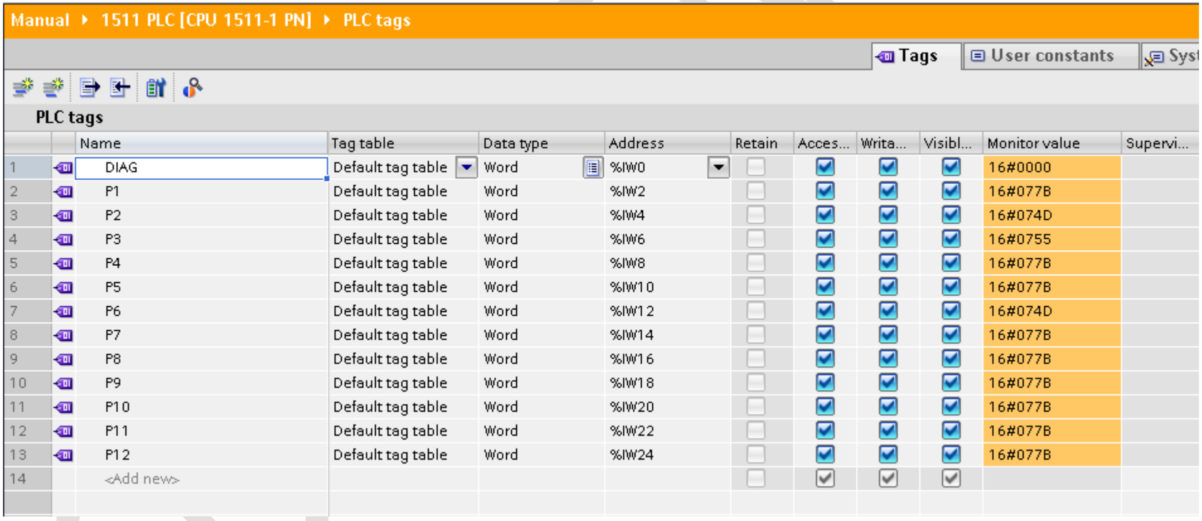


Tutorial ▸ PLC_1 [CPU 1511-1 PN] ▸ PLC tags

PLC tags

	Name	Address	Retain	Acces...	Writa...	Visibl...	Supe
1	DIAG	%IW0	□	☑	☑	☑	
2	P1	%IW2	□	☑	☑	☑	
3	P2	%IW4	□	☑	☑	☑	
4	P3	%IW6	□	☑	☑	☑	
5	P4	%IW8	□	☑	☑	☑	
6	P5	%IW10	□	☑	☑	☑	
7	P6	%IW12	□	☑	☑	☑	
8	P7	%IW14	□	☑	☑	☑	
9	P8	%IW16	□	☑	☑	☑	
10	P9	%IW18	□	☑	☑	☑	
11	P10	%IW20	□	☑	☑	☑	
12	P11	%IW22	□	☑	☑	☑	
13	P12	%IW24	□	☑	☑	☑	
14	<Add new>		□	☑	☑	☑	

5. Monitoring Result:



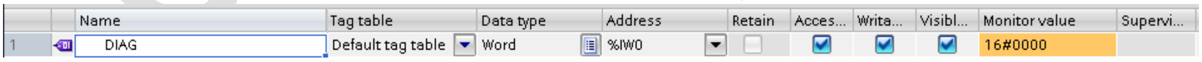
Manual ▸ 1511 PLC [CPU 1511-1 PN] ▸ PLC tags

PLC tags

	Name	Tag table	Data type	Address	Retain	Acces...	Writa...	Visibl...	Monitor value	Supervi...
1	DIAG	Default tag table	Word	%IW0	□	☑	☑	☑	16#0000	
2	P1	Default tag table	Word	%IW2	□	☑	☑	☑	16#077B	
3	P2	Default tag table	Word	%IW4	□	☑	☑	☑	16#074D	
4	P3	Default tag table	Word	%IW6	□	☑	☑	☑	16#0755	
5	P4	Default tag table	Word	%IW8	□	☑	☑	☑	16#077B	
6	P5	Default tag table	Word	%IW10	□	☑	☑	☑	16#077B	
7	P6	Default tag table	Word	%IW12	□	☑	☑	☑	16#074D	
8	P7	Default tag table	Word	%IW14	□	☑	☑	☑	16#077B	
9	P8	Default tag table	Word	%IW16	□	☑	☑	☑	16#077B	
10	P9	Default tag table	Word	%IW18	□	☑	☑	☑	16#077B	
11	P10	Default tag table	Word	%IW20	□	☑	☑	☑	16#077B	
12	P11	Default tag table	Word	%IW22	□	☑	☑	☑	16#077B	
13	P12	Default tag table	Word	%IW24	□	☑	☑	☑	16#077B	
14	<Add new>				□	☑	☑	☑		

6. Decoding the Monitor value.

- Consider the Monitor value of DIAG which is two bytes in hexadecimal format



	Name	Tag table	Data type	Address	Retain	Acces...	Writa...	Visibl...	Monitor value	Supervi...
1	DIAG	Default tag table	Word	%IW0	□	☑	☑	☑	16#0000	

Monitor value= 0000

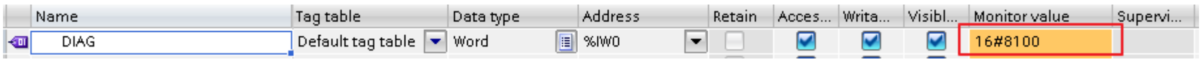
After converting it into binary we get 0000 0000 0000 0000

Refereeing to the table 5.1 above

0	0	0	0	0	0	0	0
Bit-7: 1st Power module not existed	Bit-6: 2nd Power module under voltage	Bit-5: 1st Power module under voltage	Bit-4: 2nd Power module over voltage	Bit-3: 1st Power module over voltage	Bit-2: PHY Over Temperature	Bit-1: CPU Over Temperature	Bit-0: Main-Board Over Temperature
Value: 0-NO, 1-YES	Value: 0-NO, 1-YES	Value: 0-NO, 1-YES	Value: 0-NO, 1-YES	Value: 0-NO, 1-YES	Value: 0-NO, 1-YES	Value: 0-NO, 1-YES	Value: 0-NO, 1-YES

0	0	0	0	0	0	0	0
Bit-15: Device status	Bit-14: Reserved	Bit-13: Reserved	Bit-12: Reserved	Bit-11: Reserved	Bit-10: MRP ring running status	Bit-9: MRP ring state	Bit-8: 2nd Power module not existed
Value: 0-OK, 1-failed					Value: 0-Closed, 1-Opened	Value: 0-Disabled, 1-Enabled	Value: 0-NO, 1-YES

- ✓ Based on this table you can see what even have been triggered.
- ✓ Currently no any DIAG events.
- ✓ Below is when there is any events in the switch.

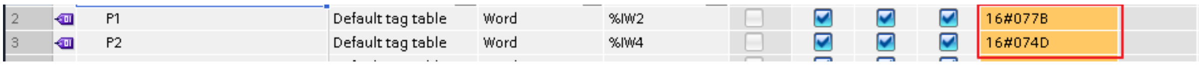


Name	Tag table	Data type	Address	Retain	Acces...	Writa...	Visibl...	Monitor value	Supervi...
DIAG	Default tag table	Word	%IW0	□	☑	☑	☑	16#8100	

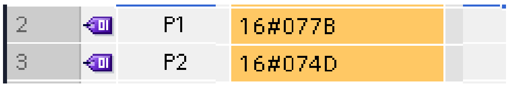
Now the value is 8100, when converted to binary format 1000 0001 0000 0000
16th bit = 1 (device status)
8th bit = 1 (2nd Power module not existed)

So from the current value we can analyze that 2nd power module is not present in the switch.

- Consider the Monitor value of P1 and P2 which is two bytes each in hexadecimal format



2	P1	Default tag table	Word	%IW2	□	☑	☑	☑	16#077B
3	P2	Default tag table	Word	%IW4	□	☑	☑	☑	16#074D

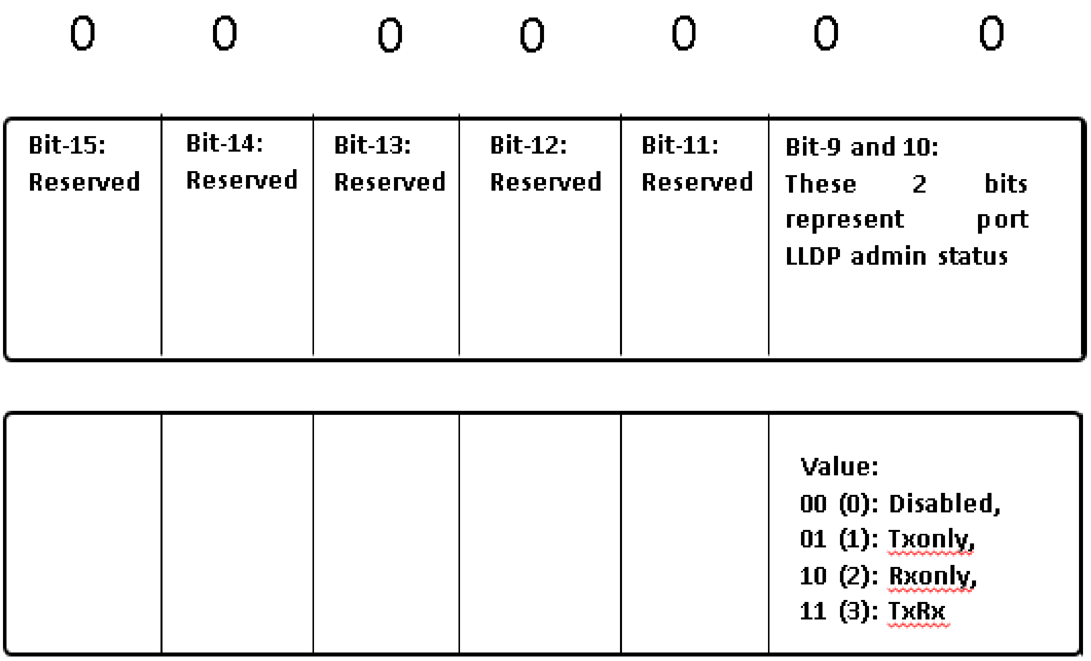


2	P1	16#077B
3	P2	16#074D

- ✓ Port 1 Monitor value 077B, when converted to binary 0000 0111 0111 1011
- ✓ Port 2 Monitor value 074D, when converted to binary 0000 0111 0100 1101
- ✓ Refereeing to the table 5.2 above

0 0 0 0 0 0 0 0 0

Bit-6,7 and 8: These 3 bits represent port current link activity	Bit-3,4 and 5: These 3 bits represent the port speed	Bit-2: Port Link Status	Bit-1: Port Duplex Mode	Bit-0: Port power status
Value: 001 (1): Disable, 010 (2): Block, 011 (3): Listen, 100 (4): Learn, 101 (5): Forward	Value: 000 : 10M, 001 : 100M, 010 : 1000M 111 : Auto	Value: 0-Link Down, 1-Link Up	Value: 0-Full Duplex, 1-Half Duplex	Value: 0-Power Down 1-Power Up



0	0	0	0	0	0 0
Bit-15: Reserved	Bit-14: Reserved	Bit-13: Reserved	Bit-12: Reserved	Bit-11: Reserved	Bit-9 and 10: These 2 bits represent port LLDP admin status
					Value: 00 (0): Disabled, 01 (1): Txonly, 10 (2): Rxonly, 11 (3): TxRx

- ✓ Based on this table you can see the difference between active ports and inactive ports.
- ✓ Currently Port-1 is inactive and Port-2 is active..

5.9. DAP Parameters

DAP parameters are used for device configuration purpose. After device is started up, PLC will read/write these parameters from/to I/O device to get/configure I/O device’s functions.
For Volktek PN switch. We provides following DAP parameters to access I/O device’s function.

Index	SubSlot	Access	Length	Usage
1	0x1	R/W	3	Used To Disable/Enable Monitoring Diagnosis
2	0x8001 ~ 0x800C	R	6	Used To Read each port status
3	0x1	R	12	Used to Read device Diagnosis information
4	0x1	R/W	10	Used to Configure Port Mirror function

Below are the detailed data structure of each parameter index. We will demo in next paragraph about how to use RDREC & WRREC function blocks to access these parameters in TIA portal.

INDEX=1, Disable/Enable Diagnosis Alarms

Offset	Value	Description	Default Value
0	0	Enable PWR Diagnosis Alarms	0
	1	Disable PWR Diagnosis Alarms	
1	0	Enable RPS Diagnosis Alarms	0
	1	Disable RPS Diagnosis Alarms	
2	0	Enable Temperature Diagnosis Alarms	0
	1	Disable Temperature Diagnosis Alarms	

INDEX=2, Read Each Port Status, Defined on each Port-Submodule

Offset	Value	Description	Default Value
0	0	Port Power Down	0
	1	Port Power Up	
1	0	Port Full Duplex Mode	0
	1	Port Half Duplex Mode	
2	0	Port Link Down	0
	1	Port Link Up	
3	0	Port Speed 10Mb	0
	1	Port Speed 100Mb	
	2	Port Speed 1Gb	
	7	Port Speed Automatic	
4	1	Port Link Activity – Disabled	5
	2	Port Link Activity – Blocked	

	3	Port Link Activity – Listen	
	4	Port Link Activity – Learn	
	5	Port Link Activity – Forward	
5	0	Port LLDP Admin Status – Disabled	0
	1	Port LLDP Admin Status – TX Only	
	2	Port LLDP Admin Status – RX Only	
	3	Port LLDP Admin Status – TX/RX	

INDEX=3, Read Device Diagnosis Status

Offset	Value	Description	Default Value
0	0	MainBoard Not Over Temperature	0
	1	MainBoard Over Temperature	
1	0	CPU Not Over Temperature	0
	1	CPU Over Temperature	
2	0	Ethernet PHY Not Over Temperature	0
	1	Ethernet PHY Over Temperature	
3	0	PWR Not Over Voltage	0
	1	PWR Over Voltage	
4	0	RPS Not Over Voltage	0
	1	RPS Over Voltage	
5	0	PWR Not Under Voltage	0
	1	PWR Under Voltage	
6	0	RPS Not Under Voltage	0
	1	RPS Under Voltage	
7	0	PWR Has Power	0
	1	PWR No Power	
8	0	RPS Has Power	0
	1	RPS No Power	
9	0	MRP Ring Disabled	0
	1	MRP Ring Enabled	
10	0	MRP Ring Opened (Meaningful if Byte#9 = 1)	0
	1	MRP Ring Closed (Meaningful if Byte#9 = 1)	
11	0	Device Has alarm	0
	1	Device Normal, No alarm generated	

INDEX=4, Configure Port Mirror

Byte Offset	Bit Offset	Bit Length	Value		Default Value
0	-	-	0	Enable/Disable Port Mirror Function	0
			1		
1	-	-	0-255	Mirror To Which Port	0
2	0	1	0	Enable/Disable Mirror from Ingress	0

			1	PORT#1	
	1	1	0	Enable/Disable Mirror from Ingress PORT#2	0
			1		
	2	1	0	Enable/Disable Mirror from Ingress PORT#3	0
			1		
	3	1	0	Enable/Disable Mirror from Ingress PORT#4	0
			1		

•

•

2	7	1	0	Enable/Disable Mirror from Ingress PORT#8	0
			1		
3	0	1	0	Enable/Disable Mirror from Ingress PORT#9	0
			1		
	1	1	0	Enable/Disable Mirror from Ingress PORT#10	0
			1		
	2	1	0	Enable/Disable Mirror from Ingress PORT#11	0
			1		
	3	1	0	Enable/Disable Mirror from Ingress PORT#12	0
			1		

•

•

5	7	1	0	Enable/Disable Mirror from Ingress PORT#32	0
			1		
6	0	1	0	Enable/Disable Mirror from Egress PORT#1	0
			1		
	1	1	0	Enable/Disable Mirror from Egress PORT#2	0
			1		
	2	1	0	Enable/Disable Mirror from Egress PORT#3	0
			1		
	3	1	0	Enable/Disable Mirror from Egress PORT#4	0
			1		
	4	1	0	Enable/Disable Mirror from Egress PORT#5	0
			1		

•

•

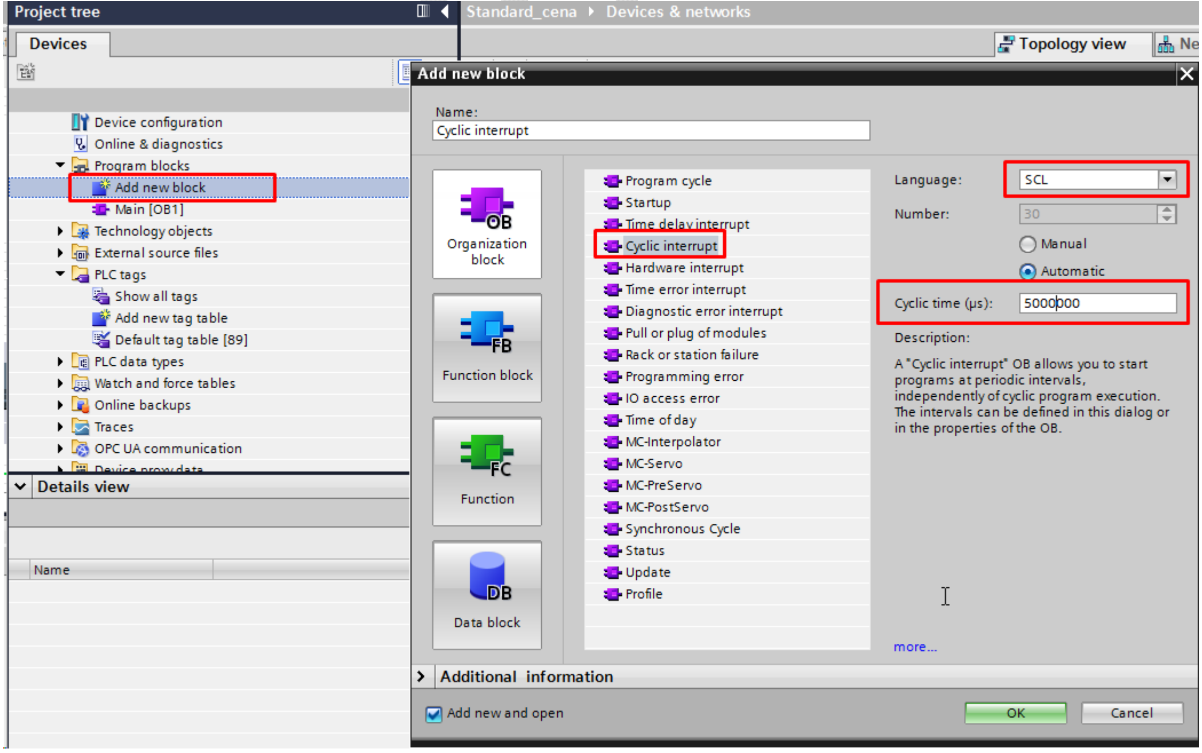
9	7	1	0	Enable/Disable Mirror from Egress PORT#32	0
			1		

Unlike Cyclic IO, DAP parameters is accessed via RDREC/WRREC function blocks from TIA portal.

Following diagrams demo how to use RDREC function block to access INDEX = 2 DAP parameter to read port status.

Index	SubSlot	Access	Length	Usage
2	0x8001 ~ 0x800C	R	6	Used To Read each port status

Add cyclic interrupt block for every 5 seconds



Name: Cyclic interrupt

Language: SCL

Number: 30

○ Manual

● Automatic

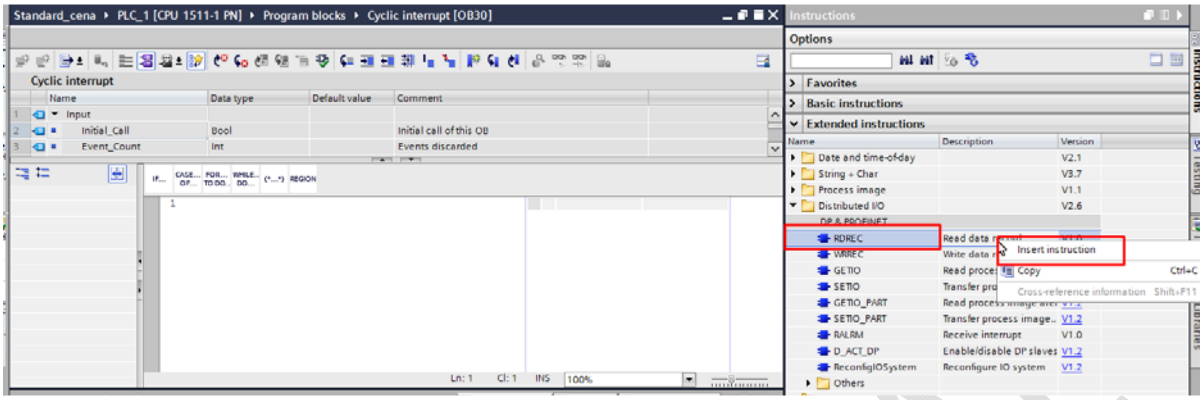
Cyclic time (µs): 5000000

Description:

A "Cyclic interrupt" OB allows you to start programs at periodic intervals, independently of cyclic program execution. The intervals can be defined in this dialog or in the properties of the OB.

☑ Add new and open

Insert RDREC Function Block

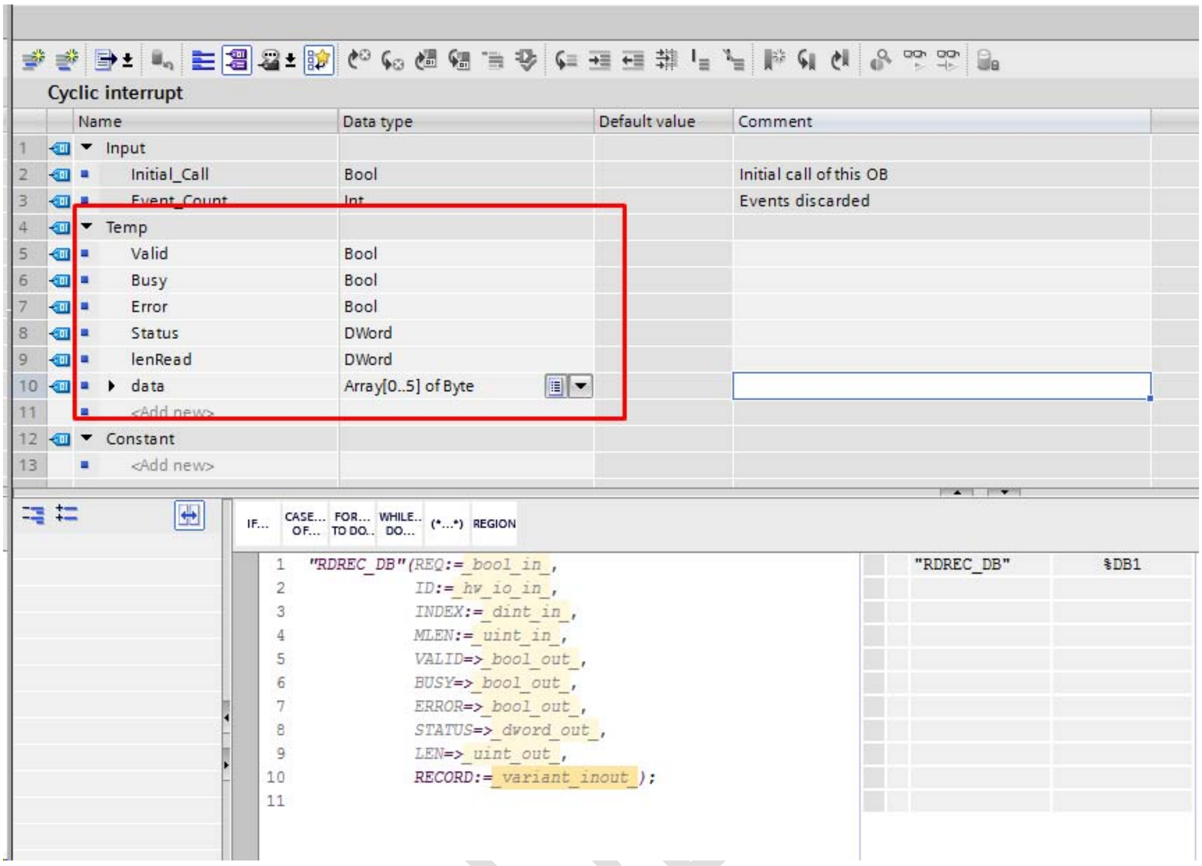


Standard_cena ▸ PLC_1 [CPU 1511-1 PN] ▸ Program blocks ▸ Cyclic interrupt [OB30]
Cyclic interrupt
IF... CASE... OF... FOR... TO DO... WHILE... DO... (*...*) REGION
Ln: 1 Cl: 1 INS 100%
Instructions
Options
Favorites
Basic instructions
Extended instructions
Insert instruction
Copy Ctrl+C
Cross-reference information Shift+F11
Instructions
Testing
Libraries

	Name	Data type	Default value	Comment
1	▾ Input			
2	▪ Initial_Call	Bool		Initial call of this OB
3	▪ Event_Count	Int		Events discarded

Name	Description	Version
▸ Date and time-of-day		V2.1
▸ String + Char		V3.7
▸ Process image		V1.1
▾ Distributed I/O		V2.6
DP & PROFINET		
RDREC	Read data r	
WRREC	Write data r	
GETIO	Read proce	
SETIO	Transfer pro	
GETIO_PART	Read process	
SETIO_PART	Transfer process image...	V1.2
RALRM	Receive interrupt	V1.0
D_ACT_DP	Enable/disable DP slaves	V1.2
ReconfigIOSystem	Reconfigure IO system	V1.2
▸ Others		

Create RDREC function block parameter as follows
Because INDEX=2 data length = 6,
therefore data array parameter should bey Array[0..5] of Byte



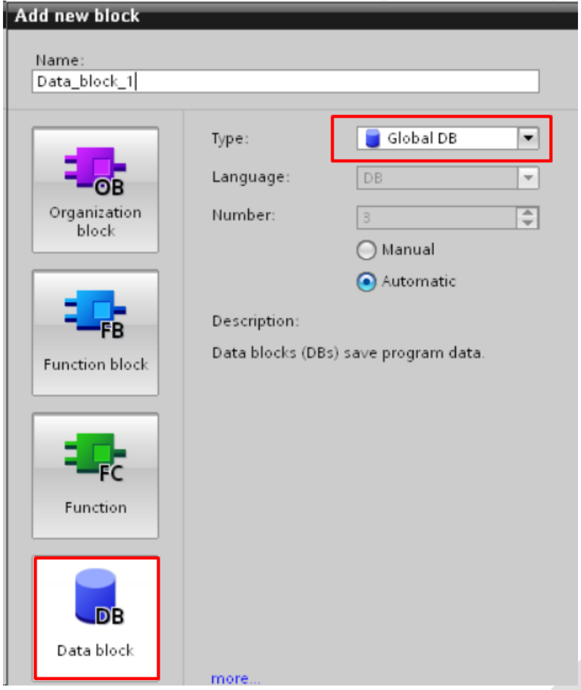
Cyclic interrupt

	Name	Data type	Default value	Comment
1	▼ Input			
2	■ Initial_Call	Bool		Initial call of this OB
3	■ Event_Count	Int		Events discarded
4	▼ Temp			
5	■ Valid	Bool		
6	■ Busy	Bool		
7	■ Error	Bool		
8	■ Status	DWord		
9	■ lenRead	DWord		
10	■ ▶ data	Array[0..5] of Byte		
11	■ <Add new>			
12	▼ Constant			
13	■ <Add new>			

```
"RDREC_DB"(REQ:=_bool_in_,
           ID:=_hw_io_in_,
           INDEX:=_dint_in_,
           MLEN:=_uint_in_,
           VALID=>_bool_out_,
           BUSY=>_bool_out_,
           ERROR=>_bool_out_,
           STATUS=>_dword_out_,
           LEN=>_uint_out_,
           RECORD:=_variant_inout_);
```

"RDREC_DB" %DB1

Create a DB to receive the output #data array in RDREC Function call


Add new block

Name: Data_block_1

Type: Global DB

Language: DB

Number: 3

○ Manual

● Automatic

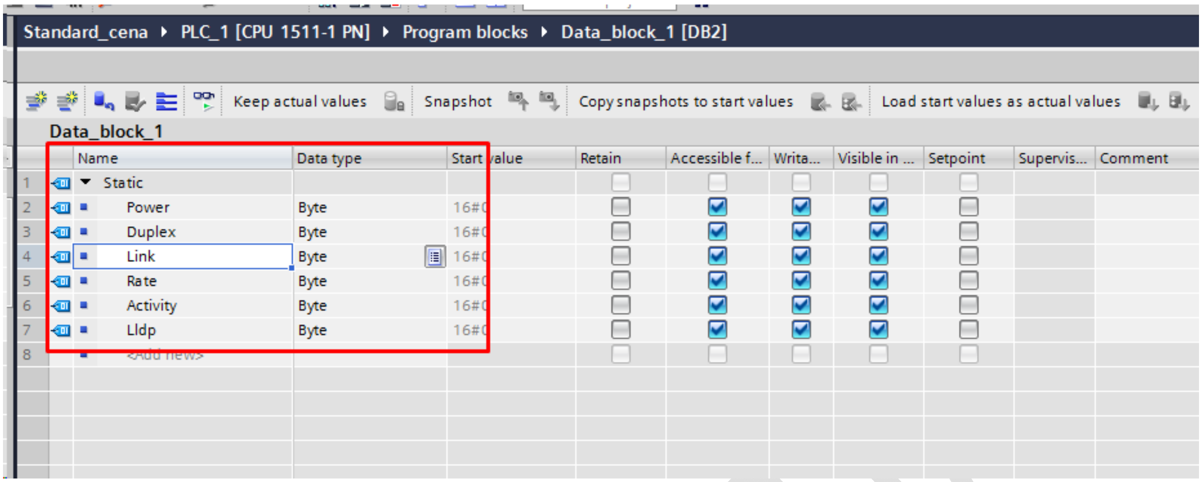
Description:

Data blocks (DBs) save program data.

There are 6 bytes of data,

Offset	Value	Description	Default Value
0	0	Port Power Down	0
	1	Port Power Up	
1	0	Port Full Duplex Mode	0
	1	Port Half Duplex Mode	
2	0	Port Link Down	0
	1	Port Link Up	
3	0	Port Speed 10Mb	0
	1	Port Speed 100Mb	
	2	Port Speed 1Gb	
	7	Port Speed Automatic	
4	1	Port Link Activity – Disabled	5
	2	Port Link Activity – Blocked	
	3	Port Link Activity – Listen	
	4	Port Link Activity – Learn	
	5	Port Link Activity – Forward	
5	0	Port LLDP Admin Status – Disabled	0
	1	Port LLDP Admin Status – TX Only	
	2	Port LLDP Admin Status – RX Only	
	3	Port LLDP Admin Status – TX/RX	

Therefore the static variables in Global DB is created as follows



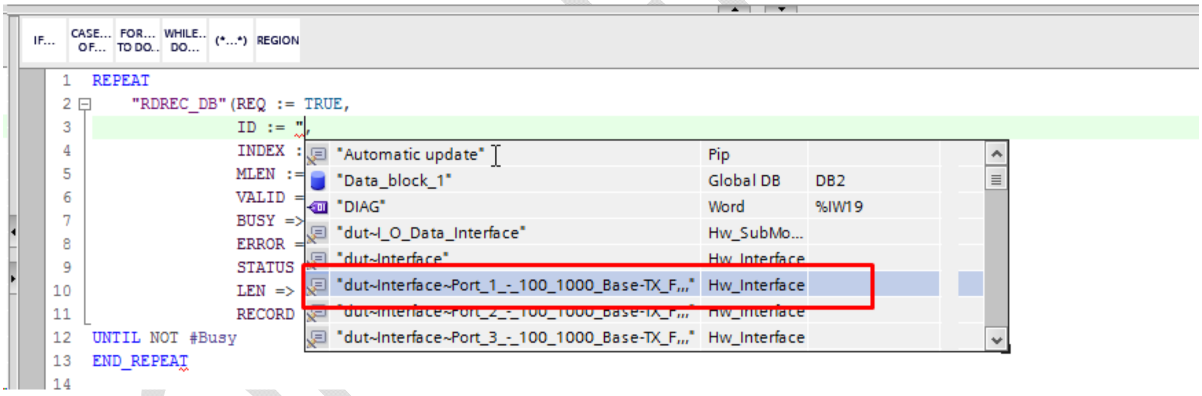
Standard_cena ▸ PLC_1 [CPU 1511-1 PN] ▸ Program blocks ▸ Data_block_1 [DB2]

Keep actual values
Snapshot
Copy snapshots to start values
Load start values as actual values

Data_block_1

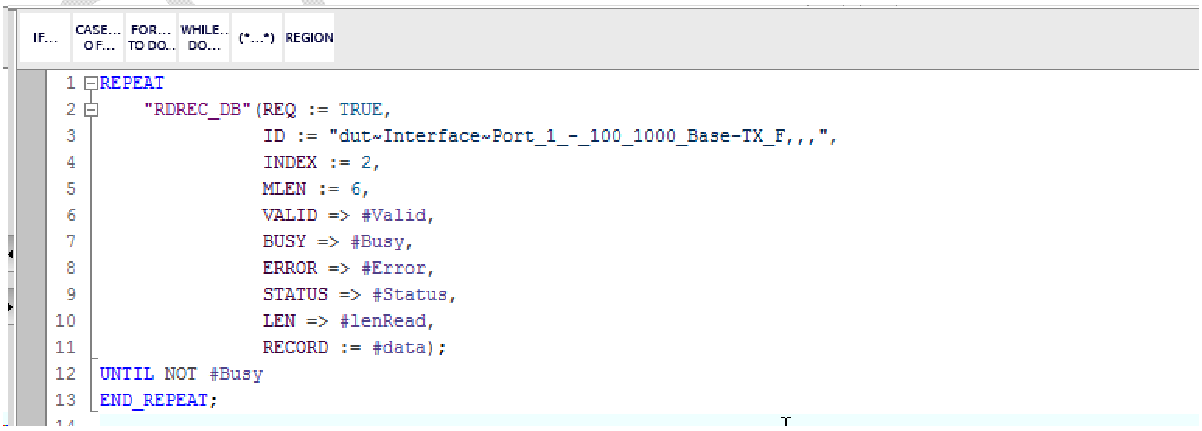
	Name	Data type	Start value	Retain	Accessible f...	Writa...	Visible in ...	Setpoint	Supervis...	Comment
1	▼ Static			□	□	□	□	□		
2	Power	Byte	16#0	□	☑	☑	☑	□		
3	Duplex	Byte	16#0	□	☑	☑	☑	□		
4	Link	Byte	16#0	□	☑	☑	☑	□		
5	Rate	Byte	16#0	□	☑	☑	☑	□		
6	Activity	Byte	16#0	□	☑	☑	☑	□		
7	Lldp	Byte	16#0	□	☑	☑	☑	□		
8	<Add new>			□	□	□	□	□		

We are going to read INDEX=2 of Port Submodule = 0x8001 (PORT#1)
Modify RDREC Function call as follows
We are going to access PORT#1, Therefore Specify ID to PORT#1



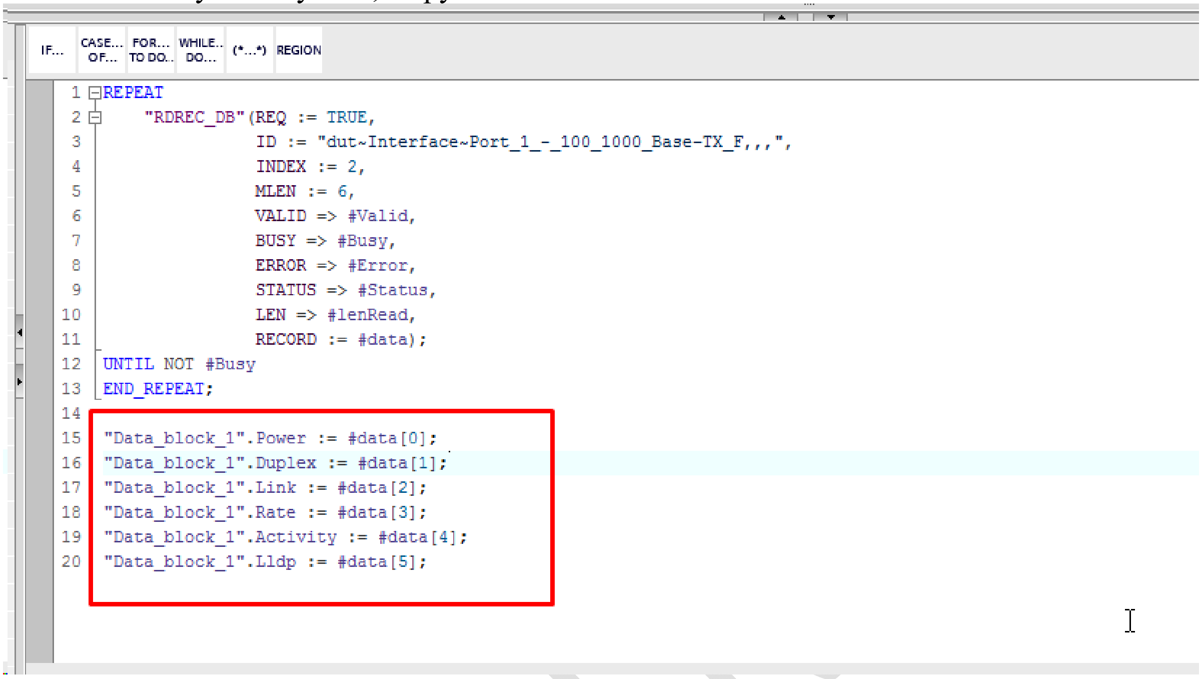
```
REPEAT
    "RDREC_DB"(REQ := TRUE,
               ID := "
               INDEX :
               MLEN :=
               VALID =
               BUSY =>
               ERROR =
               STATUS
               LEN =>
               RECORD
UNTIL NOT #Busy
END_REPEAT
```

"Automatic update"	Pip	
"Data_block_1"	Global DB	DB2
"DIAG"	Word	%IW19
"dut~I_O_Data_Interface"	Hw_SubMo...	
"dut~Interface"	Hw_Interface	
"dut~Interface~Port_1_-_100_1000_Base-TX_F,,,"	Hw_Interface	
"dut~Interface~Port_2_-_100_1000_Base-TX_F,,,"	Hw_Interface	
"dut~Interface~Port_3_-_100_1000_Base-TX_F,,,"	Hw_Interface	



```
REPEAT
    "RDREC_DB"(REQ := TRUE,
               ID := "dut~Interface~Port_1_-_100_1000_Base-TX_F,,,",
               INDEX := 2,
               MLEN := 6,
               VALID => #Valid,
               BUSY => #Busy,
               ERROR => #Error,
               STATUS => #Status,
               LEN => #lenRead,
               RECORD := #data);
UNTIL NOT #Busy
END_REPEAT;
```

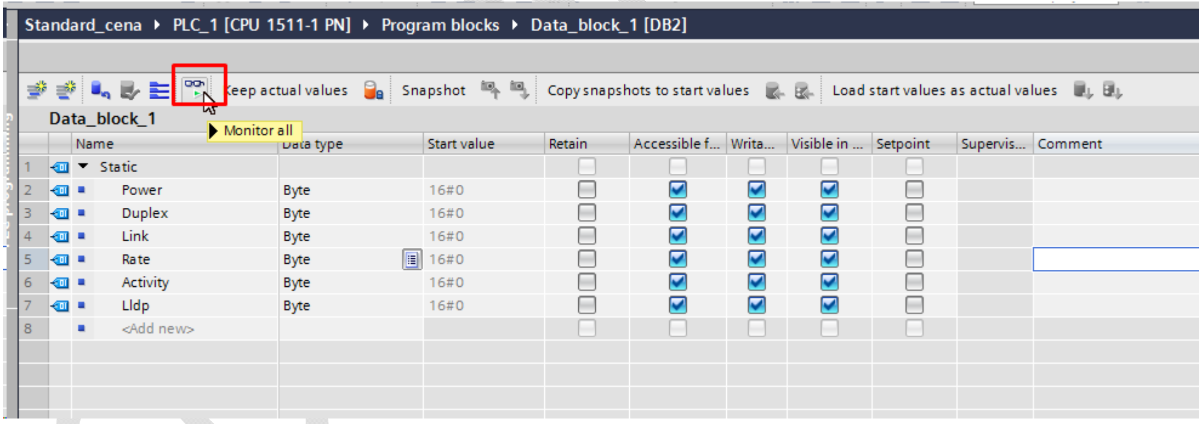
After receive Byte Array data, Copy it to static variables in Global DB



```
REPEAT
    "RDREC_DB"(REQ := TRUE,
               ID := "dut~Interface~Port_1_-_100_1000_Base-TX_F,,,",
               INDEX := 2,
               MLEN := 6,
               VALID => #Valid,
               BUSY => #Busy,
               ERROR => #Error,
               STATUS => #Status,
               LEN => #lenRead,
               RECORD := #data);
UNTIL NOT #Busy
END_REPEAT;

"Data_block_1".Power := #data[0];
"Data_block_1".Duplex := #data[1];
"Data_block_1".Link := #data[2];
"Data_block_1".Rate := #data[3];
"Data_block_1".Activity := #data[4];
"Data_block_1".Lldp := #data[5];
```

After Download, In DB, click “Monitor All”

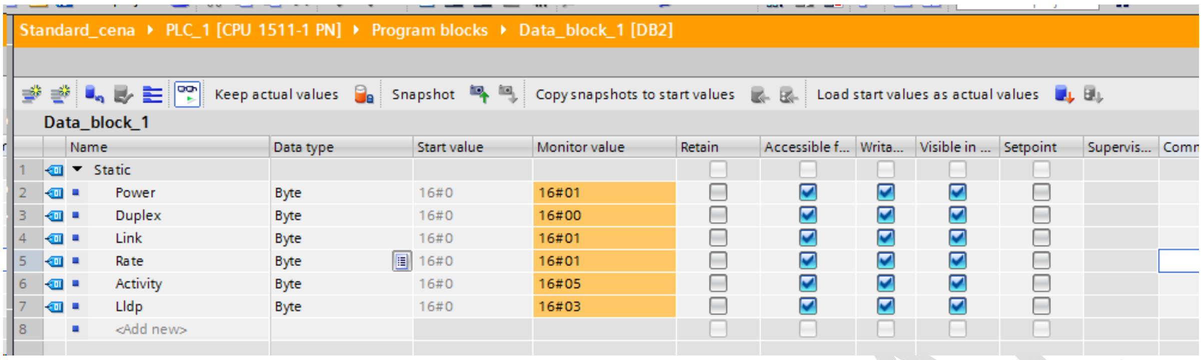

Standard_cena ▸ PLC_1 [CPU 1511-1 PN] ▸ Program blocks ▸ Data_block_1 [DB2]

Keep actual values
Snapshot
Copy snapshots to start values
Load start values as actual values
Monitor all

Data_block_1

	Name	Data type	Start value	Retain	Accessible f...	Writa...	Visible in ...	Setpoint	Supervis...	Comment
1	▼ Static			□	□	□	□	□		
2	Power	Byte	16#0	□	☑	☑	☑	□		
3	Duplex	Byte	16#0	□	☑	☑	☑	□		
4	Link	Byte	16#0	□	☑	☑	☑	□		
5	Rate	Byte	16#0	□	☑	☑	☑	□		
6	Activity	Byte	16#0	□	☑	☑	☑	□		
7	Lldp	Byte	16#0	□	☑	☑	☑	□		
8	<Add new>			□	□	□	□	□		

Volktek PN Switch reply INDEX=2 read request as follows



Standard_cena ▸ PLC_1 [CPU 1511-1 PN] ▸ Program blocks ▸ Data_block_1 [DB2]

Keep actual values
Snapshot
Copy snapshots to start values
Load start values as actual values

Data_block_1

	Name	Data type	Start value	Monitor value	Retain	Accessible f...	Writa...	Visible in ...	Setpoint	Supervis...	Comm
1	▼ Static				□	□	□	□	□		
2	Power	Byte	16#0	16#01	□	☑	☑	☑	□		
3	Duplex	Byte	16#0	16#00	□	☑	☑	☑	□		
4	Link	Byte	16#0	16#01	□	☑	☑	☑	□		
5	Rate	Byte	16#0	16#01	□	☑	☑	☑	□		
6	Activity	Byte	16#0	16#05	□	☑	☑	☑	□		
7	Lldp	Byte	16#0	16#03	□	☑	☑	☑	□		
8	<Add new>				□	□	□	□	□		

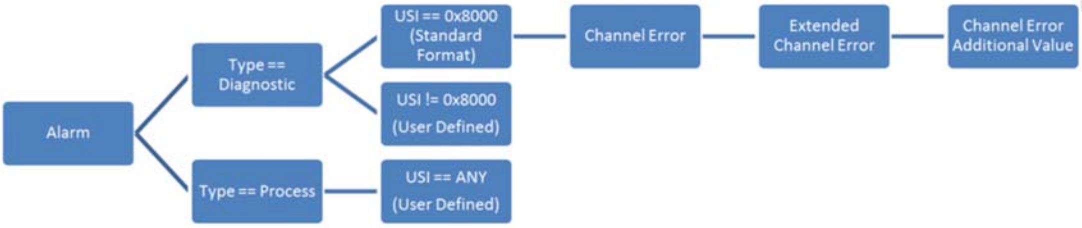
Decode data using following table, the response means
Power = 1 => Power Up
Duplex = 0 => Full Duplex
Link = 1 => Link Up
Rate = 1 => Speed 100Mb
Activity = 5 => Forwarding
LLDP = 3 => LLDP Admin tx&rx enabled

Offset	Value	Description	Default Value
0	0	Port Power Down	0
	1	Port Power Up	
1	0	Port Full Duplex Mode	0
	1	Port Half Duplex Mode	
2	0	Port Link Down	0
	1	Port Link Up	
3	0	Port Speed 10Mb	0
	1	Port Speed 100Mb	
	2	Port Speed 1Gb	
	7	Port Speed Automatic	
4	1	Port Link Activity – Disabled	5
	2	Port Link Activity – Blocked	
	3	Port Link Activity – Listen	
	4	Port Link Activity – Learn	
	5	Port Link Activity – Forward	
5	0	Port LLDP Admin Status – Disabled	0
	1	Port LLDP Admin Status – TX Only	
	2	Port LLDP Admin Status – RX Only	
	3	Port LLDP Admin Status – TX/RX	

5.10. **Diagnosis & Alarm**

Alarms are mainly PROFINET I/O transmitted high-priority events. Alarm data are exchanged between an I/O device and an I/O controller. Once any diagnosis occurs, the switch will send the “diagnosis appear” alarm to the PLC immediately. Then as the diagnosis is resolved or under control, the switch will send the “diagnosis disappear” alarm to the PLC. Besides the built-in Port MAU related diagnosis, MRP diagnosis, etc., Volktek PN switch provides following vendor-specific diagnosis. These vendor-specific diagnosis will generate a maintenance alarm delivered to PLC.
Just like Port MAU alarms, these customized alarms could be turned on/off from DAP parameters.

Alarm Types:


Alarm
Type == Diagnostic
Type == Process
USI == 0x8000 (Standard Format)
USI != 0x8000 (User Defined)
USI == ANY (User Defined)
Channel Error
Extended Channel Error
Channel Error Additional Value

All of these vendor-specific diagnosis got the same definitions of Channel No & USI

Channel No = 0x8000
User Structure Identifier (USI) = 0x8002

- PWR/RPS (Primary & Redundant Power) Under Voltage or No Power
  Channel Error Type = 2

Ext Channel Error Type	Description
1	PWR Under Voltage
2	RPS Under Voltage
3	PWR No Power
4	RPS No Power

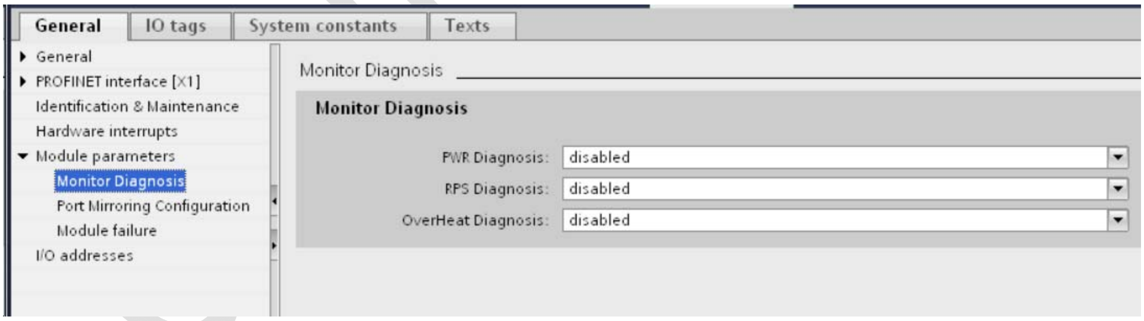
- PWR/RPS (Primary & Redundant Power) Over Voltage
  Channel Error Type = 3

Ext Channel Error Type	Description
1	PWR Over Voltage
2	RPS Over Voltage

- Main-Board/CPU/PHY Over-Heat
  Channel Error Type = 5

Ext Channel Error Type	Description
1	MainBoard Over Heat
2	CPU Over Heat
3	Ethernet PHY Over Heat

Above vendor-Specific Diagnosis could be disabled from DAP parameters



Monitor Diagnosis

PWR Diagnosis: disabled

RPS Diagnosis: disabled

OverHeat Diagnosis: disabled

6. Basic Settings

6.1. General Settings

6.1.1. System

6.1.1.1. Introduction

Management VLAN

To specify a VLAN group which can access the Switch.

- The valid VLAN range is from 1 to 4094.
- If you want to configure a management VLAN, the management VLAN should be created first and the management VLAN should have at least one member port.

Host Name

The **hostname** is same as the SNMP system name. Its length is up to 64 characters.
The first 16 characters of the hostname will be configured as the CLI prompt.

Default Settings

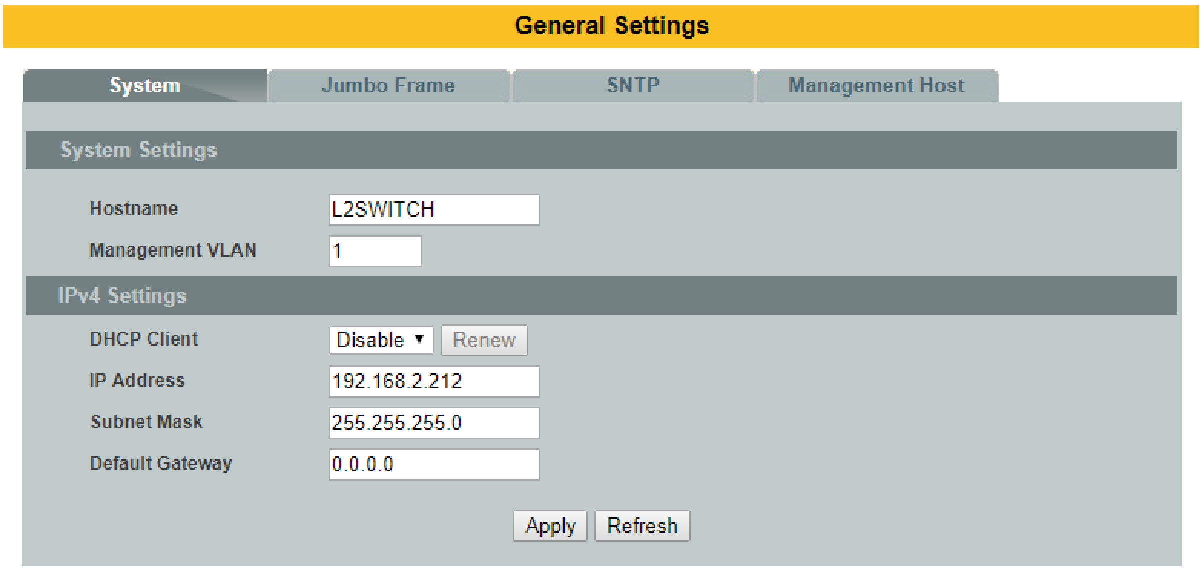
The default Hostname is L2SWITCH
The default DHCP client is disabled.
The default Static IP is 192.168.0.254
Subnet Mask is 255.255.255.0
Default Gateway is 0.0.0.0
Management VLAN is 1.

6.1.1.2. CLI Configuration

Node	Command	Description
enable	ping IPADDR [–c COUNT]	This command sends an echo request to the destination host. The –c parameter allow user to specific the packet count. The default count is 4.
enable	ping IPADDR [–s SIZE]	This command sends an echo request to the destination host. The –s parameter allow user to specific the packet size. Valid range: 0 ~ 1047 bytes.
enable	ping IPADDR [–c COUNT –s SIZE]	This command sends an echo request to the destination host. The –c parameter allow user to specific the packet count. The default count is 4. The –s parameter allow user to specific the packet size. Valid range: 0 ~ 1047 bytes.
enable	ping IPADDR [-s SIZE –c COUNT]	This command sends an echo request to the destination host. The –c parameter allow user to specific the packet count. The default count is 4. The –s parameter allow user to specific the packet size. Valid range: 0 ~ 1047 bytes.
configure	reboot	This command reboots the system.
configure	hostname STRINGS	This command sets the system's network name.
configure	interface eth0	This command enters the eth0 interface node to configure the system IP.
configure	configure terminal	This command changes the mode to config mode.

configure	interface eth0	This command changes the mode to eth0 mode.
eth0	show	This command displays the eth0 configurations.
eth0	ip addressA.B.C.D/M	This command configures a static IP and subnet mask for the system.
eth0	ip address default-gateway A.B.C.D	This command configures the system default gateway.
eth0	ip dhcp client (disable|enable|renew)	This command configures a DHCP client function for the system. Disable: Use a static IP address on the switch. Enable & Renew: Use DHCP client to get an IP address from DHCP server.
eth0	management vlan VLANID	This command configures the management vlan.
eth0	ip ipv6-addressAAAA:BBBB:CCCC:DDDD:EEEE:FFFF:GGGG:HHHH/M	This command configures a global scope of IPv6 address and subnet mask for the system.
eth0	ip ipv6-dhcp client (disable|enable|renew)	This command configures a DHCPv6 client function for the system. Disable: Use a static IP address on the switch. Enable & Renew: Use DHCPv6 client to get an IP address from DHCPv6 server.

6.1.1.3. Web Configuration



System Settings

Hostname: L2SWITCH

Management VLAN: 1

IPv4 Settings

DHCP Client: Disable ▼ Renew

IP Address: 192.168.2.212

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Parameter	Description
Hostname	Enter up to 64 alphanumeric characters for the name ofyour Switch. The hostname should be the combination of the digit or the alphabet or hyphens (-) or underscores (_).

Management VLAN	Enter a VLAN ID used for Switch management purposes.
IPv4 Settings	
DHCP Client	Select **Enable** to allow the Switch to automatically get an IP address from a DHCP server. Click **Renew** to have the Switch reget an IP address from the DHCP server. Select **Disable** if you want to configure the Switch's IP address manually.
Static IP Address	Configures a IPv4 address for your Switch in dotted decimalnotation. For example, 192.168.0.254.
Subnet Mask	Enter the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.1.
Apply	Click this buttonto take effect the settings.
Refresh	Click this button to reset the fields to the last setting.

6.1.2. Jumbo Frame

6.1.2.1. Introduction

Jumbo frames are Ethernet frames with a payload greater than 1500 bytes. Jumboframes can enhance data transmission efficiency in a network.The bigger the frame size, the better the performance.

Notice:

The jumbo frame settings will apply to all ports.
If the size of a packet exceeds the jumbo frame size, the packet will be dropped.
The available values are 1522,1536,1552, 9010, 9216,10240.

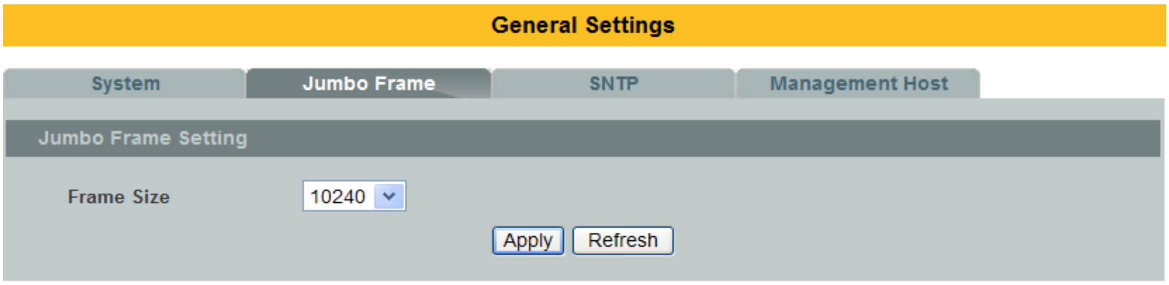
Default Settings

The default jumbo frame is 10240 bytes.

6.1.2.2. CLI Configuration

Node	Command	Description
enable	show jumboframe	This command displays the current jumbo frame settings.
configure	jumboframe(10240|1522|1536|1552|9010|9216)	This command configures the maximum number of bytes of frame size for all ports.

6.1.2.3. Web Configuration


General Settings

Jumbo Frame Setting

Frame Size: 10240

Parameter	Description
Port	This field specifies a port or a range of ports for configuration.
Frame Size	This field configures the maximum number of bytes of frame size for specified port(s).
Apply	Click this button to take effect the settings.
Refresh	Click this button to reset the fields to the last setting.

6.1.3. SNTP

6.1.3.1. Introduction

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.A less complex implementation of NTP, using the same protocol but without requiring the storage of state over extended periods of time is known as the **Simple Network Time Protocol** (**SNTP**).NTP provides Coordinated Universal Time (UTC). No information about time zones or daylight saving time is transmitted; this information is outside its scope and must be obtained separately.

UDP Port: 123.

Daylight saving is a period from late spring to early fall when many countries set theirclocks ahead of normal local time by one hour to give more daytime light in the evening.

Note:

1. The SNTP server always replies the UTC current time.
2. When the Switch receives the SNTP reply time, the Switch will adjust the time with the time zone configuration and then configure the time to the Switch.
3. If the time server's IP address is not configured, the Switch will not send any SNTP request packets.
4. If no SNTP reply packets, the Switch will retry every 10 seconds forever.
5. If the Switch has received SNTP reply, the Switch will re-get the time from NTP server every 24 hours.
6. If the time zone and time NTP server have been changed, the Switch will repeat the query process.
7. No default SNTP server.

Default Settings

```
Current Time:
---------------------------------------------
    Time: 0:3:51 (UTC)
    Date: 1970-1-1

Time Server Configuration:
---------------------------------------------
    Time Zone : +00:00
    IP Address: 0.0.0.0

DayLight Saving Time Configuration:
---------------------------------------------
    State       : disabled
    Start Date: None.
    End Date : None.
```

6.1.3.2. CLI Configuration

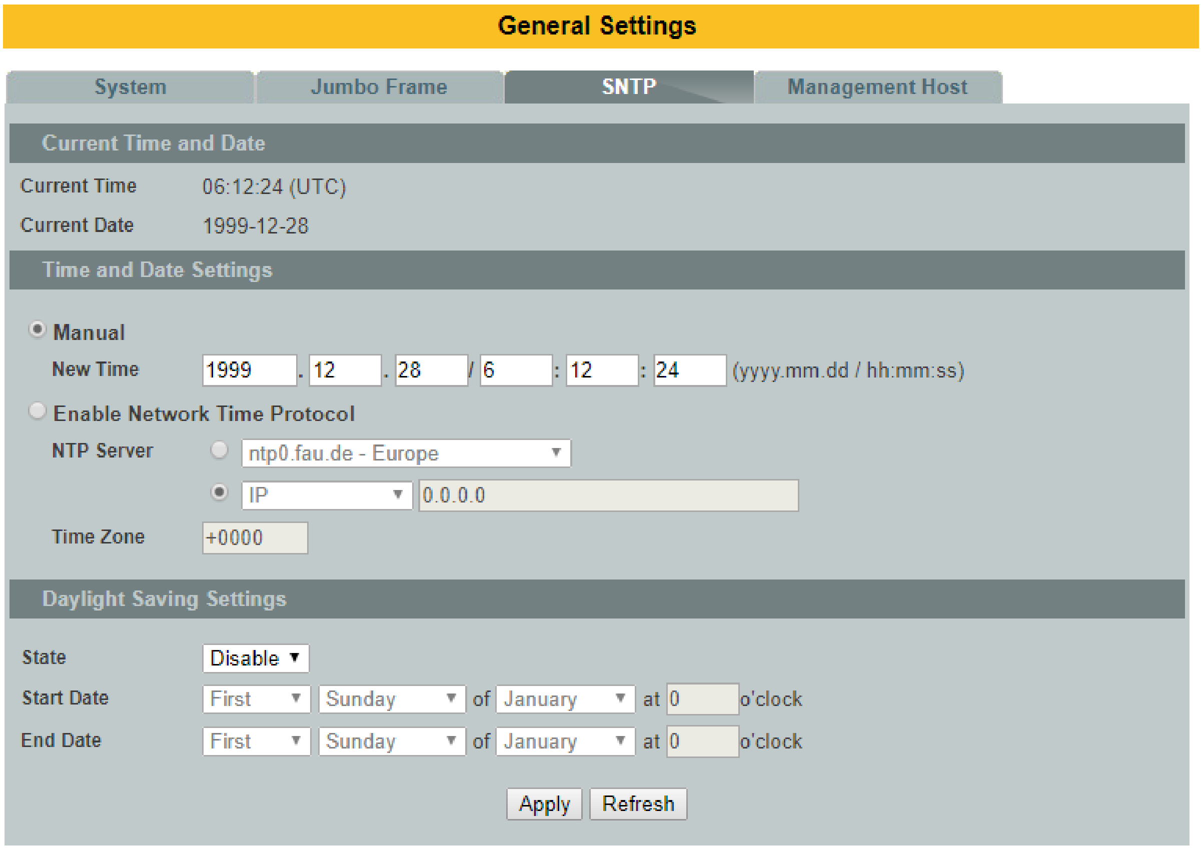
Node	Command	Description
enable	show time	This command displays current time and time configurations.
configure	time HOUR:MINUTE:SECOND	Sets the current time on the Switch. *hour*: 0-23 *min*: 0-59 *sec*: 0-59 Note: If you configure Daylight Saving Timeafter you configure the time, the Switchwill apply Daylight Saving Time.
configure	time date YEAR/MONTH/DAY	Sets the current date on the Switch. *year*: 1970- *month*: 1-12 *day*: 1-31
configure	time daylight-saving-time	This command enables the daylight saving time.
configure	time daylight-saving-time start-date(first|second|third|fourth|last)(Sunday|Monday|Tuesday|Wednesday|Thursday|Friday|Saturday) MONTH HOUR	This command sets the start time of the Daylight Saving Time.
configure	time daylight-saving-time end-date(first|second|third|fourth|last)(Sunday|Monday|Tuesday|Wednesday|Thursday|Friday|Saturday) MONTH HOUR	This command sets the end time of the Daylight Saving Time.
configure	no time daylight-saving-time	This command disables daylight saving on the Switch.
config	time ntp-server (disable|enable)	This command disables / enables the NTP server

ure		state.
configure	time ntp-server IP_ADDRESS	This command sets the IP address of your time server.
configure	time timezone STRING	Configures the time difference between UTC (formerlyknown as GMT) and your time zone. Valid Range: -1200 ~ +1200.

Example:

```
L2SWITCH(config)#time ntp-server 192.5.41.41
L2SWITCH(config)#time timezone +0800
L2SWITCH(config)#time ntp-server enable
L2SWITCH(config)#time daylight-saving-time start-datefirstMonday 6 0
L2SWITCH(config)#time daylight-saving-time end-date last Saturday 10 0
```

6.1.3.3. Web Configuration



Current Time and Date

Current Time 06:12:24 (UTC)

Current Date 1999-12-28

Time and Date Settings

● Manual

New Time 1999 . 12 . 28 / 6 : 12 : 24 (yyyy.mm.dd / hh:mm:ss)

○ Enable Network Time Protocol

NTP Server ○ ntp0.fau.de - Europe ● IP 0.0.0.0

Time Zone +0000

Daylight Saving Settings

State Disable

Start Date First Sunday of January at 0 o'clock

End Date First Sunday of January at 0 o'clock

Parameter	Description
Current Time and Date	
Current Time	This field displays the time you open / refresh this menu.
Current Date	This field displays the date you open / refresh this menu.

Time and Date Setting	
Manual	Select this option if you want to enter the system date and timemanually.
New Time	Enter the new date in year, month and day format and time in hour,minute and second format. The new date and time then appear in the**Current Date** and **Current Time** fields after you click **Apply**.
Enable Network Time Protocol	Select this option to use Network Time Protocol (NTP) for the timeservice.
NTP Server	Select a pre-designated time server or type the IP address of your timeserver. The Switch searches for the timeserver for up to 60 seconds.
Time Zone	Select the time difference between UTC (Universal Time Coordinated,formerly known as GMT, Greenwich Mean Time) and your time zone fromthe drop-down list box.
Daylight Saving Settings	
State	Select **Enable** if you want to use Daylight Saving Time. Otherwise,select **Disable** to turn it off.
Start Date	Configure the day and time when Daylight Saving Time starts if youenabled Daylight Saving Time. The time is displayed in the 24 hourformat. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on thesecond Sunday of March. Each time zone in the United States startsusing Daylight Saving Time at 2 A.M. local time. So in the United Statesyou would select **Second**, **Sunday**, **March** and **2:00**. Daylight Saving Time starts in the European Union on the last Sunday ofMarch. All of the time zones in the European Union start using DaylightSaving Time at the same moment (1 A.M. GMT or UTC). So in theEuropean Union you would select **Last**, **Sunday**, **March** and the lastfield depends on your time zone. In Germany for instance, you wouldselect **2:00** because Germany's time zone is one hour ahead of GMT orUTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if youenabled Daylight Saving Time. The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday ofOctober. Each time zone in the United States stops using Daylight SavingTime at 2 A.M. local time. So in the United States you would select **First**,**Sunday**, **November** and **2:00**. Daylight Saving Time ends in the European Union on the last Sunday ofOctober. All of the time zones in the European Union stop using DaylightSaving Time at the same moment (1 A.M. GMT or UTC). So in theEuropean Union you would select **Last**, **Sunday**, **October** and the lastfield depends on your time zone. In Germany for instance, you wouldselect **2:00** because Germany's time zone is one hour ahead of

	GMT orUTC (GMT+1).
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

6.1.4. Management Host

6.1.4.1. Introduction

The feature limits the hosts which can manage the Switch. That is, any hosts can manage the Switch via **telnet** or **web browser**. If user has configured one or more management host, the Switch can be managed by these hosts only. The feature allow user to configure management IP up to 3 entries.

Default Settings

This feature allows user to configure management host up to 3 entries.
The default is none, any host can manage the Switch via telnet or web browser.

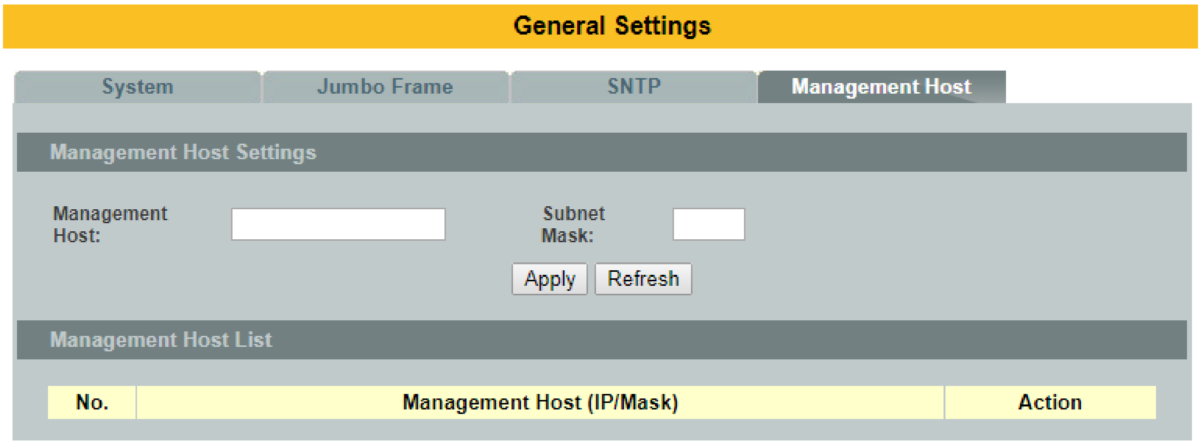
6.1.4.2. CLI Configuration

Node	Command	Description
enable	show interface eth0	The command displays the all of the interface *eth0* configurations.
eth0	show	The command displays the all of the interface *eth0* configurations.
eth0	management host A.B.C.D	The command adds a management host address.
eth0	no management host A.B.C.D	The command deletes a management host address.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#interface eth0
L2SWITCH(config-if)#management host 192.168.200.106
```

6.1.4.3. Web Configuration



Parameter	Description
Management Host	This field configures the management host.
Subnet Mask	This field you can enter the mask field, which allows all the device present in that subnet can access the switch.
Apply	Click this button to take effect the settings.
Refresh	Click this button to begin configuring this screen afresh.
Management Host List	
No.	This field displays a sequential number for each management host.
Management Host	This field displays the management host.
Action	Click the Delete buttonto remove the specified entry.

6.2. MAC Management

6.2.1. Introduction

Dynamic Address:
The MAC addresses are learnt by the switch. When the switch receives frames, it will record the source MAC, the received port and the VLAN in the address table with an age time. When the age time is expired, the address entry will be removed from the address table.

Static Address:
The MAC addresses are configured by users. The static addresses will not be aged out by the switch; it can be removed by user only. The maximum static address entry is up to 256.

The **MAC Table** (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the Switch, the MAC address of the device is shown on the Switch's MAC Table. It also shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered).

The Switch uses the **MAC Table** to determine how to forward frames. See the following figure.

1. The Switch examines the received frame and learns the port from which this source MAC address came.
2. The Switch checks to see if the frame's destination MAC address matches a source MAC address already learnt in the **MAC Table**.
   - If the Switch has already learnt the port for this MAC address, then it forwards the frame to that port.
   - If the Switch has not already learnt the port for this MAC address, then the frame is flooded to all ports. If too much port flooding, it may lead to network congestion.
   - If the Switch has already learnt the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

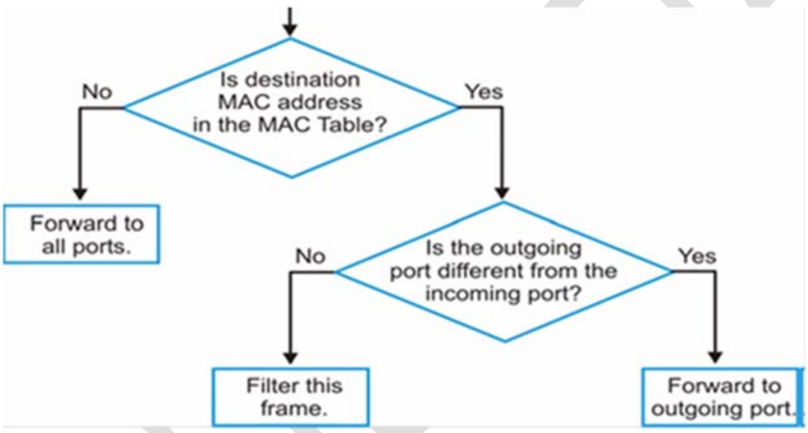

Is destination MAC address in the MAC Table?
No
Yes
Forward to all ports.
Is the outgoing port different from the incoming port?
No
Yes
Filter this frame.
Forward to outgoing port.

Figure MAC Table Flowchart

Default Settings

The default MAC address table age time is 300 seconds.

The Maximum static address entry is 256.

6.2.2. CLI Configuration

Node	Command	Description
enable	show mac-address-table aging-time	This command displays the current MAC address table age time.
enable	show mac-address-table(static|dynamic)	This command displays the current static/dynamic unicast address entries.
enable	show mac-address-table mac MACADDR	This command displays information of a specific MAC.
enable	show mac-address-table port PORT_ID	This command displays the current unicast address entries learnt by the specific port.
configure	mac-address-table static MACADDR vlan VLANID port PORT_ID	This command configures a static unicast entry.
configure	no mac-address-table static	This command removes a static unicast entry

	MACADDR vlan VLANID	from the address table.
configure	mac-address-table aging-time VALUE	This command configures the mac table aging time.
configure	clear mac address-table dynamic	This command clears the dynamic address entries.

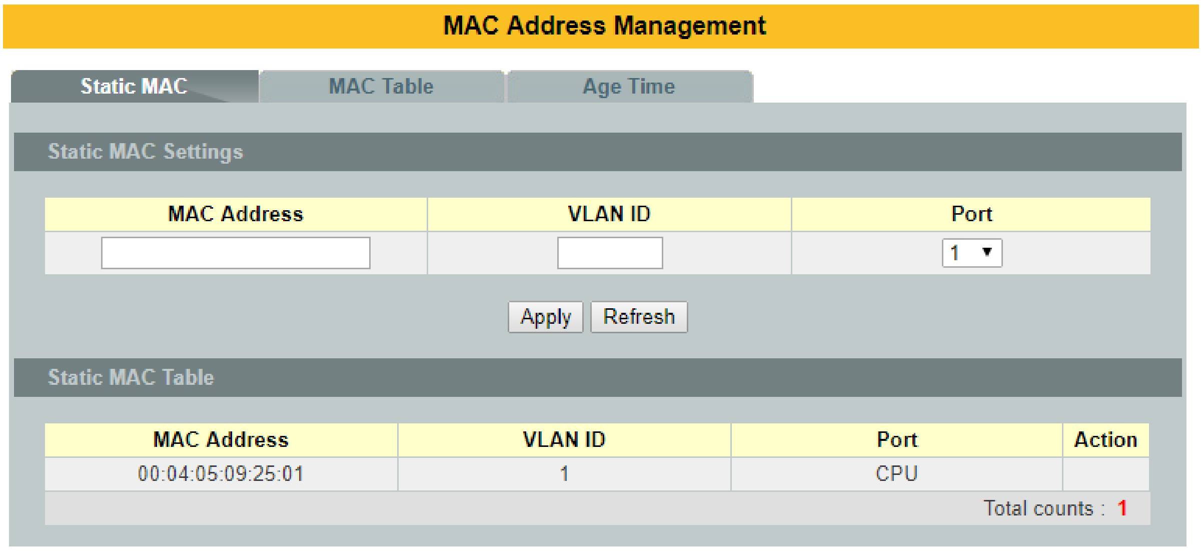
Example:

```
L2SWITCH(config)#mac-address-table static 00:11:22:33:44:55 vlan 1 port 1
```

6.2.3. Web Configuration

Static MAC

A static Media Access Control (MAC) address is an address that has been manually entered in the MAC address table, and do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port, so this may reduce the need for broadcasting.



MAC Address Management

Static MAC Settings

MAC Address	VLAN ID	Port
		1 ▼

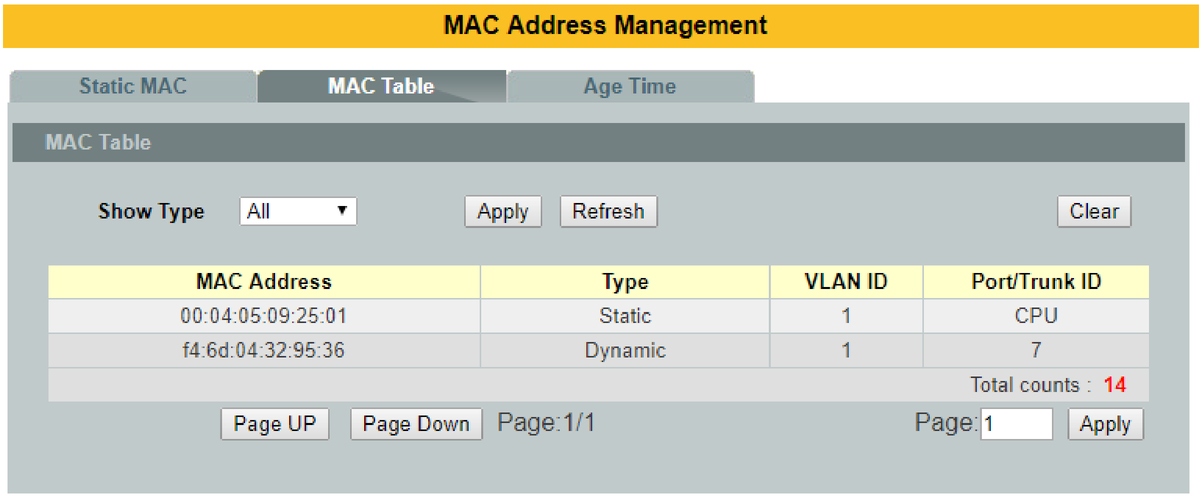
Static MAC Table

MAC Address	VLAN ID	Port	Action
00:04:05:09:25:01	1	CPU	
		Total counts : 1	

Parameter	Description
Static MAC Settings	
MAC Address	Enter the MAC address of a computer or device that you want to add to theMAC address table. Valid format is hh:hh:hh:hh:hh:hh.
VLAN ID	Enter the VLAN ID to apply to the computer or device.
Port	Enter the port number to which the computer or device is connected.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

Static MAC Table	
MAC Address	This field displays the MAC address of a manually entered MAC address entry.
VLAN ID	This field displays the VID of a manually entered MAC address entry.
Port	This field displays the port number of a manually entered MAC address entry. The MAC address with port CPU means the Switch's MAC addresses itself.
Action	Click **Delete** to remove this manually entered MAC address entry from the MAC address table. You cannot delete the Switch's MAC address from the static MAC address table.

MAC Table



Show Type: All

MAC Address	Type	VLAN ID	Port/Trunk ID
00:04:05:09:25:01	Static	1	CPU
f4:6d:04:32:95:36	Dynamic	1	7

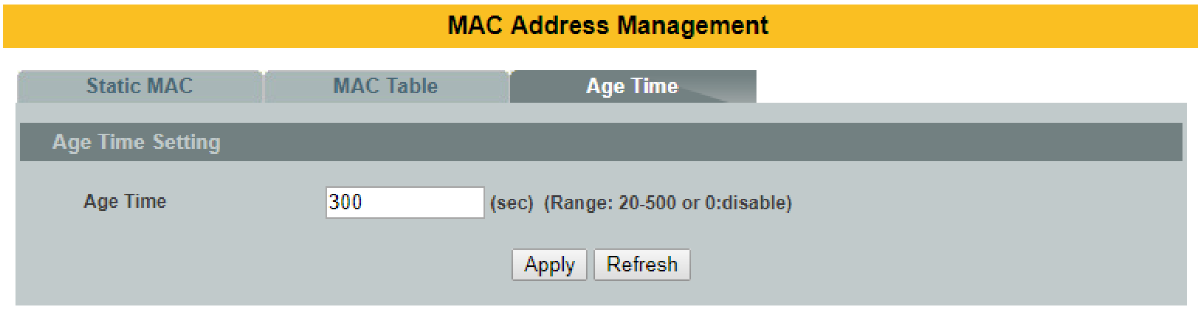
Total counts : 14

Page:1/1

Page: 1

Parameter	Description
Show Type Apply	Select **All, Static**, **Dynamic or Port** and then click **Apply** to display the corresponding MAC address entries on this screen.
Refresh	Click this to update the information in the MAC table.
Clear	It will clear all the Dynamic MAC address learnt.
MAC Address	This field displays a MAC address.
Type	This field displays whether this entry was entered manually (Static) or whether it was learned by the Switch (Dynamic).
VLAN ID	This field displays the VLAN ID of the MAC address entry.
Port Total Counts	This field displays the port number the MAC address entry is associated. It displays CPU if it is the entry for the Switch itself. The CPU means that it is the Switch's MAC. This field displays the total entries in the MAC table.

Age Time Settings



Age Time Setting

Age Time 300 (sec) (Range: 20-500 or 0:disable)

Parameter	Description
Age Time	Configure the age time; the valid range is from 20 to 500 seconds. The default value is 300 seconds.
Apply	Click Apply to take effect the settings.
Refresh	Click this to update the information in the MAC table.

6.3. Port Mirror

6.3.1. Introduction

Port-based Mirroring

The Port-Based Mirroring is used on a network switch to send a copy of network packets sent/received on one or a range of switch ports to a network monitoring connection on another switch port (**Monitor to Port**). This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system.

Port Mirroring, together with a network traffic analyzer, helps to monitor network traffic. Users can monitor the selected ports (**Source Ports**) for egress and/or ingress packets.

Source Mode:

Ingress	: The received packets will be copied to the monitor port.
Egress	: The transmitted packets will be copied to the monitor port.
Both	: The received and transmitted packets will be copied to the monitor port.

Note:

1. The monitor port cannot be a trunk member port.
2. The monitor port cannot be ingress or egress port.
3. If the Port Mirror function is enabled, the Monitor-to Port can receive mirrored packets only.
4. If a port has been configured as a source port and then user configures the port as a destination port, the port will be removed from the source ports automatically.

Default Settings

Mirror Configurations:

State : Disable

```
Monitor port        : 1
Ingress port(s)     : None
Egress port(s)      : None
```

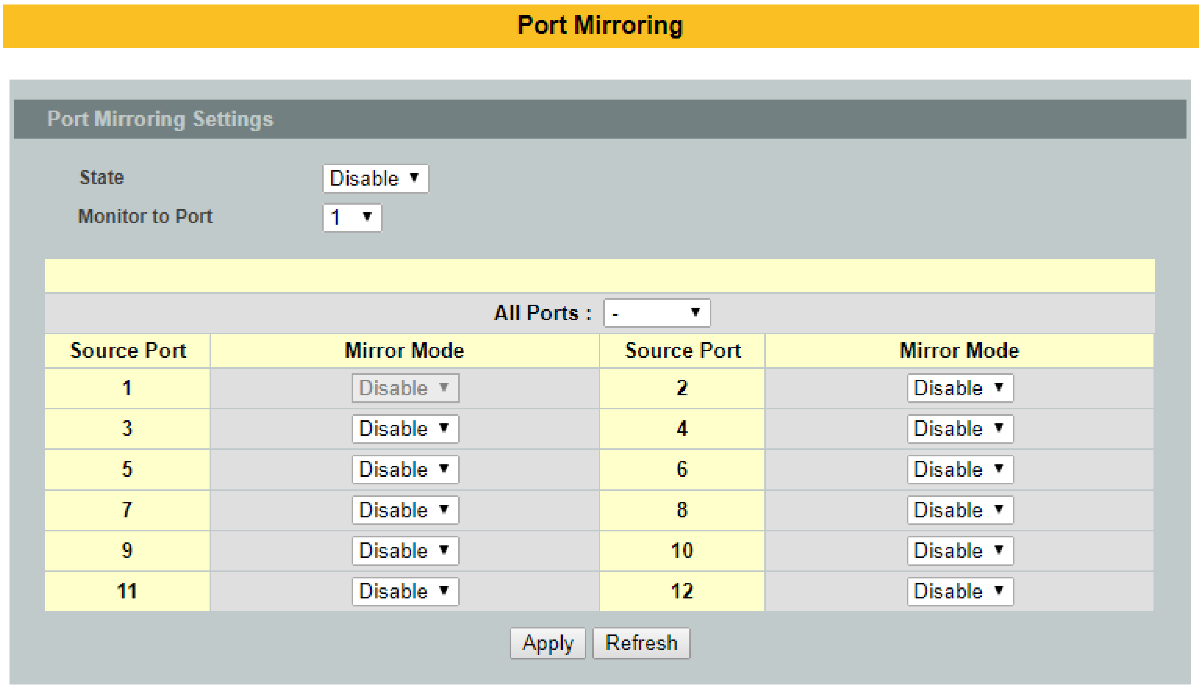
6.3.2. CLI Configuration

Node	Command	Description
enable	show mirror	This command displays the current port mirroring configurations.
configure	mirror (disable|enable)	This command disables / enables the port mirroring on the switch.
configure	mirror destination port PORT_ID	This command specifies the **monitor port** for the port mirroring.
configure	mirror source ports PORT_LIST mode *(both|ingress|egress)*	This command **adds** a port or a range of ports as the source ports of the port mirroring.
configure	no mirror source ports PORT_LIST	This command **removes** a port or a range of ports from the source ports of the port mirroring.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#mirror enable
L2SWITCH(config)#mirror destination port 2
L2SWITCH(config)#mirror source ports 3-11 mode both
```

6.3.3. Web Configuration



Port Mirroring

Port Mirroring Settings

State: Disable

Monitor to Port: 1

All Ports : -

Source Port	Mirror Mode	Source Port	Mirror Mode
1	Disable	2	Disable
3	Disable	4	Disable
5	Disable	6	Disable
7	Disable	8	Disable
9	Disable	10	Disable
11	Disable	12	Disable

Parameter	Description

State	Select **Enable** to turn on port mirroring or select **Disable** to turn it off.
Monitor to Port	Select the port which connects to a network traffic analyzer.
All Ports	Settings in this field apply to all ports. Use this field only if you want to make some settings the same for all ports. Use this field first to set the common settings and then make adjustments on a port-by-port basis.
Source Port	This field displays the number of a port.
Mirror Mode	Select **Ingress**, **Egress** or **Both** to only copy the ingress (incoming), egress (outgoing) or both (incoming and outgoing) traffic from the specified source ports to the monitor port. Select **Disable** to not copy any traffic from the specified source ports to the monitor port.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

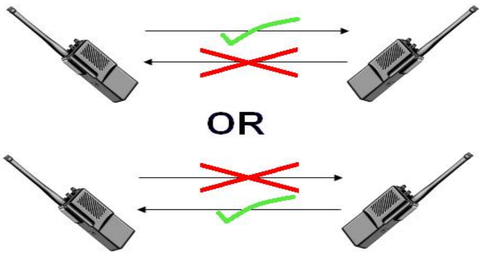
6.4. Port Settings

6.4.1. Introduction

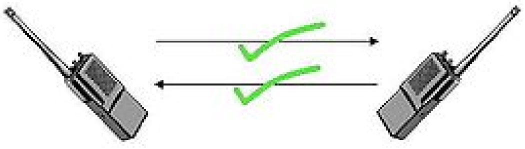
- Duplex mode

A *duplex* communication system is a system composed of two connected parties or devices that can communicate with one another in both directions.

Half Duplex:
A *half-duplex* system provides for communication in both directions, but only one direction at a time (not simultaneously). Typically, once a party begins receiving a signal, it must wait for the transmitter to stop transmitting, before replying.



Full Duplex:
A *full-duplex*, or sometimes *double-duplex* system, allows communication in both directions, and, unlike half-duplex, allows this to happen simultaneously. Land-line telephone networks are full-duplex, since they allow both callers to speak and be heard at the same time.



- Loopback Test

A loopback test is a test in which a signal in sent from a communications device and returned (looped back) to it as a way to determine whether the device is working right or as a way to pin down a failing node in a network. One type of loopback test is performed using a special plug, called a **wrap plug** that is inserted in a port on a communications device. The effect of a wrap plug is to cause transmitted (output) data to be returned as received (input) data, simulating a complete communications circuit using a single computer.

- Auto MDI-MDIX

Auto-MDIX (automatic medium-dependent interface crossover) is a computer networking technology that automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately, thereby removing the need for crossover cables to interconnect switches or connecting PCs peer-to-peer. When it is enabled, either type of cable can be used or the interface automatically corrects any incorrect cabling. For Auto-MDIX to operate correctly, the speed on the interface and duplex setting must be set to "auto". Auto-MDIX was developed by HP engineers Dan Dove and Bruce Melvin.

- Auto Negotiation

Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode.

If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using **half-duplex** mode. When the Switch’s auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.

- Flow Control

A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses.IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill and resend later.

The Switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.

Note: 1000 Base-T doesn’t support force mode.

- Cable Test.

This feature determines the quality of the cables, shorts, and cable impedance mismatch, bad connectors, termination mismatch, and bad magnetics. The feature can work on the copper Ethernet cable only.

Default Settings

The default port Speed & Duplex is auto for all ports.
The default port Flow Control is Off for all ports.

6.4.2. CLI Configuration

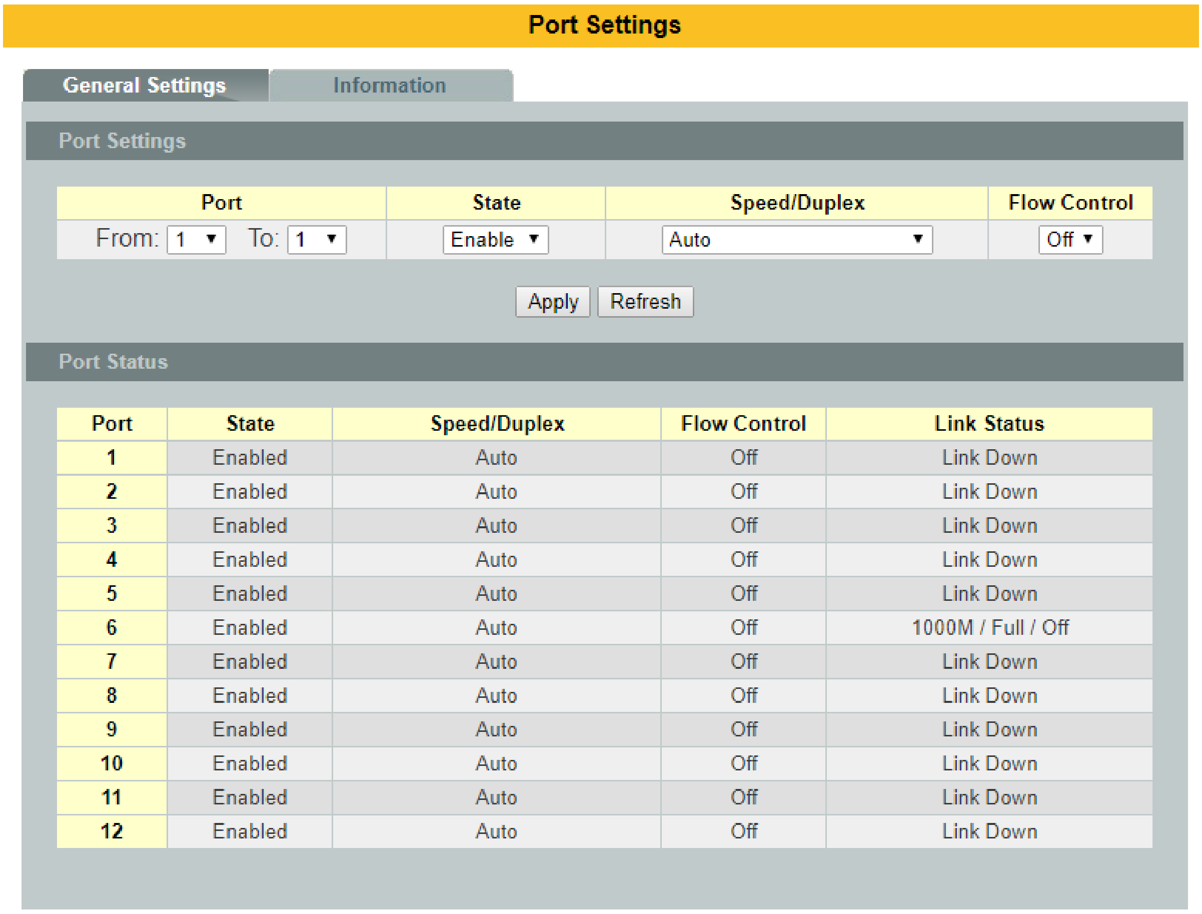
Node	Command	Description
enable	show interface IFNAME	This command displays the current port configurations.
configure	interface IFNAME	This command enters the interface configure node.
interface	show	This command displays the current port configurations.
interface	loopback (none| mac)	This command tests the loopback mode of operation for the specific port.
interface	flowcontrol (off | on)	This command disables / enables the flow control for the port.
interface	speed (auto|10-full||10-half| 100-full|100-half|1000-full)	This command configures the speed and duplex for the port.
interface	shutdown	This command disables the specific port.
interface	no shutdown	This command enables the specific port.
interface	description STRINGs	This command configures a description for the specific port.
interface	no description	This command configures the default port description.
interface	cable-test start	This command starts to diagnostics the Ethernet cable.
interface	show cable-test result	This command displays the test result of the Ethernet cable test.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	description STRINGs	This command configures a description for the specific ports.
if-range	no description	This command configures the default port description for the specific ports.
if-range	shutdown	This command disables the specific ports.
if-range	no shutdown	This command enables the specific ports.
if-range	speed (auto|10-full||10-half| 100-full|100-half|1000-full)	This command configures the speed and duplex for the port.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#interface gi1/0/1
```

L2SWITCH(config-if)#*speed auto*

6.4.3. Web Configuration



Port Settings

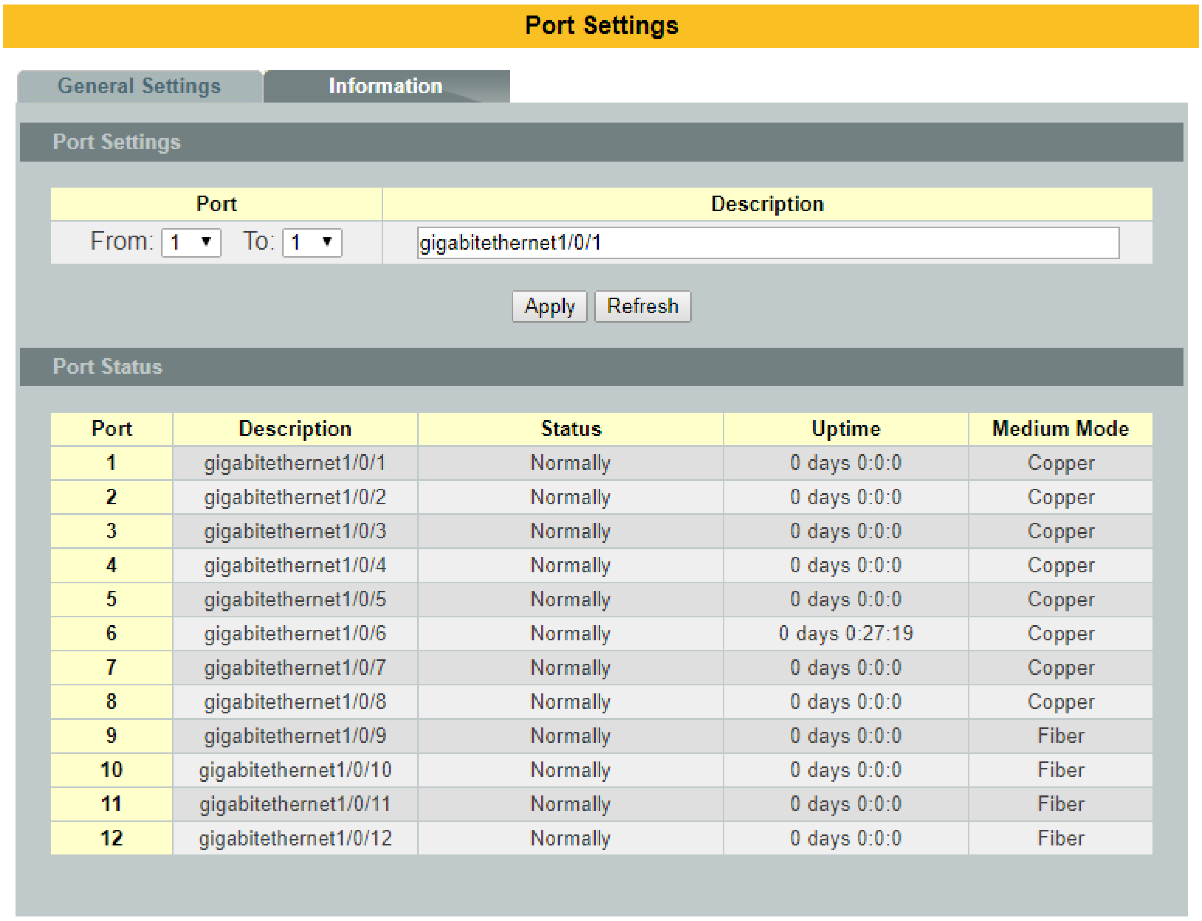
Port	State	Speed/Duplex	Flow Control
From: 1 ▾ To: 1 ▾	Enable ▾	Auto ▾	Off ▾

Port	State	Speed/Duplex	Flow Control	Link Status
1	Enabled	Auto	Off	Link Down
2	Enabled	Auto	Off	Link Down
3	Enabled	Auto	Off	Link Down
4	Enabled	Auto	Off	Link Down
5	Enabled	Auto	Off	Link Down
6	Enabled	Auto	Off	1000M / Full / Off
7	Enabled	Auto	Off	Link Down
8	Enabled	Auto	Off	Link Down
9	Enabled	Auto	Off	Link Down
10	Enabled	Auto	Off	Link Down
11	Enabled	Auto	Off	Link Down
12	Enabled	Auto	Off	Link Down

Parameter	Description
Port	Select a port or a range ports you want to configure on this screen.
State	Select **Enable** to activate the port or **Disable** to deactivate the port.
Speed/Duplex	Select the speed and duplex mode of the port. The choices are: • **Auto** • **10 Mbps / Full Duplex** • **10 Mbps / Half Duplex** • **100 Mbps / Full Duplex** • **100 Mbps / Half Duplex** • **1000 Mbps / Full Duplex**
Flow Control	Select **On** to enable access to buffering resources for the port thus ensuring lossless operation across network switches. Otherwise, select **Off** to disable it.
Apply	Click Apply to take effect the settings.

Refresh	Click Refresh to begin configuring this screen afresh.
Port	This field displays the port number.
State	This field displays whether the port is enabled or disabled.
Speed/Duplex	This field displays the speed either **10M**, **100M**or **1000M**and the duplex mode **Full** or **Half**.
Flow Control	This field displays whether the port's flow control is **On** or **Off**.
Link Status	This field displays the link status of the port. If the port is up, it displays the port's speed, duplex and flow control setting. Otherwise, it displays **Link Down** if the port is disabled or not connected to any device.

Information:



Port	Description
From: 1 ▼ To: 1 ▼	gigabitethernet1/0/1

Port	Description	Status	Uptime	Medium Mode
1	gigabitethernet1/0/1	Normally	0 days 0:0:0	Copper
2	gigabitethernet1/0/2	Normally	0 days 0:0:0	Copper
3	gigabitethernet1/0/3	Normally	0 days 0:0:0	Copper
4	gigabitethernet1/0/4	Normally	0 days 0:0:0	Copper
5	gigabitethernet1/0/5	Normally	0 days 0:0:0	Copper
6	gigabitethernet1/0/6	Normally	0 days 0:27:19	Copper
7	gigabitethernet1/0/7	Normally	0 days 0:0:0	Copper
8	gigabitethernet1/0/8	Normally	0 days 0:0:0	Copper
9	gigabitethernet1/0/9	Normally	0 days 0:0:0	Fiber
10	gigabitethernet1/0/10	Normally	0 days 0:0:0	Fiber
11	gigabitethernet1/0/11	Normally	0 days 0:0:0	Fiber
12	gigabitethernet1/0/12	Normally	0 days 0:0:0	Fiber

Parameter	**Description**
Port	Select a port or a range ports you want to configure on this screen.
Description	Configures a meaningful name for the port(s).
Port Status	

Port	This field displays the port number.
Description	The meaningful name for the port.
Status	The field displays the detail port status if the port is blocked by some protocol.
Uptime	The sustained time from last link up.
Medium Mode	The current working medium mode, copper or fiber, for the port.

7. Advanced Settings

7.1. Bandwidth Control

7.1.1. QoS

7.1.1.1. Introduction

Each egress port can support up to 8 transmit queues. Each egress transmit queue contains a list specifying the packet transmission order. Every incoming frame is forwarded to one of the 8 egress transmit queues of the assigned egress port, based on its priority. The egress port transmits packets from each of the 8 transmit queues according to a configurable scheduling algorithm, which can be a combination of Strict Priority (SP) and/or Weighted Round Robin (WRR).

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When you configure the QoS feature, you can select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to give preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

The Switch supports 802.1p priority queuing. The Switch has 8 priority queues. These priority queues are numbered from 7 (Class 7) — the highest priority queue — to 0 (Class 0) — the lowest priority queue.
The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority queues as follows:

Priority	: 0	1	2	3	4	5	6	7
Queue	: 2	0	1	3	4	5	6	7

Priority scheduling is implemented by the priority queues stated above. The Switch will empty the four hardware priority queues in order, beginning with the highest priority queue, 7, to the lowest priority queue, 0. Each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue will begin transmitting any packets it may have received.

QoS Enhancement
You can configure the Switch to prioritize traffic even if the incoming packets are not marked with IEEE 802.1p priority tags or change the existing priority tags based on the criteria you select. The Switch allows you to choose one of the following methods for assigning priority to incoming packets on the Switch:

- **802.1p Tag Priority** - Assign priority to packets based on the packet's 802.1p tagged priority.
- **Port Based QoS** - Assign priority to packets based on the incoming port on the

Switch.

- **DSCP Based QoS** - Assign priority to packets based on their Differentiated Services Code Points (DSCPs).

Note: Advanced QoS methods only affect the internal priority queue mapping for the Switch. The Switch does not modify the IEEE 802.1p value for the egress frames. You can choose one of these ways to alter the way incoming packets are prioritized or you can choose not to use any QoS enhancement setting on the Switch.

802.1p Priority

When using 802.1p priority mechanism, the packet is examined for the presence of a valid 802.1p priority tag. If the tag is present, the packet is assigned to a programmable egress queue based on the value of the tagged priority. The tagged priority can be designated to any of the available queues.

Ethernet Packet:

6	6	2	42-1496	4
DA	SA	Type / Length	Data	FCS

6	6	4	2	42-1496	4
DA	SA	802.1Q Tag	Type / Length	Data	FCS

802.1Q Tag:

2 bytes	2 bytes		
Tag Protocol Identifier (TPID)	Tag Control Information (TCI)		
16 bits	3 bits	1 bit	12 bits
TPID (0x8100)	Priority	CFI	VID

- Tag Protocol Identifier (TPID): a 16-bit field set to a value of **0x8100** in order to identify the frame as an IEEE 802.1Q-tagged frame.
- Tag Control Information (TCI)
  - Priority Code Point (PCP): a 3-bit field which refers to the IEEE 802.1p priority. It indicates the frame priority level from **0 (lowest) to 7 (highest)**, which can be used to prioritize different classes of traffic (voice, video, data, etc.).
  - Canonical Format Indicator (CFI): a 1-bit field. If the value of this field is 1, the MAC address is in non-canonical format. If the value is 0, the MAC address is in canonical format. It is always set to zero for Ethernet switches. CFI is used for compatibility between Ethernet and Token Ring networks. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be bridged to an untagged port.
  - VLAN Identifier (VID): a 12-bit field specifying the VLAN to which the frame belongs. A value of 0 means that the frame doesn't belong to any VLAN; in this case the 802.1Q tag specifies only a priority and is referred to as a **priority tag.** A value of hex 0xFFF is reserved for implementation use. All other values may be used as VLAN identifiers, allowing up to 4094 VLANs. On bridges, VLAN 1 is often reserved for management.

Priority Levels

PCP: Priority Code Point.

PCP	Network Priority	Traffic Characteristics
1	0 (lowest)	Background
0	1	Best Effort
2	2	Excellent Effort
3	3	Critical Applications
4	4	Video, <100ms latency
5	5	Video, < 10ms latency
6	6	Internetwork Control
7	7 (highest)	Network Control

DiffServ (DSCP)

Differentiated Services or **DiffServ** is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying, managing network traffic and providing Quality of Service (**QoS**) guarantees on modern IP networks. DiffServ can, for example, be used to provide low-latency, guaranteed service (**GS**) to critical network traffic such as voice or video while providing simple best-effort traffic guarantees to non-critical services such as web traffic or file transfers.

Differentiated Services Code Point (**DSCP**) is a 6-bit field in the header of IP packets for packet classification purposes. DSCP replaces the outdated IP precedence, a 3-bit field in the Type of Service byte of the IP header originally used to classify and prioritize types of traffic.

When using the DiffServ priority mechanism, the packet is classified based on the DSCP field in the IP header. If the tag is present, the packet is assigned to a programmable egress queue based on the value of the tagged priority. The tagged priority can be designated to any of the available queues.

<table>
<tr><td>Version</td><td>IHL</td><td><b>Type of Service</b></td><td colspan="3">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td colspan="2">Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="3">Header Checksum</td></tr>
<tr><td colspan="6">Source Address</td></tr>
<tr><td colspan="6">Destination Address</td></tr>
<tr><td colspan="5">Options</td><td>Padding</td></tr>
</table>

Example Internet Datagram Header

IP Header Type of Service: 8 bits

The Type of Service provides an indication of the abstract parameters of the quality of service desired. These parameters are to be used to guide the selection of the actual service parameters when transmitting a datagram through a particular network. Several networks offer service precedence, which somehow treats high precedence traffic as more important than other traffic (generally by accepting only traffic above certain precedence at time of high load). The major choice is a three way tradeoff between low-delay, high-reliability, and high-throughput.

Bits 0-2: Precedence.
Bit 3: 0 = Normal Delay, 1 = Low Delay.

Bits 4:	0 = Normal Throughput,	1 = High Throughput.
Bits 5:	0 = Normal Reliability,	1 = High Reliability.
Bit 6-7:	Reserved for Future Use.	

```
   0     1     2     3     4     5     6     7
+-----+-----+-----+-----+-----+-----+-----+-----+
|   PRECEDENCE    |  D  |  T  |  R  |  0  |  0  |
+-----+-----+-----+-----+-----+-----+-----+-----+
```

Precedence

111 - Network Control
110 - Internetwork Control
101 - CRITIC/ECP
100 - Flash Override
011 - Flash
010 - Immediate
001 - Priority
000 - Routine

The use of the Delay, Throughput, and Reliability indications may increase the cost (in some sense) of the service. In many networks better performance for one of these parameters is coupled with worse performance on another. Except for very unusual cases at most two of these three indications should be set.

The type of service is used to specify the treatment of the datagram during its transmission through the internet system. Example mappings of the internet type of service to the actual service provided on networks such as AUTODIN II, ARPANET, SATNET, and PRNET is given in "Service Mappings".

The Network Control precedence designation is intended to be used within a network only. The actual use and control of that designation is up to each network. The Internetwork Control designation is intended for use by gateway control originators only.

If the actual use of these precedence designations is of concern to a particular network, it is the responsibility of that network to control the access to, and use of, those precedence designations.

DSCP	Priority	DSCP	Priority	DSCP	Priority
0	0	1	0	2	0
. . .					
60	0	61	0	62	0
63	0				

Example:

IP Header

DSCP=50 ➔45 **C8** . . .

Queuing Algorithms

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

- **Strict-Priority (SPQ)**
  The packets on the high priority queue are always service firstly.

- **Weighted round robin (WRR)**
  Round Robin scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

  Weighted Round Robin (WRR) scheduling uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the queue **Weight** field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

Default Settings

QoS mode : High First (SPQ)

The mappings of the Priority to Queue are:

PRIO 0 ==> COSQ 1
PRIO 1 ==> COSQ 0
PRIO 2 ==> COSQ 2
PRIO 3 ==> COSQ 3
PRIO 4 ==> COSQ 4
PRIO 5 ==> COSQ 5
PRIO 6 ==> COSQ 6
PRIO 7 ==> COSQ 7

The DiffServ is disabled on the switch.

DSCP	Priority	DSCP	Priority	DSCP	Priority	DSCP	Priority
----	--------	----	--------	----	--------	----	--------
00	0	01	0	02	0	03	0
04	0	05	0	06	0	07	0
08	0	09	0	10	0	11	0
12	0	13	0	14	0	15	0
16	0	17	0	18	0	19	0
20	0	21	0	22	0	23	0
24	0	25	0	26	0	27	0
28	0	29	0	30	0	31	0

32	0	33	0	34	0	35	0
36	0	37	0	38	0	39	0
40	0	41	0	42	0	43	0
44	0	45	0	46	0	47	0
48	0	49	0	50	0	51	0
52	0	53	0	54	0	55	0
56	0	57	0	58	0	59	0
60	0	61	0	62	0	63	0

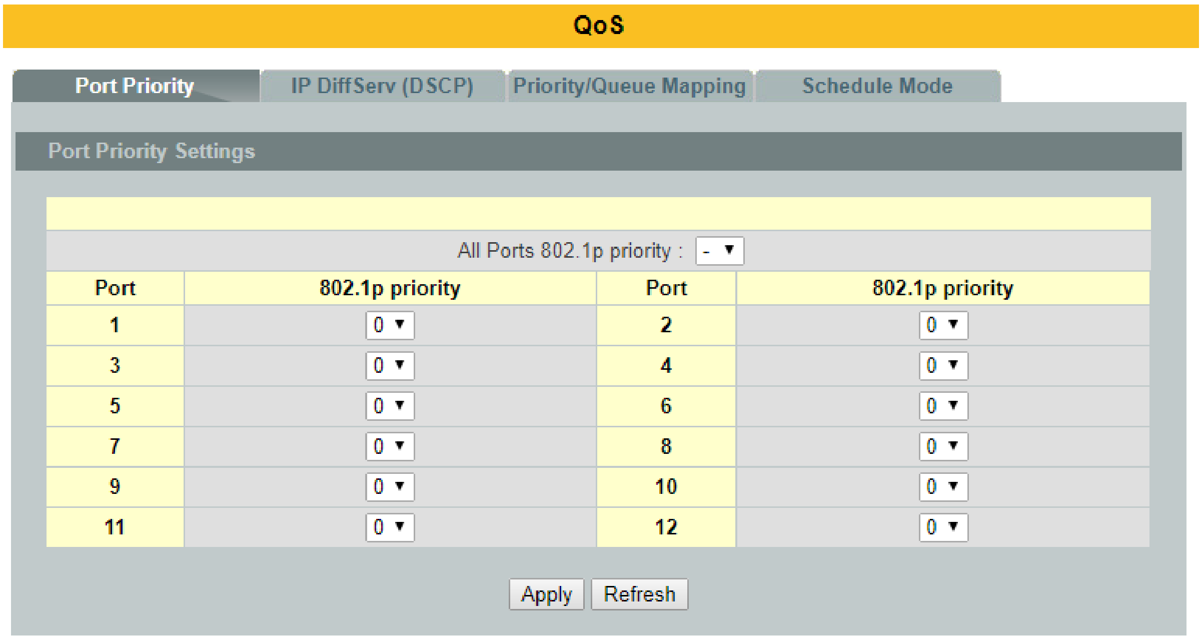
Note: If the DiffServ is disabled, the 802.1p tag priority will be used.

7.1.1.2. CLI Configuration

Node	Command	Description
enable	show queue cos-map	This command displays the current 802.1p priority mapping to the service queue.
enable	show qos mode	This command displays the current QoS scheduling mode of IEEE 802.1p.
configure	queue cos-map PRIORITYQUEUE_ID	This command configures the 802.1p priority mapping to the service queue.
configure	no queue cos-map	This command configures the 802.1p priority mapping to the service queue to default.
configure	qos mode high-first	This command configures the QoS scheduling mode to high_first, each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets.
configure	qos mode wrr-queue weights VALUE VALUE VALUE VALUE VALUE VALUE VALUE VALUE	This command configures the QoS scheduling mode to Weighted Round Robin.
interface	default-priority	This command allows the user to specify a default priority handling of untagged packets received by the Switch. The priority value entered with this command will be used to determine which of the hardware priority queues the packet is forwarded to. Default: 0.
interface	no default-priority	This command configures the default priority for the specific port to default (0).
enable	show diffserv	This command displays DiffServ configurations.
configure	diffserv (disable|enable)	This command disables / enables the DiffServ function.
configure	diffserv dscp VALUE priority VALUE	This command sets the DSCP-to-IEEE 802.1q mappings.

7.1.1.3. Web Configuration

Port Priority

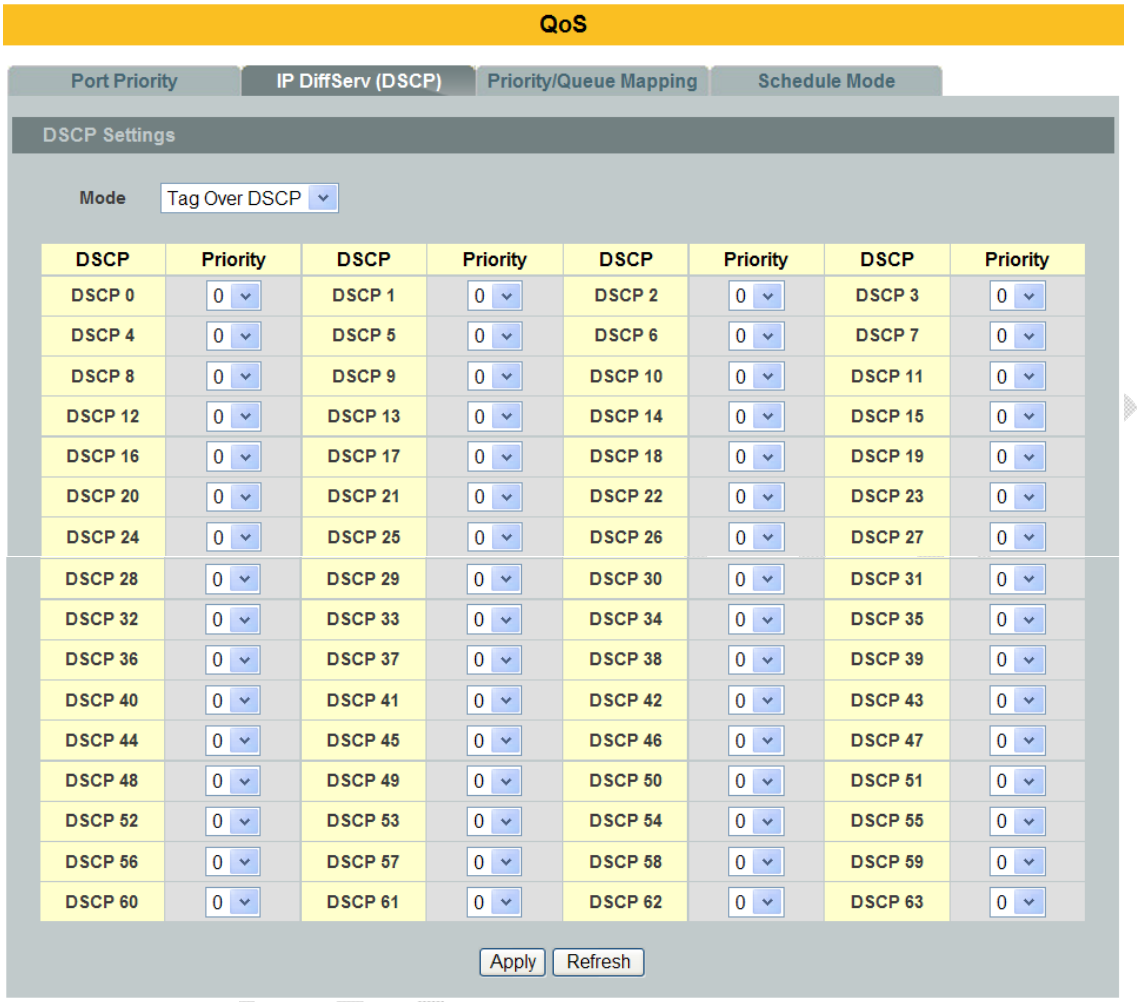


All Ports 802.1p priority : -

Port	802.1p priority	Port	802.1p priority
1	0	2	0
3	0	4	0
5	0	6	0
7	0	8	0
9	0	10	0
11	0	12	0

Parameter	Description
All Ports 802.1p priority	Use this field to set a priority for all ports. The value indicates packet priority and is added to the priority tag field of incoming packets. The values range from 0 (lowest priority) to 7 (highest priority).
Port	This field displays the number of a port.
802.1p Priority	Select a priority for packets received by the port. Only packets without802.1p priority tagged will be applied the priority you set here.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

IP DiffServ (DSCP)

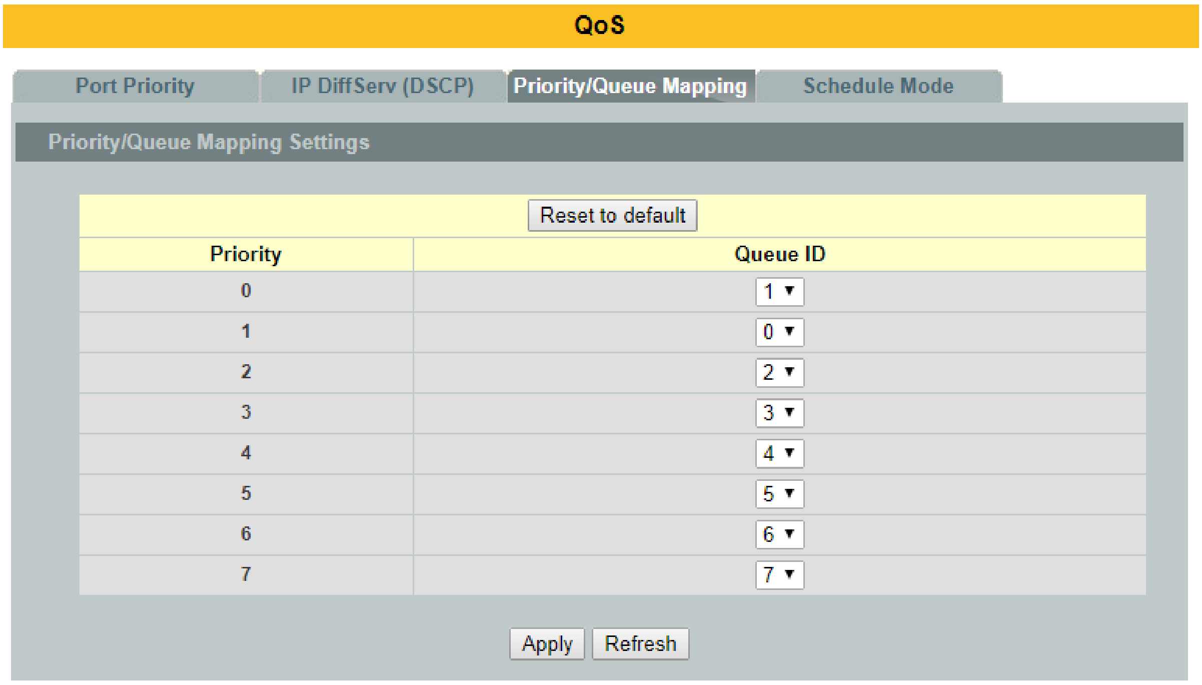


Mode: Tag Over DSCP

DSCP	Priority	DSCP	Priority	DSCP	Priority	DSCP	Priority
DSCP 0	0	DSCP 1	0	DSCP 2	0	DSCP 3	0
DSCP 4	0	DSCP 5	0	DSCP 6	0	DSCP 7	0
DSCP 8	0	DSCP 9	0	DSCP 10	0	DSCP 11	0
DSCP 12	0	DSCP 13	0	DSCP 14	0	DSCP 15	0
DSCP 16	0	DSCP 17	0	DSCP 18	0	DSCP 19	0
DSCP 20	0	DSCP 21	0	DSCP 22	0	DSCP 23	0
DSCP 24	0	DSCP 25	0	DSCP 26	0	DSCP 27	0
DSCP 28	0	DSCP 29	0	DSCP 30	0	DSCP 31	0
DSCP 32	0	DSCP 33	0	DSCP 34	0	DSCP 35	0
DSCP 36	0	DSCP 37	0	DSCP 38	0	DSCP 39	0
DSCP 40	0	DSCP 41	0	DSCP 42	0	DSCP 43	0
DSCP 44	0	DSCP 45	0	DSCP 46	0	DSCP 47	0
DSCP 48	0	DSCP 49	0	DSCP 50	0	DSCP 51	0
DSCP 52	0	DSCP 53	0	DSCP 54	0	DSCP 55	0
DSCP 56	0	DSCP 57	0	DSCP 58	0	DSCP 59	0
DSCP 60	0	DSCP 61	0	DSCP 62	0	DSCP 63	0

Parameter	Description
Mode	"Tag Over DSCP" or "DSCP Over Tag". "Tag Over DSCP" means the 802.1p tag has higher priority than DSCP.
Priority	This field displays each priority level. The values range from 0 (lowest priority) to 7 (highest priority).
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

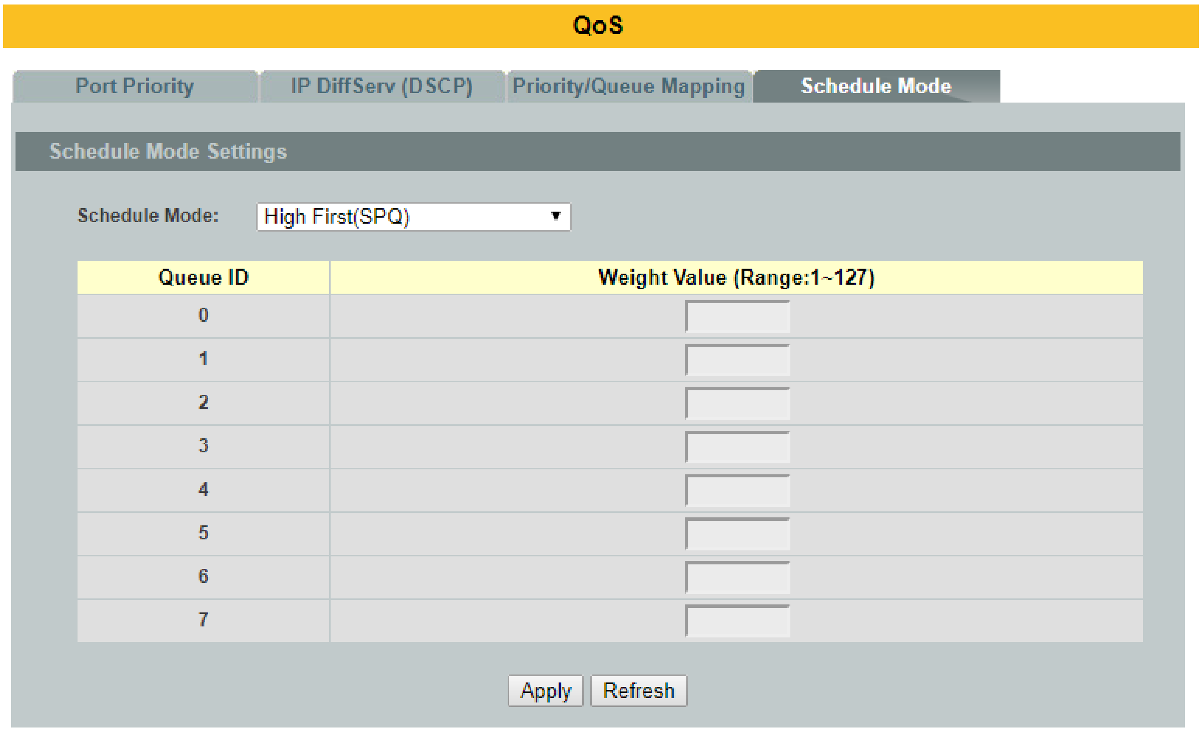
Priority/Queue Mapping



Priority	Queue ID
0	1
1	0
2	2
3	3
4	4
5	5
6	6
7	7

Parameter	Description
Reset to Default	Click this button to reset the priority to queue mappings to the defaults.
Priority	This field displays each priority level. The values range from 0 (lowest priority) to 7 (highest priority).
Queue ID	Select the number of a queue for packets with the priority level.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

Schedule Mode



Schedule Mode Settings

Schedule Mode: High First(SPQ)

Queue ID	Weight Value (Range:1~127)
0	
1	
2	
3	
4	
5	
6	
7	

Parameter	Description
Schedule Mode	Select **Strict Priority** (SP) or **Weighted Round Robin** (**WRR**). Note: Queue weights can only be changed when **Weighted Round Robin** is selected. **Weighted Round Robin** scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue **Weight** field). Queues with larger weights get more service than queues with smaller weights.
Queue ID	This field indicates which Queue (0 to 7) you are configuring. Queue 0 has the lowest priority and Queue 7 the highest priority.
Weight Value	You can only configure the queue weights when **Weighted Round Robin** is selected. Bandwidth is divided across the different traffic queues according to their weights.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

7.1.2. Rate Limitation

7.1.2.1. Storm Control

7.1.2.1.1. Introduction

A broadcast storm means that your network is overwhelmed with constant broadcast or multicast traffic. Broadcast storms can eventually lead to a complete loss of network connectivity as the packets proliferate.

Storm Control protects the Switch bandwidth from flooding packets, including broadcast packets, multicast packets, and destination lookup failure (DLF). The **Rate** is a threshold that limits the total number of the selected type of packets. For example, if the broadcast and multicast options are selected, the total amount of packets per second for those two types will not exceed the limit value.

Broadcast storm control limits the number of broadcast, multicast and unknown unicast (also referred to as Destination Lookup Failure or DLF) packets the Switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and unknown unicast packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and unknown unicast packets in your network.
Storm Control unit: 652pps.

Default Settings

Broadcast Storm Control	: 652pps.
Multicast Storm Control	: None.
DLF Storm Control	: 652pps.

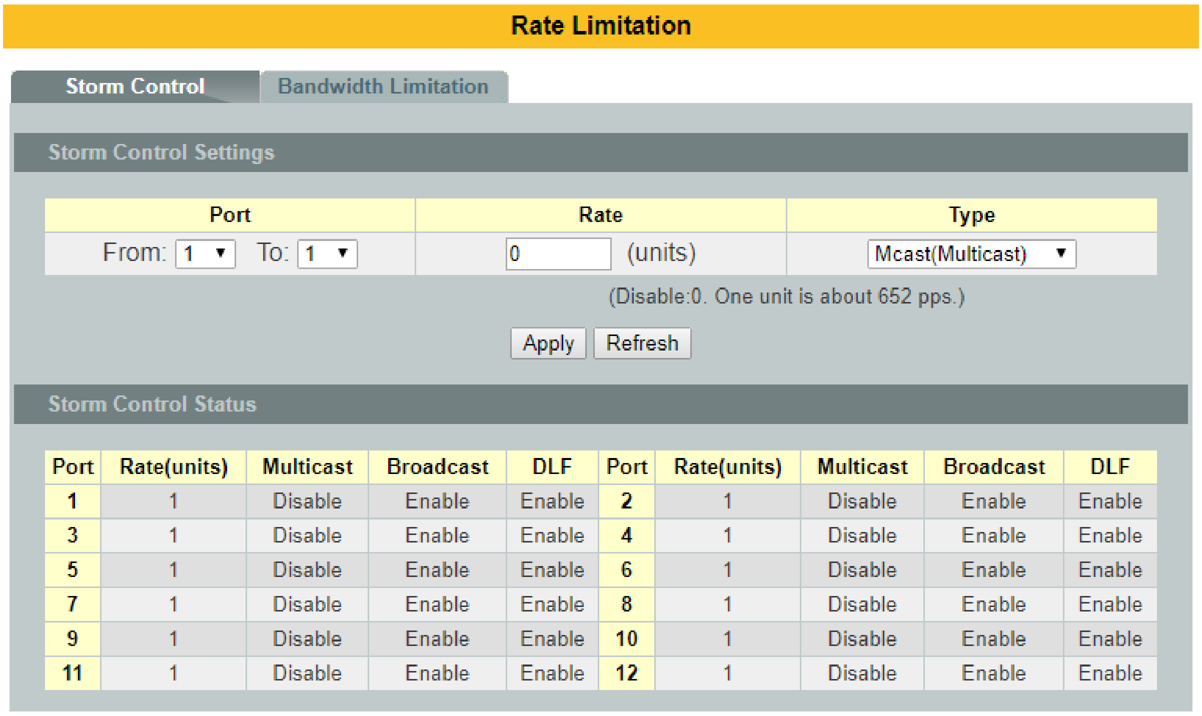
7.1.2.1.2. CLI Configuration

Node	Command	Description
enable	show storm-control	This command displays the current storm control configurations.
configure	storm-control rate RATE_LIMIT type (bcast | mcast | DLF | bcast+mcast | bcast+DLF | mcast+DLF | bcast+mcast+DLF) ports PORTLISTS	This command enables the bandwidth limit for broadcast or multicast or DLF packets and set the limitation.
configure	no storm-controltype (bcast | mcast | DLF | bcast+mcast | bcast+DLF | mcast+DLF | bcast+mcast+DLF) ports PORTLISTS	This command disables the bandwidth limit for broadcast or multicast or DLF packets.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#storm-control rate 1 type broadcast ports 1-6
L2SWITCH(config)#storm-control rate 1 type multicast ports 1-6
L2SWITCH(config)#storm-control rate 1 type DLF ports 1-6
```

7.1.2.1.3. Web Configuration



Rate Limitation

Storm Control | Bandwidth Limitation

Storm Control Settings

Port	Rate	Type
From: 1 ▼ To: 1 ▼	0 (units)	Mcast(Multicast) ▼

(Disable:0. One unit is about 652 pps.)

Apply Refresh

Storm Control Status

Port	Rate(units)	Multicast	Broadcast	DLF	Port	Rate(units)	Multicast	Broadcast	DLF
1	1	Disable	Enable	Enable	2	1	Disable	Enable	Enable
3	1	Disable	Enable	Enable	4	1	Disable	Enable	Enable
5	1	Disable	Enable	Enable	6	1	Disable	Enable	Enable
7	1	Disable	Enable	Enable	8	1	Disable	Enable	Enable
9	1	Disable	Enable	Enable	10	1	Disable	Enable	Enable
11	1	Disable	Enable	Enable	12	1	Disable	Enable	Enable

Parameter	Description
Port	Select the port number for which you want to configure storm control settings.
Rate	Select the number of packets (of the type specified in the **Type** field) per second the Switch can receive per second.
Type	Select **Broadcast** - to specify a limit for the amount of broadcast packets received per second. **Multicast** - to specify a limit for the amount of multicast packets received per second. **DLF** - to specify a limit for the amount of DLF packets received per second.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

7.1.2.2. Bandwidth Limitation

7.1.2.2.1. Introduction

The rate limitation is used to control the rate of traffic sent or received on a network interface.

Rate Limitation unit: Mbps.

Default Settings
All ports' Ingress and Egress rate limitation are disabled.

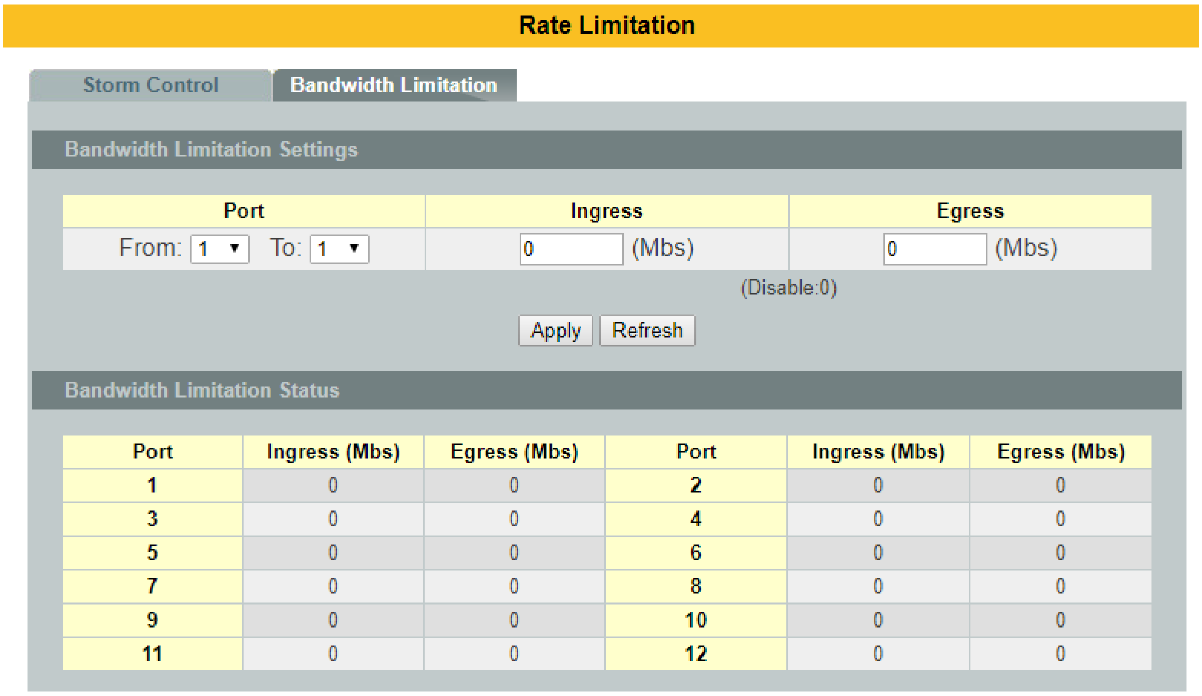
7.1.2.2.2. CLI Configuration

Node	Command	Description
enable	show bandwidth-limit	This command displays the current rate control configurations.
configure	bandwidth-limit egress RATE_LIMIT ports PORTLISTS	This command enables the bandwidth limit for outgoing packets and set the limitation.
configure	no bandwidth-limit egress ports PORTLISTS	This command disables the bandwidth limit for outgoing packets.
configure	bandwidth-limit ingress RATE_LIMIT ports PORTLISTS	This command enables the bandwidth limit for incoming packets and set the limitation.
configure	no bandwidth-limit ingress ports PORTLISTS	This command disables the bandwidth limit for incoming packets.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#bandwidth-limit egress 1 ports 1-8
L2SWITCH(config)#bandwidth-limit ingress 1 ports 1-8
```

7.1.2.2.3. Web Configuration



Rate Limitation

Bandwidth Limitation Settings

Port	Ingress	Egress
From: 1 ▾ To: 1 ▾	0 (Mbs)	0 (Mbs)

(Disable:0)

Bandwidth Limitation Status

Port	Ingress (Mbs)	Egress (Mbs)	Port	Ingress (Mbs)	Egress (Mbs)
1	0	0	2	0	0
3	0	0	4	0	0
5	0	0	6	0	0
7	0	0	8	0	0
9	0	0	10	0	0
11	0	0	12	0	0

Parameter	Description
Port	Selects a port that you want to configure.
Ingress	Configures the rate limitation for the ingress packets.
Egress	Configures the rate limitation for the egress packets.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

7.2. IGMP Snooping

7.2.1. IGMP Snooping

7.2.1.1. Introduction

The IGMP snooping is for multicast traffic. The Switch can passively snoop on IGMP packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

The Switch can passively snoop on IGMP packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks

IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.
The Switch forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your Switch.

The Switch can perform IGMP snooping on up to 4094 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs. The Switch then performs IGMP snooping on the first VLANs that send IGMP packets. Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as fixed mode. In fixed mode the Switch does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

Immediate Leave
When you enable IGMP Immediate-Leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port. You should use the Immediate-Leave feature only when there is a single receiver present on every port in the VLAN. (Immediate Leave is only supported on IGMP Version 2 hosts).

The switch uses IGMP snooping Immediate Leave to remove from the forwarding table an interface that sends a leave message without the switch sending group-specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Immediate Leave ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are simultaneously in use.

Fast Leave
The switch allow user to configure a delay time. When the delay time is expired, the switch removes the interface from the multicast group.

Last Member Query Interval
Last Member Query Interval: The Last Member Query Interval is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages.

Without Immediate Leave, when the switch receives an IGMP leave message from a subscriber on a receiver port, it sends out an IGMP specific query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership.

IGMP Querier
There is normally only one Querier per physical network. All multicast routers start up as a Querier on each attached network. If a multicast router hears a Query message from a router **with a lower IP address**, it MUST become a Non-Querier on that network. If a router has not heard a Query message from another router for [Other Querier Present Interval], it resumes the role of Querier. Routers periodically [Query Interval]send a General Query on each attached network

for which this router is the Querier, to solicit membership information. On startup, a router SHOULD send [Startup Query Count] General Queries spaced closely together [Startup Query Interval] in order to quickly and reliably determine membership information. A General Query is addressed to the all-systems multicast group (224.0.0.1), has a Group Address field of 0, and has a Max Response Time of [Query Response Interval].

Port IGMP Querier Mode

- **Auto:**

  The Switch uses the port as an IGMP query port if the port receives IGMP query packets.

- **Fixed:**

  The Switch always treats the port(s) as IGMP query port(s). This is for when connecting an IGMP multicast server to the port(s). The Switch always forwards the client's **report/leave** packets to the port.

  Normally, the port is connected to an IGMP server.

- **Edge:**

  The Switch does not use the port as an IGMP query port. The IGMP query packets received by this port will be dropped.

  Normally, the port is connected to an IGMP client.

Note: The Switch will forward the IGMP join and leave packets to the query port.

Configurations:

Users can enable/disable the IGMP Snooping on the Switch. Users also can enable/disable the IGMP Snooping on a specific VLAN. If the IGMP Snooping on the Switch is disabled, the IGMP Snooping is disabled on all VLANs even some of the VLAN IGMP Snooping are enabled.

Default Settings

If received packets are not received after 400 seconds, all multicast entries will be deleted.
The default global IGMP snooping state is disabled.
The default VLAN IGMP snooping state is disabled for all VLANs.
The unknown multicast packets will be dropped.
The default port Immediate Leave state is disabled for all ports.
The default port Querier Mode state is auto for all ports.
The IGMP snooping Report Suppression is disabled.

Notices: There are a global state and per VLAN states. When the global state is disabled, the IGMP snooping on the Switch is disabled even per VLAN states are enabled. When the global state is enabled, user must enable per VLAN states to enable the IGMP Snooping on the specific VLAN.

7.2.1.2. CLI Configuration

Node	Command	Description
enable	show igmp-snooping	This command displays the current IGMP snooping configurations.

enable	show igmp-snooping counters	This command displays the current IGMP snooping counters.
enable	show igmp-snooping querier	This command displays the current IGMP Querier.
enable	show multicast	This command displays the multicast group in IP format.
configure	clear igmp-snooping counters	This command clears all of the IGMP snooping counters.
configure	igmp-snooping (disable | enable)	This command disables / enables the IGMP snooping on the switch.
configure	igmp-snooping vlan VLANID	This command enables the IGMP snooping function on a VLAN or range of VLANs.
configure	no igmp-snooping vlan VLANID	This command disables the IGMP snooping function on a VLAN or range of VLANs.
configure	igmp-snooping unknown-multicast(drop|flooding)	This command configures the process for unknown multicast packets when the IGMP snooping function is enabled. *drop:* Drop all of the unknown multicast packets.
configure	igmp-snooping report-suppression (disable|enable)	This command disables / enables the IGMP snooping report suppression function on the switch.
configure	clear igmp-counters	This command clears the IGMP snooping counters.
configure	clear igmp-counters (port|vlan)	This command clears the IGMP snooping counters for port or vlan.
interface	igmp-querier-mode (auto|fixed|edge)	This command specifies whether or not and under what conditions the port(s) is (are) IGMP query port(s). The Switch forwards IGMP join or leave packets to an IGMP query port, treating the port as being connected to an IGMP multicast router (or server). You must enable IGMP snooping as well. (Default:auto)
interface	igmp-immediate-leave	This command enables the IGMP Snooping immediate leave function for the specific interface.
interface	no igmp-immediate-leave	This command disables the IGMP Snooping immediate leave function for the specific interface.
interface	igmp-snooping group-limit VALUE	This command configures the maximum groups for the specific interface.
interface	no igmp-snooping group-limit	This command removes the limitation of the maximum groups for the specific interface.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.

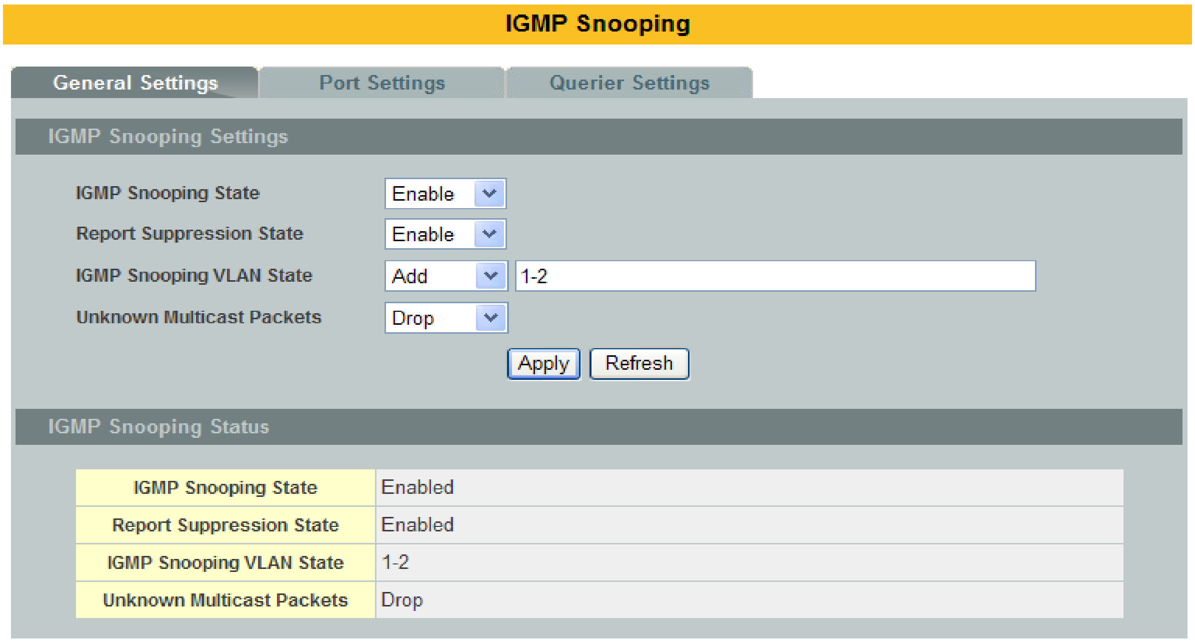
if-range	igmp-immediate-leave	This command enables the IGMP Snooping immediate leave function for the specific ports.
if-range	no igmp-immediate-leave	This command disables the IGMP Snooping immediate leave function for the specific ports.
if-range	igmp-snooping group-limit VALUE	This command configures the maximum groups for the specific ports.
if-range	no igmp-snooping group-limit	This command removes the limitation of the maximum groups for the specific ports.
if-range	igmp-querier-mode (auto|fixed|edge)	This command specifies whether or not and under what conditions the ports are IGMP query port(s). The Switch forwards IGMP join or leave packets to an IGMP query port, treating the port as being connected to an IGMP multicast router (or server). You must enable IGMP snooping as well. (Default:auto)

Example:

```
L2SWITCH(config)#igmp-snooping enable
L2SWITCH(config)#igmp-snooping vlan 1
L2SWITCH(config)#igmp-snooping querier enable
L2SWITCH(config)#igmp-snooping querier vlan 1
L2SWITCH(config)#interface 1/0/1
L2SWITCH(config-if)#igmp-immediate-leave
L2SWITCH(config-if)#igmp-querier-mode fixed
L2SWITCH(config-if)#igmp-snooping group-limit 20
```

7.2.1.3. Web Configuration

General Settings



IGMP Snooping

IGMP Snooping Settings

IGMP Snooping State	Enable
Report Suppression State	Enable
IGMP Snooping VLAN State	Add 1-2
Unknown Multicast Packets	Drop

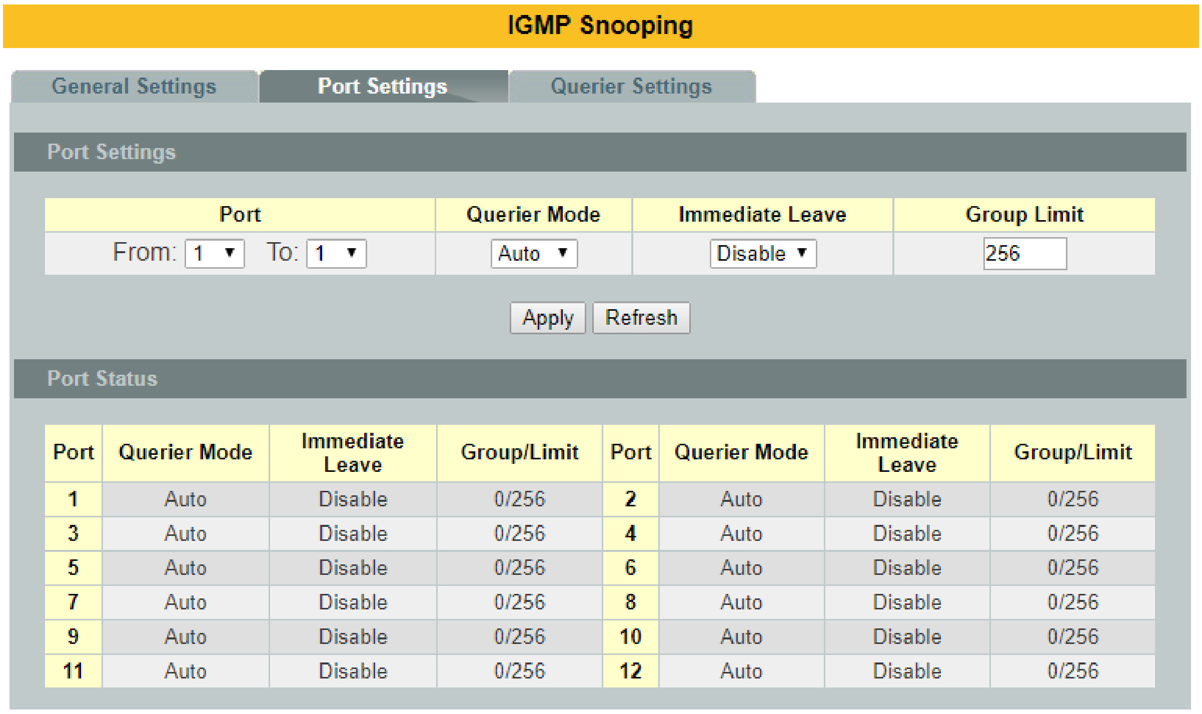
IGMP Snooping Status

IGMP Snooping State	Enabled
Report Suppression State	Enabled
IGMP Snooping VLAN State	1-2
Unknown Multicast Packets	Drop

Parameter	**Description**
IGMP Snooping State	Select **Enable** to activate IGMP Snooping to forward group multicast traffic only to ports that are members of that group. Select **Disable** to deactivate the feature.
Report Suppression State	Select **Enable/Disable** to activate/deactivate IGMP Snooping report suppression function.
IGMP Snooping VLAN State	Select **Add** and enter VLANs upon which the Switch is to perform IGMP snooping. The valid range of VLAN IDs is between 1 and 4094. Use a comma (,) or hyphen (-) to specify more than one VLANs. Select **Delete** and enter VLANs on which to have the Switch not perform IGMP snooping.
Unknown Multicast Packets	Specify the action to perform when the Switch receives an unknown multicast frame. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last setting.
IGMP Snooping State	This field displays whether IGMP snooping is globally enabled or disabled.
Report Suppression State	This field displays whether IGMP snooping report suppression is enabled or disabled.
IGMP Snooping VLAN State	This field displays VLANs on which the Switch is to perform IGMP snooping. None displays if you have not enabled IGMP snooping on any port yet.

Unknown Multicast Packets	This field displays whether the Switch is set to discard or flood unknown multicast packets.

Port Settings



Port	Querier Mode	Immediate Leave	Group Limit
From: 1 ▼ To: 1 ▼	Auto ▼	Disable ▼	256

Port	Querier Mode	Immediate Leave	Group/Limit	Port	Querier Mode	Immediate Leave	Group/Limit
1	Auto	Disable	0/256	2	Auto	Disable	0/256
3	Auto	Disable	0/256	4	Auto	Disable	0/256
5	Auto	Disable	0/256	6	Auto	Disable	0/256
7	Auto	Disable	0/256	8	Auto	Disable	0/256
9	Auto	Disable	0/256	10	Auto	Disable	0/256
11	Auto	Disable	0/256	12	Auto	Disable	0/256

Parameter	**Description**
Querier Mode	Select the desired setting, **Auto**, **Fixed**, or **Edge**. **Auto** means the Switch uses the port as an IGMP query port if the port receives IGMP query packets. **Fixed** means the Switch always treats the port(s) as IGMP query port(s). This is for when connecting an IGMP multicast server to the port(s). **Edge** means the Switch does not use the port as an IGMP query port. In this case, the Switch does not keep a record of an IGMP router being connected to this port and the Switch does not forward IGMP join or leave packets to this port.
Immediate Leave	Select individual ports on which to enable immediate leave.
Group Limit	Configures the maximum group for the port or a range of ports.
Apply	Click Apply to apply the settings.
Refresh	Click this to reset the fields.
Port	The port ID.
Querier Mode	The Querier mode setting for the specific port.
Immediate Leave	The Immediate Leave setting for the specific port.

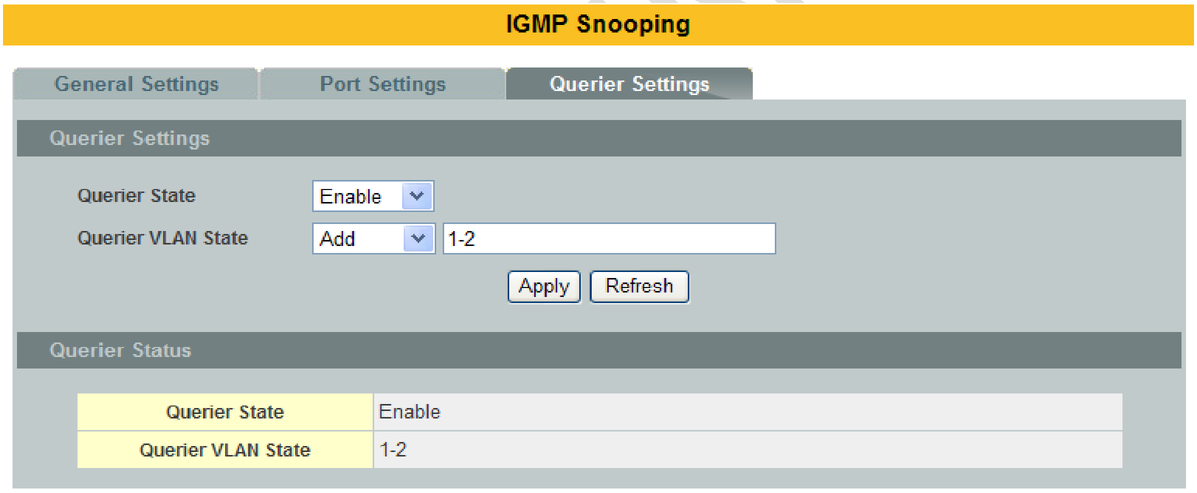
Group Limit	The current joining group count and the maximum group count.

7.2.2. IGMP Snooping Querier Settings

7.2.2.1. CLI Configurations

Node	Command	Description
configure	igmp-snooping querier (disable | enable)	This command disables / enables the IGMP snooping querier on the Switch.
configure	igmp-snooping querier vlan VLANIDs	This command enables the IGMP snooping querier function on a VLAN or range of VLANs.
configure	no igmp-snooping querier vlan VLANIDs	This command disables the IGMP snooping querier function on a VLAN or range of VLANs.

7.2.2.2. Web Configurations



Querier State: Enable

Querier VLAN State: Add 1-2

Querier State	Enable
Querier VLAN State	1-2

Parameter	Description
Querier State	This field configures the global Querier state.
Querier VLAN State	This field enables the Querier state in a vlan or a range of vlan.
Apply	Click Apply to apply the settings.
Refresh	Click this to reset the fields to the last setting.
Querier State	This filed indicates the current global Querier status.
Querier VLAN State	This field indicates the Querier status in vlan.

7.2.3. IGMP Snooping Filter

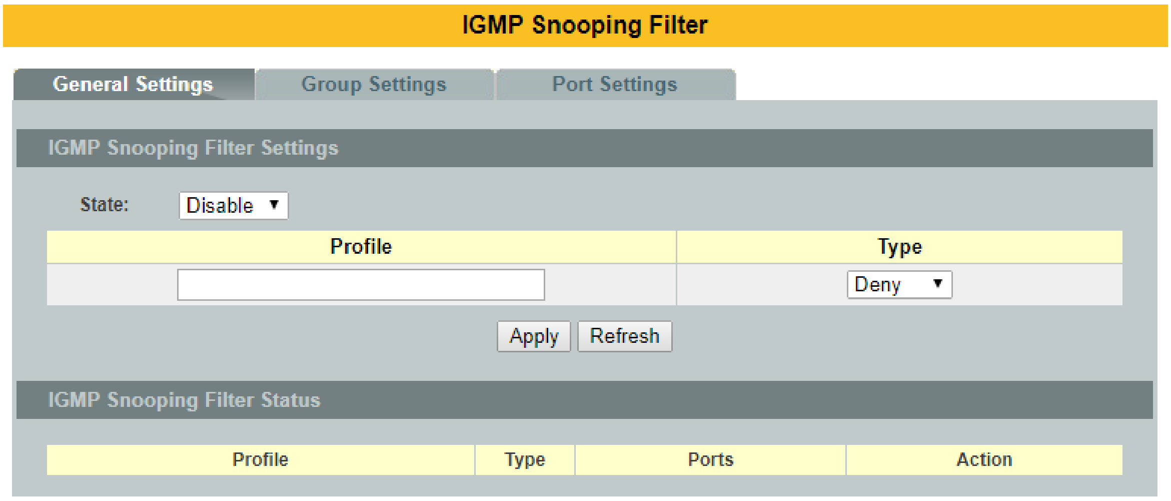
The IGMP Snooping Filter allows users to configure one or some of range or multicast address to drop or to forward them.

7.2.3.1. CLI Configurations

Node	Command	Description
enable	show igmp-snooping filtering	This command displays the IGMP snooping filtering configurations.
configure	igmp-snooping filtering (enable|disable)	This command enables/disables the IGMP snooping filtering profiles on the Switch.
configure	igmp-snooping filtering profile	This command enters the IGMP snooping filtering profiles configuration node.
configure	no igmp-snooping filtering all	This command removes all of the IGMP snooping filtering profiles from the Switch.
configure	no igmp-snooping filtering STRINGS	This command removes the IGMP snooping filtering profiles by name from the Switch.
config-igmp	Group GROUP_ID start-address START-ADDR end-address END-ADDR	This command configures the group configurations, including group index and start multicast address and end multicast address.
config-igmp	type (deny|permit)	This command configures the type of deny or permit for the group.
config-igmp	no group GROUP-ID	This command removes the group configurations.
config-igmp	no group all	This command removes all of the group configurations.
config-igmp	type (deny|permit)	This command configures the type of deny or permit for the group.
interface	igmp-snooping filtering profile STRING	This command enables the IGMP snooping filtering profiles on the specific port.
interface	no igmp-snooping filtering profile STRINGS	This command disables the IGMP snooping filtering profiles on the specific port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-config	igmp-snooping filtering profile STRING	This command enables the IGMP snooping filtering profiles on the range of ports.
if-config	no igmp-snooping filtering profile STRINGS	This command disables the IGMP snooping filtering profiles on the range of ports.

7.2.3.2. Web Configurations

General Settings:



IGMP Snooping Filter Settings

State: Disable

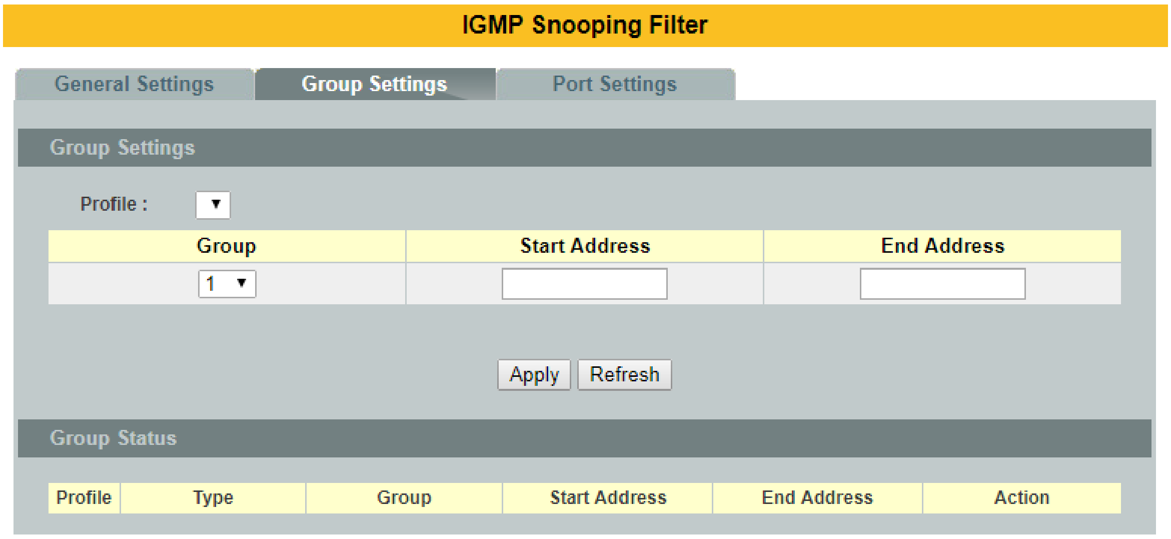
Profile	Type
	Deny

IGMP Snooping Filter Status

Profile	Type	Ports	Action

Parameter	Description
IGMP Filtering State	This field configures the global IGMP Filtering state.
Profile	This field creates the IGMP Filtering profile.
Type	The field configures the type of action for the profile.
Apply	Click Apply to apply the settings.
Refresh	Click this to reset the fields to the last setting.
IGMP Filtering Status	
Profile	The profile name.
Type	The type of action.
Ports	The field indicates the ports that the IGMP Filtering profile is activated.
Action	Click the "Delete" button to delete the profile.

Group Settings:



IGMP Snooping Filter

Group Settings

Profile : ▼

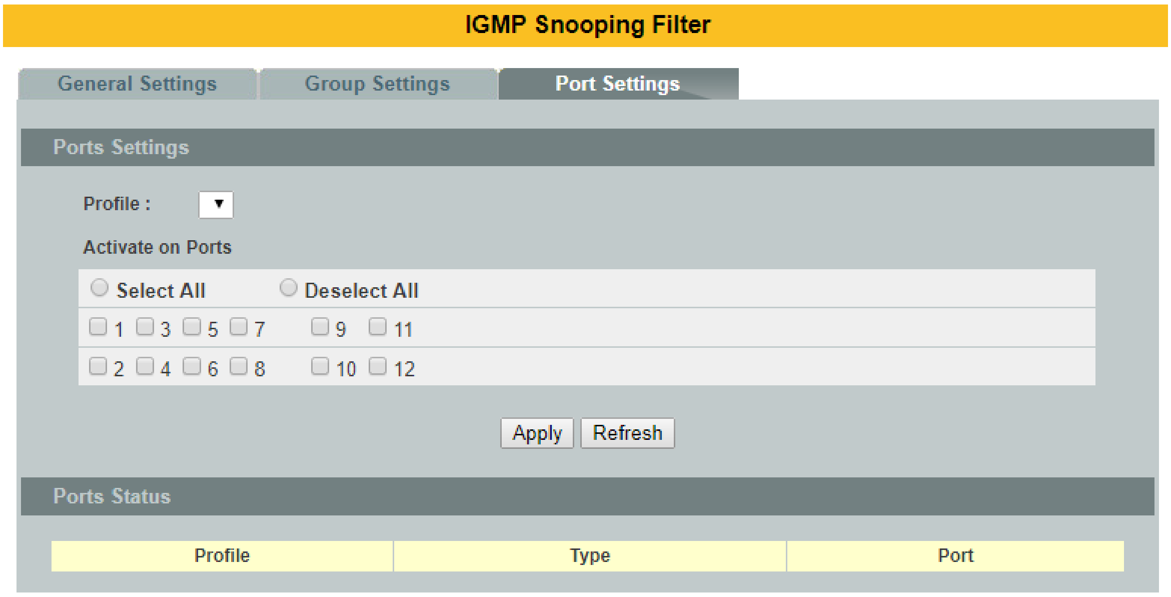
Group	Start Address	End Address
1 ▼		

Group Status

Profile	Type	Group	Start Address	End Address	Action

Parameter	Description
Profile	This field selects the profile which you want to configure the group.
Group	This field selects the group index.
Start Address	The field configures the first multicast address of the group.
End Address	The field configures the last multicast address of the group.
Apply	Click Apply to apply the settings.
Refresh	Click this to reset the fields to the last setting.

Port Settings:



IGMP Snooping Filter

General Settings | Group Settings | Port Settings

Ports Settings

Profile : ▾

Activate on Ports

○ Select All ○ Deselect All

□ 1 □ 3 □ 5 □ 7 □ 9 □ 11

□ 2 □ 4 □ 6 □ 8 □ 10 □ 12

Apply Refresh

Ports Status

Profile	Type	Port

Parameter	Description
Profile	This field selects the profile which you want to activate on the ports.
Activate IGMP Filtering on Ports	Selects the ports which you want to activate the IGMP Filtering profile.
Apply	Click Apply to apply the settings.
Refresh	Click this to reset the fields to the last setting.

7.2.4. **Multicast Address**

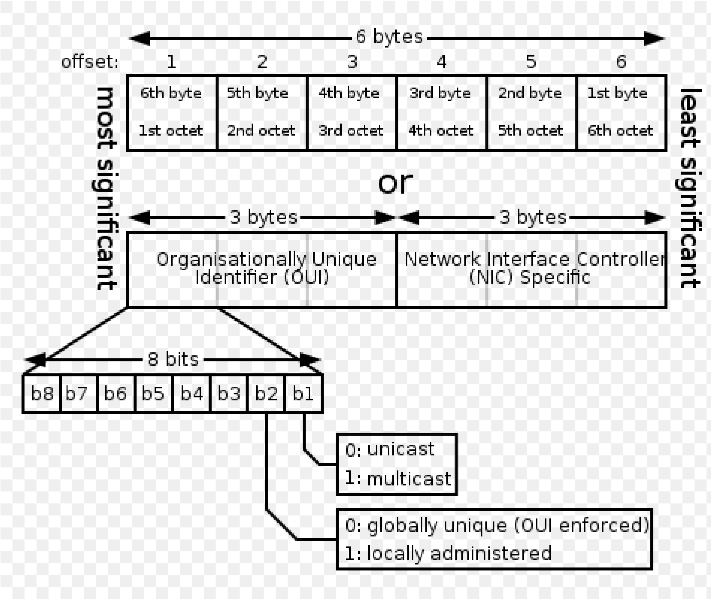
7.2.4.1. Introduction

A multicast address is associated with a group of interested receivers. According to RFC 3171, addresses 224.0.0.0 to 239.255.255.255, the former Class D addresses, are designated as multicast addresses in IPv4.

The IANA owns the OUI MAC address 01:00:5e, therefore multicast packets are delivered by using the Ethernet MAC address range 01:00:5e:00:00:00 - 01:00:5e:7f:ff:ff. This is 23 bits of available address space.

The first octet (01) includes the broadcast/multicast bit. The lower 23 bits of the 28-bit multicast IP address are mapped into the 23 bits of available Ethernet address space. This means that there is ambiguity in delivering packets. If two hosts on the same subnet each subscribe to a different multicast group whose address differs only in the first 5 bits, Ethernet packets for both multicast groups will be delivered to both hosts, requiring the network software in the hosts to discard the unrequired packets.

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development Purposes.



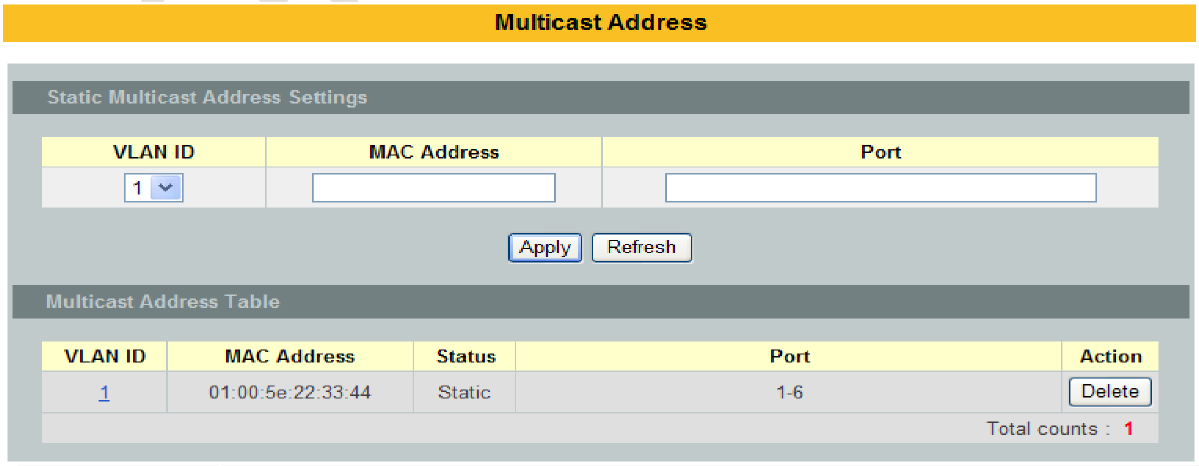
IP multicast address	Description
224.0.0.0	Base address (reserved)
224.0.0.1	The All Hosts multicast group that contains all systems on the same network segment
224.0.0.2	The All Routers multicast group that contains all routers on the same network segment
224.0.0.5	The Open Shortest Path First (OSPF) AllSPF Routers address. Used to send Hello packets to all OSPF routers on a network segment
224.0.0.6	The OSPF AllD Routers address. Used to send OSPF routing information to OSPF designated routers on a network segment
224.0.0.9	The RIP version 2 group address, used to send routing information using the RIP protocol to all RIP v2-aware routers on a network segment
224.0.0.10	EIGRP group address. Used to send EIGRP routing information to all EIGRP routers on a network segment

224.0.0.13	PIM Version 2 (Protocol Independent Multicast)
224.0.0.18	Virtual Router Redundancy Protocol
224.0.0.19 - 21	IS-IS over IP
224.0.0.22	IGMP Version 3 (Internet Group Management Protocol)
224.0.0.102	Hot Standby Router Protocol Version 2
224.0.0.251	Multicast DNS address
224.0.0.252	Link-local Multicast Name Resolution address
224.0.1.1	Network Time Protocol address
224.0.1.39	Cisco Auto-RP-Announce address
224.0.1.40	Cisco Auto-RP-Discovery address
224.0.1.41	H.323 Gatekeeper discovery address

7.2.4.2. CLI Configuration

Node	Command	Description
enable	show mac-address-table multicast	This command displays the current static/dynamic multicast address entries.
enable	show mac-address-table multicast vlan VLANID	This command displays the current static/dynamic multicast address entries with a specific vlan.
configure	mac-address-table multicast MACADDR vlan VLANID ports PORTLIST	This command configures a static multicast entry.
configure	no mac-address-table multicast MACADDR	This command removes a static multicast entry from the address table.

7.2.4.3. Web Configuration



Multicast Address

Static Multicast Address Settings

VLAN ID	MAC Address	Port
1		

Apply Refresh

Multicast Address Table

VLAN ID	MAC Address	Status	Port	Action
1	01:00:5e:22:33:44	Static	1-6	Delete

Total counts : 1

Parameter	Description

VLAN ID	Configures the VLAN that you want to configure.
MAC Address	Configures the multicast MAC which will not be aged out. Valid format is hh:hh:hh:hh:hh:hh.
Port	Configures the member port for the multicast address.
Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.

7.3. VLAN

7.3.1. Port Isolation

7.3.1.1. Introduction

The port isolation is a port-based virtual LAN feature. It partitions the switching ports into virtual private domains designated on a per port basis. Data switching outside of the port's private domain is not allowed. It will ignore the packets' tag VLAN information.

This feature is a per port setting to configure the egress port(s) for the specific port to forward its received packets. If the CPU port (port 0) is not an egress port for a specific port, the host connected to the specific port cannot manage the Switch.

If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. **CPU** refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.

Example: If you want to allow port-1 and port-3 to talk to each other, you must configure as below:

```
L2SWITCH(config)#interface 1/0/1
L2SWITCH(config-if)#port-isolation ports 3
L2SWITCH(config-if)#exit
  ; Allow the port-1 to send its ingress packets to port-3.

L2SWITCH(config)#interface 1/0/3
L2SWITCH(config-if)#port-isolation ports 1
L2SWITCH(config-if)#exit
  ; Allow the port-3to send its ingress packets to port-1
```

7.3.1.2. CLI Configuration

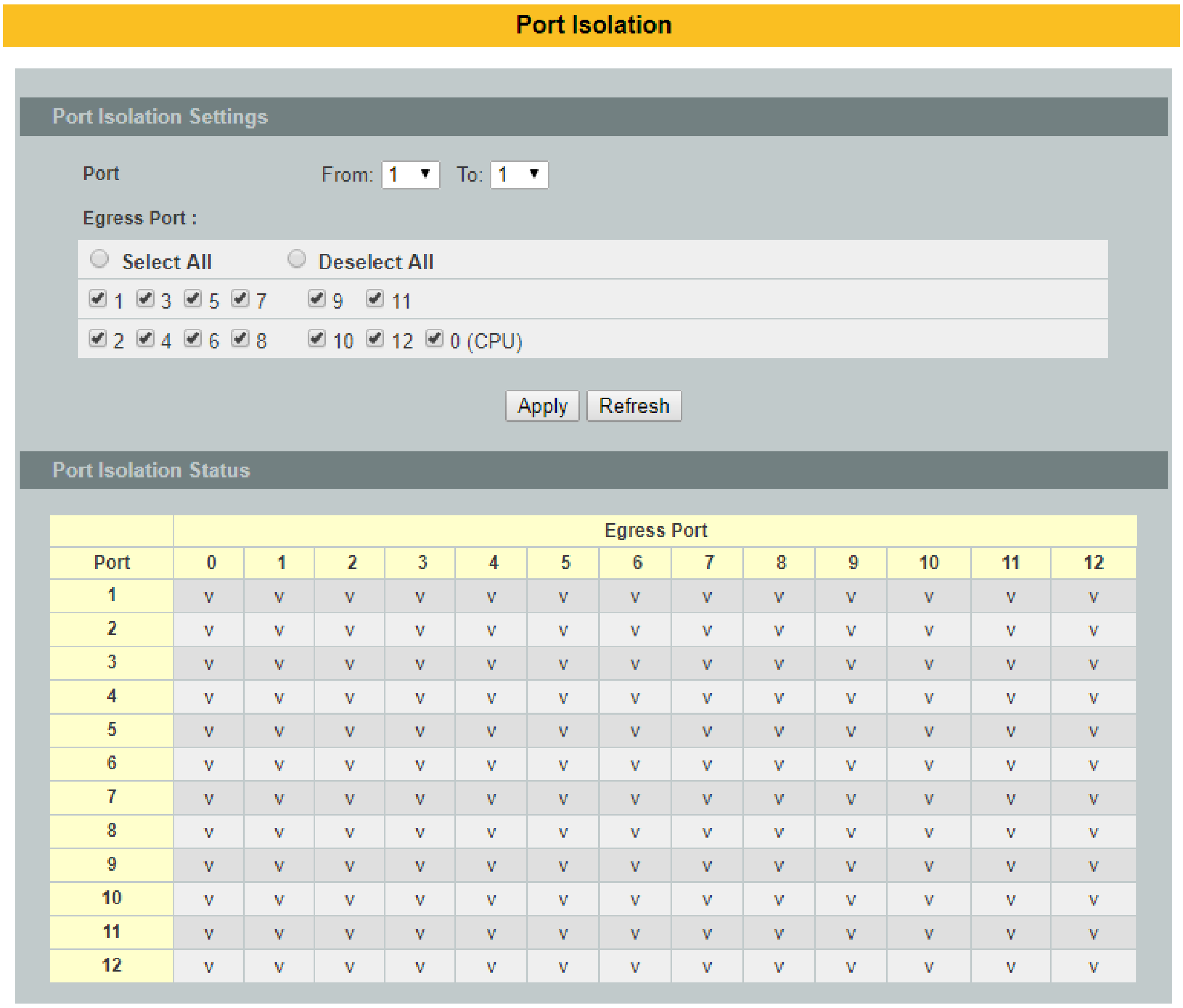
Node	Command	Description
enable	show port-isolation	This command displays the current port isolation configurations. "V" indicates the port's packets can be sent to that port. "-" indicates the port's packets cannot be sent to that

		port.
interface	port-isolation ports PORTLISTS	This command configures a port or a range of ports to egress traffic from the specific port.
interface	no port-isolation	This command configures all ports to egress traffic from the specific port.

Example:

```
L2SWITCH(config)#interface 1/0/2
L2SWITCH(config-if)#port-isolation ports 3-10
```

7.3.1.3. Web Configuration



Port Isolation

Port Isolation Settings

Port From: 1 ▼ To: 1 ▼

Egress Port :

○ Select All ○ Deselect All

☑ 1 ☑ 3 ☑ 5 ☑ 7 ☑ 9 ☑ 11

☑ 2 ☑ 4 ☑ 6 ☑ 8 ☑ 10 ☑ 12 ☑ 0 (CPU)

Port Isolation Status

	Egress Port												
Port	0	1	2	3	4	5	6	7	8	9	10	11	12
1	v	v	v	v	v	v	v	v	v	v	v	v	v
2	v	v	v	v	v	v	v	v	v	v	v	v	v
3	v	v	v	v	v	v	v	v	v	v	v	v	v
4	v	v	v	v	v	v	v	v	v	v	v	v	v
5	v	v	v	v	v	v	v	v	v	v	v	v	v
6	v	v	v	v	v	v	v	v	v	v	v	v	v
7	v	v	v	v	v	v	v	v	v	v	v	v	v
8	v	v	v	v	v	v	v	v	v	v	v	v	v
9	v	v	v	v	v	v	v	v	v	v	v	v	v
10	v	v	v	v	v	v	v	v	v	v	v	v	v
11	v	v	v	v	v	v	v	v	v	v	v	v	v
12	v	v	v	v	v	v	v	v	v	v	v	v	v

Parameter	Description
Port	Select a port number to configure its port isolation settings. Select **All Ports** to configure the port isolation settings for all ports on the Switch.
Egress Port	An egress port is an outgoing port, that is, a port through which a data packet leaves.

	Selecting a port as an outgoing port means it will communicate with the port currently being configured.
Select All/ Deselect All	Click **Select All** to mark all ports as egress ports and permit traffic. Click **Deselect All** to unmark all ports and isolate them. Deselecting all ports means the port being configured cannot communicate with any other port.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last setting.
Port Isolation Status	"V" indicates the port's packets can be sent to that port. "-" indicates the port's packets cannot be sent to that port.

7.3.2. 802.1Q VLAN

7.3.2.1. Introduction

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the Broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

VID- VLAN ID is the identification of the VLAN, which is basically used by the standard 802.1Q. It has 12 bits and allow the identification of 4096 (2^12) VLANs. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID

2 bytes	3 bits	1 bit	12 bits

- Forwarding Tagged and Untagged Frames

Each port on the Switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the Switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1QVLAN-aware switch, the Switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

- 802.1QPort base VLAN

With port-based VLAN membership, the port is assigned to a specific VLAN independent of the user or system attached to the port. This means all users attached to the port should be members of the same VLAN. The network administrator typically performs the VLAN assignment. The port configuration is static and cannot be automatically changed to another VLAN without manual reconfiguration.

As with other VLAN approaches, the packets forwarded using this method do not leak into other VLAN domains on the network. After a port has been assigned to a VLAN, the port cannot send to or receive from devices in another VLAN without the intervention of a Layer 3 device.

The device that is attached to the port likely has no understanding that a VLAN exists. The device simply knows that it is a member of a subnet and that the device should be able to talk to all other members of the subnet by simply sending information to the cable segment. The switch is responsible for identifying that the information came from a specific VLAN and for ensuring that the information gets to all other members of the VLAN. The switch is further responsible for ensuring that ports in a different VLAN do not receive the information.

This approach is quite simple, fast, and easy to manage in that there are no complex lookup tables required for VLAN segmentation. If port-to-VLAN association is done with an application-specific integrated circuit (ASIC), the performance is very good. An ASIC allows the port-to-VLAN mapping to be done at the hardware level.

Default Settings

The default PVID is 1 for all ports.
The default Acceptable Frame is All for all ports.
All ports join in the VLAN 1.

Notices

The maximum VLAN group is 4094.

7.3.2.2. CLI Configuration

Node	Command	Description
enable	show vlan VLANID	This command displays the VLAN

		configurations.
configure	vlan <1~4094>	This command enables a VLAN and enters the VLAN node.
configure	no vlan <1~4094>	This command deletes a VLAN.
vlan	show	This command displays the current VLAN configurations.
vlan	name STRING	This command assigns a name for the specific VLAN. The VLAN name should be the combination of the digit or the alphabet or hyphens (-) or underscores (_). The maximum length of the name is 16 characters.
vlan	no name	This command configures the vlan name to default. Note: The default vlan name is "VLAN"+vlan_ID, VLAN1, VLAN2,…
vlan	add PORTLISTS	This command adds a port or a range of ports to the vlan.
vlan	fixed PORTLISTS	This command assigns ports for permanent member of the vlan.
vlan	no fixed PORTLISTS	This command removes all fixed member from the vlan.
vlan	Tagged PORTLISTS	This command assigns ports for tagged member of the VLAN group. The ports should be one/some of the permanent members of the vlan.
vlan	no tagged PORTLISTS	This command removes all tagged member from the vlan.
vlan	Untagged PORTLISTS	This command assigns ports for untagged member of the VLAN group. The ports should be one/some of the permanent members of the vlan.
vlan	no untagged PORTLISTS	This command removes all untagged member from the vlan.
interface	acceptable frame type (all|tagged|untagged)	This command configures the acceptable frame type. all - acceptable all frame types. tagged - acceptable tagged frame only. untagged – acceptable untagged frame only.
interface	pvid VLANID	This command configures a VLAN ID for the port default VLAN ID.
interface	no pvid	This command configures 1 for the port default VLAN ID.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.

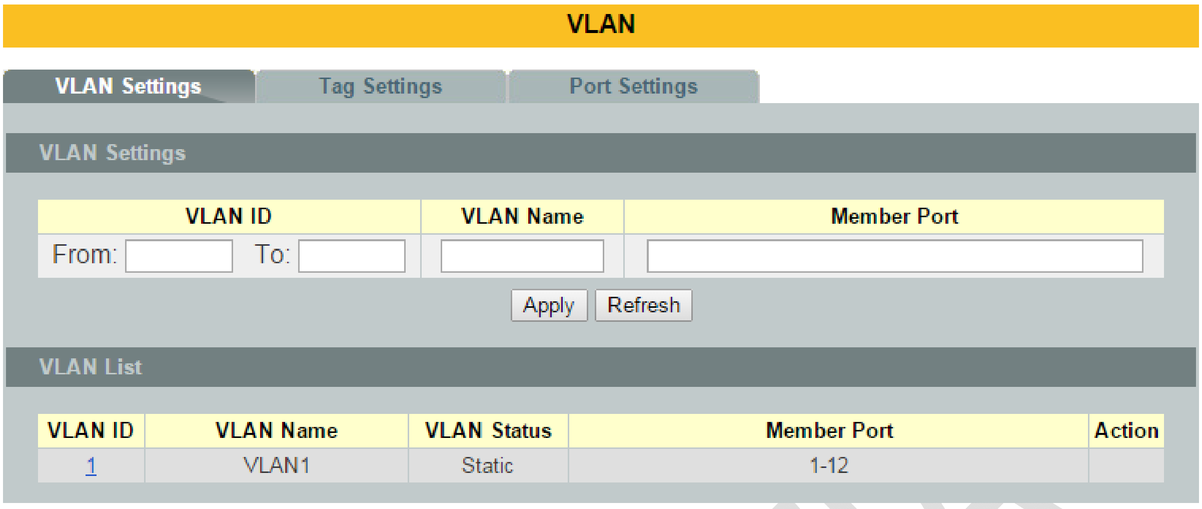
if-range	pvid VLANID	This command configures a VLAN ID for the port default VLAN ID.
if-range	no pvid	This command configures 1 for the port default VLAN ID.
configure	vlan range STRINGS	This command configures a range of vlans.
configure	no vlan range STRINGS	This command removes a range of vlans.
vlan-range	add PORTLISTS	This command adds a port or a range of ports to the vlans.
vlan-range	fixed PORTLISTS	This command assigns ports for permanent member of the VLAN group.
vlan-range	no fixed PORTLISTS	This command removes all fixed member from the vlans.
vlan-range	taggedPORTLISTS	This command assigns ports for tagged member of the VLAN group. The ports should be one/some of the permanent members of the vlans.
vlan-range	no tagged PORTLISTS	This command removes all tagged member from the vlans.
vlan-range	untaggedPORTLISTS	This command assigns ports for untagged member of the VLAN group. The ports should be one/some of the permanent members of the vlans.
vlan-range	no untagged PORTLISTS	This command removes all untagged member from the vlans.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#vlan 2
L2SWITCH(config-vlan)#fixed 1-6
L2SWITCH(config-vlan)#untagged 1-3
```

7.3.2.3. Web Configuration

VLAN Settings

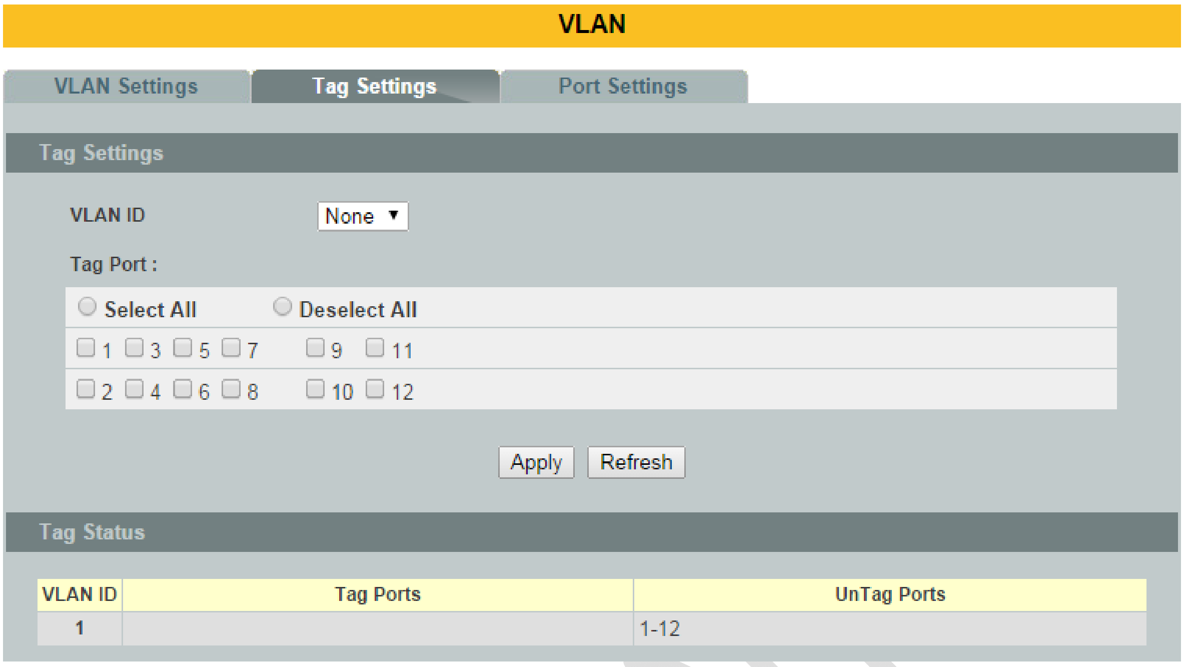


VLAN ID		VLAN Name	Member Port
From:	To:		

VLAN ID	VLAN Name	VLAN Status	Member Port	Action
1	VLAN1	Static	1-12	

Parameter	**Description**
VLAN ID	Enter the VLAN ID for this entry; the valid range is between 1 and 4094.
VLAN Name	Enter a descriptive name for the VLAN for identification purposes. The VLAN name should be the combination of the digit or the alphabet or hyphens (-) or underscores (_). The maximum length of the name is 16 characters.
Member Port	Enter the port numbers you want the Switch to assign to the VLAN as members. You can designate multiple port numbers individually by using a comma (,) and by range with a hyphen (-).
Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.
VLAN List	
VLAN ID	This field displays the index number of the VLAN entry. Click the number to modify the VLAN.
VLAN Name	This field displays the name of the VLAN.
VLAN Status	This field displays the status of the VLAN. **Static** or **Dynamic** (802.1QVLAN).
Member Port	This field displays which ports have been assigned as members of the VLAN. This will display **None** if no ports have been assigned.
Action	Click **Delete** to remove the VLAN. The VLAN 1 cannot be deleted.

Tag Settings



Tag Settings

VLAN ID: None ▼

Tag Port :

○ Select All ○ Deselect All

□ 1 □ 3 □ 5 □ 7 □ 9 □ 11

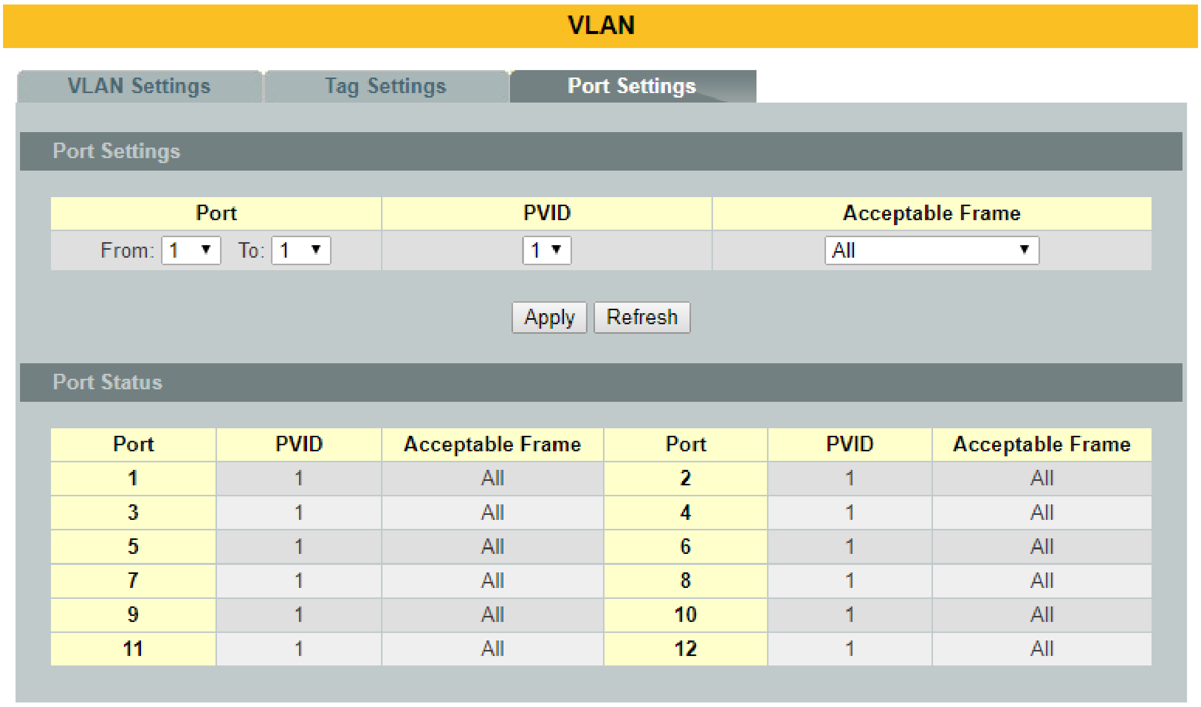
□ 2 □ 4 □ 6 □ 8 □ 10 □ 12

Tag Status

VLAN ID	Tag Ports	UnTag Ports
1		1-12

Parameter	Description
VLAN ID	Select a VLAN ID to configure its port tagging settings.
Tag Port	Selecting a port which is a member of the selected VLAN ID will make it a tag port. This means the port will tag all outgoing frames transmitted with the VLAN ID.
Select All	Click **Select All** to mark all member ports as tag ports.
Deselect All	Click **Deselect All** to mark all member ports as untag ports.
Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.
Tag Status	
VLAN ID	This field displays the VLAN ID.
Tag Ports	This field displays the ports that have been assigned as tag ports.
Untag Ports	This field displays the ports that have been assigned as untag ports.

Port Settings



Port Settings

Port	PVID	Acceptable Frame
From: 1 ▼ To: 1 ▼	1 ▼	All ▼

Port Status

Port	PVID	Acceptable Frame	Port	PVID	Acceptable Frame
1	1	All	2	1	All
3	1	All	4	1	All
5	1	All	6	1	All
7	1	All	8	1	All
9	1	All	10	1	All
11	1	All	12	1	All

Parameter	**Description**
Port	Select a port number to configure from the drop-down box. Select **All** to configure all ports at the same time.
PVID	Select a **PVID** (Port VLAN ID number) from the drop-down box.
Acceptable Frame	Specify the type of frames allowed on a port. Choices are **All**, **VLAN Untagged Only** or **VLAN Tagged Only**. - Select **All** from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. - Select **VLAN Tagged Only** to accept only tagged frames on this port. All untagged frames will be dropped. - Select **VLAN Untagged Only** to accept only untagged frames on this port. All tagged frames will be dropped.
Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.
Port Status	
Port	This field displays the port number.
PVID	This field displays the Port VLAN ID number.
Acceptable Frame	This field displays the type of frames allowed on the port. This will either display **All** or **VLAN Tagged Only or VLAN Untagged Only.**

7.3.3. MAC VLAN

7.3.3.1. Introduction

The MAC base VLAN allows users to create VLAN with MAC address. The MAC address can be the leading three or more bytes of the MAC address.

For example, 00:01:02 or 00:03:04:05 or 00:01:02:03:04:05.

When the Switch receives packets, it will compare MAC-based VLAN configures. If the SA is matched the MAC-based VLAN configures, the Switch replace the VLAN with user configured and them forward them.

For example:

Configurations: 00:01:02, VLAN=23, Priority=2.

The packets with SA=00:01:02:xx:xx:xx will be forwarded to VLAN 22 member ports.

Notices: The 802.1Q port base VLAN should be created first.

7.3.3.2. CLI Configuration

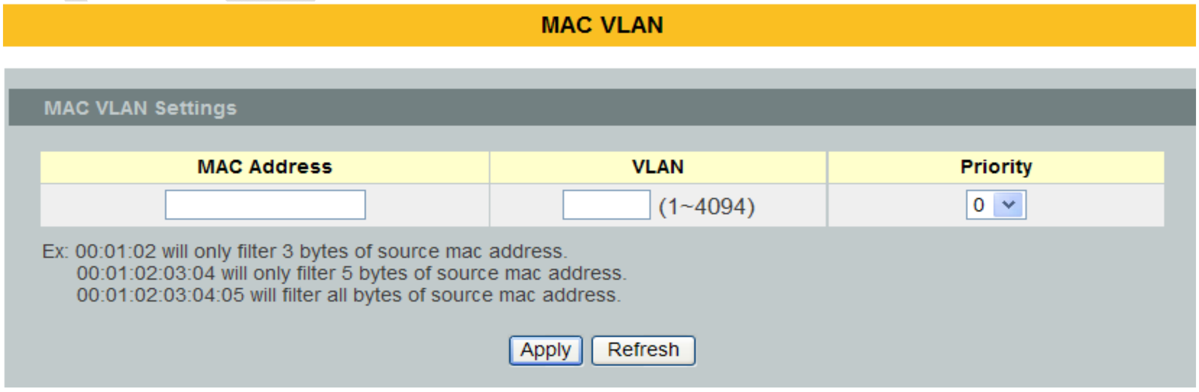
Node	Command	Description
enable	show mac-vlan	This command displays the all of the mac-vlan configurations.
configure	mac-vlan STRINGS vlan VLANID priority <0-7>	This command creates a mac-vlan entry with the leading three or more bytes of mac address and the VLAN and the priority.
configure	no mac-vlan entry STRINGS	This command deletes a mac-vlan entry.
configure	no mac-vlan all	This command deletes all of the mac-vlan entries.

Where the STRINGS is the leading three or more bytes of the mac address.

Example:

```
L2SWITCH(config)#mac-vlan 00:01:02:03:04vlan 111 priority 1
L2SWITCH(config)#mac-vlan 00:01:02:22:04vlan 121 priority 1
L2SWITCH(config)#mac-vlan 00:01:22:22:04:05 vlan 221 priority 1
```

7.3.3.3. Web Configuration

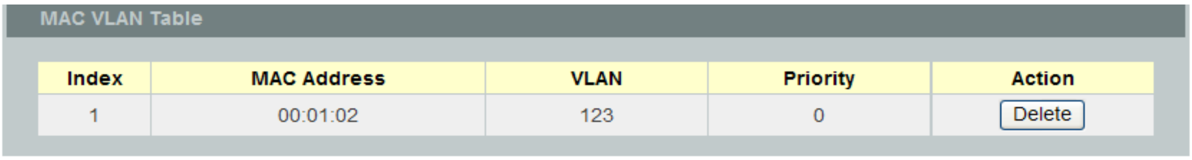


MAC VLAN

MAC VLAN Settings

MAC Address	VLAN	Priority
	(1~4094)	0

Ex: 00:01:02 will only filter 3 bytes of source mac address.
00:01:02:03:04 will only filter 5 bytes of source mac address.
00:01:02:03:04:05 will filter all bytes of source mac address.



MAC VLAN Table

Index	MAC Address	VLAN	Priority	Action
1	00:01:02	123	0	Delete

Parameter	Description
MAC Address	Configures the leading three or more bytes of the MAC address.
VLAN	Configures the VLAN.
Priority	Configures the 802.1Q priority.
Action	Click the “Delete” button to delete the protocol VLAN profile.

7.4. Link Layer Discovery Protocol (LLDP)

7.4.1. Introduction

The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station’s point of attachment to the IEEE 802 LAN required by those management entity or entities.

The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

Default Settings

The LLDP on the Switch is disabled.

Tx Interval : 30 seconds.
Tx Hold : 4 times.
Time To Live : 120 seconds.

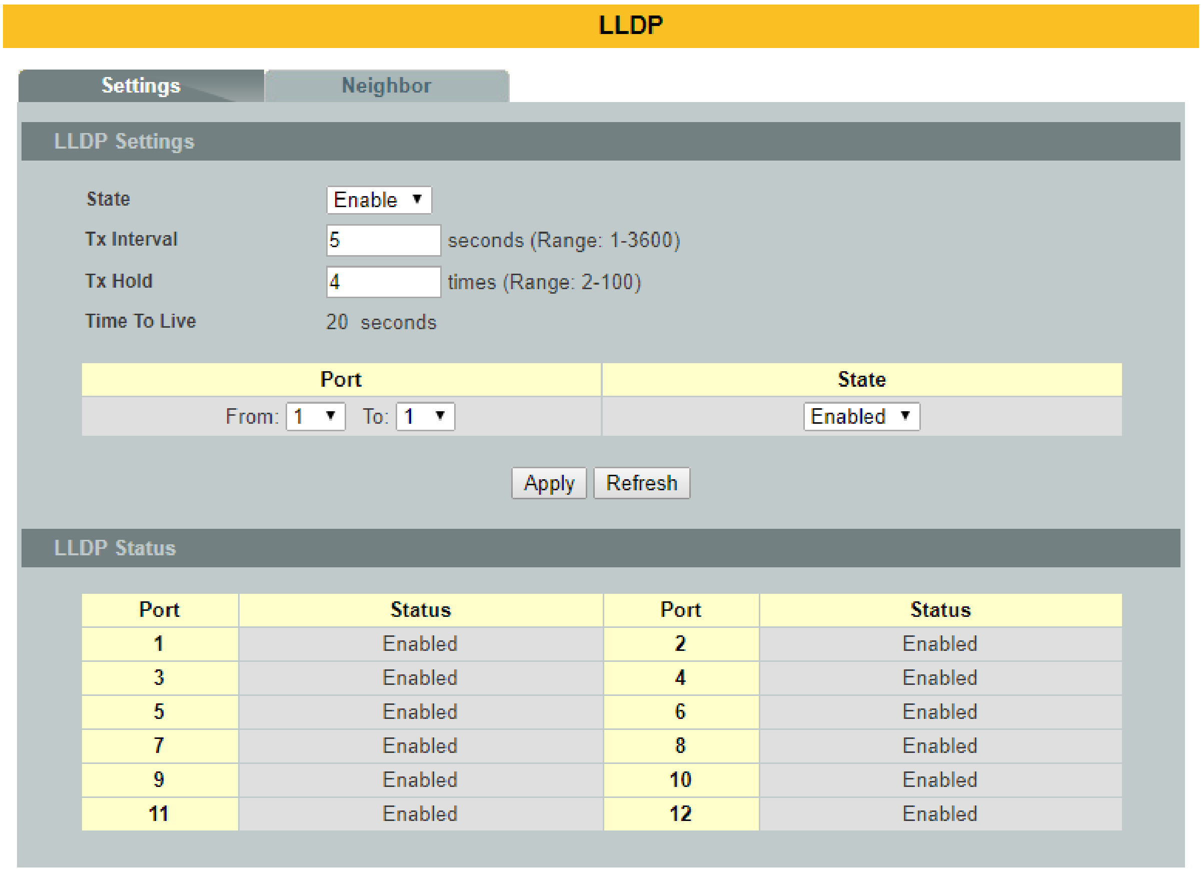
Port	Status	Port	Status
----	-------	----	-------
1	Enable	2	Enable
3	Enable	4	Enable
5	Enable	6	Enable
7	Enable	8	Enable
9	Enable	10	Enable
11	Enable	12	Enable

7.4.2. CLI Configuration

Node	Command	Description

enable	show lldp	This command displays the LLDP configurations.
enable	show lldp neighbor	This command displays all of the ports' neighbor information.
configure	lldp (disable|enable)	This command globally enables / disables the LLDP function on the Switch.
configure	lldp tx-interval	This command configures the interval to transmit the LLDP packets.
configure	lldp tx-hold	This command configures the tx-hold time which determines the TTL of the Switch's message. (TTL=tx-hold * tx-interval)
interface	lldp-agent (disable|enable|rx-only|tx-only)	This command configures the LLDP agent function. disable – Disable the LLDP on the specific port. enable – Transmit and Receive the LLDP packet on the specific port. tx-only – Transmit the LLDP packet on the specific port only. rx-only – Receive the LLDP packet on the specific port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	lldp-agent (disable|enable|rx-only|tx-only)	This command configures the LLDP agent function. disable – Disable the LLDP on the specific port. enable – Transmit and Receive the LLDP packet on the specific port. tx-only – Transmit the LLDP packet on the specific port only. rx-only – Receive the LLDP packet on the specific port.

7.4.3. Web Configuration



LLDP

LLDP Settings

State: Enable

Tx Interval: 5 seconds (Range: 1-3600)

Tx Hold: 4 times (Range: 2-100)

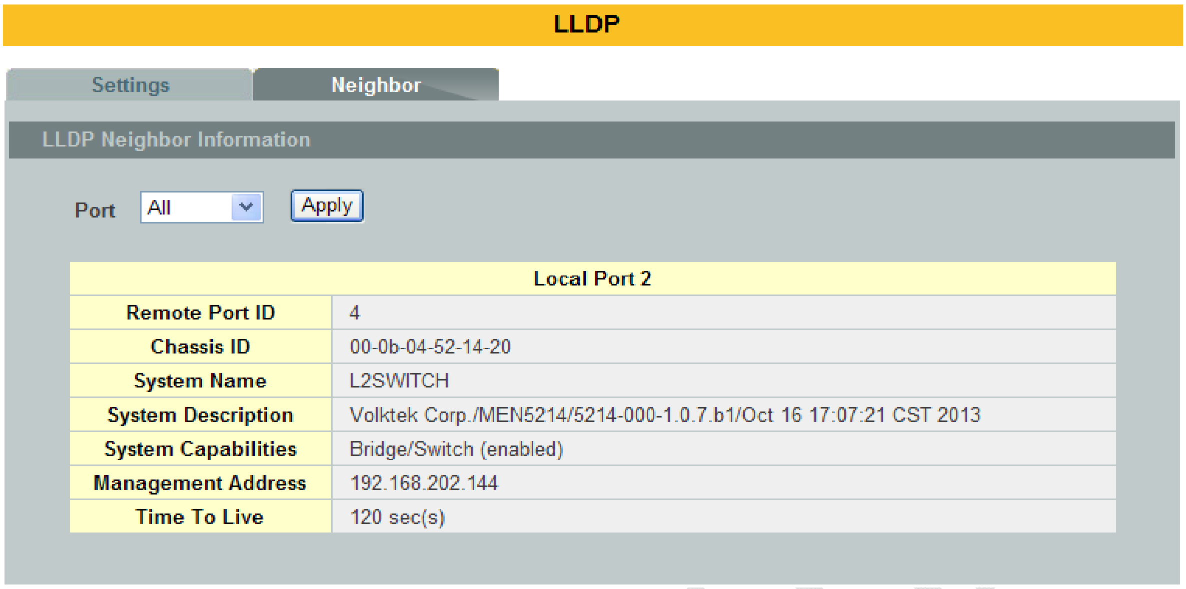
Time To Live: 20 seconds

Port	State
From: 1 To: 1	Enabled

LLDP Status

Port	Status	Port	Status
1	Enabled	2	Enabled
3	Enabled	4	Enabled
5	Enabled	6	Enabled
7	Enabled	8	Enabled
9	Enabled	10	Enabled
11	Enabled	12	Enabled

Parameter	Description
State	Globally enables / disables the LLDP on the Switch.
Tx Interval	Configures the interval to transmit the LLDP packets.
Tx Hold	Configures the tx-hold time which determines the TTL of the Switch's message. (TTL=tx-hold * tx-interval)
Time To Live	The hold time for the Switch's information.
Port	The port range which you want to configure.
State	Enables / disables the LLDP on these ports.
LLDP Status	
Port	The Port ID.
State	The LLDP state for the specific port.



LLDP

LLDP Neighbor Information

Port: All

Local Port 2	
Remote Port ID	4
Chassis ID	00-0b-04-52-14-20
System Name	L2SWITCH
System Description	Volktek Corp./MEN5214/5214-000-1.0.7.b1/Oct 16 17:07:21 CST 2013
System Capabilities	Bridge/Switch (enabled)
Management Address	192.168.202.144
Time To Live	120 sec(s)

Parameter	**Description**
Port	Select the port(s) which you want to display the port's neighbor information.
Local Port	The local port ID.
Remote Port ID	The connected port ID.
Chassis ID	The neighbor's chassis ID.
System Name	The neighbor's system name.
System Description	The neighbor's system description.
System Capabilities	The neighbor's capability.
Management Address	The neighbor's management address.
Time To Live	The hold time for the neighbor's information.

7.5. Loop Detection

7.5.1. Introduction

Loop detection is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

The loop detection function sends probe packets periodically to detect if the port connect to a network in loop state. The Switch shuts down a port if the Switch detects that probe packets loop back to the same port of the Switch.

Loop Recovery:
When the loop detection is enabled, the Switch will send one probe packets every two seconds and then listens this packet. If it receives the packet at the same port, the Switch will disable this port. After the time period, ***recovery time*,** the Switch will enable this port and do loop detection again.

The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop detection feature.

Default Settings

The default global Loop-Detection state is disabled.
The default Loop Detection Destination MAC is **00:0b:04:AA:AA:AB**
The default Port Loop-Detection state is disabled for all ports.
The default Port Loop-Detection status is unblocked for all ports.

```
The loop detection on the Switch is disabled.
Loop Detection Destination MAC=00:0b:04:aa:aa:ab
                      Recovery                                    Recovery
Port     State     Status     State     Time     Port     State     Status     State     Time
---- -------- -------   -------- ----     ---- -------- -------   -------- ----
  1     Disabled Normal     Enabled   1          2     Disabled Normal     Enabled   1
  3     Disabled Normal     Enabled   1          4     Disabled Normal     Enabled   1
  5     Disabled Normal     Enabled   1          6     Disabled Normal     Enabled   1
       .     .     .     .     .     .     .     .     .     .     .     .     .     .     .     .
```

7.5.2. CLI Configuration

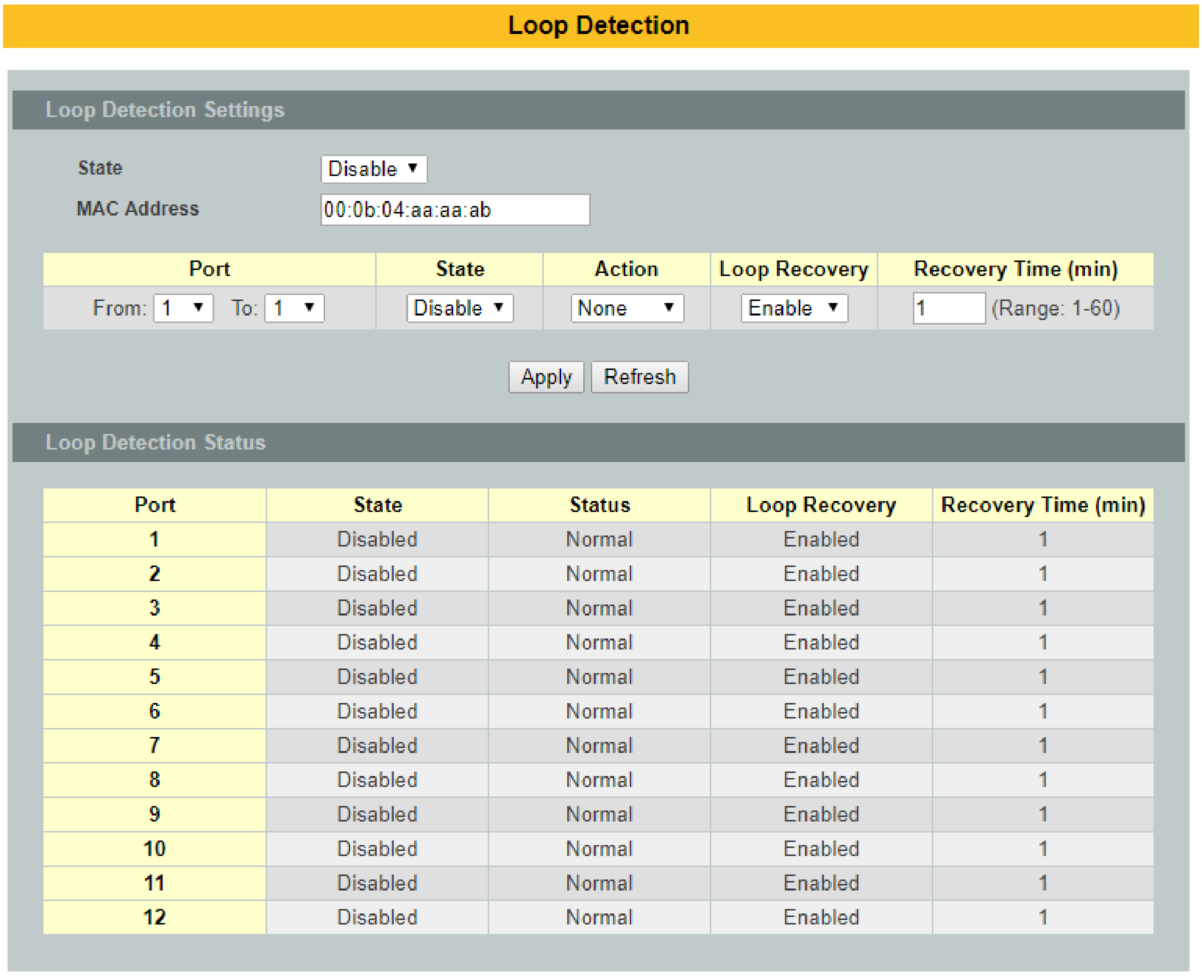
Node	Command	Description
enable	show loop-detection	This command displays the current loop detection configurations.
configure	loop-detection (disable | enable)	This command disables / enables the loop detection on the switch.
configure	loop-detection address MACADDR	This command configures the destination MAC for the loop detection special packets.
configure	no loop-detection address	This command configures the destination MAC to default (00:0b:04:AA:AA:AB).
interface	loop-detection (disable | enable)	This command disables / enables the loop detection on the port.
interface	no shutdown	This command enables the port. It can unblock port blocked by loop detection.
interface	loop-detection recovery (disable | enable)	This command enables / disables the recovery function on the port.
interface	loop-detection recovery time VALUE	This command configures the recovery period time.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	loop-detection (disable |	This command disables / enables the loop

	enable)	detection on the ports.
if-range	loop-detection recovery (disable | enable)	This command enables / disables the recovery function on the port.
if-range	loop-detection recovery time VALUE	This command configures the recovery period time.

Example:

```
L2SWITCH(config)#loop-detection enable
L2SWITCH(config)#interface 1/0/1
L2SWITCH(config-if)#loop-detection enable
```

7.5.3. Web Configuration



Loop Detection

Loop Detection Settings

State: Disable

MAC Address: 00:0b:04:aa:aa:ab

Port	State	Action	Loop Recovery	Recovery Time (min)
From: 1 To: 1	Disable	None	Enable	1 (Range: 1-60)

Loop Detection Status

Port	State	Status	Loop Recovery	Recovery Time (min)
1	Disabled	Normal	Enabled	1
2	Disabled	Normal	Enabled	1
3	Disabled	Normal	Enabled	1
4	Disabled	Normal	Enabled	1
5	Disabled	Normal	Enabled	1
6	Disabled	Normal	Enabled	1
7	Disabled	Normal	Enabled	1
8	Disabled	Normal	Enabled	1
9	Disabled	Normal	Enabled	1
10	Disabled	Normal	Enabled	1
11	Disabled	Normal	Enabled	1
12	Disabled	Normal	Enabled	1

Parameter	Description
State	Select this option to enable loop guard on the Switch.
MAC Address	Enter the destination MAC address the probe packets will be sent to. If the port receives these same packets the port will be shut down.
Port	Select a port on which to configure loop guard protection.

State	Select **Enable** to use the loop guard feature on the Switch.
Manual Recovery	You can unblock the port manually or select none to unblock itself after recovery time.
Recovery State	Specify the port needs to be recovered or kept blocking after loop detection
Recovery Time	Specify the recovery time in minutes that the Switch will wait before reactivating the port. This can be between 1 to 60 minutes.
Apply Refresh Loop Detection Status	Click **Apply** to save your changes to the Switch. Click **Refresh** to begin configuring this screen afresh.
Port	This field displays a port number.
State	This field displays if the loop guard feature is enabled.
Status	This field displays if the port is blocked.
Recovery state	This field displays if the loop recovery feature is enabled.
Recovery Time (min)	This field displays the recovery time for the loop recovery feature.

7.6. MRP

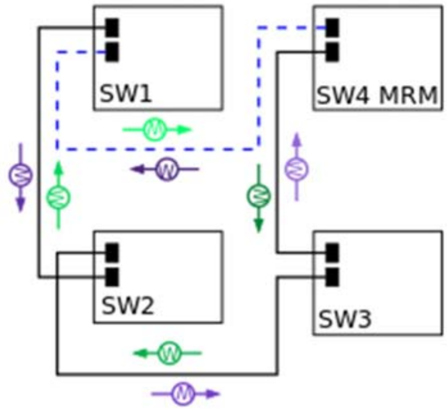
7.6.1. Introduction

Media Redundancy Protocol (MRP) is a data network protocol that allows rings of industrial ethernet switches to overcome any single failure with recovery time much faster than achievable with Spanning Tree Protocol. It is suitable to most Industrial Ethernet applications.

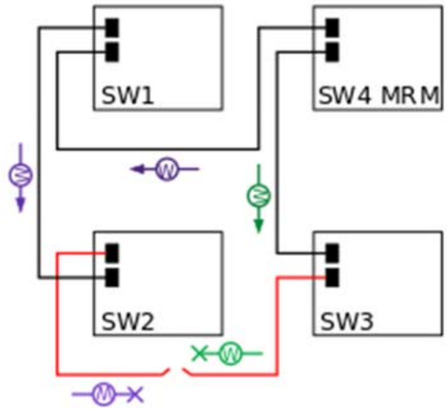
In an MRP ring, the ring manager is named Media Redundancy Manager (MRM), while ring clients are named Media Redundancy Clients (MRCs).

MRM and MRC ring ports supports three status: disabled, blocked, and forwarding. Disabled ring ports drops all the received frames. Blocked ring ports drop all the received frames except the MRP control frames. Forwarding ring ports forward all the received frames.

During normal operation, the network works in the Ring-Closed status. In this status, one of the MRM ring ports is blocked, while the other is forwarding. Conversely, both ring ports of all MRCs are forwarding. Loops are avoided because the physical ring topology is reduced to a logical stub topology.



In case of failure, the network works in the Ring-Open status. For instance, in case of failure of a link connecting two MRCs, both ring ports of the MRM are forwarding; the MRCs adjacent to the failure have a blocked and a forwarding ring port; the other MRCs have both ring ports forwarding. Also, in the Ring-Open status, the network logical topology is a stub.

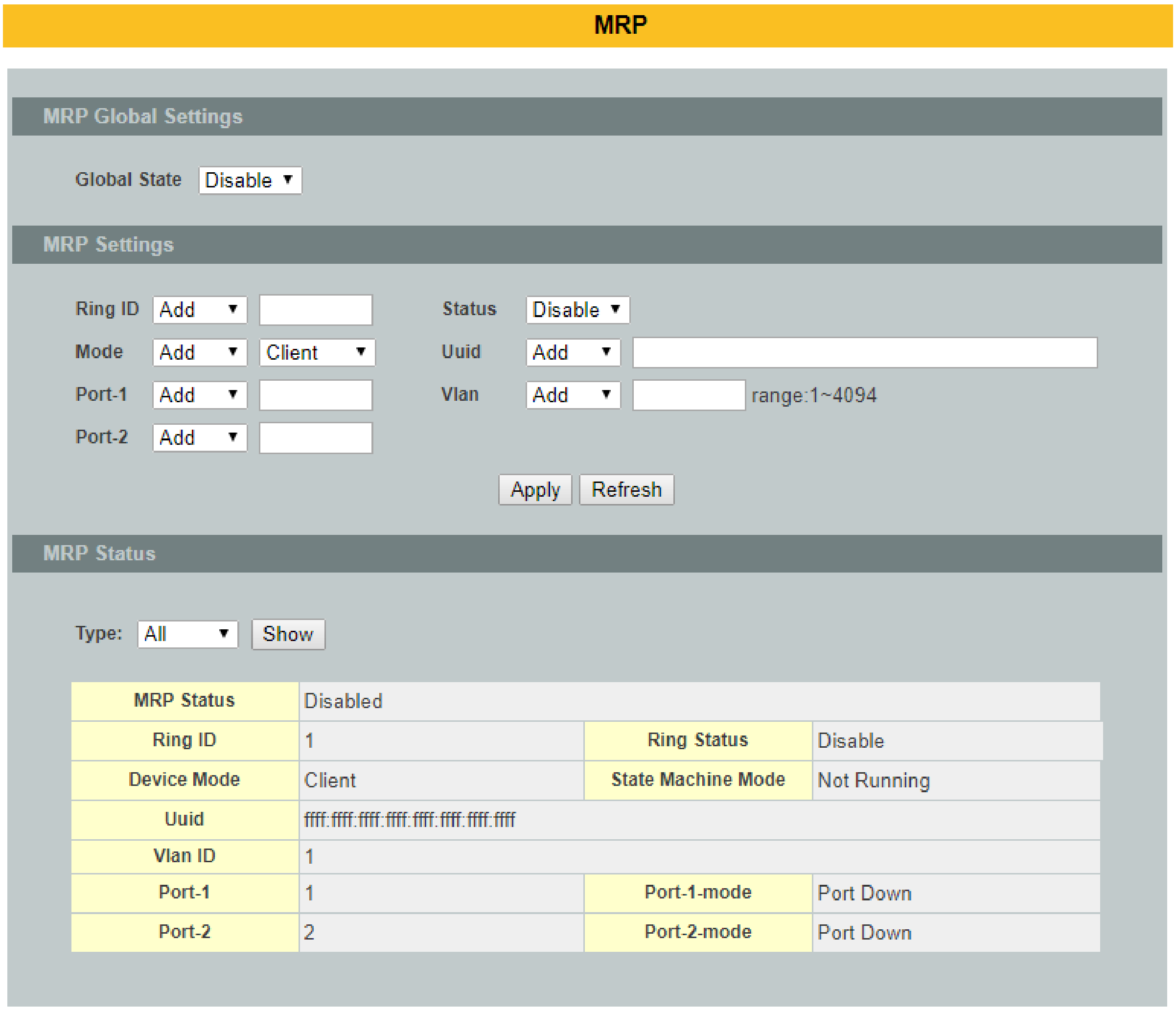


7.6.2. CLI configuration

Node	Command	Description
enable	show mrp information	This command displays the overall mrp's configured information and also global mrp settings
enable	show mrp ring-id [RING_ID]	This command displays the mrp information of the specific
configure	mrp enable	This command enables the media redundancy protocol on the switch.
configure	no mrp enable	This command disables media redundancy protocol on the switch.
configure	Mrp ring-id <1-4>	This command creates the particular ring with mentioned ID

configure-mrp	ring enable	This command enables the particular ring
configure-mrp	ring mode (client|manager)	This command configures the node to be either manager or client.
configure-mrp	ring port-1 <1-12>	This command configures the port-1 for the ring on the Switch.
configure-mrp	ring port-2 <1-12>	This command configures the port-2 for the ring on the Switch.
configure-mrp	ring vlan	This command configures on which VLAN this ring should be enabled.
configure-mrp	ring uuid	This command configures the universal unique identifier (UUID) for the ring. It's a string in hexadecimal format representing the ring to which this switch belongs to. ex: 1a1b:225c:ef34:5671:9bcd:a018:ba34:5679
configure-mrp	no ring enable	This command disables the particular ring
configure-mrp	no ring mode	This command removes the node mode.
configure-mrp	no ring port-1	This command removes the port-1 for the ring on the Switch.
configure-mrp	no ring port-2	This command removes the port-2 for the ring on the Switch.
configure-mrp	no ring vlan	This command removes the ring on that VLAN.
configure-mrp	no ring uuid	This command removes the universal unique identifier (UUID) for the ring.

7.6.3. WEB configuration



MRP

MRP Global Settings

Global State: Disable ▾

MRP Settings

Ring ID: Add ▾
Mode: Add ▾ Client ▾
Port-1: Add ▾
Port-2: Add ▾
Status: Disable ▾
Uuid: Add ▾
Vlan: Add ▾ range:1~4094

MRP Status

Type: All ▾

MRP Status	Disabled		
Ring ID	1	Ring Status	Disable
Device Mode	Client	State Machine Mode	Not Running
Uuid	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff		
Vlan ID	1		
Port-1	1	Port-1-mode	Port Down
Port-2	2	Port-2-mode	Port Down

Parameter	Description
MRP settings	
Global State	Enables/Disable the global Media Redundancy Protocol ring function
Ring ID	Configures the particular ring with mentioned ID
Mode	Configures the switch as either Client or Manager mode
Port-1	Configures the Port-1 (primary) port for the ring.
Port-2	Configures the Port-2 (secondary) port for the ring.
Status	Enable or disable the status of this particular ring.
UUID	Configures the universal unique identifier (UUID) for the ring. It’s a string in hexadecimal format representing the ring to which this

	switch belongs to. ex: 1a1b:225c:ef34:5671:9bcd:a018:ba34:5679
VLAN	Configures on which VLAN this ring should be enabled.
MRP Status	
Type	Which MRP ring status to be displayed.
MRP Status	The current state of the particular MRP ring.
Ring ID	ID number of the ring
Device Mode	Whether the switch is in Client or Manager mode.
Uuid	Assigned UUID is displayed here
Vlan ID	Shows in which VLAN this ring belongs to.
Port-1	The current Port-1 port.
Port-2	The current Port-2 port.
Ring Status	Current MRP ring status
State Machine Mode	Display whether the state machine is running or not
Port-1-mode	The current Port-1 port status.
Port-2-mode	The current Port-2 port status.

7.7. STP

7.7.1. Introduction

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a Switch to interact with other (R)STP compliant switches in your network to ensure that only one path exists between any two stations on the network.

The Switch supports Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) as defined in the following standards.

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol

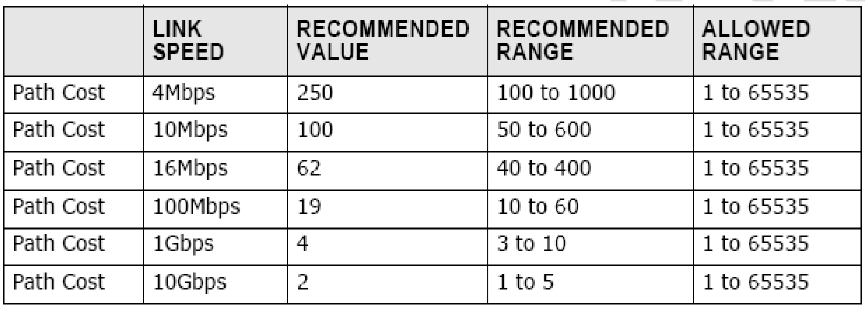
The Switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required

as the device that causes a topology change first notifies the root bridge and then the root bridge notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database.
In STP, the port states are Blocking, Listening, Learning, Forwarding.
In RSTP, the port states are Discarding, Learning, and Forwarding.

Note: In this document, “STP” refers to both STP and RSTP.

STP Terminology

- The root bridge is the base of the spanning tree.
- Path cost is the cost of transmitting a frame onto a LAN through that port. There commended cost is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.



	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

- On each bridge, the bridge communicates with the root through the root port. The root port is the port on this Switch with the lowest path cost to the root (the root path cost). If there is no root port, then this Switch has been accepted as the root bridge of the spanning tree network.
- For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

Forward Time (Forward Delay):

This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30seconds.

Max Age:

This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that age out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, anew root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.

Hello Time:

This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.

Path Cost:

Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge, the slower the media, the higher the cost.

How STP Works?

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed. Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

802.1D STP

The Spanning Tree Protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN. It is based on an algorithm invented by Radia Perlman while working for Digital Equipment Corporation. In the OSI model for computer networking, STP falls under the OSI layer-2. Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links. Bridge loops must be avoided because they result in flooding the network.

The Spanning Tree Protocol (STP) is defined in the IEEEStandard802.1D. As the name suggests, it creates a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches), and disables those links that are not part of the tree, leaving a single active path between any two network nodes.

STP switch port states

- Blocking - A port that would cause a switching loop, no user data is sent or received but it may go into forwarding mode if the other links in use were to fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state.
- Listening - The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state.
- Learning - While the port does not yet forward frames (packets) it does learn source addresses from frames received and adds them to the filtering database (switching

database)

- Forwarding - A port receiving and sending data, normal operation. STP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.
- Disabled - Not strictly part of STP, a network administrator can manually disable a port

802.1w RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of the Spanning Tree Protocol: Rapid Spanning Tree Protocol (RSTP), which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP. While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a second.

RSTP bridge port roles:

- Root - A forwarding port that is the best port from Non-root-bridge to Root-bridge
- Designated - A forwarding port for every LAN segment
- Alternate - An alternate path to the root bridge. This path is different than using the root port.
- Backup - A backup/redundant path to a segment where another bridge port already connects.
- Disabled - Not strictly part of STP, a network administrator can manually disable a port

Edge Port:

They are attached to a LAN that has no other bridges attached. These edge ports transition directly to the forwarding state. RSTP still continues to monitor the port for BPDUs in case a bridge is connected. RSTP can also be configured to automatically detect edge ports. As soon as the bridge detects a BPDU coming to an edge port, the port becomes a non-edge port.

Forward Delay:

The range is from 4 to 30 seconds. This is the maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding).

Transmission Limit:

This is used to configure the minimum interval between the transmissions of consecutive RSTP BPDUs. This function can only be enabled in RSTP mode. The range is from 1 to 10 seconds.

Hello Time:

Set the time at which the root switch transmits a configuration message. The range is from 1 to 10 seconds.

Bridge priority:

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will become the root device.

Port Priority:

Set the port priority in the switch. Low numeric value indicates a high priority. A port with lower priority is more likely to be blocked by STP if a network loop is detected. The valid value is from 0 to 240.

Path Cost:

The valid value is from 1 to 200000000. Higher cost paths are more likely to be blocked by STP if a network loop is detected.

BPDU Guard

This is a per port setting. If the port is enabled in BPDU guard and receive any BPDU, the port will be set to disable to avoid the error environments. User must enable the port by manual.

BPDU Filter

It is a feature to filter sending or receiving BPDUs on a switch port. If the port receives any BPDUs, the BPDUs will be dropped.

Notice:

If both of the BPDU filter and BPDU guard are enabled, the BPDU filter has the high priority.

Root Guard

The Root Guard feature forces an interface to become a designated port to prevent surrounding switches from becoming a root switch. In other words, Root Guard provides a way to enforce the root bridge placement in the network. The Root Guard feature prevents a Designated Port from becoming a Root Port. If a port on which the Root Guard feature receives a superior BPDU, it moves the port into a root-inconsistent state (effectively equal to a listening state), thus maintaining the current Root Bridge status. The port can be moved to forwarding state if no superior BPDU received by this port for three hello times.

Default Settings

STP/RSTP	: disabled.
STP/RSTP mode	: RSTP.
Forward Time	: 15 seconds.
Hello Time	: 2 seconds.
Maximum Age	: 20 seconds.
System Priority	: 32768.
Transmission Limit	: 3 seconds.
Per port STP state	: enabled.
Per port Priority	: 128.
Per port Edge port	: disabled.
Per port BPDU filter	: disabled.
Per port BPDU guard	: disabled.
Per port BPDU Root guard: disabled.	
Per port Path Cost	: depend on port link speed.

Example: Bandwidth ->STP Port Cost Value

10 Mbps	-> 100
100 Mbps	-> 19

1 Gbps -> 4
10 Gbps -> 2

7.7.2. CLI Configuration

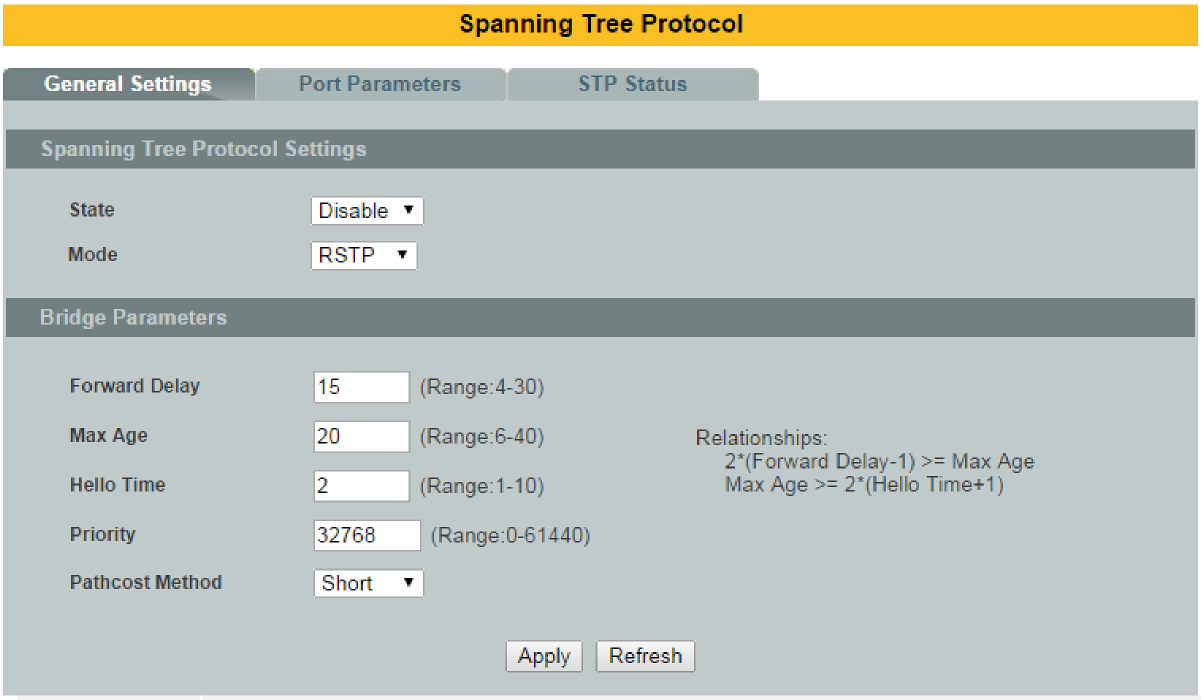
Node	Command	Description
enable	show spanning-tree active	This command displays the spanning tree information for only active port(s)
enable	show spanning-tree blocked ports	This command displays the spanning tree information for only blocked port(s)
enable	show spanning-tree port detail PORT_ID	This command displays the spanning tree information for the interface port.
enable	show spanning-tree statistics PORT_ID	This command displays the spanning tree information for the interface port.
enable	show spanning-tree summary	This command displays the summary of port states and configurations
enable	clear spanning-tree counters	This command clears spanning-tree statistics for all ports.
enable	clear spanning-tree counters PORT_ID	This command clears spanning-tree statistics for a specific port.
configure	spanning-tree (disable | enable)	This command disables / enables the spanning tree function for the system.
configure	spanning-tree algorithm-timer forward-time TIME max-age TIME hello-time TIME	This command configures the bridge times (forward-delay, max-age, hello-time).
configure	no spanning-tree algorithm-timer	This command configures the default values for forward-time & max-age& hello-time.
configure	spanning-tree forward-time<4-30>	This command configures the bridge forward delay time(sec).
configure	no spanning-tree forward-time	This command configures the default values for forward-time.
configure	spanning-tree hello-time <1-10>	This command configures the bridge hello time(sec).
configure	no spanning-tree hello-time	This command configures the default values for hello-time.
configure	spanning-tree max-age <6-40>	This command configures the bridge message max-age time(sec).
configure	no spanning-tree max-age	This command configures the default values for max-age time.
configure	spanning-tree mode (rstp|stp)	This command configures the spanning mode.
configure	spanning-tree pathcost method (short|long)	This command configures the path cost method.
configure	spanning-tree priority<0-61440>	This command configures the priority for the system.
configure	no spanning-tree priority	This command configures the default

		values for the system priority.
interface	spanning-tree(disable|enable)	This command configures enables/disables the STP function for the specific port.
interface	spanning-tree bpdufilter(disable|enable)	This command configures enables/disables the bpdu filter function for the specific port.
interface	spanning-tree bpduguard(disable|enable)	This command configures enables/disables the bpdu guard function for the specific port.
interface	spanning-tree rootguard (disable|enable)	This command enables/disables the BPDU Root guard port setting for the specific port.
interface	spanning-tree edge-port(disable|enable)	This command enables/disables the edge port setting for the specific port.
interface	spanning-tree cost VALUE	This command configures the cost for the specific port. Cost range: 16-bit based value range 1-65535, 32-bit based value range 1-200000000.
interface	no spanning-tree cost	This command configures the path cost to default for the specific port.
interface	spanning-tree port-priority<0-240>	This command configures the port priority for the specific port. Default: 128.
interface	no spanning-tree port-priority	This command configures the port priority to default for the specific port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	spanning-tree(disable|enable)	This command configures enables/disables the STP function for the specific port.
if-range	spanning-tree bpdufilter(disable|enable)	This command configures enables/disables the bpdu filter function for the specific port.
if-range	spanning-tree bpduguard(disable|enable)	This command configures enables/disables the bpdu guard function for the specific port.
if-range	spanning-tree rootguard (disable|enable)	This command enables/disables the BPDU Root guard port setting for the specific port.
if-range	spanning-tree edge-port(disable|enable)	This command enables/disables the edge port setting for the specific port.
if-range	spanning-tree cost VALUE	This command configures the cost for the specific port. Cost range:

		16-bit based value range 1-65535, 32-bit based value range 1-200000000.
if-range	no spanning-tree cost	This command configures the path cost to default for the specific port.
if-range	spanning-tree port-priority<0-240>	This command configures the port priority for the specific port. Default: 128.
if-range	no spanning-tree port-priority	This command configures the port priority to default for the specific port.

7.7.3. Web Configuration

General Settings



Spanning Tree Protocol

Spanning Tree Protocol Settings

State: Disable ▼

Mode: RSTP ▼

Bridge Parameters

Forward Delay: 15 (Range:4-30)

Max Age: 20 (Range:6-40)

Hello Time: 2 (Range:1-10)

Priority: 32768 (Range:0-61440)

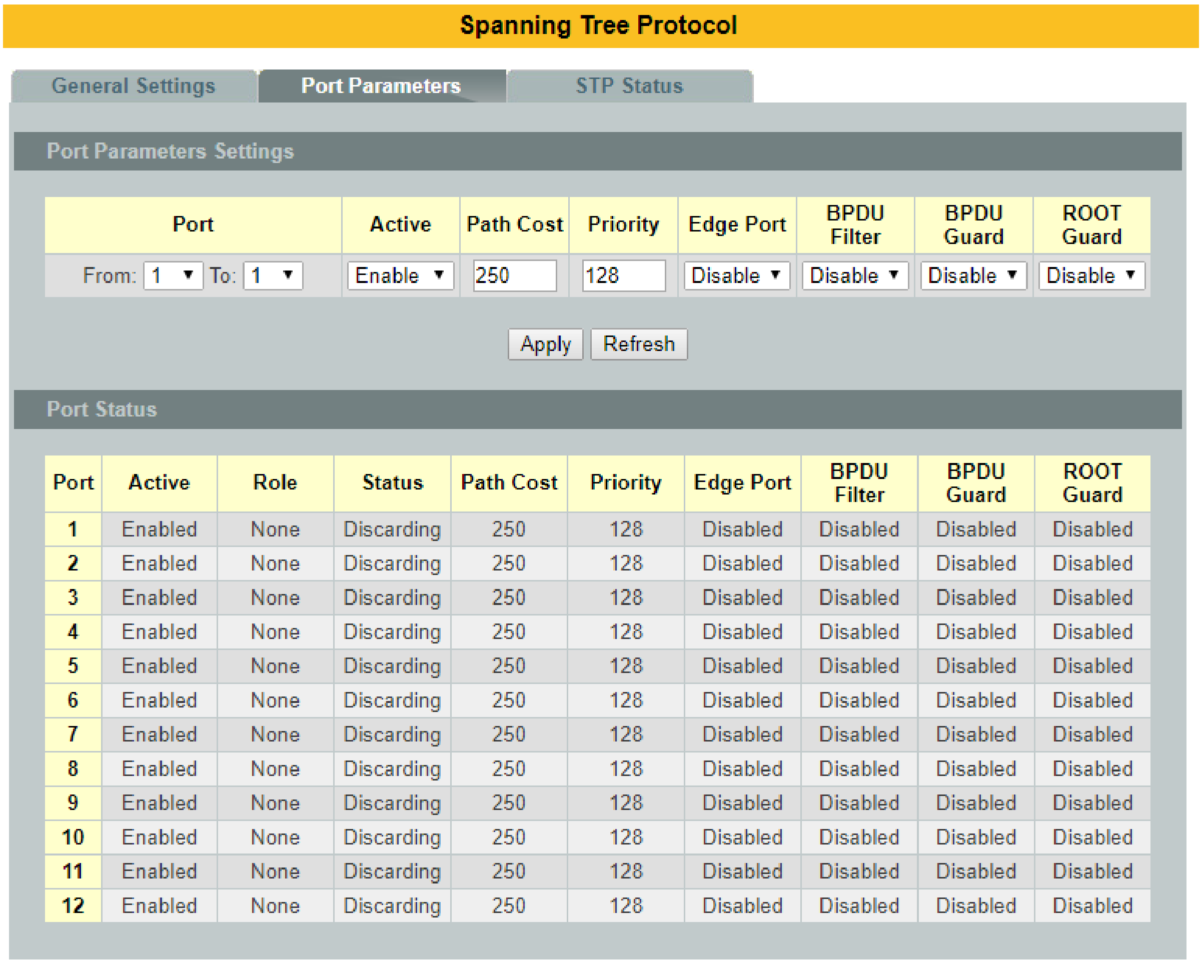
Pathcost Method: Short ▼

Relationships:
2*(Forward Delay-1) >= Max Age
Max Age >= 2*(Hello Time+1)

Parameter	Description
State	Select **Enabled** to use Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP).
Mode	Select to use either Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP).
Forward Time	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30seconds.
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports(except for designated ports) should receive BPDUs at regular intervals. Any port that age out STP information (provided in the last BPDU)becomes the designated port for the attached LAN. If it is a root port, anew root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Priority	Priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value)becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch.

	Enter a value from 0~61440. The lower the numeric value you assign, the higher the priority for this bridge. Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay.
Pathcost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost.

Port Parameters



Spanning Tree Protocol

Port Parameters Settings

Port	Active	Path Cost	Priority	Edge Port	BPDU Filter	BPDU Guard	ROOT Guard
From: 1 ▼ To: 1 ▼	Enable ▼	250	128	Disable ▼	Disable ▼	Disable ▼	Disable ▼

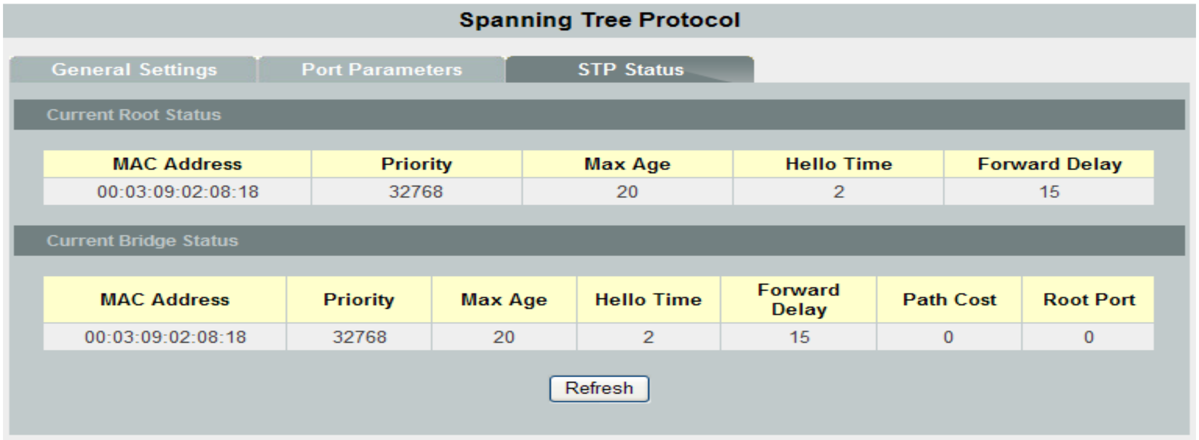
Port Status

Port	Active	Role	Status	Path Cost	Priority	Edge Port	BPDU Filter	BPDU Guard	ROOT Guard
1	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
2	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
3	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
4	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
5	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
6	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
7	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
8	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
9	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
10	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
11	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
12	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled

Parameter	Description
Port	Selects a port that you want to configure.
Active	Enables/Disables the spanning tree function for the specific port.
Path Cost	Configures the path cost for the specific port.
Priority	Configures the priority for the specific port.
EdgePort	Configures the port type for the specific port. Edge or Non-Edge.

BPDU Filter	Enables/Disables the BPDU filter function for the specific port.
BPDU Guard	Enables/Disables the BPDU guard function for the specific port.
ROOT Guard	Enables/Disables the BPDU root guard function for the specific port.
Port Status	
Active	The state of the STP function.
Role	The port role. Should be one of the Alternated / Designated / Root / Backup / None.
Status	The port's status. Should be one of the Discarding / Blocking / Listening / Learning / Forwarding / Disabled.
Path Cost	The port's path cost.
Priority	The port's priority.
Edge Port	The state of the edge function.
BPDU Filter	The state of the BPDU filter function.
BPDU Guard	The state of the BPDU guard function.
ROOT Guard	The state of the BPDU Root guard function.

STP Status



Spanning Tree Protocol

Current Root Status

MAC Address	Priority	Max Age	Hello Time	Forward Delay
00:03:09:02:08:18	32768	20	2	15

Current Bridge Status

MAC Address	Priority	Max Age	Hello Time	Forward Delay	Path Cost	Root Port
00:03:09:02:08:18	32768	20	2	15	0	0

Parameter	Description
Current Root Status	
MAC address	This is the MAC address of the root bridge.
Priority	**Root** refers to the base of the spanning tree (the root bridge). This field displays the root bridge's priority. This Switch may also be the root bridge.

MAX Age	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Hello Time	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Forward Delay	This is the time (in seconds) the root switch will wait before changing states.
Current Bridge Status	
MAC address	This is the MAC address of the current bridge.
Priority	Priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay.
MAX Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that age out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch.
Forward Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost.
Root Cost	This is the number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.

8. Security

8.1. ACL

8.1.1. Introduction

L2 Access control list (**ACL**) is a list of permissions attached to an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.

L2 ACL function allows user to configure a few rules to reject packets from the specific ingress ports or all ports. These rules will check the packets' source MAC address and destination MAC address. If packets match these rules, the system will do the actions "deny". "deny" means rejecting these packets.
The Action Resolution engine collects the information (action and metering results) from the hit entries: if more than one rule matches, the actions and meter/counters are taken from the policy associated with the matched rule with highest priority.

L2 ACL Support:

1. Filter a specific source MAC address.
   Command: *sourcemac host MACADDR*
2. Filter a specific destination MAC address.
   Command: *destination mac host MACADDR*
3. Filter a range of source MAC address.
   Command: *sourcemac MACADDR MACADDR*
   The second MACADDR is a mask, for example: ffff.ffff.0000
4. Filter a range of destination MAC address.
   Command: *destination macMACADDR MACADDR*
   The second MACADDR is a mask, for example: ffff.ffff.0000

L3 ACL Support:

1. Filter a specific source IP address.
   Command: *source ip host IPADDR*
2. Filter a specific destination IP address.
   Command: *destination ip host IPADDR*
3. Filter a range of source IP address.
   Command: *source ip IPADDRIPADDR*
   The second IPADDR is a mask, for example: 255.255.0.0
4. Filter a range of destination IP address.
   Command: *destination ip IPADDRIPADDR*

L4 ACL Support:

1. Filter a UDP/TCP source port.
2. Filter a UDP/TCP destination port.

Default Settings

Maximum profile	: 64.
Maximum profile name length	: 16.

Notices

The ACL name should be the combination of the digit or the alphabet.

8.1.2. CLI Configuration

Node	Command	Description
enable	show access-list	This command displays all of the access control profiles.
configure	access-list STRING	This command creates a new access control profile. Where the STRING is the profile name.
configure	no access-list STRING	This command deletes an access control profile.
acl	show	This command displays the current access control profile.
acl	action (disable|drop|permit)	This command actives this profile. disable – disable the profile. drop – If packets match the profile, the packets will be dropped. permit – If packets match the profile, the packets will be forwarded.
acl	destination mac hostMACADDR	This command configures the destination MAC and mask for the profile.
acl	destination mac MACADDR MACADDR	This command configures the destination MAC and mask for the profile.
acl	destination mac MACADDR MACADDR	This command configures the destination MAC and mask for the profile. The second MACADDR parameter is the mask for the profile.
acl	no destination mac	This command removes the destination MAC from the profile.
acl	ethertype STRING	This command configures the ether type for the profile. Where the STRING is a hex-decimal value. e.g.: 08AA.
acl	no ethertype	This command removes the limitation of the ether type from the profile.
acl	source mac host MACADDR	This command configures the source MAC and mask for the profile.
acl	source mac MACADDR MACADDR	This command configures the source AMC and mask for the profile.
acl	no source mac	This command removes the source MAC and mask from the profile.
acl	source ip host IPADDR	This command configures the source IP address for the profile.
acl	source ip IPADDR IPMASK	This command configures the source IP address and mask for the profile.
acl	no source ip	This command removes the source IP address from the

		profile.
acl	destination ip host IPADDR	This command configures a specific destination IP address for the profile.
acl	destination ip IPADDR IPMASK	This command configures the destination IP address and mask for the profile.
acl	no destination ip	This command removes the destination IP address from the profile.
acl	l4-source-port IPADDR	This command configures UDP/TCP source port for the profile.
acl	no l4-source-port IPADDR	This command removes the UDP/TCP source port from the profile.
acl	L4-destination-port PORT	This command configures the UDP/TCP destination port for the profile.
acl	no l4-destination-port	This command removes the UDP/TCP destination port from the profile.
acl	vlan VLANID	This command configures the VLAN for the profile.
acl	no vlan	This command removes the limitation of the VLAN from the profile.
acl	source interface PORT_ID	This command configures the source interface for the profile.
acl	no source interface PORT_ID	This command removes the source interface from the profile.

Where the MAC mask allows users to filter a range of MAC in the packets' source MAC or destination MAC.
For example:

```
source mac 00:01:02:03:04:05 ff:ff:ff:ff:00
```

➔ The command will filter source MAC range from 00:01:02:03:00:00 to 00:01:02:03:ff:ff

Where the IPMASK mask allows users to filter a range of IP in the packets' source IP or destination IP.
For example:

```
source ip 172.20.1.1 255.255.0.0
```

➔ The command will filter source IP range from 172.20.0.0 to 172.20.255.255

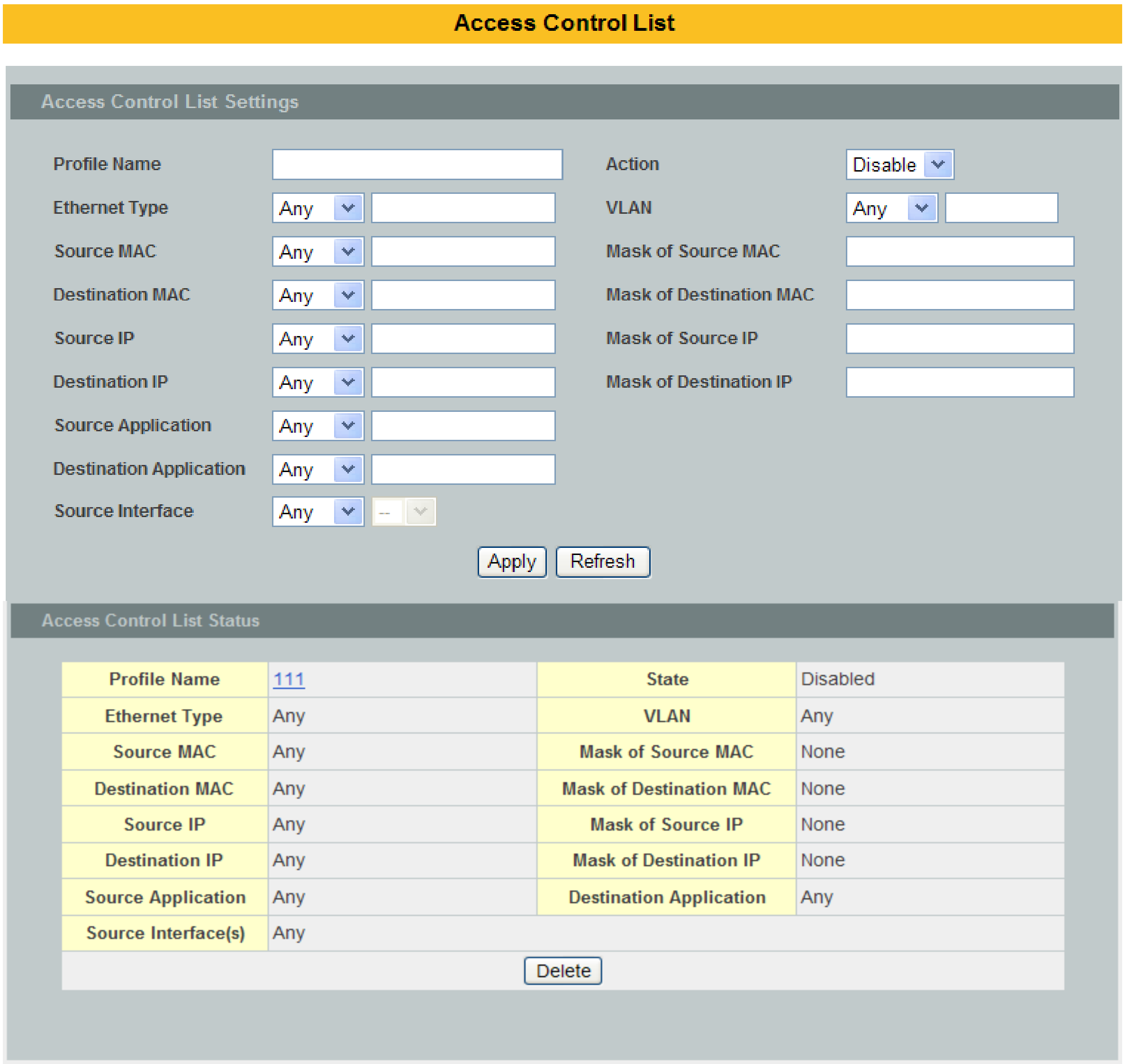
Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#access-list 111
L2SWITCH(config-acl)#vlan 2
L2SWITCH(config-acl)#source interface 1
L2SWITCH(config-acl)#show
    Profile Name: 111
    Activate: disabled
    VLAN: 2
    Source Interface: 1
```

Destination MAC Address: any
Source MAC Address: any
Ethernet Type: any
Source IP Address: any
Destination IP Address: any
Source Application: any
Destination Application: any

Note: Any: Don't care.

8.1.3. Web Configuration



Access Control List

Access Control List Settings

Profile Name		Action	Disable
Ethernet Type	Any	VLAN	Any
Source MAC	Any	Mask of Source MAC	
Destination MAC	Any	Mask of Destination MAC	
Source IP	Any	Mask of Source IP	
Destination IP	Any	Mask of Destination IP	
Source Application	Any		
Destination Application	Any		
Source Interface	Any --		

Access Control List Status

Profile Name	111	State	Disabled
Ethernet Type	Any	VLAN	Any
Source MAC	Any	Mask of Source MAC	None
Destination MAC	Any	Mask of Destination MAC	None
Source IP	Any	Mask of Source IP	None
Destination IP	Any	Mask of Destination IP	None
Source Application	Any	Destination Application	Any
Source Interface(s)	Any		

Parameter	Description
Profile Name	The access control profile name.

State	Disables / Drop / Permits the access control on the Switch.
Ethernet Type	Configures the Ethernet type of the packets that you want to filter.
VLAN	Configures the VLAN of the packets that you want to filter.
Source MAC	Configures the source MAC of the packets that you want to filter.
Mask of Source MAC	Configures the bitmap mask of the source MAC of the packets that you want to filter. If the Source MAC field has been configured and this field is empty, it means the profile will filter the one MAC configured in Source MAC field.
Destination MAC	Configures the destination MAC of the packets that you want to filter.
Mask of Destination MAC	Configures the bitmap mask of the destination MAC of the packets that you want to filter. If the Destination MAC field has been configured and this field is empty, it means the profile will filter the one MAC configured in Destination MAC field.
Source IP	Configures the source IP of the packets that you want to filter.
Mask of Source IP	Configures the bitmap mask of the source IP of the packets that you want to filter. If the Source IP field has been configured and this field is empty, it means the profile will filter the one IP configured in Source IP field.
Destination IP	Configures the destination IP of the packets that you want to filter.
Mask of Destination IP	Configures the bitmap mask of the destination IP of the packets that you want to filter. If the Destination IP field has been configured and this field is empty, it means the profile will filter the one IP configured in Destination IP field.
Source Application	Configures the source UDP/TCP ports of the packets that you want to filter.
Destination Application	Configures the destination UDP/TCP ports of the packets that you want to filter.
Source Interface(s)	Configures one or a rage of the source interfaces of the packets that you want to filter.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

9. Monitor

9.1. Alarm

9.1.1. Introduction

The feature displays if there are any abnormal situation need process immediately.

Note: The Alarm DIP Switch allow users to configure if send alarm message when the corresponding event occurs.

For Example:

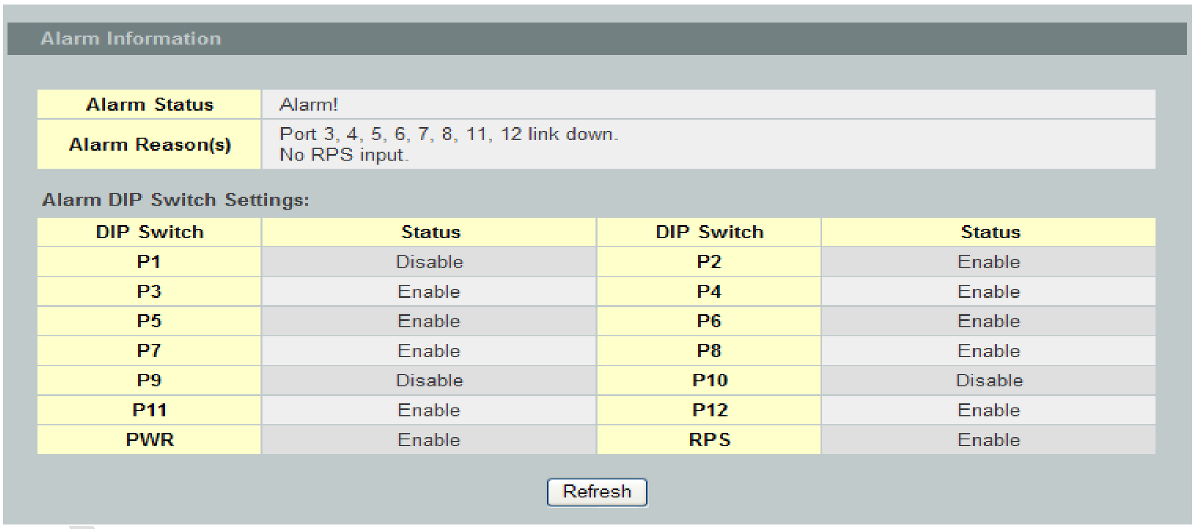
P1: ON, The Switch will send alarm message when port 1 is link down.
PWR: ON, The Switch will send alarm message when the main power supply disconnect.
RPS: ON, The Switch will send alarm message when the redundant power supply disconnect.

9.1.2. CLI Configuration

Node	Command	Description
enable	show alarm-info	This command displays alarm information.

9.1.3. Web Configuration

Alarm Information



Alarm Information

Alarm Status	Alarm!
Alarm Reason(s)	Port 3, 4, 5, 6, 7, 8, 11, 12 link down. No RPS input.

Alarm DIP Switch Settings:

DIP Switch	Status	DIP Switch	Status
P1	Disable	P2	Enable
P3	Enable	P4	Enable
P5	Enable	P6	Enable
P7	Enable	P8	Enable
P9	Disable	P10	Disable
P11	Enable	P12	Enable
PWR	Enable	RPS	Enable

Parameter	Description
Alarm Information	
Alarm Status	This field indicates if there is any alarm events.
Alarm Reason(s)	This field displays all of the detail alarm events.
Alarm DIP Switch Settings	
DIP Switch	The field displays the DIP Switch name.
Status	The field indicates the DIP Switch current status.

9.2. Hardware Information

9.2.1. Introduction

The feature displays some hardware information to monitor the system to guarantee the network correctly.

A. Displays the board's and CPU's and MAC chip's temperature.
B. Displays the 1.0V and 2.5V and 3.3V input status.

9.2.2. CLI Configuration

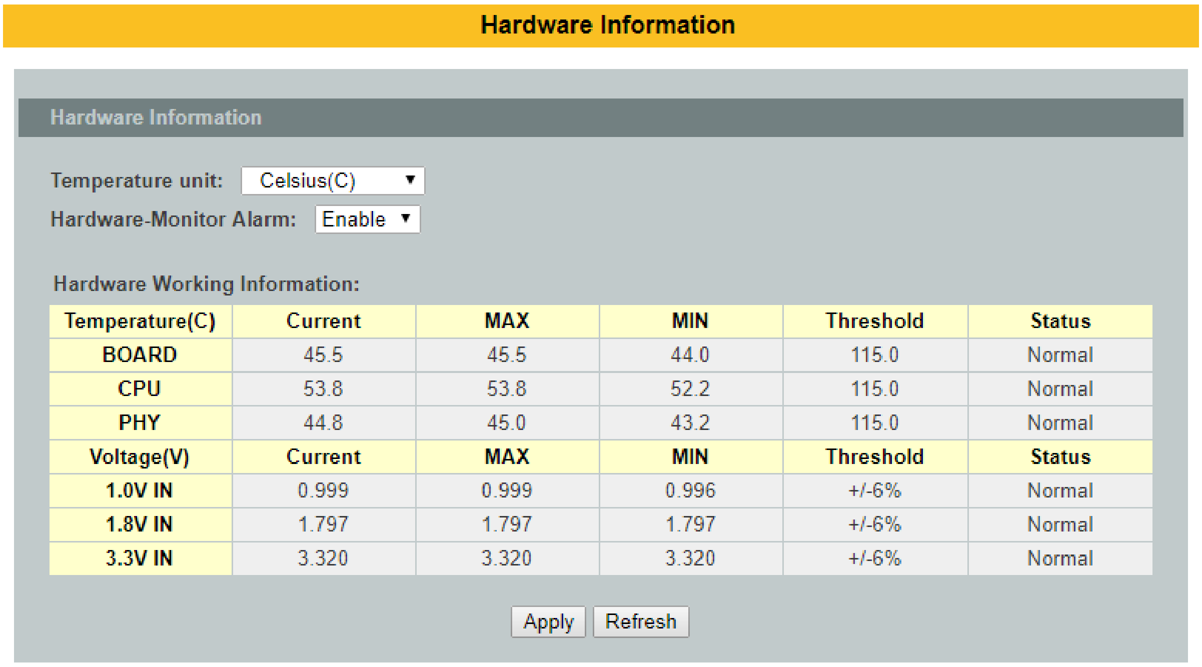
Node	Command	Description
enable	show hardware-monitor (C|F)	This command displays hardware working information.

Example:

```
L2SWITCH#show hardware-monitor C
Hardware Working Information:
Temperature(C)   Current    MAX     MIN     Threshold   Status
--------------   ---------  ------- --------  -----------  --------
   BOARD          41.2       41.8    30.8      80.0       Normal
   CPU          64.0       64.2    37.5      80.0      Normal
   PHY          49.5       49.5    31.0      80.0      Normal

  Voltage(V)     Current     MAX     MIN     Threshold    Status
--------------   ---------  ------- --------  -----------  --------
   1.0V IN       0.993     1.005    0.984     +/-5%       Normal
   1.8V IN       1.829     1.829    1.813     +/-5%       Normal
   3.3V IN       3.333     3.333    3.333     +/-5%       Normal
```

9.2.3. Web Configuration



Hardware Information

Hardware Information

Temperature unit: Celsius(C)

Hardware-Monitor Alarm: Enable

Hardware Working Information:

Temperature(C)	Current	MAX	MIN	Threshold	Status
BOARD	45.5	45.5	44.0	115.0	Normal
CPU	53.8	53.8	52.2	115.0	Normal
PHY	44.8	45.0	43.2	115.0	Normal
Voltage(V)	Current	MAX	MIN	Threshold	Status
1.0V IN	0.999	0.999	0.996	+/-6%	Normal
1.8V IN	1.797	1.797	1.797	+/-6%	Normal
3.3V IN	3.320	3.320	3.320	+/-6%	Normal

Parameter	Description
Hardware Information	
Temperature unit	This field allows you to select unit in Celsius (C) or Fahrenheit (F)
Hardware monitor alarm	This field allows to enable/disable the hardware-Monitor alarm to be reported or not
Hardware Working Information	
Temperature	The field displays the temperature information of board, CPU and PHY
Voltage	The field indicates the voltage level status.

9.3. Port Statistics

9.3.1. Introduction

This feature helps users to monitor the ports' statistics, to display the link up ports' traffic utilization only.

9.3.2. CLI Configuration

Node	Command	Description
enable	show port-statistics	This command displays the link up ports' statistics.

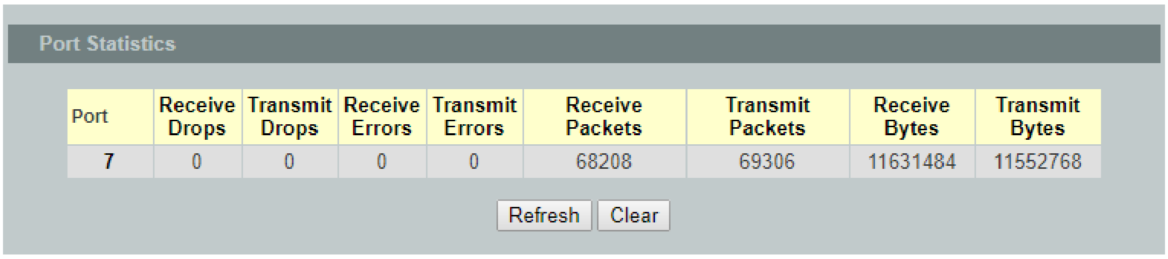
Example:

```
L2SWITCH#show port-statistics

                Packets                 Bytes              Errors              Drops
Port        Rx       Tx            Rx        Tx        Rx        Tx        Rx        Tx
----    -------- --------   -------- --------  -------- --------  -------- --------
 7       1154       2           108519    1188      0          0          0          0
```

9.3.3. Web Configuration

Port Statistics



Port Statistics

Port	Receive Drops	Transmit Drops	Receive Errors	Transmit Errors	Receive Packets	Transmit Packets	Receive Bytes	Transmit Bytes
7	0	0	0	0	68208	69306	11631484	11552768

Parameter	Description
Port	Select a port or a range of ports to display their statistics.
Receive Drops	The field displays the received drop count.
Transmit Drops	The field displays the transmitted drop count.
Receive Errors	The field displays the received error count.

Transmit Errors	The field displays the transmitted error count.
Receive Packets	The field displays the received packet count.
Transmit Packets	The field displays the transmitted packet count.
Receive Bytes	The field displays the received byte count.
Transmit Bytes	The field displays the transmitted byte count.
Refresh	Click this button to refresh the screen quickly.

9.4. Port Utilization

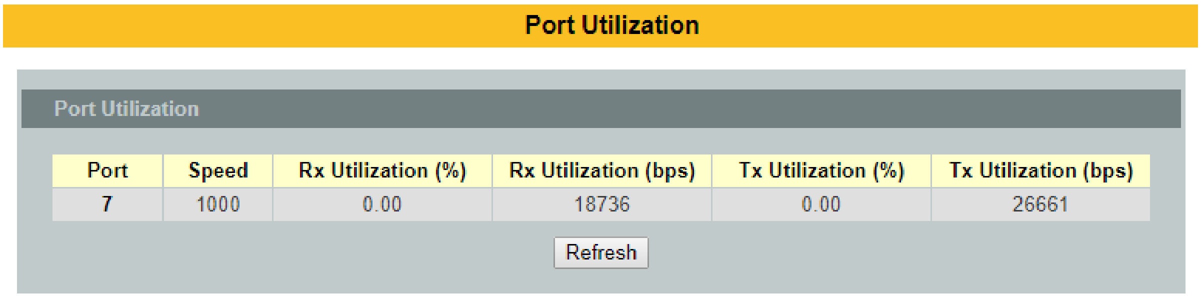
9.4.1. Introduction

This feature helps users to monitor the ports' traffic utilization, to display the link up ports' traffic utilization only.

9.4.2. CLI Configuration

Node	Command	Description
enable	show port-utilization	This command displays the link up ports' traffic utilization.

9.4.3. Web Configuration



Port Utilization

Port Utilization

Port	Speed	Rx Utilization (%)	Rx Utilization (bps)	Tx Utilization (%)	Tx Utilization (bps)
7	1000	0.00	18736	0.00	26661

Parameter	Description
Port	Select a port or a range of ports to display their RMON statistics.
Speed	The current port speed.
Rx Utilization (%)	The port receiving traffic utilization in percentage
Rx Utilization (bps)	The port receiving traffic utilization in bits per second
Tx Utilization (%)	The port transmitting traffic utilization in percentage
Tx Utilization (bps)	The port transmitting traffic utilization in bits per second
Refresh	Click this button to refresh the screen quickly.

9.5. RMON Statistics

9.5.1. Introduction

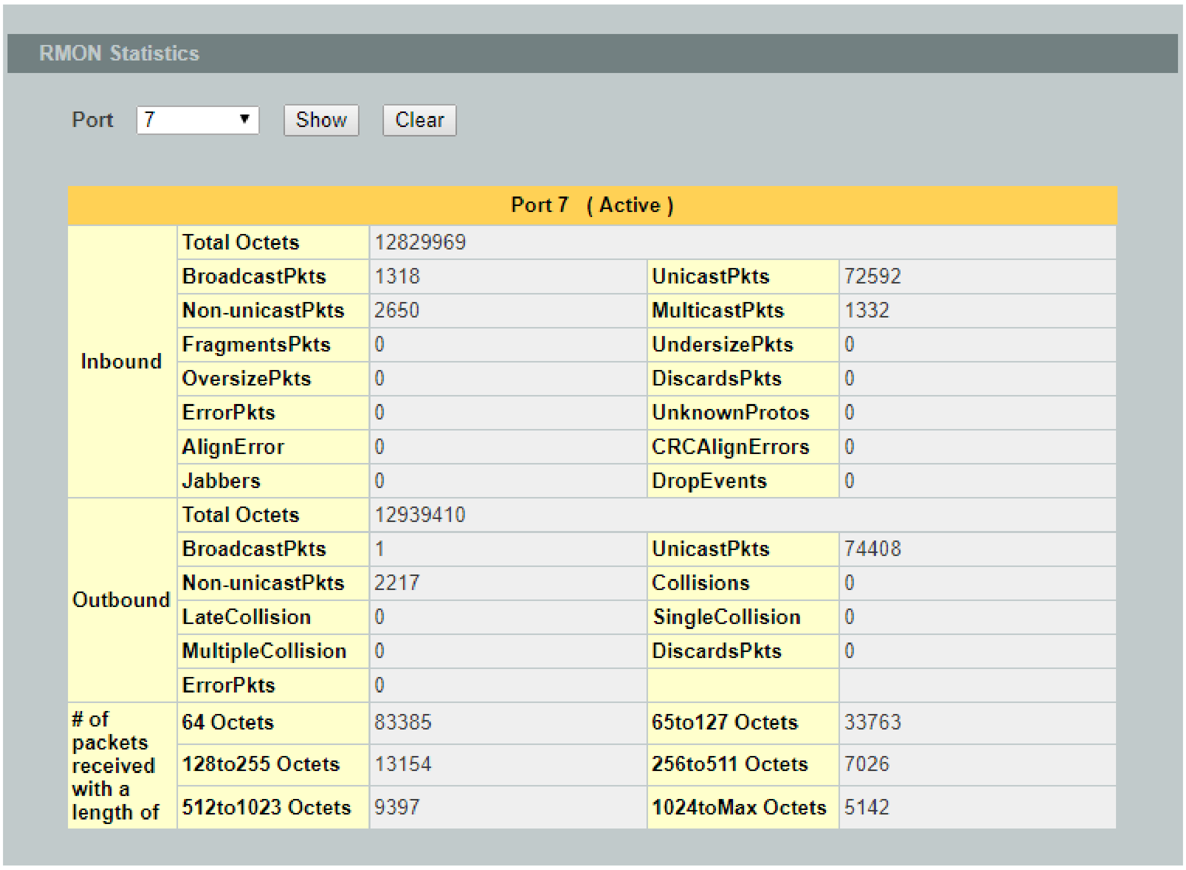
This feature helps users to monitor or clear the port's RMON statistics.

9.5.2. CLI Configuration

Node	Command	Description
enable	show rmon statistics	This command displays the RMON statistics.
configure	clear rmon statistics [IFNAME]	This command clears one port's or all ports' RMON statistics.

9.5.3. Web Configuration

RMON Statistics



Port 7

Port 7 (Active)				
Inbound	Total Octets	12829969		
	BroadcastPkts	1318	UnicastPkts	72592
	Non-unicastPkts	2650	MulticastPkts	1332
	FragmentsPkts	0	UndersizePkts	0
	OversizePkts	0	DiscardsPkts	0
	ErrorPkts	0	UnknownProtos	0
	AlignError	0	CRCAlignErrors	0
	Jabbers	0	DropEvents	0
Outbound	Total Octets	12939410		
	BroadcastPkts	1	UnicastPkts	74408
	Non-unicastPkts	2217	Collisions	0
	LateCollision	0	SingleCollision	0
	MultipleCollision	0	DiscardsPkts	0
	ErrorPkts	0		
# of packets received with a length of	64 Octets	83385	65to127 Octets	33763
	128to255 Octets	13154	256to511 Octets	7026
	512to1023 Octets	9397	1024toMax Octets	5142

Parameter	Description
Port	Select a port or a range of ports to display their RMON statistics.
Show	Show them.
Clear	Clear the RMON statistics for the port or a range of ports.

9.6. SFP Information

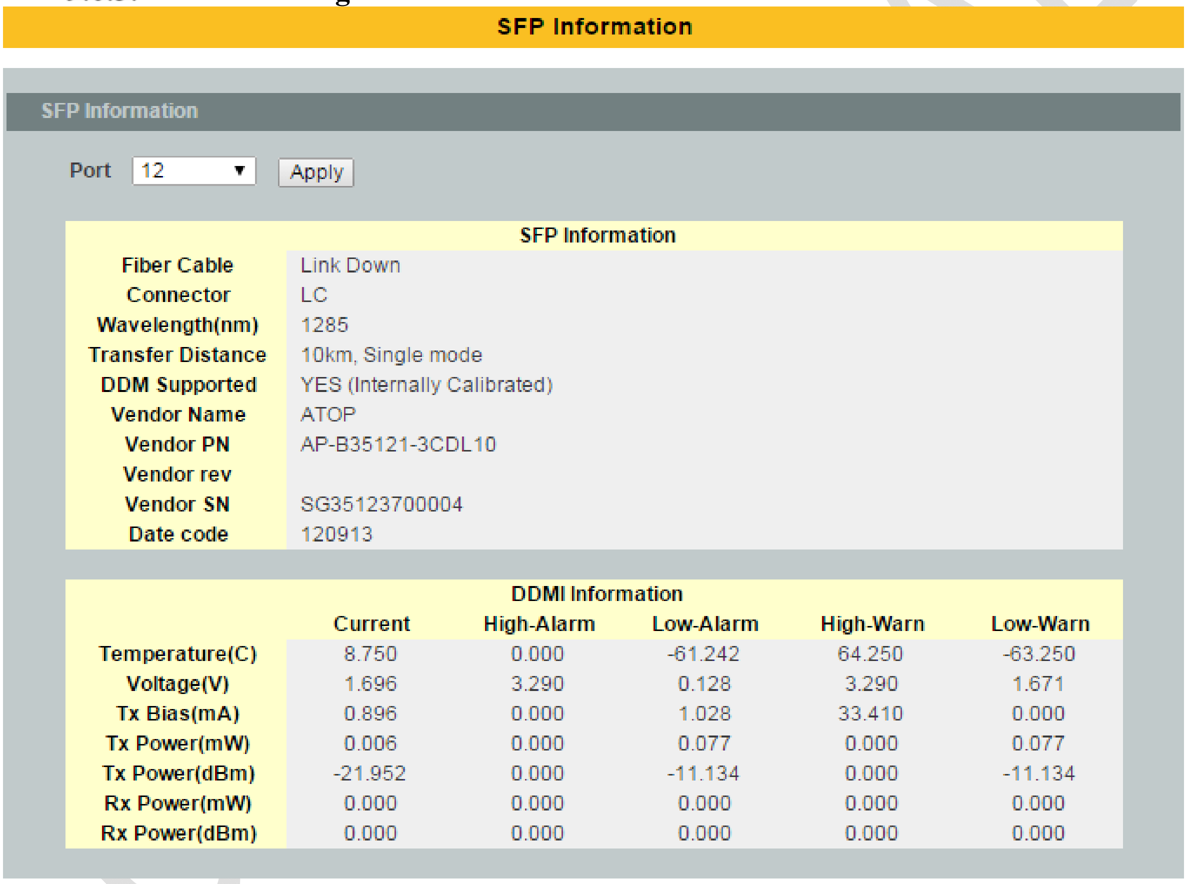
9.6.1. Introduction

The SFP information allows user to know the SFP module’s information, such as vendor name, connector type, revision, serial number, manufacture date, and to know the DDMI information if the SFP modules have supported the DDMI function.

9.6.2. CLI Configuration

Node	Command	Description
enable	show sfp info port PORT_ID	This command displays the SFP information.
enable	show sfp ddmi port PORT_ID	This command displays the SFP DDMI status.

9.6.3. Web Configuration



SFP Information

SFP Information

Port 12 ▼ Apply

SFP Information	
Fiber Cable	Link Down
Connector	LC
Wavelength(nm)	1285
Transfer Distance	10km, Single mode
DDM Supported	YES (Internally Calibrated)
Vendor Name	ATOP
Vendor PN	AP-B35121-3CDL10
Vendor rev	
Vendor SN	SG35123700004
Date code	120913

DDMI Information

	Current	High-Alarm	Low-Alarm	High-Warn	Low-Warn
Temperature(C)	8.750	0.000	-61.242	64.250	-63.250
Voltage(V)	1.696	3.290	0.128	3.290	1.671
Tx Bias(mA)	0.896	0.000	1.028	33.410	0.000
Tx Power(mW)	0.006	0.000	0.077	0.000	0.077
Tx Power(dBm)	-21.952	0.000	-11.134	0.000	-11.134
Rx Power(mW)	0.000	0.000	0.000	0.000	0.000
Rx Power(dBm)	0.000	0.000	0.000	0.000	0.000

Parameter	Description
Port	Select a port number to configure.
Apply	Click Apply to display the SFP information.
Fiber Cable	To indicate if the fiber cable is connected.
Connector	Code of optical connector type.
Vendor Name	SFP vendor name.
Vendor PN	Part Number.
Vendor rev	Revision level for part number.

Vendor SN	Serial number (ASCII).
Date Code	Manufacturing date code.

Notice: If the fiber cable is not connected, the Rx Power fields are not available.

9.7. Traffic Monitor

9.7.1. Introduction

The function can be enabled/disabled on a specific port or globally be enabled disabled on the Switch.

The function will monitor the broadcast / multicast / broadcast and multicast packets rate. If the packet rate is over the user's specification, the port will be blocked. And if the recovery function is enabled, the port will be enabled after recovery time.

Default Settings

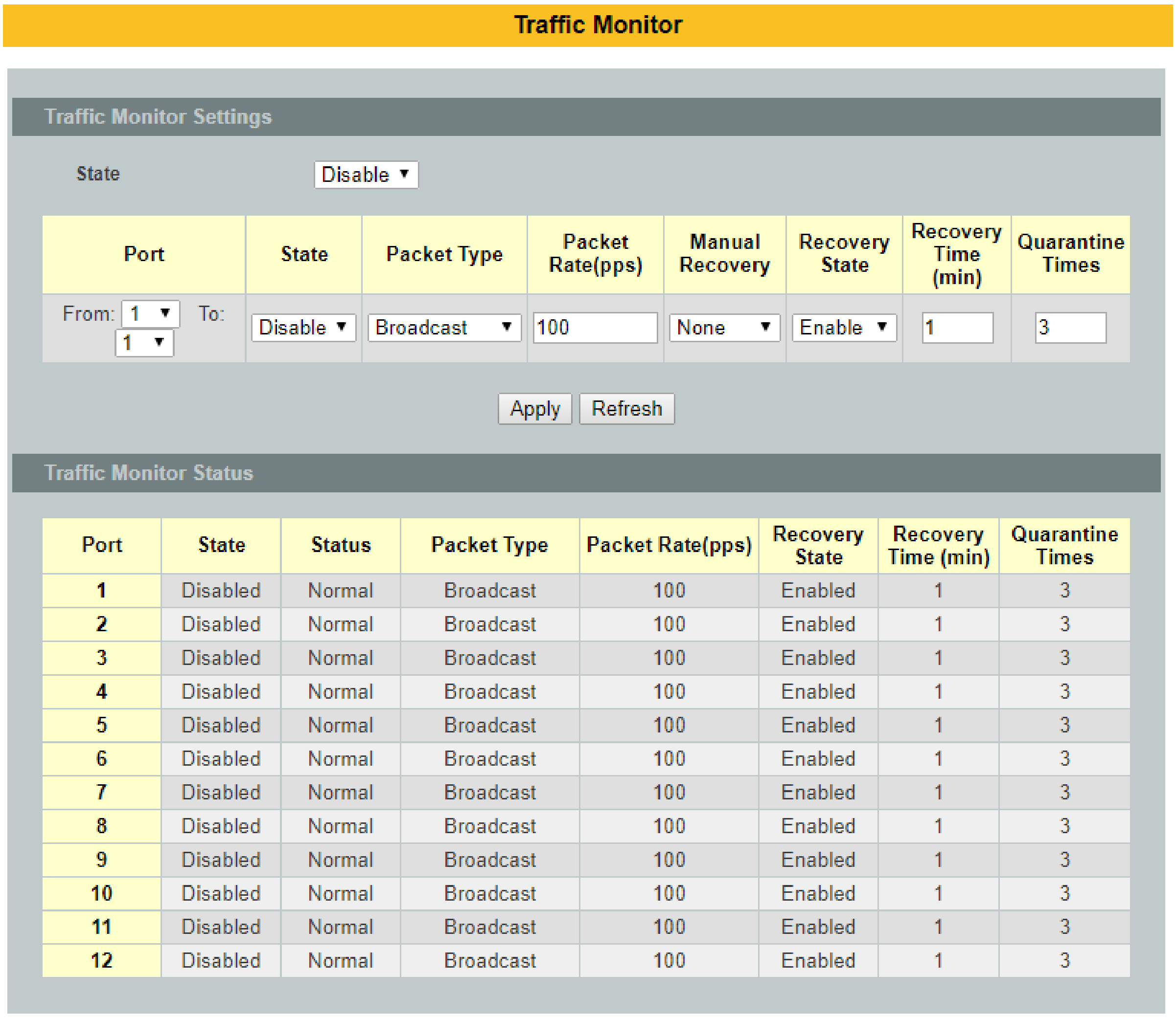
```
                                  Packet        Packet              Recovery
Port   State       Status     Type            Rate(pps)   State        Time(min)
----   --------   -------   -----------   ---------   --------   ---------
 1     Disabled   Normal     Bcast           1000          Enabled     1
 2     Disabled   Normal     Bcast           1000          Enabled     1
 3     Disabled   Normal     Bcast           1000          Enabled     1
 4     Disabled   Normal     Bcast           1000          Enabled     1
 5     Disabled   Normal     Bcast           1000          Enabled     1
 6     Disabled   Normal     Bcast           1000          Enabled     1
      .    .    .    .    .    .    .    .    .    .    .    .    .    .    .
```

9.7.2. CLI Configuration

Node	Command	Description
enable	show traffic-monitor	This command displays the traffic monitor configurations and current status.
configure	traffic-monitor (disable|enable)	This command enables / disables the traffic monitor on the Switch.
interface	traffic-monitor (disable|enable)	This command enables / disables the traffic monitor on the port.
interface	traffic-monitor rateRATE_LIMIT type (bcast|mcast|bcast+mcast)	This command configures the packet rate and packet type for the traffic monitor on the port. bcast – Broadcast packet. mcast – Multicast packet.
interface	traffic-monitor recovery (disable|enable)	This command enables / disables the recovery function for the traffic monitor on the port.
interface	traffic-monitor recovery time VALUE	This command configures the recovery time for the traffic monitor on the port.
configure	interface range	This command enters the interface configure node.

	gigabitethernet1/0/PORTLISTS	
if-range	traffic-monitor (disable|enable)	This command enables / disables the traffic monitor on the port.
if-range	traffic-monitor rateRATE_LIMIT type (bcast|mcast|bcast+mcast)	This command configures the packet rate and packet type for the traffic monitor on the port. bcast – Broadcast packet. mcast – Multicast packet.
if-range	traffic-monitor recovery (disable|enable)	This command enables / disables the recovery function for the traffic monitor on the port.
if-range	traffic-monitor recovery time VALUE	This command configures the recovery time for the traffic monitor on the port.

9.7.3. Web Configuration



Traffic Monitor

Traffic Monitor Settings

State: Disable ▼

Port	State	Packet Type	Packet Rate(pps)	Manual Recovery	Recovery State	Recovery Time (min)	Quarantine Times
From: 1 ▼ To: 1 ▼	Disable ▼	Broadcast ▼	100	None ▼	Enable ▼	1	3

Traffic Monitor Status

Port	State	Status	Packet Type	Packet Rate(pps)	Recovery State	Recovery Time (min)	Quarantine Times
1	Disabled	Normal	Broadcast	100	Enabled	1	3
2	Disabled	Normal	Broadcast	100	Enabled	1	3
3	Disabled	Normal	Broadcast	100	Enabled	1	3
4	Disabled	Normal	Broadcast	100	Enabled	1	3
5	Disabled	Normal	Broadcast	100	Enabled	1	3
6	Disabled	Normal	Broadcast	100	Enabled	1	3
7	Disabled	Normal	Broadcast	100	Enabled	1	3
8	Disabled	Normal	Broadcast	100	Enabled	1	3
9	Disabled	Normal	Broadcast	100	Enabled	1	3
10	Disabled	Normal	Broadcast	100	Enabled	1	3
11	Disabled	Normal	Broadcast	100	Enabled	1	3
12	Disabled	Normal	Broadcast	100	Enabled	1	3

Parameter	Description
Port	Select a port or a range of ports to display their RMON statistics.
Speed	The current port speed.
Rx Utilization (%)	The port receiving traffic utilization in percentage
Rx Utilization (bps)	The port receiving traffic utilization in bits per second
Tx Utilization (%)	The port transmitting traffic utilization in percentage
Tx Utilization (bps)	The port transmitting traffic utilization in bits per second
Refresh	Click this button to refresh the screen quickly.

10. Management

10.1. SNMP

10.1.1. SNMP

10.1.1.1Introduction

Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.
SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

Support below MIBs:

- RFC 1157 A Simple Network Management Protocol
- RFC 1213 MIB-II
- RFC 1493 Bridge MIB
- RFC 1643 Ethernet Interface MIB
- RFC 1757 RMON Group 1,2,3,9

SNMP community act like passwords and are used to define the security parameters of SNMP clients in an SNMP v1 and SNMP v2c environments. The default SNMP community is "public" for both SNMP v1 and SNMP v2c before SNMP v3 is enabled. Once SNMP v3 is enabled, the communities of SNMP v1 and v2c have to be unique and cannot be shared.

Network ID of Trusted Host:

The IP address is a combination of the Network ID and the Host ID.

Network ID = (Host IP & Mask).

User need only input the network ID and leave the host ID to 0. If user has input the host ID, such as 192.168.1.102, the system will reset the host ID, such as 192.168.1.0

Note: Allow user to configure the community string and rights only.
User configures the Community String and the Rights and the Network ID of Trusted Host=0.0.0.0, Subnet Mask=0.0.0.0. It means that all hosts with the community string can access the Switch.

Default Settings

SNMP	: disabled.
System Location	: L2SWITCH. (Maximum length 64 characters)
System Contact	: None. (Maximum length 64 characters)
System Name	: None. (Maximum length 64characters)
Trap Receiver	: None.
Community Name	: None.
The maximum entry for community	: 3.
The maximum entry for trap receiver	: 5.

10.1.1.2CLI Configuration

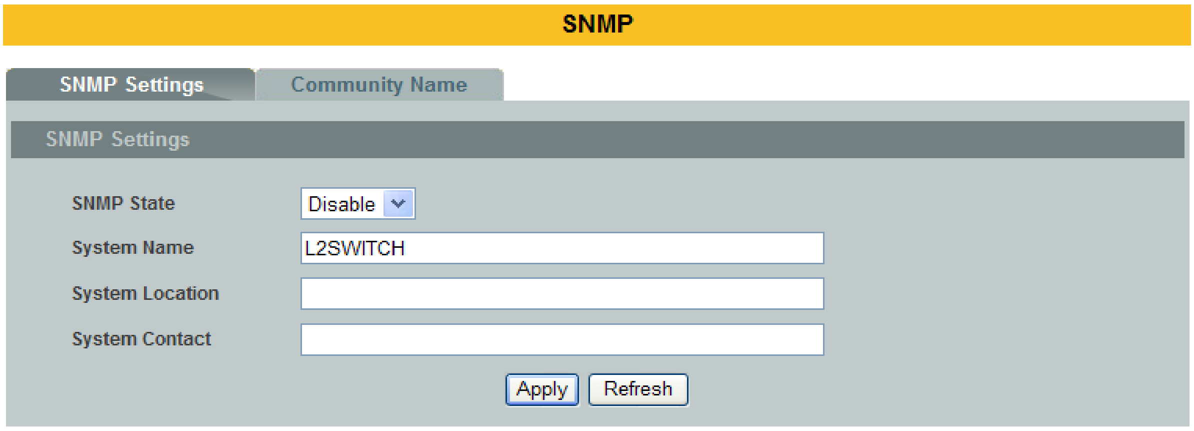
Node	Command	Description
enable	show snmp	This command displays the SNMP configurations.
configure	snmp community STRING (ro|rw) trusted-host IPADDR	This command configures the SNMP community name.
configure	snmp (disable|enable)	This command disables/enables the SNMP on the switch.
configure	snmp system-contact STRING	This command configures contact information for the system.
configure	snmp system-location STRING	This command configures the location information for the system.
configure	snmp system-name STRING	This command configures a name for the system. (The System Name is same as the host name)
configure	snmp trap-receiver IPADDR VERSION COMMUNITY	This command configures the trap receiver's configurations, including the IP address, version (v1 or v2c) and community.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#snmp enable
L2SWITCH(config)#snmp community public rw trusted-host 192.168.200.106/24
L2SWITCH(config)#snmp trap-receiver 192.168.200.106 v2c public
L2SWITCH(config)#snmp system-contact IT engineer
L2SWITCH(config)#snmp system-location Branch-Office
```

10.1.1.3Web Configuration

SNMP Setting:



SNMP

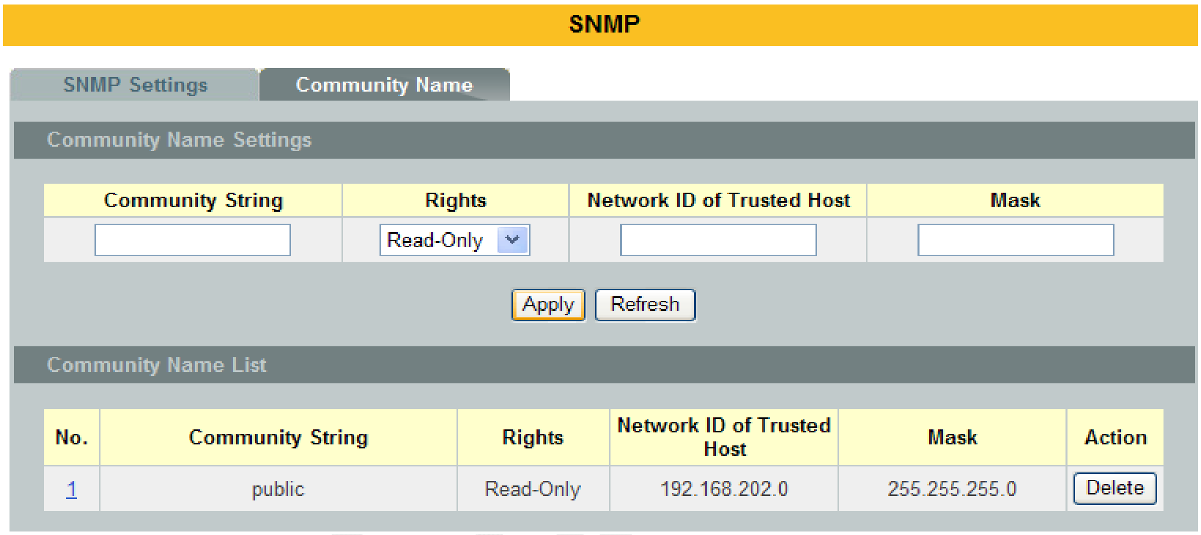
SNMP Settings

SNMP State	Disable
System Name	L2SWITCH
System Location	
System Contact	

Parameter	Description
SNMP State	Select **Enable** to activate SNMP on the Switch. Select **Disable** to not use SNMP on the Switch.

System Name	Type a System Name for the Switch. (The System Name is same as the host name)
System Location	Type a System Location for the Switch.
System Contact	Type a System Contact for the Switch.
Apply	Click Apply to configure the settings.
Refresh	Click this button to reset the fields to the last setting.

Community Name:



Community String	Rights	Network ID of Trusted Host	Mask
	Read-Only		

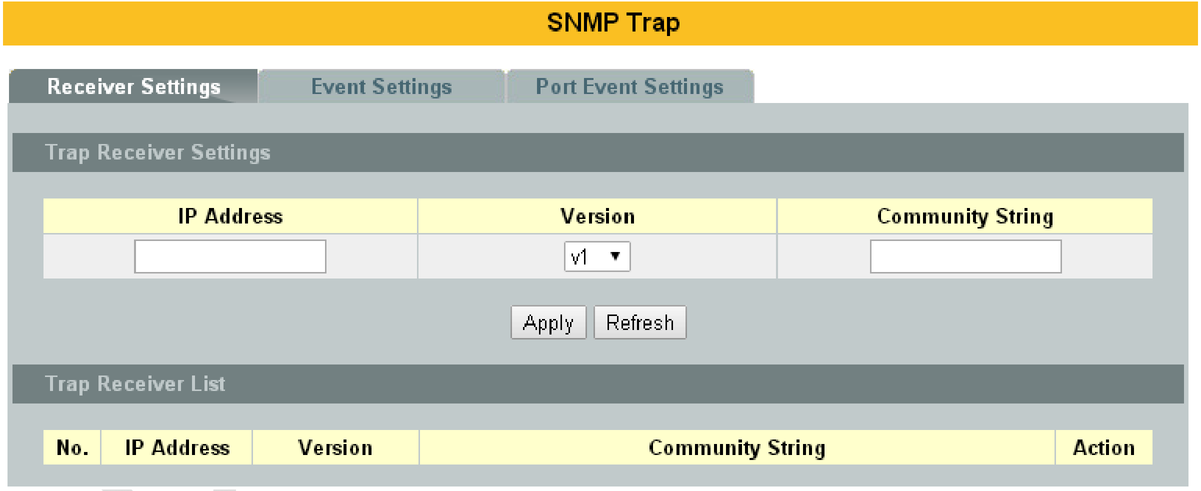
No.	Community String	Rights	Network ID of Trusted Host	Mask	Action
1	public	Read-Only	192.168.202.0	255.255.255.0	Delete

Parameter	Description
Community String	Enter a Community string, this will act as a password for requests from the management station. An SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the management station (the SNMP manager) and the device (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.
Rights	Select Read-Only to allow the SNMP manager using this string to collect information from the Switch. Select Read-Write to allow the SNMP manager using this string to create or edit MIBs (configure settings on the Switch).
Network ID of Trusted Host	Type the IP address of the remote SNMP management station in dotted decimal notation, for example 192.168.1.0.
Mask	Type the subnet mask for the IP address of the remote SNMP management station in dotted decimal notation, for example 255.255.255.0.

Apply	Click **Apply** to configure the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Community Name List	
No.	This field indicates the community number. It is used for identification only. Click on the individual community number to edit the community settings.
Community String	This field displays the SNMP community string. An SNMP community string is a text string that acts as a password.
Right	This field displays the community string's rights. This will be **Read Only** or **Read Write**.
Network ID of Trusted Host	This field displays the IP address of the remote SNMP management station after it has been modified by the subnet mask.
Subnet Mask	This field displays the subnet mask for the IP address of the remote SNMP management station.
Action	Click **Delete** to remove a specific Community String.

10.1.2. SNMP Trap

Receiver Settings



SNMP Trap

Trap Receiver Settings

IP Address	Version	Community String
	v1 ▼	

Trap Receiver List

No.	IP Address	Version	Community String	Action

Parameter	**Description**
IP Address	Enter the IP address of the remote trap station in dotted decimal notation.
Version	Select the version of the Simple Network Management Protocol to use. **v1** or **v2c**.
Community String	Specify the community string used with this remote trap station.
Apply	Click **Apply** to configure the settings.

Refresh	Click **Refresh** to begin configuring this screen afresh.
Trap Receiver List	
No.	This field displays the index number of the trap receiver entry. Click the number to modify the entry.
IP Address	This field displays the IP address of the remote trap station.
Version	This field displays the version of Simple Network Management Protocol in use. **v1** or **v2c**.
Community String	This field displays the community string used with this remote trap station.
Action	Click **Delete** to remove a configured trap receiver station.

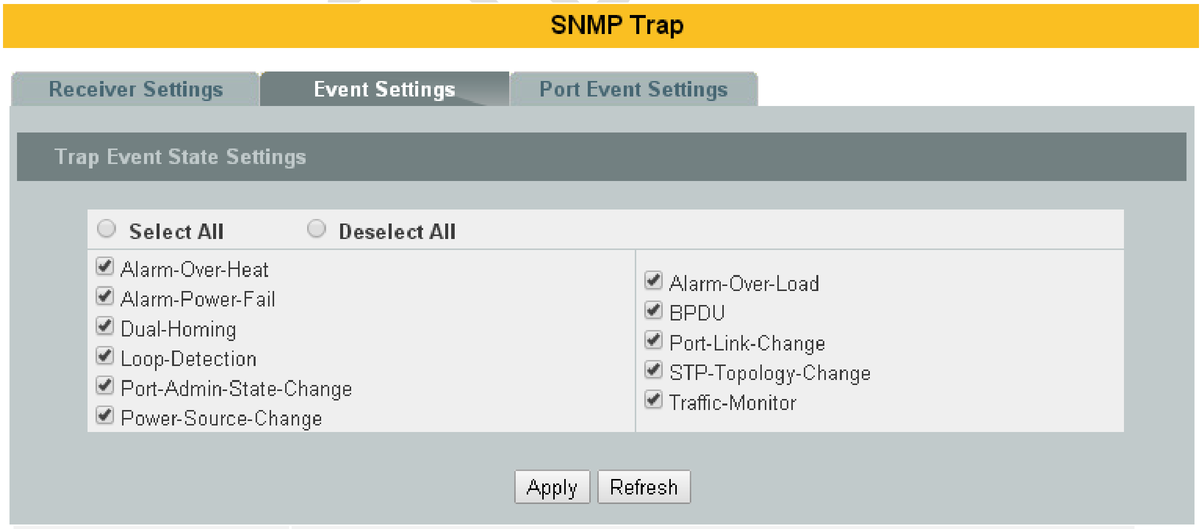
Event Settings
The features allow users to enable/disables individual trap notification.

alarm-over-heat	- Trap when system’s temperature is too high.
alarm-over-load	- Trap when system is over load.
alarm-power-fail	- Trap when system power is over voltage/under voltage/ RPS over voltage/RPS under voltage.
bpdu	- Trap when port is blocked by BPDU Guard/BDPU Root Guard/BPDU port state changed.
dual-homing	- Trap when port is blocked by Dual Homing.
dying-gasy	- Trap when system is power off.
loop-detection	- Trap when port is blocked by Loop Detection.
pd-alive	- Trap when PD device has no responses.
port-admin-state-change	- Trap when port is enabled/disable by administrator.
port-link-change	- Trap when port is link up/down change.
power-source-change	- Trap when the power source has been changed. (AC to DC or DC to AC)
stp-topology-change	- Trap when the STP topology change.
traffic-monitor	- Trap when port is blocked by Traffic Monitor.
xpress-ring	- Trap when port is blocked by Xpress Ring.

CLI Configurations

Node	Command	Description
enable	show snmp trap-event	This command displays the SNMP configurations.
configure	snmp trap-event alarm-over-heat (disable/enable)	This command enables/disables the alarm-over-heat trap.
configure	snmp trap-event alarm-over-load (disable/enable)	This command enables/disables the alarm-over-load trap.

configure	snmp trap-event alarm-power-fail (enable/enable)	This command enables/disables the alarm-power-fail trap.
configure	snmp trap-event bpdu (disable/enable)	This command enables/disables the BPDU port state change/BPDU Root Guard/BPDU Guard trap.
configure	snmp trap-event dual-homing (disable/enable)	This command enables/disables the dual-homing trap.
configure	snmp trap-event dying-gasp (disable/enable)	This command enables/disables the dying-gasp trap.
configure	snmp trap-event loop-detection (disable/enable)	This command enables/disables the loop-detection trap.
configure	snmp trap-event pd-alive (disable/enable)	This command enables/disables the pd-alive trap.
configure	snmp trap-event port-admin-state-change (disable/enable)	This command enables/disables the port-admin-state-change trap.
configure	snmp trap-event port-link-change (disable/enable)	This command enables/disables the port-link-change trap.
configure	snmp trap-event power-source-change (disable/enable)	This command enables/disables the power-source-change trap.
configure	snmp trap-event stp-topology-change (disable/enable)	This command enables/disables the stp-topology-change trap.
configure	snmp trap-event traffic-monitor (disable/enable)	This command enables/disables the traffic-monitor trap.
configure	snmp trap-event xpress-ring (disable/enable)	This command enables/disables the xpress-ring trap.



SNMP Trap

Receiver Settings | Event Settings | Port Event Settings

Trap Event State Settings

○ Select All ○ Deselect All

☑ Alarm-Over-Heat
☑ Alarm-Power-Fail
☑ Dual-Homing
☑ Loop-Detection
☑ Port-Admin-State-Change
☑ Power-Source-Change

☑ Alarm-Over-Load
☑ BPDU
☑ Port-Link-Change
☑ STP-Topology-Change
☑ Traffic-Monitor

Apply Refresh

Parameter	Description
Trap Event State Settings	
Select all	Enables all of trap events.
Deselect All	Disables all os trap events.

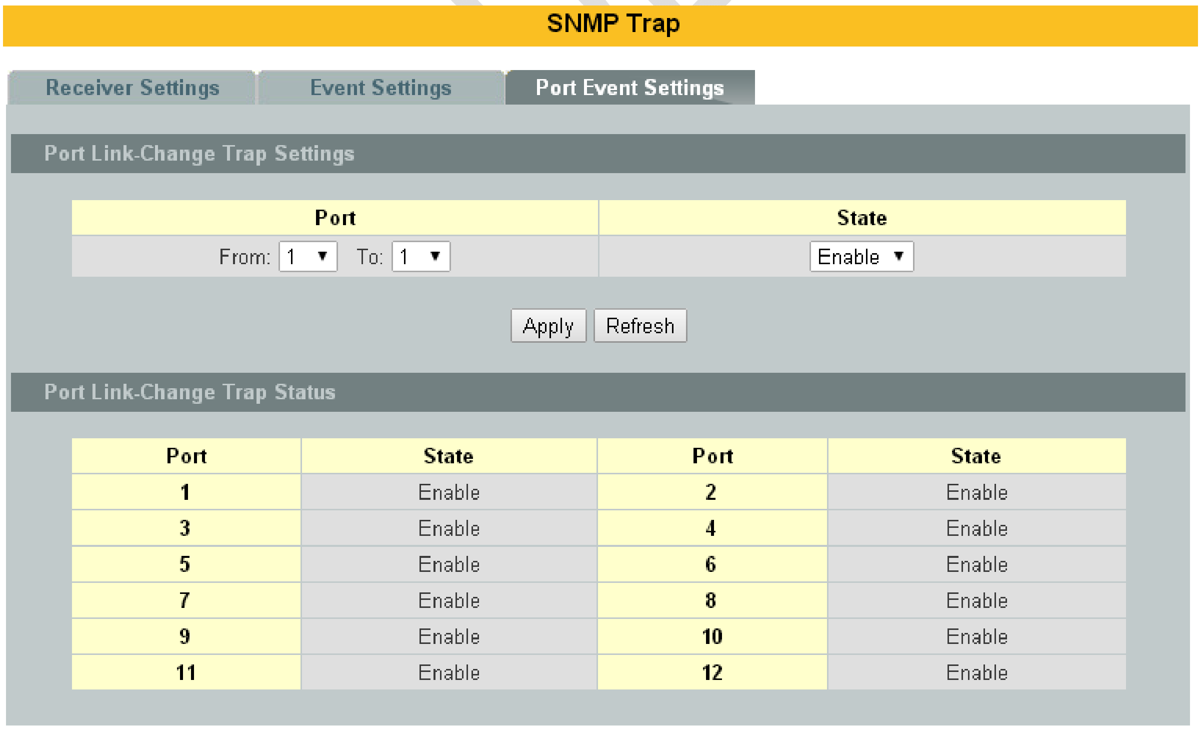
Apply	Click **Apply** to configure the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.

Port Event Settings

The features allow users to enable/disables port-link-change trap notification by individual port.

CLI Configurations

Node	Command	Description
enable	show snmp port-link-change-trap	This command displays the SNMP port link-change trap configurations.
interface	snmp port-link-change-trap	This command enables the link change trap on the specific port.
interface	no snmp port-link-change-trap	This command disables the link change trap on the specific port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	snmp port-link-change-trap	This command enables the link change trap on the specific ports.
if-range	no snmp port-link-change-trap	This command disables the link change trap on the specific ports.



Port Link-Change Trap Settings

Port	State
From: 1 ▼ To: 1 ▼	Enable ▼

Port Link-Change Trap Status

Port	State	Port	State
1	Enable	2	Enable
3	Enable	4	Enable
5	Enable	6	Enable
7	Enable	8	Enable
9	Enable	10	Enable
11	Enable	12	Enable

Parameter	Description

Trap Event State Settings	
Port	Selects the range of ports.
State	Selects the state for the ports..
Apply	Click **Apply** to configure the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.

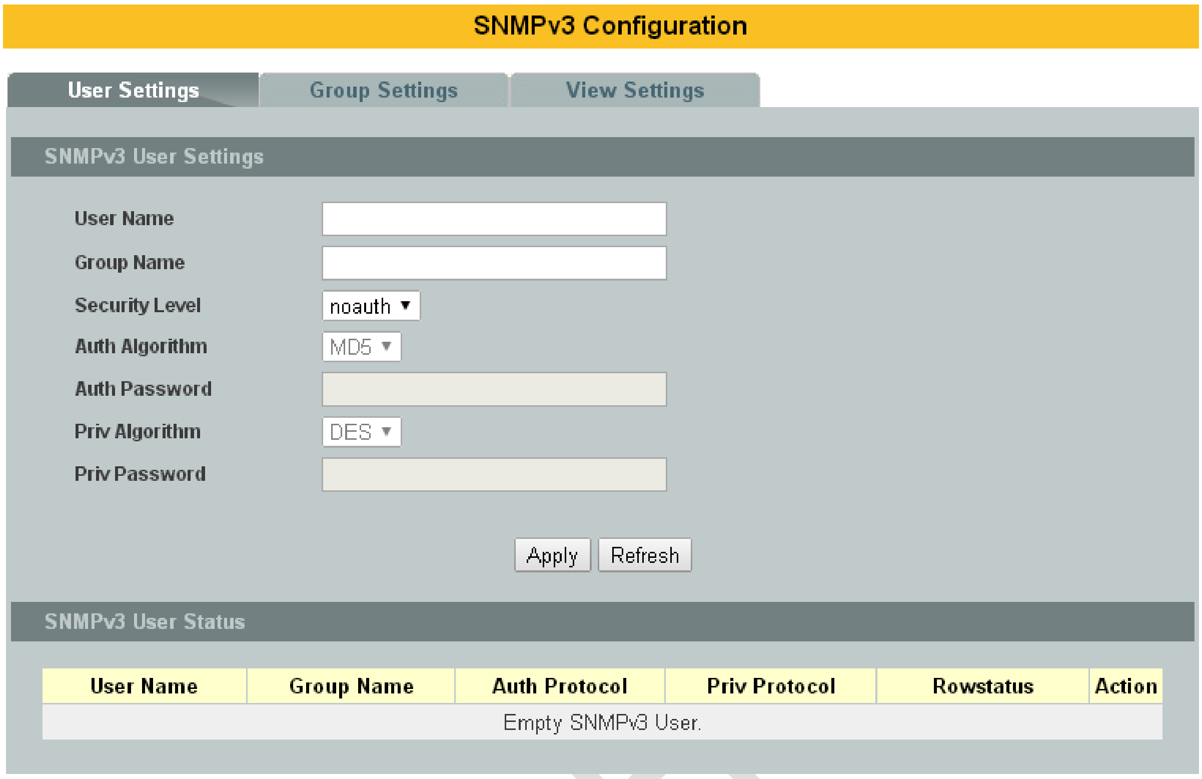
10.1.3. SNMPv3

CLI Configuration

Node	Command	Description
enable	show snmp user	This command displays all snmp v3 users.
enable	show snmp group	This command displays all snmp v3 groups.
enable	show snmp view	This command displays all snmp v3 view.
configure	snmp user USERNAME GROUPNAME noauth	Configures v3 user of non- authentication.
configure	snmp user USERNAME GROUPNAME auth (MD5|SHA) STRINGS	Configures v3 user of authentication.
configure	snmp user USERNAME GROUPNAME priv (MD5|SHA) STRINGS des STRINGS	Configures v3 user of authentication and encryption.
configure	snmp group GROUPNAME noauth (read STRINGS write STRINGS notify STRINGS)	Configures v3 group of non- authentication.
configure	snmp group GROUPNAME auth (read STRINGS write STRINGS notify STRINGS)	Configures v3 group of authentication.
configure	snmp group GROUPNAME priv (read STRINGS write STRINGS notify STRINGS)	Configures v3 group of authentication and encryption.
configure	snmp view VIEWNAME STRINGS (included|excluded)	To identify the sub tree.
configure	no snmp user USERNAME GROUPNAME	This command removes a v3 user from switch.
configure	no snmp group GROUPNAME	This command removes a v3 group from switch.
configure	no snmp view VIEWNAME STRINGS	This command removes a v3 view from switch.

Web Configuration

SNMPv3 User



SNMPv3 Configuration

SNMPv3 User Settings

User Name	
Group Name	
Security Level	noauth
Auth Algorithm	MD5
Auth Password	
Priv Algorithm	DES
Priv Password	

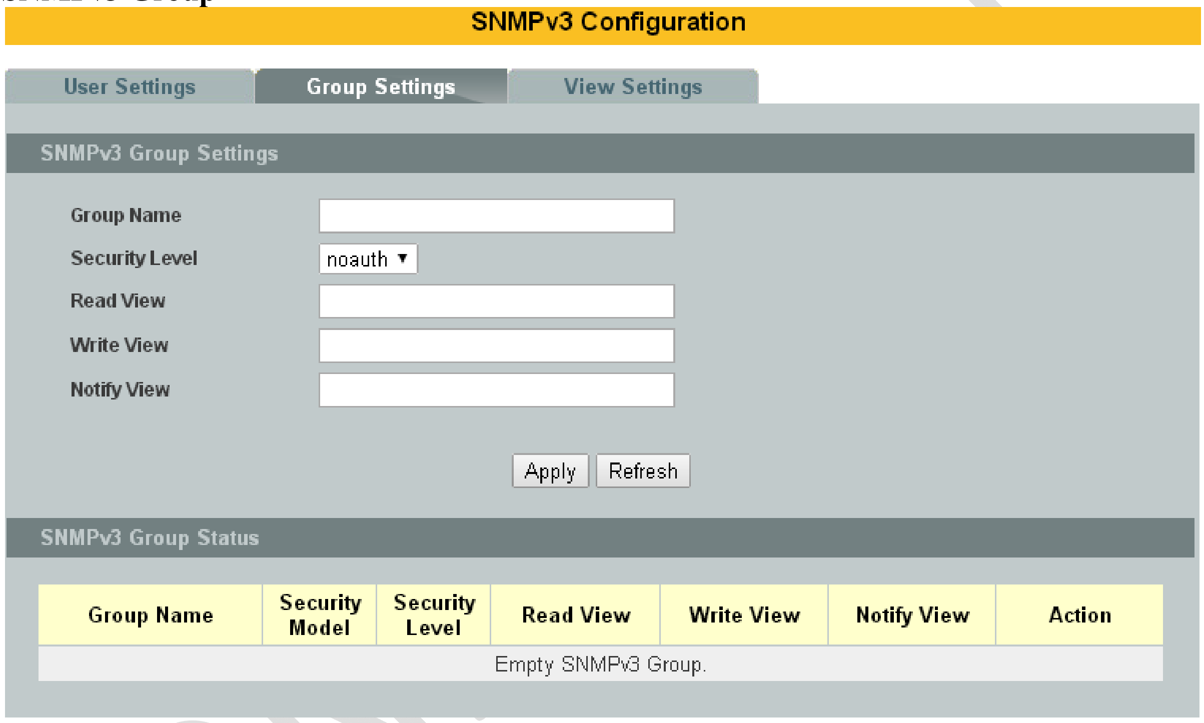
SNMPv3 User Status

User Name	Group Name	Auth Protocol	Priv Protocol	Rowstatus	Action
Empty SNMPv3 User.					

Parameter	Description
User Name	Enter the v3 user name.
Group Name	Map the v3 user name into a group name.
Security Level	Select the security level of the v3 user to use. **noauth** means no authentication and no encryption. **auth** means messages are authenticated but not encrypted. **priv** means messages are authenticated and encrypted.
Auth Algorithm	Select **MD5** or **SHA** Algorithm when security level is **auth** or **priv.**
Auth Password	Set the password for this user when security level is **auth** or **priv.** (pass phrases must be at least 8 characters long!)
Priv Algorithm	Select **DES**encryption when security level is **priv.**
Priv Password	Set the password for this user when security level is **priv.** (pass phrases must be at least 8 characters long!)
Apply	Click **Apply** to configure the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
SNMPv3 User Status	
User Name	This field displays the v3 user name.

Group Name	This field displays the group name which the v3 user mapping.
Auth Protocol	These fields display the security level to this v3 user.
Priv Protocol	
Rowstatus	This field displays the v3 user Row status.
Action	Click **Delete** to remove a v3 user.

SNMPv3 Group



SNMPv3 Group Settings

Group Name

Security Level: noauth

Read View

Write View

Notify View

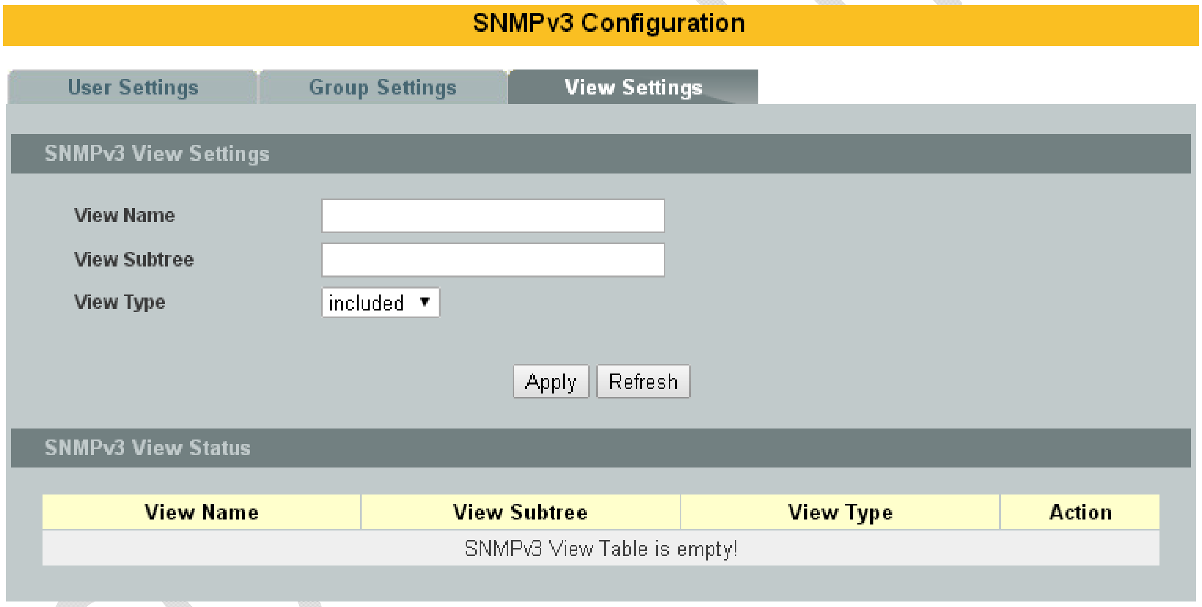
SNMPv3 Group Status

Group Name	Security Model	Security Level	Read View	Write View	Notify View	Action
Empty SNMPv3 Group.						

Parameter	**Description**
Group Name	Enter the v3 user name.
Security Level	Select the security level of the v3 group to use.
Read View	Note that if a group is defined without a read view than all objects are available to read. (default value is **none**.)
Write View	if no write or notify view is defined, no write access is granted and no objects can send notifications to members of the group. (default value is **none**.)
Notify View	By using a notify view, a group determines the list of notifications its users can receive.(default value is **none**.)
Apply	Click **Apply** to configure the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.

SNMPv3 Group Status	
Group Name	This field displays the v3 user name.
Security Model	This field displays the security model of the group. Always displayed **v3**: User-based Security Model (USM)
Security Level	This field displays the security level to this group.
Read View	These fields display the View list of this group.
Write View	
Notify View	
Action	Click **Delete** to remove a v3 group.

SNMPv3 View



View Name	View Subtree	View Type	Action
SNMPv3 View Table is empty!			

Parameter	Description
View Name	Enter the v3 view name for creating an entry in the SNMPv3 MIB view table.
View Subtree	The OID defining the root of the subtree to add to (or exclude from) the named view.
View Type	Select **included** or **excluded** to define subtree adding to the view or not.
Apply	Click **Apply** to configure the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.

SNMPv3 View Status	
View Name	This field displays the v3 view name.
View Subtree	This field displays the subtree.
View Type	This field displays the subtree adding to the view or not.
Action	Click **Delete** to remove a v3 view.

10.2. Maintenance

10.2.1. CLI Configuration

Node	Command	Description
enable	show config-change-status	This command displays the configurations status if there are default values.
configure	reboot	This command reboots the system.
configure	reload default-config	This command copies a default-config file to replace the current one. **Note:** The system will reboot automatically to take effect the configurations.
configure	write memory	This command writes current operating configurations to the configuration file.
configure	archive download-config <URL PATH>	This command downloads a new copy of configuration file from TFTP server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file
configure	archive upload-config <URL PATH>	This command uploads the current configurations file to a TFTP server.
configure	archive download-fw<URL PATH>	This command downloads a new copy of firmware file from TFTP / FTP / HTTP server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file

Example:

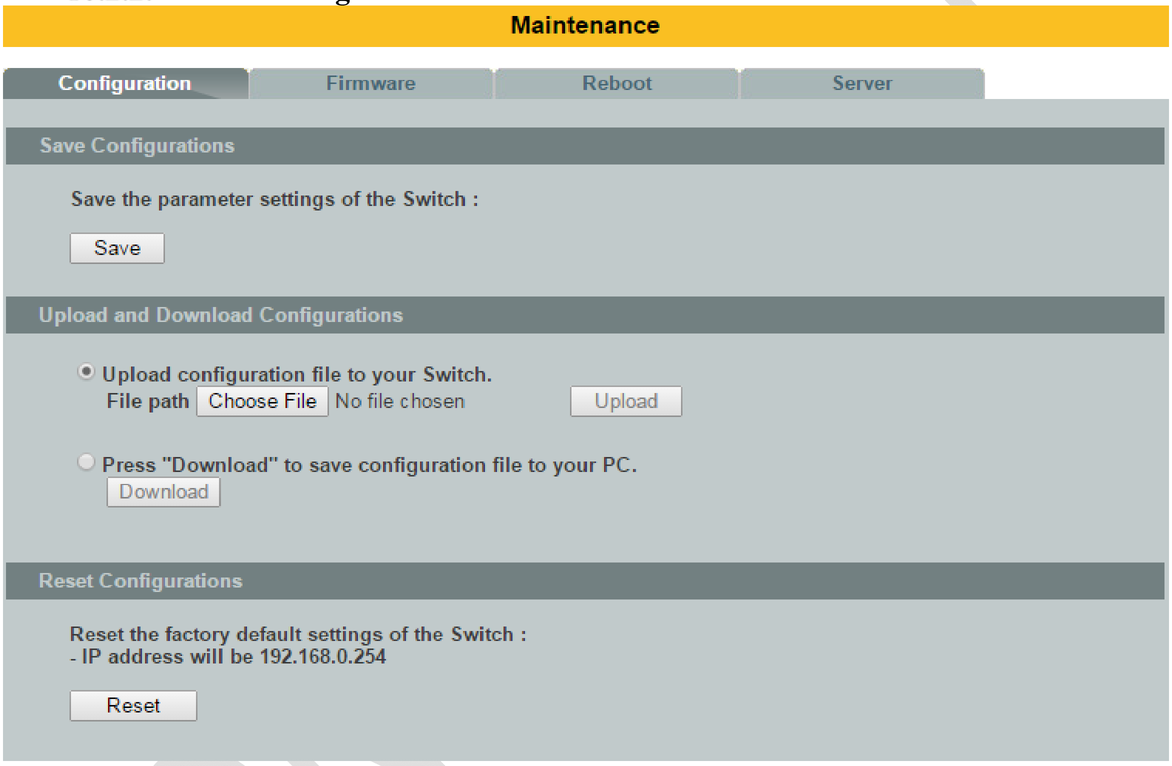
```
L2SWITCH#configure terminal
L2SWITCH(config)#interface eth0
L2SWITCH(config-if)#ip address 172.20.1.101/24
L2SWITCH(config-if)#ip address default-gateway 172.20.1.1
L2SWITCH(config-if)#management vlan 1
```

Enable the DHCP client function for the switch.

- L2SWITCH#*configure terminal*
- L2SWITCH(config)#*interface eth0*
- L2SWITCH(config-if)#*ip dhcp client enable*

```
L2SWITCH#show config-change-status
The user configuration file is default.
The configurations have been modified.
```

10.2.2. Web Configuration


Maintenance

Configuration | Firmware | Reboot | Server

Save Configurations

Save the parameter settings of the Switch :

Save

Upload and Download Configurations

● Upload configuration file to your Switch.
File path Choose File No file chosen Upload

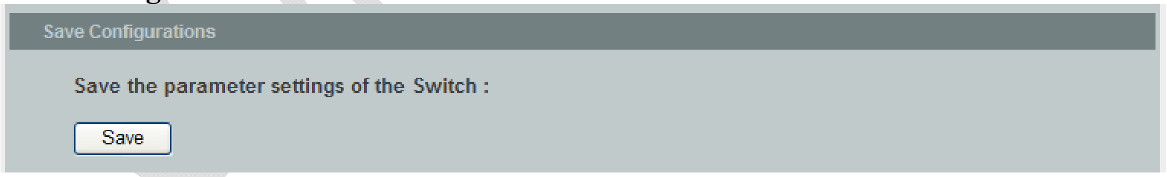
○ Press "Download" to save configuration file to your PC.
Download

Reset Configurations

Reset the factory default settings of the Switch :
- IP address will be 192.168.0.254

Reset

Save Configurations

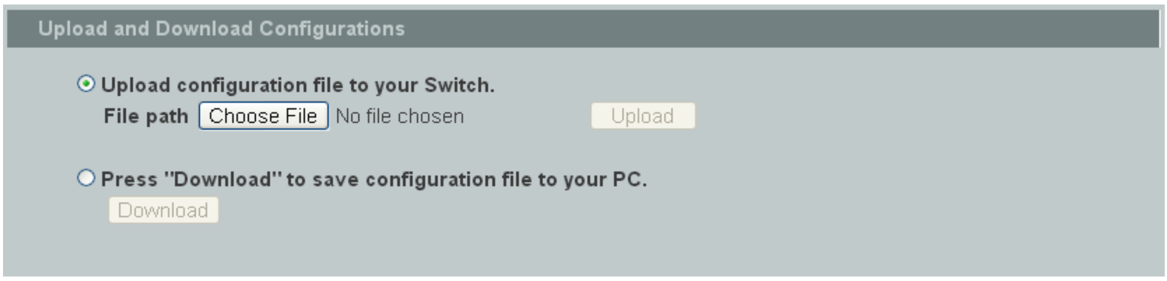

Save Configurations

Save the parameter settings of the Switch :

Save

Press the Save button to save the current settings to the NV-RAM (flash).

Upload / Download Configurations to /from a your server



Upload and Download Configurations

○ Upload configuration file to your Switch.

File path Choose File No file chosen Upload

○ Press "Download" to save configuration file to your PC.

Download

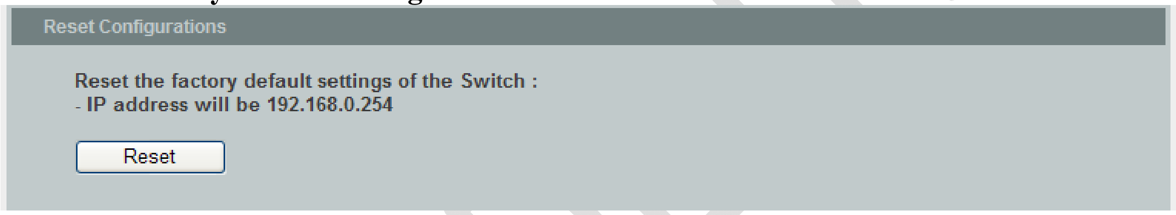
Follow the steps below to save the configuration file to your PC.

- Select the "Press "Download" to save configurations file to your PC".
- Click the "Download" button to start the process.

Follow the steps below to load the configuration file from your PC to the Switch.

- Select the "Upload configurations file to your Switch".
- Select the full path to your configuration file.
- Click the Upload button to start the process.

Reset the factory default settings of the Switch



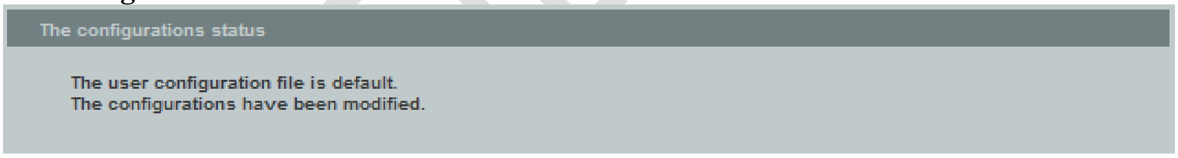
Reset Configurations

Reset the factory default settings of the Switch :
- IP address will be 192.168.0.254

Reset

Press the Reset button to set the settings to factory default configurations.

The configuration status



The configurations status

The user configuration file is default.
The configurations have been modified.

Display the configuration status of recorded in the NV-RAM.

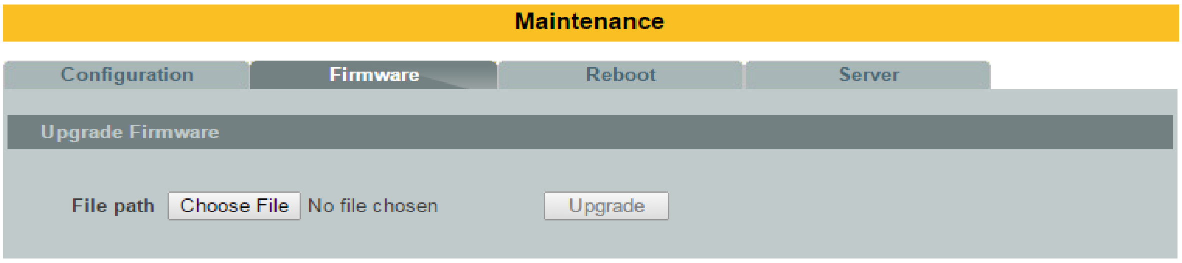
Notice:
If the user has changed any configurations, the message displays "The configurations have been modified!" Otherwise, the message "The configurations are default values."

There are two conditions will change message from "The configurations have been modified!" to "The configurations are default values."

1. Click "Reset configuration" in web management or do cli command, reload default-config.
2. Click "Upload configuration" in web management or do cli command, "archive download-config xxx".

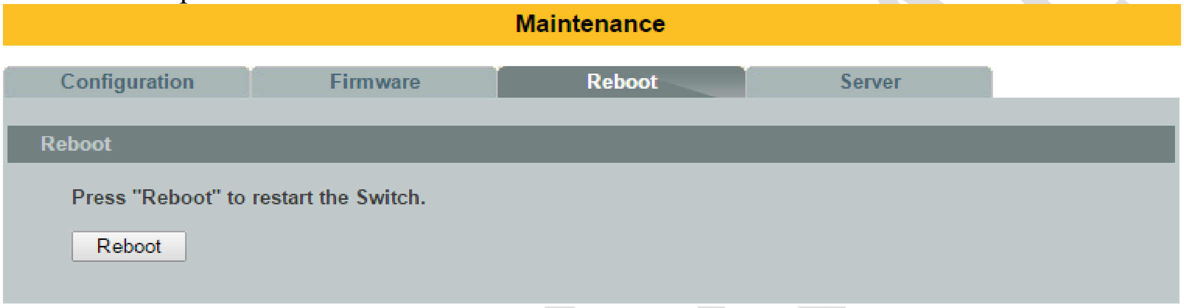
Firmware

Type the path and file name of the firmware file you wish to upload to the Switch in the **File path** text box or click **Browse** to locate it. Click **Upgrade** to load the new firmware.



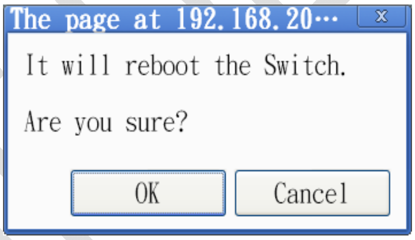
Reboot

Reboot allows you to restart the Switch without physically turning the power off. Follow the steps below to reboot the Switch.



Press "Reboot" to restart the Switch.

- In the **Reboot** screen, click the **Reboot** button. The following screen displays.



It will reboot the Switch.

Are you sure?

- Click **OK** again and then wait for the Switch to restart. This takes up to two minutes. This does not affect the Switch's configuration.

10.2.3. Server Control

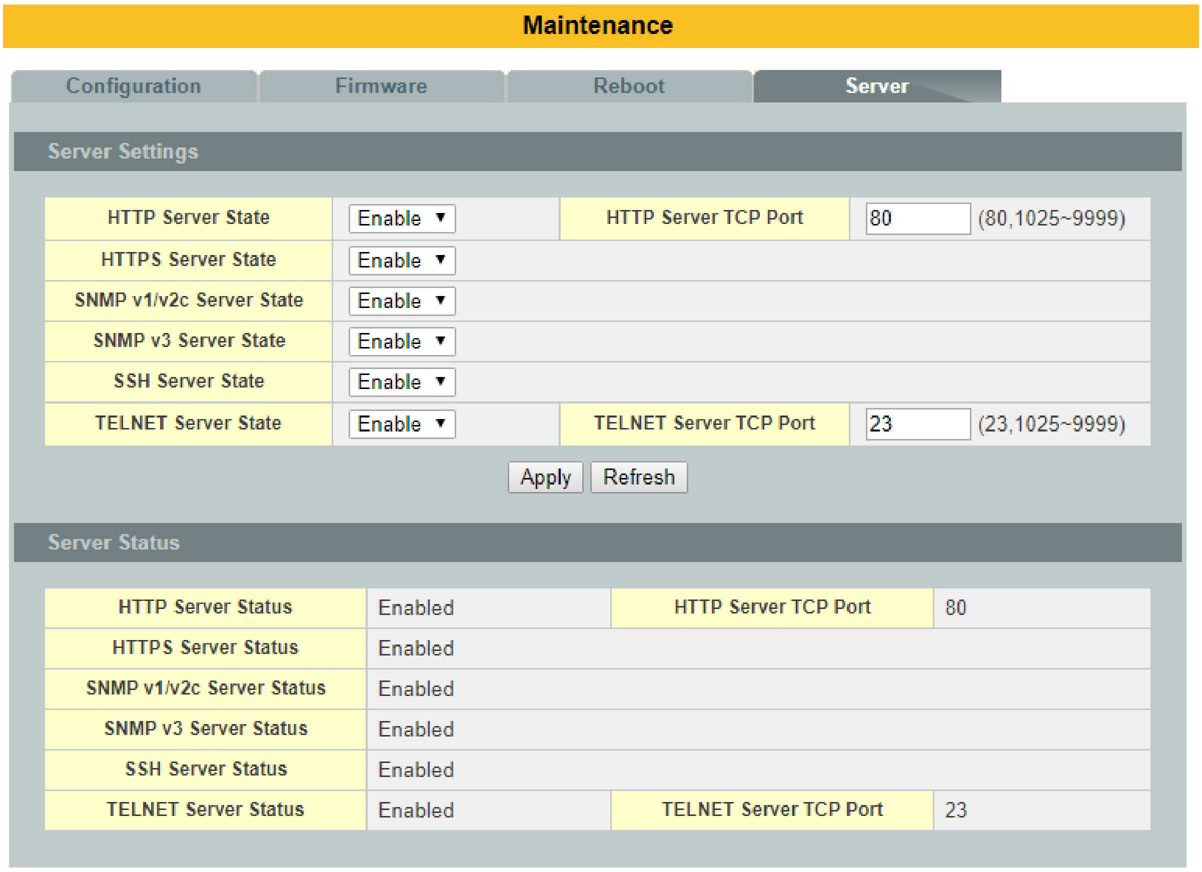
The function allows users to enable or disable the SSH or Telnet or Web service individual using the CLI or GUI.

CLI Configuration

Node	Command	Description
enable	show server status	This command displays the current server status.
configure	ssh server	This command enables the ssh on the Switch.
configure	no ssh server	This command disables the ssh on the Switch.
configure	telnet server	This command enables the telnet on the Switch.
configure	no telnet server	This command disables the telnet on the Switch.
configure	web server	This command enables the web on the Switch.

configure	no web server	This command disables the web on the Switch.

Web Configuration



Server Settings

HTTP Server State	Enable	HTTP Server TCP Port	80	(80,1025~9999)
HTTPS Server State	Enable			
SNMP v1/v2c Server State	Enable			
SNMP v3 Server State	Enable			
SSH Server State	Enable			
TELNET Server State	Enable	TELNET Server TCP Port	23	(23,1025~9999)

Server Status

HTTP Server Status	Enabled	HTTP Server TCP Port	80
HTTPS Server Status	Enabled		
SNMP v1/v2c Server Status	Enabled		
SNMP v3 Server Status	Enabled		
SSH Server Status	Enabled		
TELNET Server Status	Enabled	TELNET Server TCP Port	23

Parameter	**Description**
Server Settings	
HTTP Server State	Selects Enable or Disable to enable or disable the HTTP service.
HTTP Server TCP Port	Configures the TCP port for the HTTP service.
SSH Server State	Selects Enable or Disable to enable or disable the SSH service.
Telnet Server State	Selects Enable or Disable to enable or disable the Telnet service.
TELNET Server TCP Port	Configures the TCP port for the Telnet service.
Apply	Click Apply to configure the settings.
Refresh	Click this button to reset the fields to the last setting.
Server Status	

HTTP Server Status	Displays the current HTTP service status.
HTTP Server TCP Port	Displays the current TCP port of the HTTP server.
SSH Server Status	Displays the current SSH service status.
Telnet Server Status	Displays the current Telnet service status.
TELNET Server TCP Port	Displays the current TCP port of the TELNET server.

10.3. System log

10.3.1. Introduction

The syslog function records some of system information for debugging purpose. Each log message recorded with one of these levels, **Alert/Critical/Error/Warning/Notice/Information.** The syslog function can be enabled or disabled. The default setting is disabled. The log message is recorded in the Switch file system. If the syslog server's IP address has been configured, the Switch will send a copy to the syslog server.

The log message file is limited in 4KB size. If the file is full, the oldest one will be replaced.

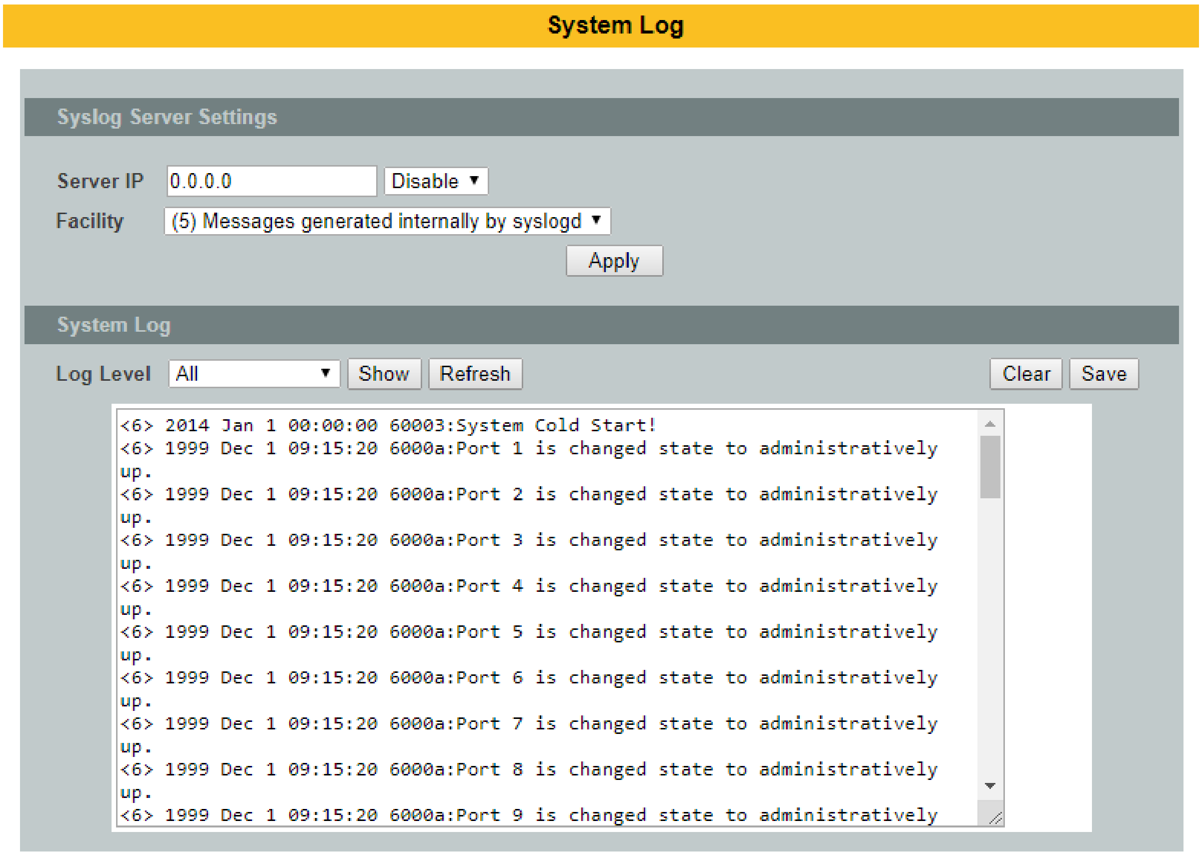
10.3.2. CLI Configuration

Node	Command	Description
enable	show syslog	The command displays the entire log message recorded in the Switch.
enable	show syslog level LEVEL	The command displays the log message with the LEVEL recorded in the Switch.
enable	show syslog server	The command displays the syslog server configurations.
configure	clear syslog	The command clears the syslog message.
configure	syslog-server (disable|enable)	The command disables / enables the syslog server function.
configure	syslog-server ipv4-ip IPADDR	The command configures the syslog server's IP address in IPv4 format.
configure	syslog-server ipv6-ip IPADDR	The command configures the syslog server's IP address in IPv6 format.
configure	syslog-server facility	The command configures the syslog facility level.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#syslog-server ipv4-ip 192.168.200.106
L2SWITCH(config)#syslog-server enable
```

10.3.3. Web Configuration



Server IP: 0.0.0.0 Disable

Facility: (5) Messages generated internally by syslogd

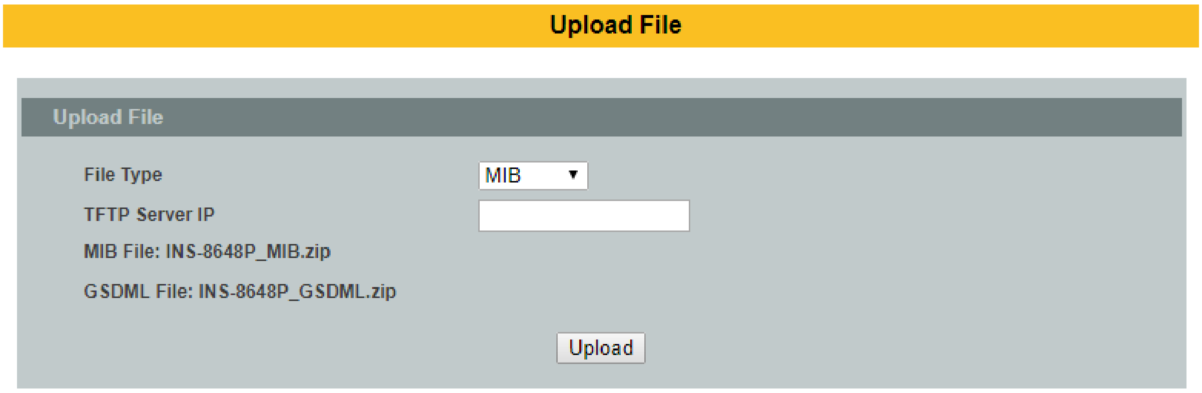
Log Level: All

```
<6> 2014 Jan 1 00:00:00 60003:System Cold Start!
<6> 1999 Dec 1 09:15:20 6000a:Port 1 is changed state to administratively
up.
<6> 1999 Dec 1 09:15:20 6000a:Port 2 is changed state to administratively
up.
<6> 1999 Dec 1 09:15:20 6000a:Port 3 is changed state to administratively
up.
<6> 1999 Dec 1 09:15:20 6000a:Port 4 is changed state to administratively
up.
<6> 1999 Dec 1 09:15:20 6000a:Port 5 is changed state to administratively
up.
<6> 1999 Dec 1 09:15:20 6000a:Port 6 is changed state to administratively
up.
<6> 1999 Dec 1 09:15:20 6000a:Port 7 is changed state to administratively
up.
<6> 1999 Dec 1 09:15:20 6000a:Port 8 is changed state to administratively
up.
<6> 1999 Dec 1 09:15:20 6000a:Port 9 is changed state to administratively
```

Parameter	**Description**
Server IP	Enter the Syslog server IP address. Select **Enable** to activate switch sent log message to Syslog server when any new log message occurred.
Facility	Selects the facility level..
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Log Level	Select **Alert/Critical/Error/Warning/Notice/Information** to choose which log message to want to see.
Clear	Click Clear to clear all of log message.
Save	Click Save to save all of log message into NV-RAM.

10.4. Upload file

You can upload MIB file or GSD file present in the switch to remote TFTP server for your reference. The uploaded file name will be
IEN-8648_MIB.zip for MIB File and
IEN-8648_GSDML.zip for GSDML File.


Upload File

Upload File

File Type: MIB

TFTP Server IP:

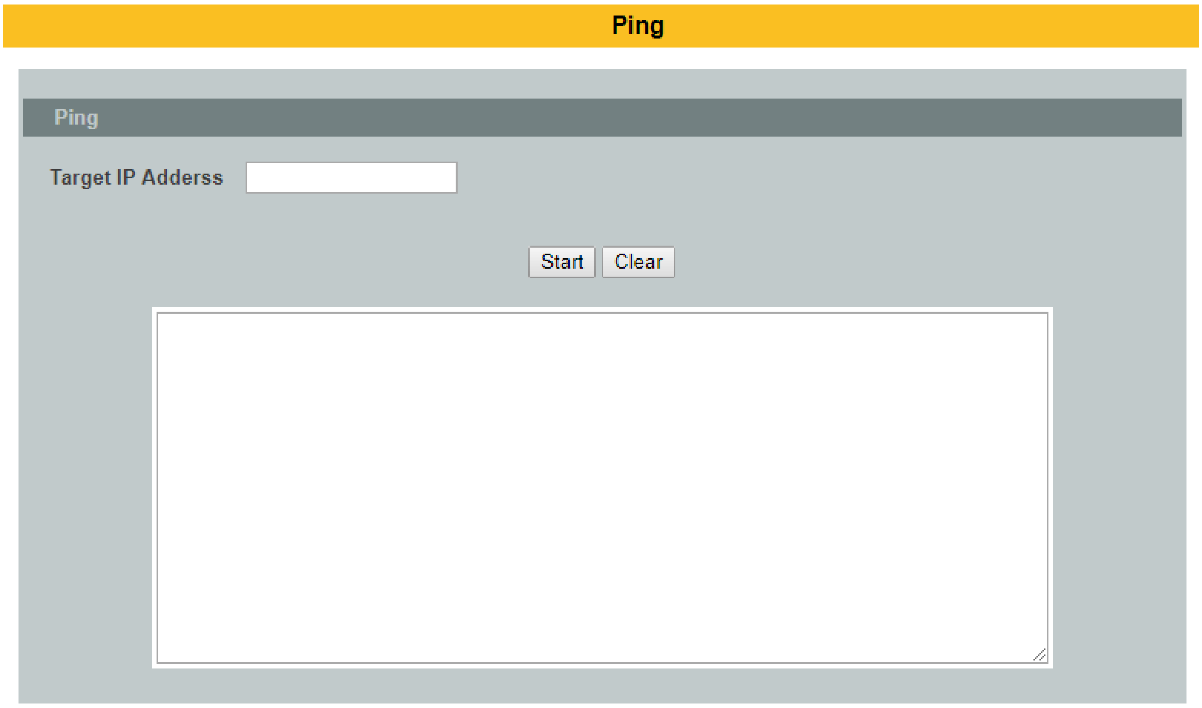
MIB File: INS-8648P_MIB.zip

GSDML File: INS-8648P_GSDML.zip

File Type	Select whether you need to upload either MIB file or GSDML file
IP Address	Enter the IP address of the remote TFTP server in dotted decimal notation.

10.5. Ping

You can ping to any switch using its IP address.


Ping

Ping

Target IP Adderss:

IP Address	Enter the IP address of the remote switch you need to ping in dotted decimal notation.
Start	Enter to ping
Clear	Clears the information in table

10.6. User Account

10.6.1. Introduction

The Switch allows users to create up to 6 user account. The user name and the password should be the combination of the digit or the alphabet. The last admin user account cannot be deleted. Users should input a valid user account to login the CLI or web management.

User Authority:
The Switch supports two types of the user account, admin and normal. The **default** user's account is **username(admin) / password(admin)**.

- admin - read / write.
- normal - read only.
  ; Cannot enter the privileged mode in CLI.
  ; Cannot apply any configurations in web.

The Switch also supports backdoor user account. In case of that user forgot their user name or password, the Switch can generate a backdoor account with the system's MAC. Users can use the new user account to enter the Switch and then create a new user account.

Default Settings

Maximum user account	: 6.
Maximum user name length	: 32.
Maximum password length	: 32.
Default user account for privileged mode	: admin / admin.

Notices

The Switch allows users to create up to 6 user account.
The user name and the password should be the combination of the digit or the alphabet.
The last admin user account cannot be deleted.
The maximum length of the username and password is 32 characters.

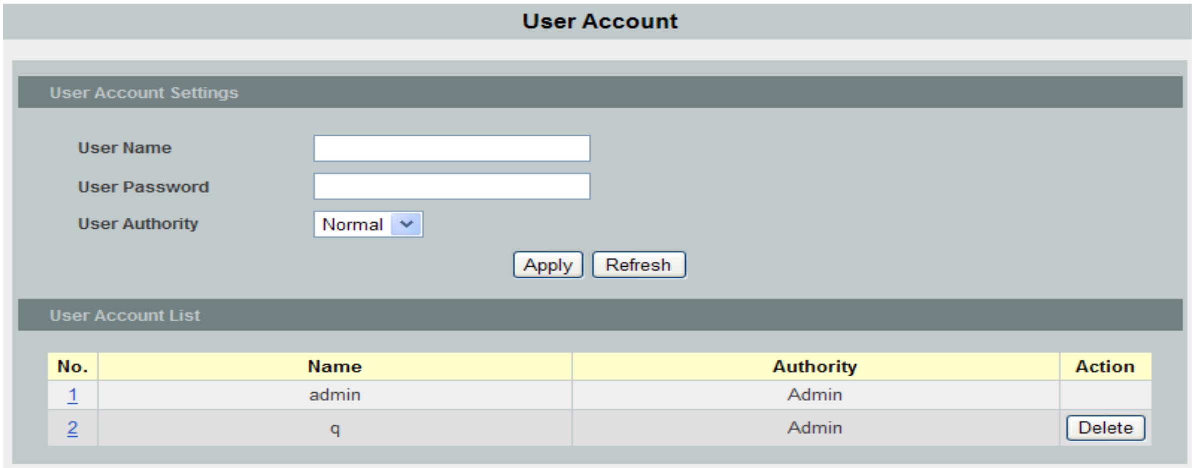
10.6.2. CLI Configuration

Node	Command	Description
enable	show user account	This command displays the current user accounts.
configure	add user USER_ACCOUNT PASSWORD (normal|admin)	This command adds a new user account.
configure	delete user USER_ACCOUNT	This command deletes a present user account.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#add user q q admin
L2SWITCH(config)#add user 1 1 normal
```

10.6.3. Web Configuration



User Account

User Account Settings

User Name:

User Password:

User Authority: Normal

User Account List

No.	Name	Authority	Action
1	admin	Admin	
2	q	Admin	Delete

Parameter	Description
User Name	Type a new username or modify an existing one.
User Password	Type a new password or modify an existing one. Enter up to 32 alphanumeric or digit characters.
User Authority	Select with which group the user associates: **admin** (read and write) or **normal** (read only) for this user account.
Apply	Click **Apply** to add/modify the user account.
Refresh	Click **Refresh** to begin configuring this screen afresh.
User Account List	
No.	This field displays the index number of an entry.
User Name	This field displays the name of a user account.
User Password	This field displays the password.
User Authority	This field displays the associated group.
Action	Click the **Delete** button to remove the user account. Note: You cannot delete the last admin accounts.

Customer support

For all questions relate to the IEN-8648-PN or any other Volktek product, please contact Volktek customer support:

Address	Volktek Customer Support 4F, 192 Liancheng Road, Zhonghe District, New Taipei City 23553, Taiwan
Phone	+886-2-8242-1000
Fax	+886-2-8242-3333
E-mail	*support@volktek.com*
Website	www.volktek.com

ISO 9001 Certified