# SFC8100 Series Switch

# User Guide

# Contents

# 1. **Introduction**

## 1.1. **Product Introduction**

### 1.1.1. **Product overview**

The SFC8100 Series products are managed 10 Gigabit Ethernet switches designed for industrial use. They feature 10/100/1000Mbps TP ports and SFP slots that support 100M/1G/10G Base-X.

The 10-Gigabit Managed Industrial Ethernet Switches can automatically identify the correct transmission speed and determine the Port's Full/Half Duplex mode. These switches can handle large-scale data transmission in secure topologies connected to backbones or servers. Additionally, to ensure low latency and high data integrity, they support the store-and-forward transmission method, which removes unnecessary traffic and relieves congestion on critical network paths.

Through an intelligent address recognition algorithm, this industrial managed 10 Gigabit Ethernet switch can recognize up to 32.000 different MAC addresses and provide complete transmission speed filtering and forwarding capabilities.
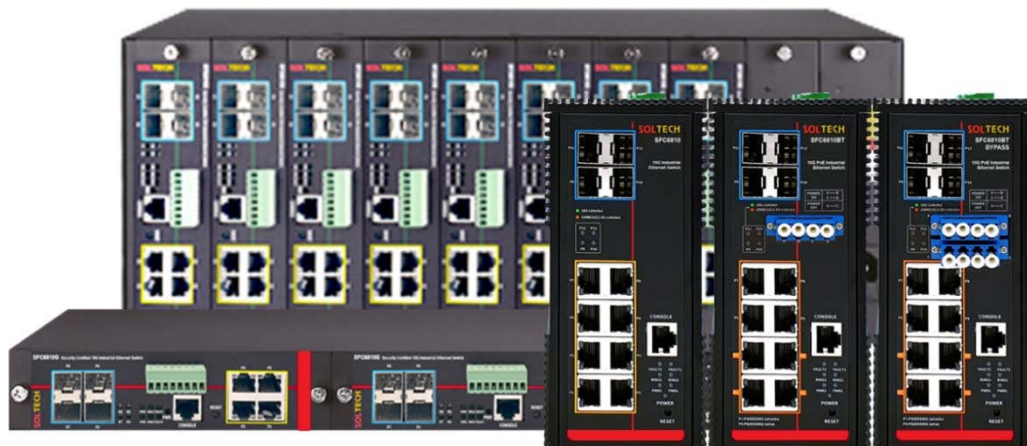


| Model | TP Port (1Gbps) | PoE Port | SFP Slot (10Gbps) | Operating Temperature | Remarks (S-Ring, ERPS, Power Redundancy) |
|---|---|---|---|---|---|
| SFC8100 | 8 ports | - | 4 slots | -40℃ ~ 80℃ | |
| SFC8100-BP_2x2 | 8 ports | - | 4 slots | -40℃ ~ 80℃ | 2x2 BYPASS Support |
| SFC8100-BP_4x4 | 8 ports | - | 4 slots | -40℃ ~ 80℃ | 4x4 BYPASS Support |
| SFC8100BT | 8 ports | 4PoE (at)+ 4PoE (bt) / PoE 240W | 4 slots | -40℃ ~ 70℃ | |
| SFC8100BT-BP_2x2 | 8 ports | 4PoE (at)+ 4PoE (bt) / PoE 240W | 4 slots | -40℃ ~ 70℃ | 2x2 BYPASS Support |
| SFC8100BT-BP_4x4 | 8 ports | 4PoE (at)+ 4PoE (bt) / PoE 240W | 4 slots | -40℃ ~ 70℃ | 4x4 BYPASS Support |
| SFC8100G | 4 ports | - | 4 slots | 0℃ ~ 60℃ | |

## 1.2. Product Features

## 1.2.1. Physical Port

### 1.2.1.1. SFC8100

- 8 10/100/1000BASE-T RJ45 Copper ports with LED

- 4 100/1000/10GBASE-X SFP+ slot

- SFP Slot status LED

- Console interface for basic managements and setup

- Redundant power with reverse polarity protection

### 1.2.1.2. SFC8100-BP_2x2

- 8 10/100/1000BASE-T RJ45 Copper ports with LED

- 4 100/1000/10GBASE-X/SFP+ slot

- SFP Slot status LED

- LC Type 2x2 Bypass Ports

- Console interface for basic managements and setup

- Redundant power with reverse polarity protection

### 1.2.1.3. SFC8100-BP_4x4

- 8 10/100/1000BASE-T RJ45 Copper ports with LED

- 4 100/1000/10GBASE-X/SFP+ slot

- SFP Slot status LED

- LC Type 4x4 Bypass Ports

- Console interface for basic managements and setup

- Redundant power with reverse polarity protection

## 1.2.1.4. SFC8100BT

- 8 10/100/1000BASE-T RJ45 Copper ports with LED

- IEEE 802.3af/at 4 Port(5~8 Port) + IEEE 802.3af/at/bt 4 Port(1~4 Port)

- PoE Budget : 240W

- 4 100/1000/10GBASE-X/SFP+ slot

- SFP Slot status LED

- Console interface for basic managements and setup

- Redundant power with reverse polarity protection

## 1.2.1.5. SFC8100BT-BP_2x2

- 8 10/100/1000BASE-T RJ45 Copper ports with LED

- IEEE 802.3af/at 4 Port(5~8 Port) + IEEE 802.3af/at/bt 4 Port(1~4 Port)

- PoE Budget : 240W

- 4 100/1000/10GBASE-X/SFP+ slot

- SFP Slot status LED

- LC Type 2x2 Bypass Ports

- Console interface for basic managements and setup

- Redundant power with reverse polarity protection

## 1.2.1.6. SFC8100BT-BP_4x4

- 8 10/100/1000BASE-T RJ45 Copper ports with LED

- IEEE 802.3af/at 4 Port(5~8 Port) + IEEE 802.3af/at/bt 4 Port(1~4 Port)

- PoE Budget : 240W

- 4 100/1000/10GBASE-X/SFP+ slots

- SFP Slot status LED

- LC Type 4x4 Bypass Ports

- Console interface for basic managements and setup

- Redundant power with reverse polarity protection

## 1.2.1.7. **SFC8100G-1U**

- SFC8100G-1U : Supports 2-slot operation with SFC8100G Module

- Dual power redundancy support and power LED

- SFC8100G Module
    - 4 10/100/1000BASE-T RJ45 Copper ports with LED
    - 4 100/1000/10GBASE-X/SFP+ slots
    - SFP Slot status LED
    - Console interface for basic managements and setup

## 1.2.1.8. **SFC8100G-4U**

- SFC8100G-4U : Supports 8-slot operation with SFC8100G Module

- Dual power redundancy support and power LED

- SFC8100G Module
    - 4 10/100/1000BASE-T RJ45 Copper ports with LED
    - 4 100/1000/10GBASE-X/SFP+ slots
    - SFP Slot status LED
    - Console interface for basic managements and setup

## 1.2.2. Common features

## 1.2.2.1. Layer2 Features

- High performance of Store-and-Forward architecture and runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth

- Storm Control support
  - Broadcast / Multicast / Unknown unicast

- Supports VLAN
  - IEEE 802.1Q tagged VLAN
  - Up to 255 VLANs groups, out of 4094 VLAN IDs
  - Supports provider bridging (VLAN Q-in-Q, IEEE 802.1ad)
  - Private VLAN Edge (PVE)
  - Protocol-based VLAN
  - MAC-based VLAN
  - Voice VLAN
  - GVRP (GARP VLAN Registration Protocol)

- Supports Spanning Tree Protocol
  - IEEE 802.1D Spanning Tree Protocol (STP)
  - IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
  - IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), spanning tree by VLAN
  - BPDU Guard

- Supports Link Aggregation
  - 802.3ad Link Aggregation Control Protocol (LACP)
  - Cisco ether-channel (static trunk)
  - Maximum 10 trunk groups, up to 16 ports per trunk group

- Provides port mirroring (1-to-1 / Many-to-1)

- Port mirroring to monitor the incoming or outgoing traffic on a particular port

- Loop protection to avoid broadcast loops

## 1.2.2.2. Power over Ethernet (*SFC8100BT, SFC8100BT-BP)

- Complies with IEEE 802.3af / at / bt Power over Ethernet PSE

- Selectable PoE mode : IEEE 802.3af/at/bt

- Ports 1 to 4 support up to Max. 90 watts; port 5 to 8 support up to Max. 30 watts

- Each port supports 56V DC power to PoE powered device

- PoE budget: 240W

- Auto detects Powered Device (PD)

- Circuit protection prevents power interference between ports

## 1.2.2.3. Quality of Service

- Ingress Shaper and Egress Rate Limit per port bandwidth control

- 8 priority queues on all switch ports

- Traffic classification
  - IEEE 802.1p CoS
  - TOS / DSCP / IP Precedence of IPv4/IPv6 packets
  - IP TCP/UDP port number
  - Typical network application

- Strict priority and Weighted Round Robin (WRR) Cos policies

- Supports QoS and In/Out bandwidth control on each port

- Traffic-policing on the switch port

- DSCP remarking

## 1.2.2.4. Multicast

- Supports IPv4 IGMP Snooping v1, v2 and v3

- Supports IPv6 MLD Snooping v1 and v2

- Querier mode support

- IPv4 IGMP Snooping port filtering

- IPv6 MLD Snooping port filtering

- Multicast VLAN Registration(MVR) support

## 1.2.2.5. Security

- Authentication
    - Built-in RADIUS client to co-operate with the RADIUS servers
    - TACACS+ login users access authentication
    - RADIUS / TACACS+ users access authentication
    - Guest VLAN assigns clients to a restricted VLAN with limited services

- Access Control List
    - IP-based Access Control List (ACL)
    - MAC-based Access Control List

- Source MAC / IP address binding

- DHCP Snooping to filter un-trusted DHCP messages

- Dynamic ARP Inspection discards ARP packets with invalid MAC address to IP address binding

- IP Source Guard prevents IP spoofing attacks

- Auto DoS rule to defend DoS attack

- IP address access management to prevent unauthorized intruder

## 1.2.2.6. Management

- IPv4 and IPv6 dual stack management

- Switch Management Interfaces

    - Console / Telnet Command Line Interface
    - Web(http/https) switch management
    - SNMP v1, V2c, and v3 switch management
    - SSH v2.0 service secure access
    - HTTPS SSL/TLS v1.2 Service for Secure Connections

- SNMP Management

    - Four RMON groups (history, statistics, alarms, and events)
    - SNMP trap for interface Link Up and Link Down notification

- IPv6 IP Address / NTP / DNS management

- Built-in Trivial File Transfer Protocol (TFTP) client

- BOOTP and DHCP for IP address assignment

- System Maintenance

    - Firmware upload/download via HTTP/TFTP

    - Reset button for system reboot or reset to factory default

    - Dual images

- DHCP Relay

- DHCP Option82

- DHCP Server

- User Privilege levels control

- NTP (Network Time Protocol)

- Link Layer Discovery Protocol (LLDP) and LLDP-MED

- Network Diagnostic

    - ICMPv6 / ICMPv4 Remote Ping

    - Cable Diagnostic technology provides the mechanism to detect and report potential cabling issues

- SMTP / Syslog remote alarm

- System Log

## 1.2.2.7. Redundant Power System

- DC 36~56V Dual power (SFC8100 / SFC8100-BP)

- DC 56V only products (SFC8100BT, SFC8100BT-BP)

- SFC8100G-1U supports AC/DC redundancy power

    - AC Power : 100~240Vac, 50/60Hz

    - DC Power : 36~56Vdc

    SFC8100G-4U supports AC Power redundancy

    - AC Power : 100~240Vac, 50/60Hz

- Active-active redundant power failure protection

- Backup of catastrophic power failure on one supply

- Fault tolerance and resilience

- Reverse polarity protection

SOLTECH
INFONET INC.

## 1.3. Product Specification

| Product | SFC8100 | SFC8100-BP_2x2<br>SFC8100-BP_4x4 | SFC8100BT | SFC8100BT-BP_2x2<br>SFC8100BT-BP_4x4 | SFC8100G-1U<br>SFC8100G-4U |
|---|---|---|---|---|---|
| **Hardware Specifications** | | | | | |
| Copper Ports | 8 10/100/1000Mbps RJ45 auto-MDI/MDI-X Ports | | | | 4 10/100/1000Mbps RJ45 auto-MDI/MDI-X Ports |
| Fiber Slots | 4 100/1000/10000Mbps SFP Slots | | | | |
| Console | 1 x RJ45 serial port (Baud Rate : 115200) | | | | |
| Reset Button | < 2sec : No Action<br><10sec : Default Reset (keep ip address)<br>>10sec : Factory Reset (All the configurations to default values) | | | | |
| Power Requirements | DC 36 ~ 56V | | DC 56V | | AC 100 ~240V<br>DC 36 ~ 56V |
| Power Consumption | DC 12.7W /<br>DC 23.9W | DC 13.9W /<br>DC 25.1W | DC 14.7W /<br>DC 266W | DC 15.9W /<br>DC 267.2W | 1U : 26.1W /  49.8W<br>4U : 168.6W / 201.7W |
| Operating Temperature | -40℃ ~ 80℃ | | -40℃ ~ 70℃ | | 0℃ ~ 60℃ |
| Size (WxDxH) | 74x130x166.5 (mm) | | | | 1U: 416x241x44(mm)<br>4U: 443.5x256x174.5(mm) |
| **Switching Specifications** | | | | | |
| Switch Architecture | Store-and-Forward | | | | Store-and-Forward |
| Switch Fabric | 96Gbps | | | | 88Gbps |
| Throughput | 71.4Mpps | | | | 65.4Mpps |
| CPU | CPU MIPS24Kec Core 500MHz (32bit) | | | | |
| RAM/<br>Flash Memory | 256MB/16MB | | | | |
| MAC Address Table | 32K | | | | |
| Data Buffer | 32Mb | | | | |

| Flow Control | IEEE 802.3x pause frame for full duplex<br>Back pressure for half duplex | |
|---|---|---|
| Jumbo Frame | 10K | |
| Alarm Contact | 1 relay output with current carrying capacity of 12~24Vdc @ 1A | 2 relay output with current carrying capacity of 12~24Vdc @ 1A |
| Digital Input | 1 input with the same ground, but electrically isolated from the electronics. | 2 input with the same ground, but electrically isolated from the electronics. |
| **Software Functions** | | |
| Port Configuration | - Port disable / enable<br>- Auto-negotiation 10/100/1000Mbps full and half duplex mode selection<br>- Flow Control disable / enable | |
| Port Status | Display each ports speed duplex mode, link status, flow control status, auto-negotiation status | |
| VLAN | Port-Based / 802.1Q Tagged Based VLAN, Up to 255 VLAN groups<br>Q-in-Q tunneling<br>Private VLAN Edge (PVE)<br>MAC-based VLAN<br>Protocol-based VLAN<br>Voice VLAN<br>MVR (Multicast VLAN Registration)<br>Up to 255 VLAN groups, out of 4096 VLAN ID | |
| Link Aggregation | IEEE 802.3ad LACP / Static Trunk<br>Supports 5 groups of 8-Port trunk | |
| QoS | 4 Priority Queue and traffic classification based on 802.1p priority, DSCP field in IP packet | |
| IGMP/MLD snooping | IGMP (v1/v2/v3) Snooping, up to 255 multicast Groups<br>MLD (v1/v2) Snooping, up to 255 multicast Groups | |
| Access Control List | IP-Based ACL / MAC-Based ACL<br>Up to 123 entries | |
| Bandwidth Control | Per port bandwidth control<br>Ingress: 500Kb ~ 1000Mbps<br>Egress: 500Kb ~ 1000Mbps | |

| Port Mirror | One to Multi-port and the monitor mode is RX |
|---|---|
| SNMP MIBs | RFC-1213 MIB-II<br>IF-MIB<br>RFC-1493 Bridge MIB<br>RFC-1643 Ethernet MIB<br>RFC-2863 Interface MIB<br>RFC-2665 Ether-Like MIB<br>RFC-2819 RMON MIB (Group 1,2,3,9)<br>RFC-2737 Entity MIB<br>RFC-2618 RADIUS Client MIB<br>RFC-2933 IGMP-STD_MIB<br>RFC3411 SNMP-Frameworks-MIB<br>LLDP<br>MAU_MIB |
| Ring Protocol | ERPS, STP, RSTP, MSTP, S-Ring |
| Inter-VLAN Routing | Supported |
| Static Routes | 128 IPv4 Routes |
| **Standards Conformance** | |
| Network Standards | IEEE 802.3 10Base-T Ethernet<br>IEEE 802.3u 100Base-TX/100Base-FX Fast Ethernet<br>IEEE 802.3z Gigabit Ethernet (SX/LX)<br>IEEE 802.3ab Gigabit 1000T<br>IEEE 802.3x Flow Control and Back pressure<br>IEEE 802.3ad Port trunk with LACP<br>IEEE 802.1D Spanning tree protocol<br>IEEE 802.1w Rapid Spanning Tree protocol<br>IEEE 802.1s Multiple spanning tree protocol<br>IEEE 802.1p Class of service<br>IEEE 802.1Q VLAN Tagging<br>IEEE 802.1ab LLDP<br>RFC 768 UDP<br>RFC 793 TFTP<br>RFC 791 IP<br>RFC 792 ICMP<br>RFC 2068 HTTP |

| | |
|---|---|
| | RFC 1112 IGMP version 1 |
| | RFC 2236 IGMP version 2 |
| | RFC 3376 IGMP version 3 |
| | RFC3590 MLDv1 |
| | RFC4604 MLDv2 |
| | ITU-T G.8032 Ethernet Ring Protection Switching |
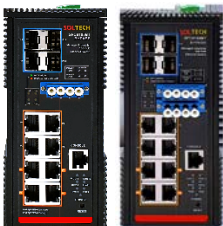
## 1.4. Product Contents

| | SFC8100 Series | SFC8100-1U | SFC8100-1U(DC) | SFC8100-4U |
|---|---|---|---|---|
| Industrial Managed 10G Ethernet Switch | O | X (Sold separately) | X (Sold separately) | X (Sold separately) |
| Wall Mount Bracket | O | X | X | X |
| DIN-Rail Mount Bracket | O | X | X | X |
| Rack Mount Bracket | X | O | O | O |
| Fixed Screw | O | O | O | O |
| AC Power Cable | X | 2 EA | 1 EA | 2 EA (Sold separately Power Module) |

If any of the contents are missing or damaged and need to be repaired, please repack the product and accessories in the box and contact the manufacturer or dealer.

# 2. Exterior

## 2.1. Model & Exterior

| Model | Exterior | Port Information | Product Size |
|---|---|---|---|
| SFC8100 |  | 10/100/1000BASE-T Port 8<br>1G/10G SFP Slot 4<br>Console Port 1<br>RESET Switch 1 (for Default-config) | 74x130x166.5 (mm) |
| SFC8100-BP |  | 10/100/1000BASE-T Port 8<br>1G/10G SFP Slot 4<br>BYPASS 4x4, 2x2<br>Console Port 1<br>RESET Switch 1 (for Default-config) | 74x130x166.5 (mm) |
| SFC8100BT |  | 10/100/1000BASE-T Port 8<br>4 PoE(at) + 4 PoE(bt)<br>1G/10G SFP Slot 4<br>Console Port 1<br>RESET Switch 1 (for Default-config) | 74x130x166.5 (mm) |
| SFC8100BT-BP |  | 10/100/1000BASE-T Port 8<br>4 PoE(at) + 4 PoE(bt)<br>1G/10G SFP Slot 4<br>BYPASS 4x4, 2x2<br>Console Port 1<br>RESET Switch 1 (for Default-config) | 74x130x166.5 (mm) |
| SFC8100G |  | 10/100/1000BASE-T Port 4<br>1G/10G SFP Slot 4<br>Console Port 1<br>RESET Switch 1 (for Default-config) | 173x152x43 (mm) |
| SFC8100G-1U |  | SFC8100G Slot 2 | 416x241x44 (mm) |
| SFC8100G-4U |  | SFC8100G Slot 8 | 444x256x174 (mm) |

## 2.2. LED Condition

The front panel LED indicates the immediate status of power, system status, port link/active and PoE to monitor, diagnose and resolve potential issues with connected devices.

The following diagram shows the switch LED indicators for each product in the SFC8100 Series.

## 2.2.1. SFC8100 / SFC8100BP



| | LED | Color | Status | Status Description |
|---|---|---|---|---|
| **System** | POWER | Green | On | Switch Power On |
| | PWR1 | Green | On | Power Input 1 |
| | PWR2 | Green | On | Power Input 2 |
| **S-RING** | RING1 | Green | On | S-Ring ID 1 Slave Mode |
| | | | Flashing | S-Ring ID 1 Master Mode |
| | RING2 | Green | On | S-Ring ID 2 Slave Mode |
| | | | Flashing | S-Ring ID 2 Master Mode |
| | FAULT1 | Green | On | S-Ring ID 1 Failover |
| | FAULT2 | Green | On | S-Ring ID 2 Failover |
| **UTP (1~8)** | 10/100Mbps Link/ACT | Orange | On | UTP port link up |
| | | | Off | UTP port link down |
| | 1000Mbps Link/ACT | Green | | |
| | | | Flashing | Data communicating |
| **SFP (9~12)** | 100M/1Gbps Link/ACT | Orange | On | SFP Port link up |
| | | | Off | SFP Port link down |
| | 10Gbps Link/ACT | Green | | |
| | | | Flashing | Data communicating |

## 2.2.2. SFC8100BT / SFC8100BT-BP



| | LED | Color | Status | Status Description |
|---|---|---|---|---|
| System | POWER | Green | On | Switch Power On |
| | PWR1 | Green | On | Power Input 1 |
| | PWR2 | Green | On | Power Input 2 |
| S-RING | RING1 | Green | On | S-Ring ID 1 Slave Mode |
| | | | Flashing | S-Ring ID 1 Master Mode |
| | RING2 | Green | On | S-Ring ID 2 Slave Mode |
| | | | Flashing | S-Ring ID 2 Master Mode |
| | FAULT1 | Green | On | S-Ring ID 1 Failover |
| | FAULT2 | Green | On | S-Ring ID 2 Failover |
| UTP (1~8) | 10/100/1000Mbps Link/ACT | Green | On | UTP port link up |
| | | | Off | UTP port link down |
| | | | Flashing | Data communicating |
| PoE (1~8) | PoE PWR | Orange | On | PD (Powered Device) is connected to the port and receiving power |
| | | | Off | No PD is connected to the port or Power is not supplied due to the power limit of the port |
| | | | Flashing | PoE current has overloaded |
| SFP (9~12) | 100M/1Gbps Link/ACT | Orange | On | SFP slot status is connected |
| | | | Off | SFP slot status is not connected |
| | 10Gbps Link/ACT | Green | Flashing | Data communicating |

## 2.2.3. SFC8100G / SFC8100G-1U / SFC8100G-4U



| | LED | Color | Status | Status Description |
|---|---|---|---|---|
| System | POWER | Green | On | Switch Power On |
| | PWR1 | Green | On | Power Input 1 |
| | PWR2 | Green | On | Power Input 2 |
| S-RING | RING1 | Green | On | S-Ring ID 1 Slave Mode |
| | | | Flashing | S-Ring ID 1 Master Mode |
| | RING2 | Green | On | S-Ring ID 2 Slave Mode |
| | | | Flashing | S-Ring ID 2 Master Mode |
| | FAULT1 | Green | On | S-Ring ID 1 Failover |
| | FAULT2 | Green | On | S-Ring ID 2 Failover |
| UTP (1~4) | 10/100Mbps Link/ACT | Orange | On | UTP port link up |
| | | | Off | UTP port link down |
| | 1000Mbps Link/ACT | Green | | |
| | | | Flashing | Data communicating |
| SFP (5~8) | 100M/1Gbps Link/ACT | Orange | On | SFP slot status is connected |
| | | | Off | SFP slot status is not connected |
| | 10Gbps Link/ACT | Green | | |
| | | | Flashing | Data communicating |

## 2.3. Power Input Method

At the top of the SFC8100 Series products (SFC8100, SFC8100BP, SFC8100BT, SFC8100BT-BP), there are two power input slots labeled as "Power1" and "Power2". Depending on the product, the following DC power can be supplied.

- SFC8100, SFC8100BP        : DC Power Input 36~56Vdc@1A ~ / Support Redundant Power System

- SFC8100BT, SFC8100BT-BP : DC Power Input 54~56Vdc@4A ~ / Support Redundant Power System
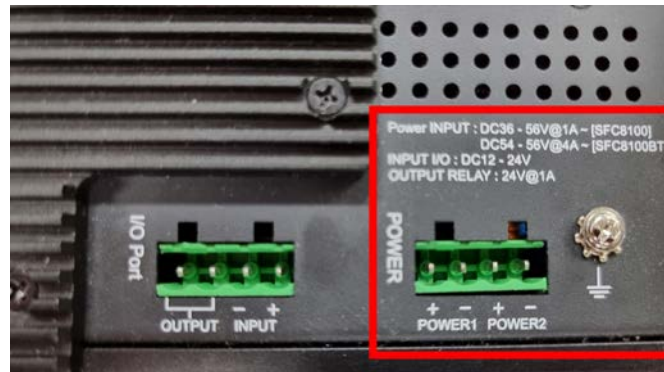


- Among the chassis models of SFC8100G, the SFC8100G-1U product has two power input slots at the rear (AC power input, DC power input), while the SFC8100G-4U product has two power input slots at the front. Depending on the product, the following AC and DC power inputs are supported

- SFC8100G-1U:  AC Power Input 100~240Vac/50~60Hz 1ea, DC Power Input 36~56Vdc 1ea,
                Support Redundant Power System

- SFC8100G-4U: AC Power Input 100 ~ 240Vac / 50 ~ 60Hz 2ea, Support Redundant Power System



SFC8100G-1U Power Supply Unit        SFC8100G-4U Power Supply Unit
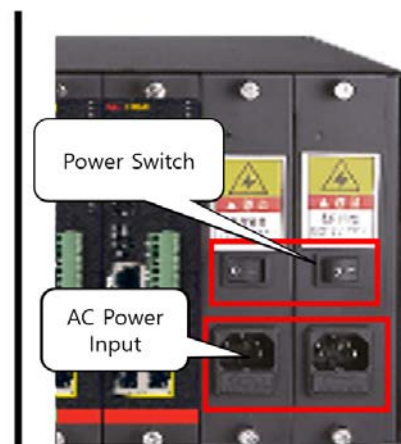
**Power Notice**:

1. The SFC8100 Series products provide reverse voltage protection. If the polarity of the input voltage is reversed, the product will not function.

2. The device requires power to operate. It will not function until power is supplied. If the user's network needs to be active at all times, consider using an Uninterrupted Power Supply (UPS) device. This can prevent network data loss or network downtime.

3. Installing surge suppression devices in some areas can protect the Ethernet PoE Switch from damage caused by unrelated surges or currents, ensuring its safety.

4. Chassis grounding is the practice of connecting the metal frame of electrical devices to the common return part of the circuit's power. While grounding is not always required, a decrease in insulation resistance between the power supply and equipment can lead to problems.

## 2.4. I/O Port Connect Method

At the top of the SFC8100 Series products (SFC8100, SFC8100BP, SFC8100BT, SFC8100BT-BP), there is one set of I/O input (I/O IN+, IN-) and output (I/O OUT) as shown in the diagram below
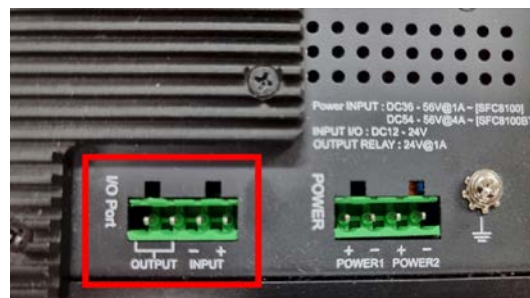


At the top front of SFC8100G-1U/4U, there are two sets of I/O inputs (I/O IN1, I/O IN2) and outputs (I/O OUT1, I/O OUT2) as shown in the diagram below



Power Notice :

- The I/O INPUT should use voltage within the range of 12 ~ 24VDC.

- The I/O OUTPUT should use voltage within the range of 12 ~ 24VDC and current less than 1A. Usage of AC voltage or current greater than 1A is prohibited.

## 2.5. BYPASS Connection Method

In the SFC8100 Series, the front panel of SFC8100-BP(2x2), SFC8100-BP(4x4), SFC8100BT-BP(2x2), and SFC8100BT-BP(4x4) models features LC-type BYPASS ports.



SFC8100-BP (2X2)    SFC8100-BP (4X4)    SFC8100BT-BP (2X2)    SFC8100BT-BP (4X4)

The 2x2 port is appropriate for Wavelength Division Multiplexing (WDM), while the 4x4 port is appropriate for the 2Core method.

The SFC8100-BP(2x2), SFC8100-BP(4x4), SFC8100BT-BP(2x2), and SFC8100BT-BP(4x4) models have BYPASS ports categorized as 2x2 and 4x4, but the connection method is the same.

The BYPASS ports are configured as A, B, C, and D.
When power is supplied, the BYPASS ports are connected as follows: A ➔ B, C ➔ D, allowing fiber data to flow.
When power is disconnected, the connection switches to A ➔ C, continuing the flow of fiber data.
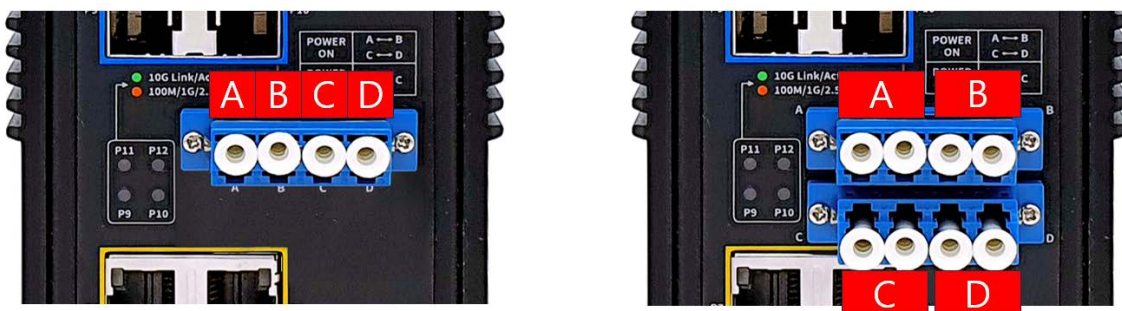


2x2 BYPASS Port                          4x4 BYPASS Port

| BYPASS Fiber Data Flow | |
|---|---|
| Power ON | A ←→ B |
| | C ←→ D |
| Power OFF | A ←→ C |

The followings are data flow examples for the BYPASS product during connection and power on/off.

## 2.5.1. SFC8100-BP (2x2), SFC8100BT-BP (2x2)
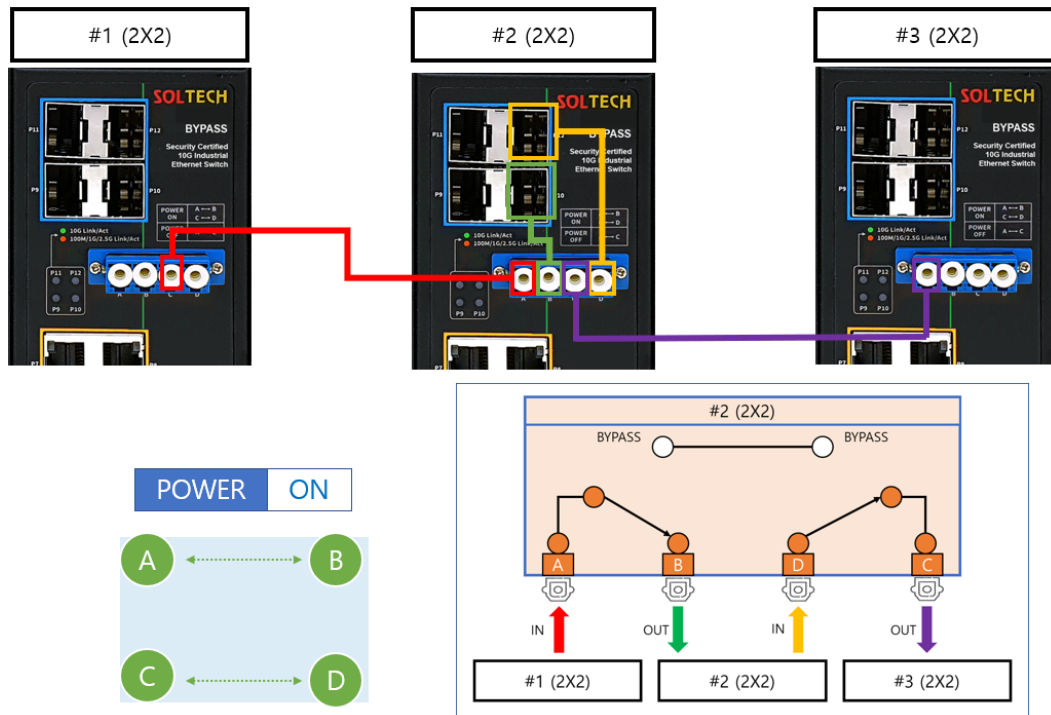


**#2 SFC8100-BP(2X2) POWER ON**
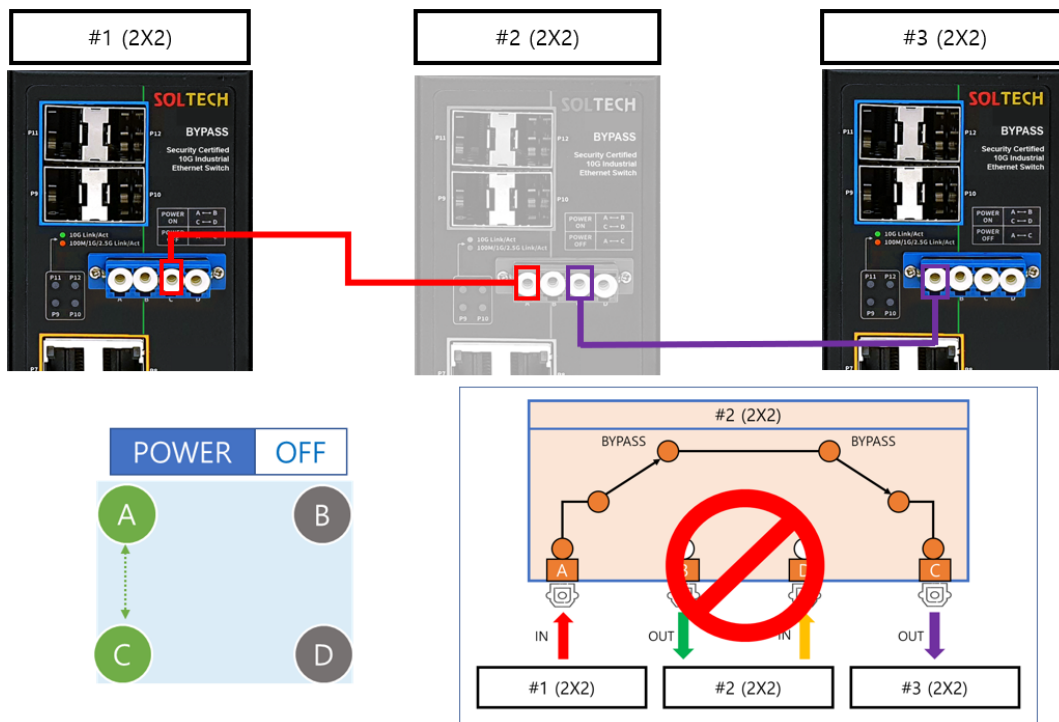


**#2 SFC8100-BP(2X2) POWER OFF**

## 2.5.2. SFC8100-BP (4x4), SFC8100BT-BP (4x4)
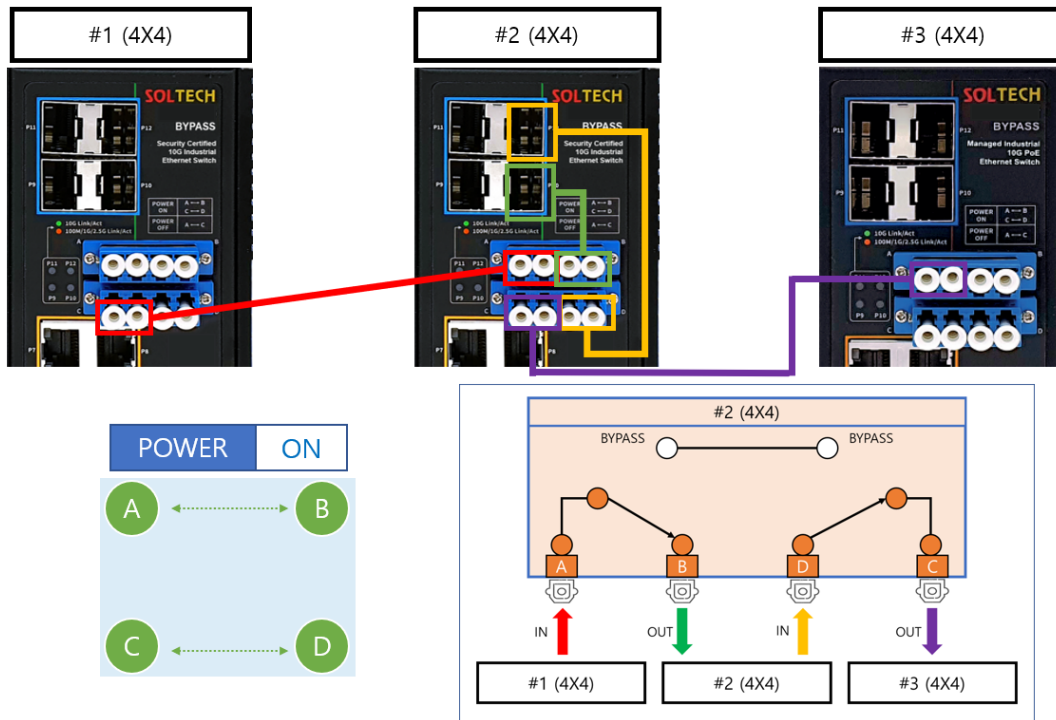


**#2 SFC8100-BP(4X4) POWER ON**
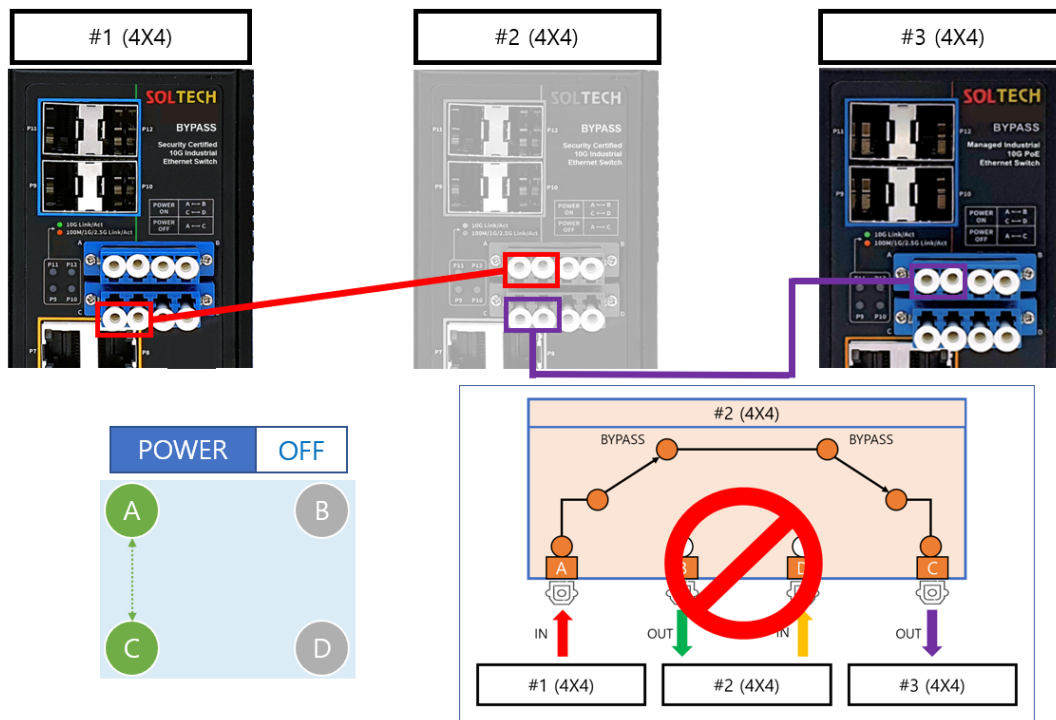


**#2 SFC8100-BP(4X4) POWER OFF**

# 3. **Installation of bracket**

In the basic accessories of the SFC8100 Series products (SFC8100, SFC8100BP, SFC8100BT, SFC8100BT-BP), Wall Mount brackets and DIN-Rail Mount brackets are included. These brackets can be used for mounting the product on walls or DIN-Rails. Bracket installation is completed by aligning the screw holes and assembling the included screws, as shown in the diagram below.

Wall Mount brackets installation

DIN-Rail Mount brackets installation

SOLTECH
INFONET INC.

The basic accessories of the SFC8100G-1U and SFC8100G-4U products include Rack Mount brackets. These brackets allow for mounting on a 19-inch Rack. Bracket installation is completed by aligning the screw holes and fixing them to the 19-inch Rack, as shown in the diagram below.
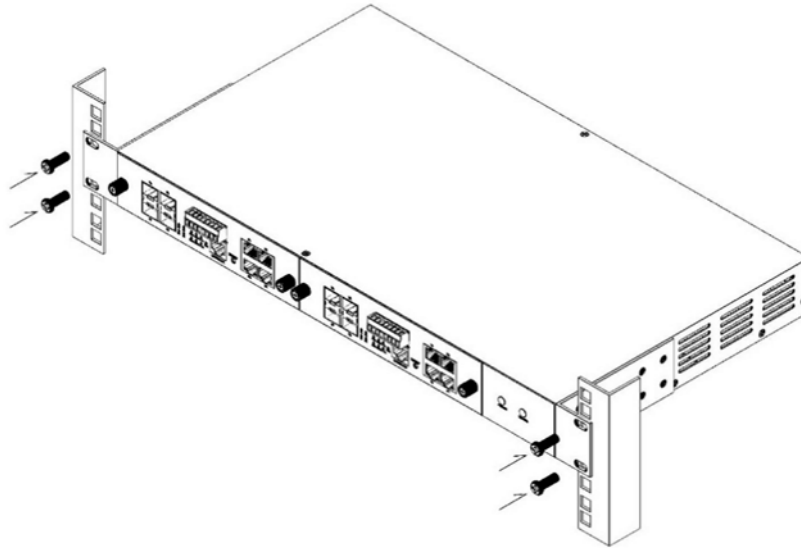


SFC8100G-1U Rack Mounting Diagram
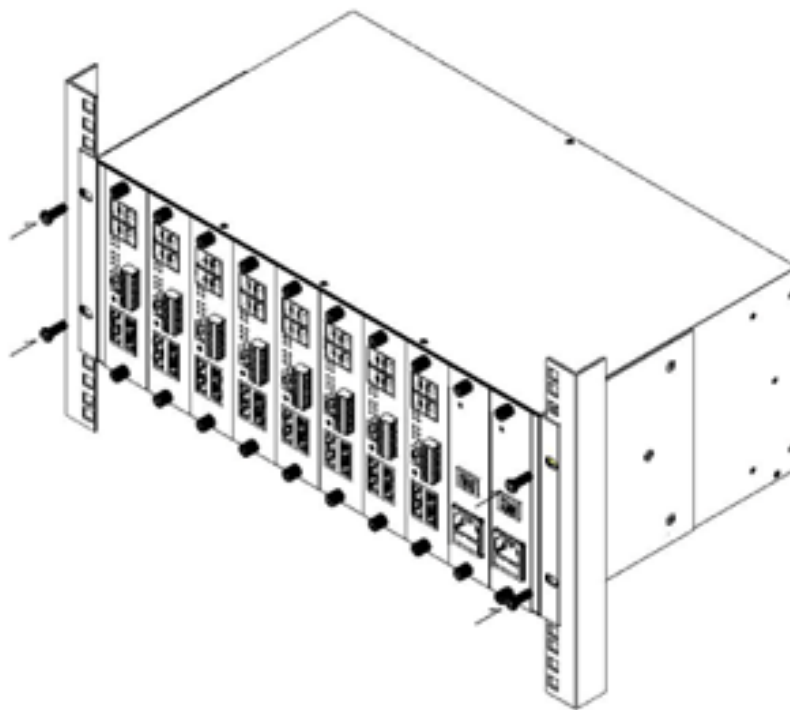


SFC8100G-4U Rack Mounting Diagram

# 4. **Installation of Product**

In this section, we will explain the installation of the Industrial Managed 10G Ethernet Switch and the procedure for connecting devices to the switch. Please follow the steps provided below in the given order to install the Industrial Managed 10G Ethernet Switch on a desktop or shelf.

## 4.1. Installation Procedure for SFC8100 SERIES

Step 1

Place the SFC8100/SFC8100-BP near a 36 ~ 56VDC 60W-rated power source.

Place SFC8100BT/SFC8100BT-BP, near a 56VDC 300W-rated power source.

Place SFC8100G-1U/SFC8100G-4U, near a 100 ~ 240Vac power source.

Notice: When using the PoE feature of SFC8100BT/SFC8100BT-BP, a power source with a capacity of 300W or more is required for stable PoE operation.

Step 2

Maintain sufficient ventilation space between the Industrial Managed 10G Ethernet Switch and surrounding objects.

Step 3

Connect the switch to your network devices.

Notice: The connection to the Industrial Managed 10G Ethernet Switch requires UTP Category 5E specification or higher network cables.

Step 4

Switch Power Supply

A. Connect the power cable to the Industrial Managed 10G Ethernet Switch.

B. Connect the power source cable to the power outlet.

Notice: When the Industrial Managed 10G Ethernet Switch receives power, the power LED (Green) will be continuously lit.

## 4.2. Installation of SFP Module

SFP transceivers module(in the following sections referred to as SFP module) typically provide Hot-pluggable and Hot-swappable functionality. Users can remove or insert the module into the SFP slot of the Industrial Managed 10G Ethernet Switch without the need to power off the switch.
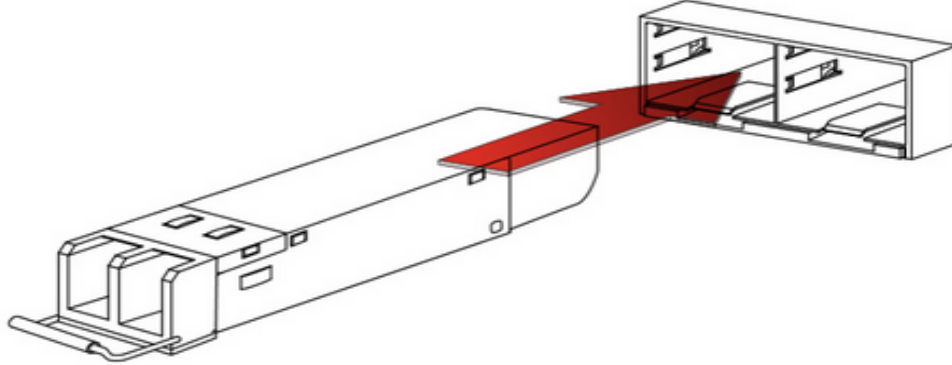


Plug-in the SFP Transceiver Module

Before connecting to other switches, workstations, or media converters, please check the following

A. Ensure that both sides of the SFP module have the same media type.
For example Connect 1000BASE-SX to 1000BASE-SX. / Connect 1000BASE-LX to 1000BASE-LX.

B. Ensure that the SFP module matches the type of fiber optic cable.
For 1000BASE-SX SFP module, use Multi-mode fiber cables with Duplex LC connectors.
For 1000BASE-LX SFP module, use Single-mode fiber cables with Duplex LC connectors.

## 4.3. Installation of Fiber Optic Cable

A. Connect the network cable with Duplex LC connectors to the SFP module.
B. Connect the other end cable to the device with an SFP module inserted into the fiber NIC
(e.g., Gigabit Ethernet Switch or Media Converter)
C. Check the SFP module's proper functioning by using the LED LINK/ACT near the SFP slot on the front of the switch.
D. If the link fails, please check the connection mode of the SFP slot.
Some Fiber NICs may require setting the link mode to '1000 Force.'
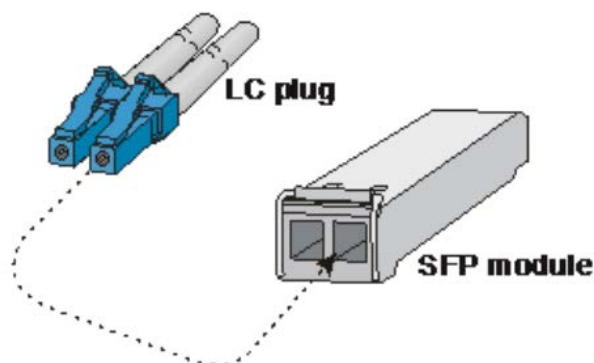
# 4.4. Removing Transceiver Module

A. Check if there is current network activity on the port with the SFP module to be removed, or Disable the port through the Switch/Converter's management interface.

B. Remove the Fiber cable smoothly.

C. Hold the handle of the SFP module horizontally.

D. Carefully pull the module out by holding the handle smoothly.
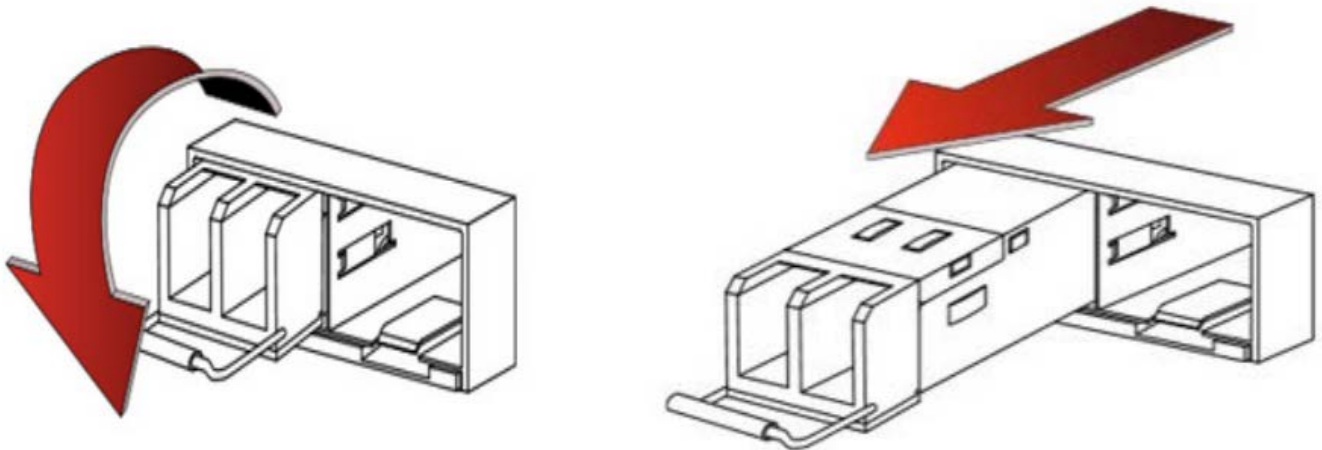


Notice: Please do not pull out the SFP module wildly.

It can damage the Industrial Managed 10G Ethernet Switch or SFP slot.

# 4.5. Operating System

This switch is positioned at the front-end of IT equipment such as IP cameras, IP phones, PCs, printers, and storage devices, where it handles packets from each terminal. It forwards multiple 2nd-layer Virtual LANs (VLANs) to other switches/routers for network segmentation, or it is deployed at connection points between networks with different 3rd-layer VLANs, forwarding IP packets between VLAN interfaces with different address ranges.

In the switch operating environment, it may include external entities such as a log server for storing and managing logs generated by the switch, an authentication server for administrator authentication, an SNMP server for switch management, and an NTP server for time synchronization. Additionally, depending on the product and the required functionalities provided by the switch, other external entities may be included in the operating environment.

The base Operating System Version : RTOS eCos 3.0

-   OpenSSL Version 1.1.1

-   SSH 2.0 – Dropbear_2018.76

# 5. Switch Access Guide

Here's a brief introduction on how to access device

## 5.1. The Initial Defaults Values

The initial values of the equipment are as follows:

| Items | Defaults Values | Note |
|---|---|---|
| Administrator account | admin | |
| Administrator password | admin | |
| Operating mode change password | admin | Same as the Administrator password |
| Console | Enabled | Baud rate : 115200, Data bits : 8 Parity : None Stop bits : 1 |
| SNMP | Disabled | |
| Telnet | Disabled | |
| SSH | Enabled | |
| HTTP/HTTPS | Enabled | HTTP redirection Enabled |
| Default IP Address | 192.168.10.100 | Subnet mask 255.255.255.0/24 |
| Port state | Enabled | |
| Audit data generation | Enabled | |

## 5.2. WEB Interface

## 5.2.1. WEB Login

This page provides a brief overview of accessing the web interface.

1. Users must know IPv4 Address of device to WEB set.

2. Connect AP (LAN interface) with PC (LAN port) using enclosed LAN cable.

3. Access WEB using IPv4 address of AP. (Initial IP - 192.168.10.100).



Privacy error page appears.
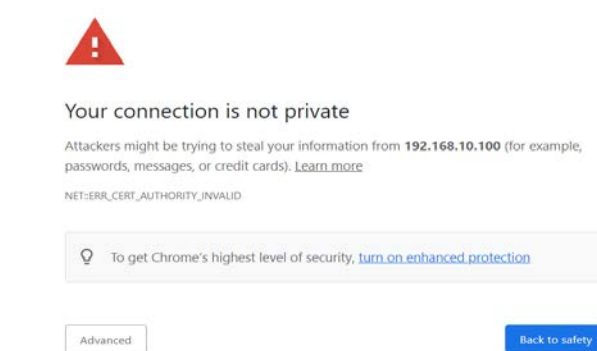


Click Advanced.
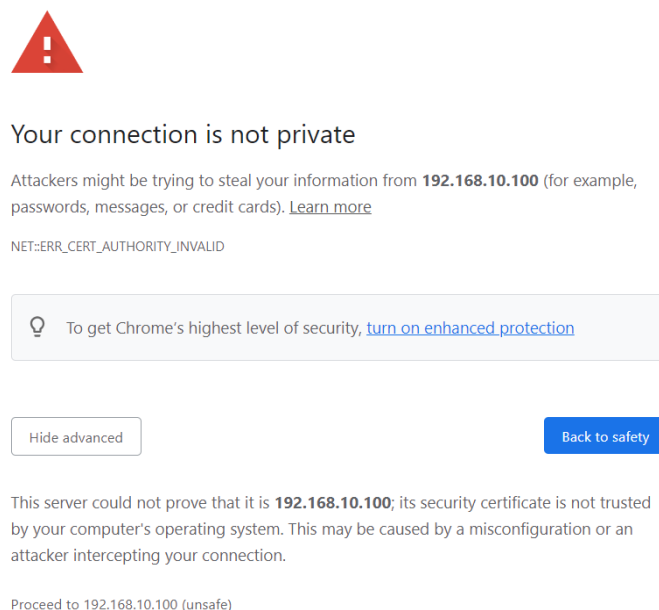


Click Proceed to 192.168.10.100(unsafe)

Sign in page appears.



Enter your Username and Password, then click on "Sign in." (Default ID: admin, PW: admin)

4. Successfully connected to the equipment's web interface.
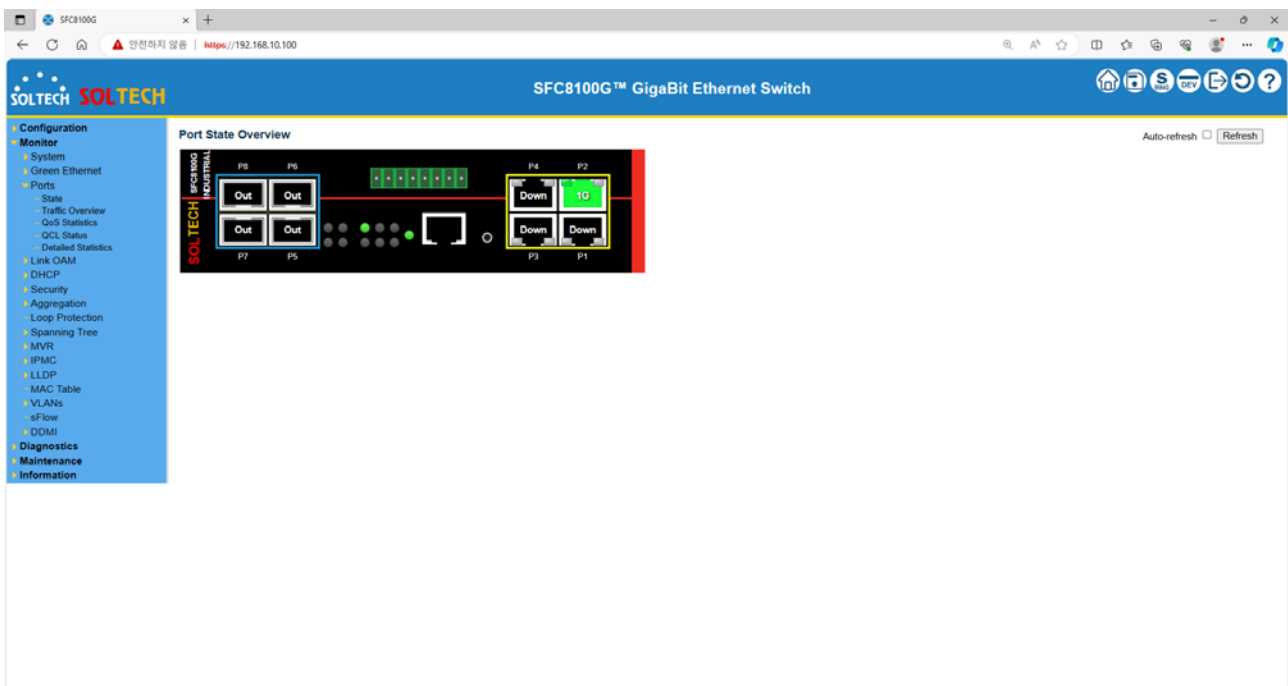
## 5.3. CLI Interface

## 5.3.1. CLI Basic Symbol

This page is the description of symbols commonly used in CLI(Command Line Interface) commands.

| Symbol | Description |
|---|---|
| < > | The symbol indicates that you have to enter a value directly. Put in English, numbers, or special characters. |
| { } | The symbol indicates optional items. You have to choose one. |
| [ ] | The symbol indicates optional items. You do not have to choose at all |
| ( ) | The symbol used to indicate mandatory items that must be filled |
| * | The symbol used in the Port interface to select the entire port |
| \| | The symbol used as a delimiter to represent multiple items |

## 5.3.2. Console

Console setting is used for simple setting, the device has to connect one to one.

Please connect device with RS-232port of PC using Console cable, which is enclosed.

Setting method of below is made by Tera Term(freeware).

1. Setup → Serial Port
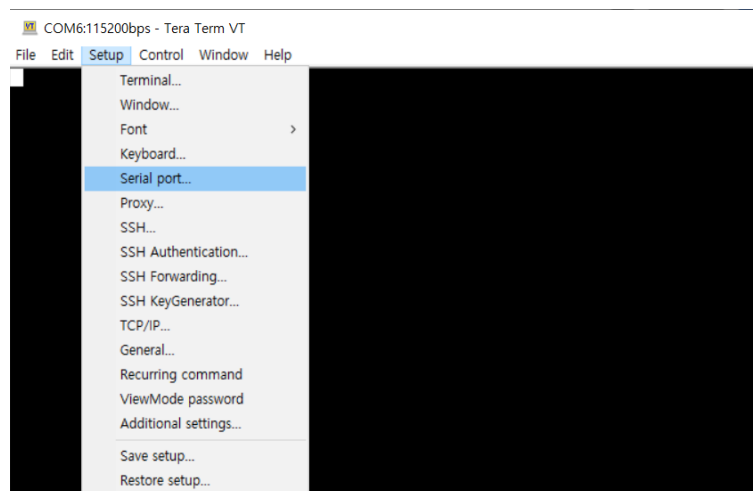
2. Set Serial Port.(Set Speed 115200 like below)
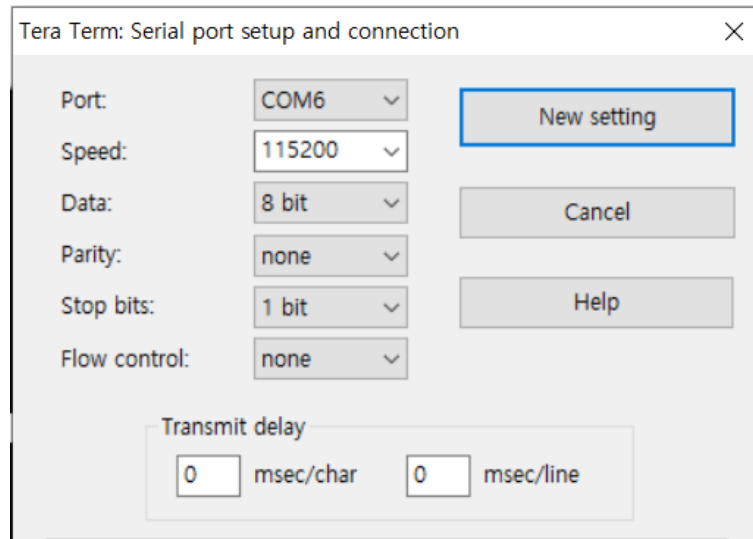


3. Access Device with Console.(New Connection Alt+N)
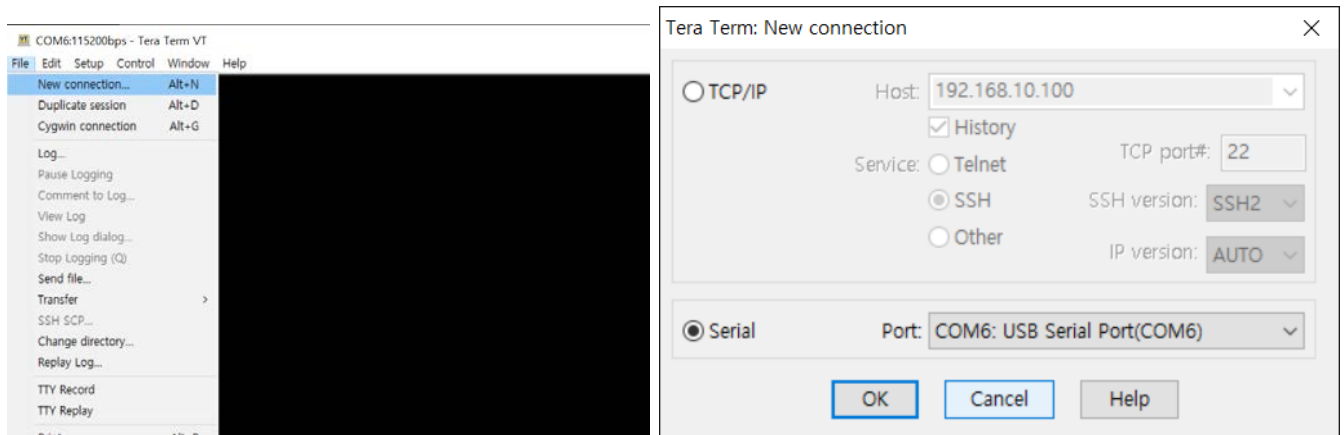


The initial ID and password are both "admin."

4. You are currently connected to the console.(Initial ID-admin, PW-admin or the password you previously set)

After entering the password, type "enable" to enter switch operational mode. (Please reconfirm the password.)

## 5.3.3. Telnet

This page provides an explanation of Telnet connection.

You should follow the same configuration steps as mentioned in item 2 of the console connection.
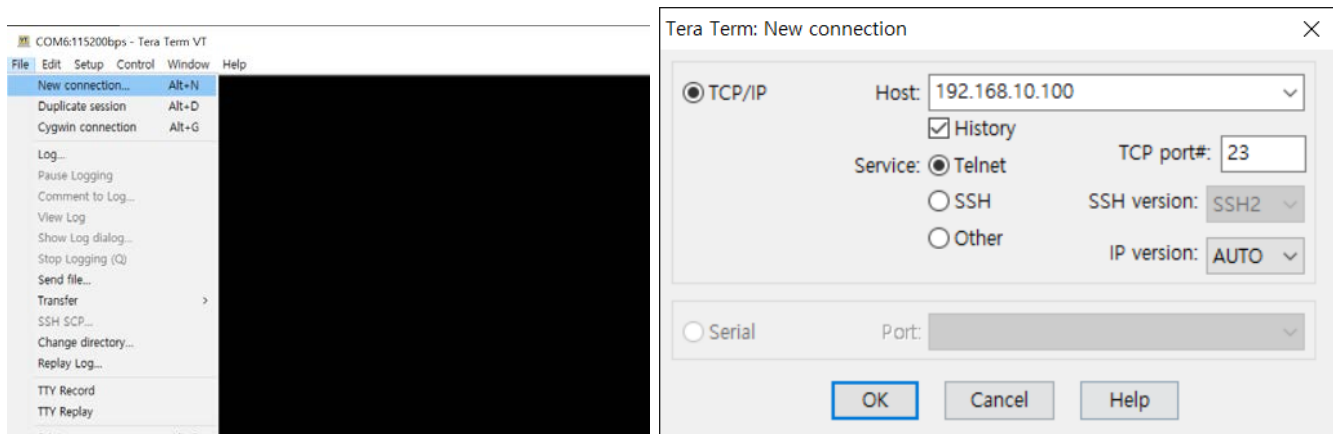


Telnet allows for switch access from a computer within the same network.



After entering the password, type "enable" to enter switch operational mode. (Please reconfirm the password.)

## 5.3.4. SSH

This page provides an explanation of SSH connection.

You should follow the same configuration steps as mentioned in item 2 of the console connection.
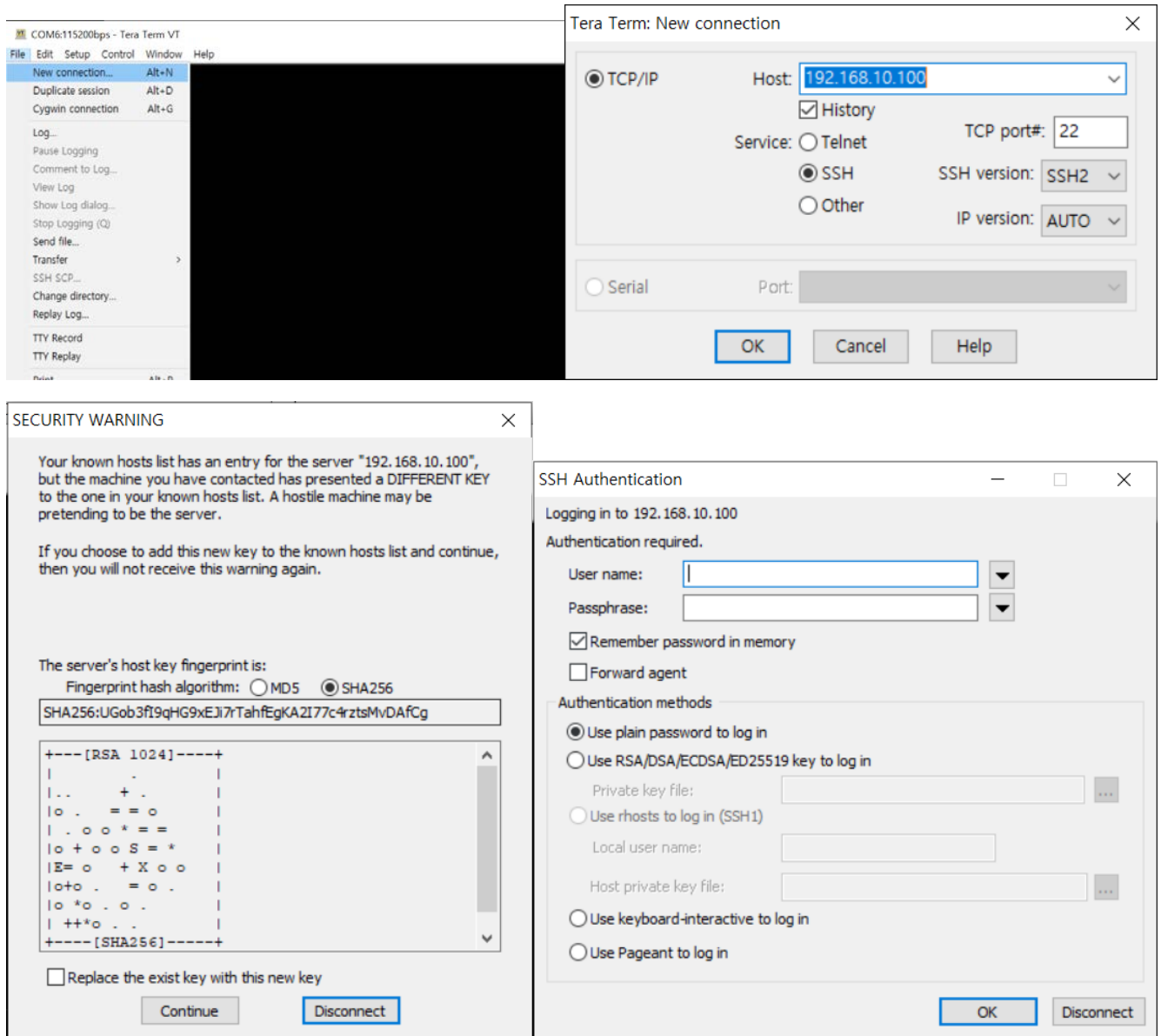


Click "Continue (C)" on the security warning window

Enter your username and password in the SSH Authentication window.



After entering the password, type "enable" to enter switch operational mode. (Please reconfirm the password.)

## 5.4. CLI Basic Command

This page provides an explanation of basic commands used in the Command-Line Interface (CLI).

## 5.4.1. CLI Basic use Key

✓   **TAB key**

When entering a command, pressing the TAB key will either display the next possible command or complete the existing command. When you see '<cr>' displayed in the CLI, it indicates that you can input the command at that point.

✓   **Help**

```
# help
Help may be requested at any point in a command by entering a question
mark '?'.  If nothing matches, the help list will be empty and you must
backup until entering a '?' shows the available options.
Two styles of help are provided:

1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.

2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
```

✓   **'?' key**

Help may be requested at any point in a command by entering a question mark '?'.

```
# ?
clear          Reset functions
configure      Enter configuration mode
copy           Copy from source to destination
delete         Delete one file in flash: file system
dir             Directory of all files in flash: file system
disable        Turn off privileged commands
do             To run exec commands in the configuration mode
enable         Turn on privileged commands
erps           Ethernet Ring Protection Switching
exit           Exit from EXEC mode
firmware       Firmware upgrade/swap
help           Description of the interactive help system
ip             IPv4 commands
```

```
ipv6          IPv6 configuration commands
link-oam       Link OAM configuration
logout        Exit from EXEC mode
more          Display file
no            Negate a command or set its defaults
ping          Send ICMP echo messages
platform      Platform configuration
reload         Reload system.
send           Send a message to other tty lines
show          Show running system information
terminal      Set terminal line parameters
veriphy       VeriPHY keyword
```

✓  **'??' key**

Enter the '??' key, it displays the complete list of commands that can be written in the current state.

## 5.4.2. CLI Basic use Mode

| Command Mode | Access Method | Prompt | Exit or Access Previous Mode |
|---|---|---|---|
| **User Mode** | This is the first level of access. Perform basic tasks and list system information. | **Switch>** | Logout, Exit Command |
| **Privileged Mode** | From the User Mode, enter the "enable" command. | **Switch#** | Exit, Logout, Disable Command |
| **Global Config Mode** | From the Privileged Mode, enter the "configuration terminal" command. | **Switch (Config)#** | Exit, End Command |
| **Interface Config Mode** | From the Global Config mode, enter the "interface <port#>" "interface <VLAN number>" command. | **Switch (config-if)#** **Switch (config-if-vlan)#** | Exit, End Command |

## 5.4.3. CLI Basic Command

✓  **Login**

Users need to input username and password when login firstly.

```
[Console] Username: admin
[Console] Password:
>
```

✓  **Logout**

To log out the current user or log in as a new user, please log out.

```
switch# logout
Exit BYE !!!
###: Press ENTER to get started
```

✓  **Enable**

To Turn on privileged commands, you can use the "enable" command.

```
> enable
Password: *******
#
```

✓  **Disable**

To Turn off privileged commands, you can use the "disable" command.

```
# disable
>
```

✓  **Exit**

To exit mode, you can use the "exit" command.

```
> exit
Exit BYE !!!
###: Press ENTER to get started
```

✓  **Clear**

To delete the remaining records, you can use the "Clear" command.

```
# clear ?
    access           Access management
    access-list      Access list
    eps              Ethernet Protection Switching.
    erps             Ethernet Ring Protection Switching
    ip               Interface Internet Protocol configuration commands
    ipv6             IPv6 configuration commands
    lacp             Clear LACP statistics
    link-oam          Clear Link OAM statistics
    lldp             Clears LLDP statistics.
    logging           System logging message
    mac               MAC Address Table
    mep               Maintenance Entity Point
    mvr               Multicast VLAN Registration configuration
    sflow            Statistics flow.
    spanning-tree    STP Bridge
    statistics       Clear statistics for one or more given interfaces
```

✓  **No**

To negate a command or set its defaults, you can use the "no" command.

```
# no ?
    debug            Debugging functions
    port-security    Port security (MAC limiter)
    terminal         Set terminal line parameters
```

✓  **Terminal**

To set terminal line parameters, you can use the "terminal" command.

```
# terminal ?
    editing          Enable command line editing
    exec-timeout     Set the EXEC timeout
    help             Description of the interactive help system
    history          Control the command history function
    length           Set number of lines on a screen
    width            Set width of the display terminal
```

SOLTECH
INFONET INC.

✓ **Show**

To Show running system information, you can use the "show" command.

```
# show ?
  aaa              Authentication, Authorization and Accounting methods
  access           Access management
  access-list      Access list
  aggregation      Aggregation port configuration
  audit-log        System Audit Log message
  clock            Configure time-of-day clock
  ddmi             DDMI configuration
  eps              Ethernet Protection Switching
  erps             Ethernet Ring Protection Switching
  green-ethernet   Shows green Ethernet status for the switch.
  history          Display the session command history
  interface        Interface status and configuration
  ip               Internet Protocol
  ipmc             IPv4/IPv6 multicast configuration
  ipv6             IPv6 configuration commands
  lacp             LACP configuration/status
  line             TTY line information
  link-oam         Link OAM configuration
  lldp             Display LLDP neighbors information.
  logging          System logging message
  loop-protect     Loop protection configuration
  mac              Mac Address Table information
  mep              Maintenance Entity Point
  module-status    Print Modulte Trhead Status
  monitor          Monitoring different system events
  mvr              Multicast VLAN Registration configuration
  ntp              Configure NTP
  platform         Platform configuration
  poe              Power Over Ethernet.
  port-security    Port Security status - Port Security is a module with no
                   direct configuration.
  privilege        Display command privilege
  process          process
  pvlan            PVLAN configuration
  qos              Quality of Service
```

```
    radius-server      RADIUS configuration
    rmon              RMON statistics
    running-config     Show running system information
    scan-agent        SCAN-AGENT Module
    sflow             Statistics flow.
    snmp              Display SNMP configurations
    spanning-tree      STP Bridge
    sring             SRING Module
    switchport         Display switching mode characteristics
    system            system
    tacacs-server      TACACS+ configuration
    terminal          Display terminal configuration parameters
    user-privilege     Users privilege configuration
    users             Display information about terminal lines
    version           System hardware and software status
    vlan              VLAN status
    voice             Voice appliance attributes
    web               Web
```

✓ **Configure**

To Enter configuration mode, you can use the "configure" command.

```
# configure ?
    terminal    Configure from the terminal
# configure terminal
(config)#
```

✓ **Save-config**

To save the current configuration settings to the Startup-Config, you can use the "save-config" command. This command can be used regardless of the mode.

```
# save-config
###: Running-config saved (by:1) !!!
###: Running-config saved !!!
# copy running-config startup-config
Building configuration...
% Saving 930 bytes to flash:startup-config
```

✓ **Copy running-config startup-config**

To save the running-configuration settings to the Startup-Config, you can use the "copy running-config startup-config" command.
This command can only be used in Privileged mode.

```
# copy running-config startup-config
Building configuration...
% Saving 930 bytes to flash:startup-config
```

✓ **Dir**

To view the Config file currently stored in Flash, you can use the 'dir' command.

```
# dir
Directory of flash:
    r- 1970-01-01 00:00:00      316 default-config
    rw 1970-01-01 07:43:36     1083 startup-config
2 files, 1399 bytes total.
```

# 6. **Switch Management Guide**

## 6.1. **System**

## 6.1.1. **System Configuration**

## 6.1.1.1. **Information**

WEB MENU Configuration>System>Information

The switch system information is provided here.

### System Information Configuration

| System Contact | |
| --- | --- |
| System Name | |
| System Location | |

**System Information Configuration**

| Object | Description |
| --- | --- |
| **System Contact** | The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255. |
| **System Name** | An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255. |
| **System Location** | The physical location of this node(for example, telephone closet, third floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

SOLTECH
INFONET INC.

## EXAMPLE WEB CONFIGURATION

✓    **System Contact**

**System Information Configuration**

| System Contact | SOLTECH |
|---|---|
| System Name | |
| System Location | |

✓    **System Name**

**System Information Configuration**

| System Contact | |
|---|---|
| System Name | TESTSWITCH |
| System Location | |

✓    **System Location**

**System Information Configuration**

| System Contact | |
|---|---|
| System Name | |
| System Location | SOLTECH-LAB |

## EXAMPLE CLI CONFIGURATION

✓    **System Contact**

```
(config)# snmp-server contact <line255>
(config)# snmp-server contact SOLTECH
```

✓    **System Name**

```
(config)# hostname <host_name>
(config)# hostname TESTSWITCH
```

✓    **System Location**

```
(config)# snmp-server location <line255>
(config)# snmp-server location SOLTECH-LAB
```

SOLTECH
INFONET INC.

## 6.1.1.2. IP

WEB MENU Configuration>System>IP

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

**IP Configuration**

| Mode | Host ▾ | |
|---|---|---|
| DNS Server 0 | No DNS server ▾ | |
| DNS Server 1 | No DNS server ▾ | |
| DNS Server 2 | No DNS server ▾ | |
| DNS Server 3 | No DNS server ▾ | |
| DNS Proxy | ☐ | |

**IP Interfaces**

| Delete | VLAN | DHCPv4 | | | IPv4 | | DHCPv6 | | | IPv6 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Enable | Fallback | Current Lease | Address | Mask Length | Enable | Rapid Commit | Current Lease | Address | Mask Length |
| ☐ | 1 | ☐ | 0 | | 192.168.10.101 | 24 | ☐ | ☐ | | | |

Add Interface

**IP Routes**

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

Add Route

### IP Configuration

| Object | Description |
|---|---|
| **Mode** | Configure whether the IP stack should act as a Host or a Router. |
| **DNS Server** | This setting controls the DNS name resolution done by the switch. |
| **DNS Proxy** | When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network. |

### IP Interfaces

| Object | Description |
|---|---|
| **Delete** | Select this option to delete an existing IP interface. |
| **VLAN** | The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. |
| **IPv4 DHCP Enabled** | Enable the DHCPv4 client by checking this box. |
| **IPv4 DHCP Fallback Timeout** | The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. |
| **IPv4 DHCP Current Lease** | For DHCP interfaces with an active lease, this column show the current interface address, as provided by the DHCP server. |
| **IPv4 Address** | The IPv4 address of the interface in dotted decimal notation. |
| **IPv4 Mask** | The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address. |
| **DHCPv6 Enable** | Enable the DHCPv6 client by checking this box. |
| **DHCPv6 Rapid Commit** | Enable the DHCPv6 Rapid-Commit option by checking this box. |
| **DHCPv6 Current Lease** | For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server. |
| **IPv6 Address** | The IPv6 address of the interface. |
| **IPv6 Mask** | The IPv6 network mask, in number of bits (prefix length). Valid values are between 1 and 128 bits for a IPv6 address. |

**IP Routes**

| Object | Description |
|---|---|
| **Delete** | Select this option to delete an existing IP route. |
| **Network** | The destination IP network or host address of this route. |
| **Mask Length** | The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. |
| **Gateway** | The IP address of the IP gateway. |
| **Next Hop VLAN (Only for IPv6)** | The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. The given VID ranges from 1 to 4095 and will be effective only when the corresponding IPv6 interface is valid. |

**Buttons**

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

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

[Apply] : Click to apply changes.

[Apply&Save] : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

✓ **IP Configuration**

➢ *Mode*

- Mode Host

**IP Configuration**

| Mode | Host ∨ | |
|---|---|---|
| DNS Server 0 | No DNS server ∨ | |
| DNS Server 1 | No DNS server ∨ | |
| DNS Server 2 | No DNS server ∨ | |
| DNS Server 3 | No DNS server ∨ | |
| DNS Proxy | ☐ | |

- Mode Router

**IP Configuration**

| Mode | Router ∨ | |
|---|---|---|
| DNS Server 0 | No DNS server ∨ | |
| DNS Server 1 | No DNS server ∨ | |
| DNS Server 2 | No DNS server ∨ | |
| DNS Server 3 | No DNS server ∨ | |
| DNS Proxy | ☐ | |

➢ *DNS Server*

- Configured IPv4 or IPv6

**IP Configuration**

| Mode | Host |
|---|---|
| DNS Server 0 | Configured IPv4 or IPv6 | 8.8.8.8 |
| DNS Server 1 | No DNS server | |
| DNS Server 2 | No DNS server | |
| DNS Server 3 | No DNS server | |
| DNS Proxy | ☐ | |

**IP Configuration**

| Mode | Host |
|---|---|
| DNS Server 0 | Configured IPv4 or IPv6 | 2001:4860:4860::8888 |
| DNS Server 1 | No DNS server | |
| DNS Server 2 | No DNS server | |
| DNS Server 3 | No DNS server | |
| DNS Proxy | ☐ | |

- From any DHCPv4 Interfaces

**IP Configuration**

| Mode | Host |
|---|---|
| DNS Server 0 | From any DHCPv4 interfaces | |
| DNS Server 1 | No DNS server | |
| DNS Server 2 | No DNS server | |
| DNS Server 3 | No DNS server | |
| DNS Proxy | ☐ | |

- From this DHCPv4 Interfaces (VLAN1)

**IP Configuration**

| Mode | Host |
|---|---|
| DNS Server 0 | From this DHCPv4 interface | 1 |
| DNS Server 1 | No DNS server | |
| DNS Server 2 | No DNS server | |
| DNS Server 3 | No DNS server | |
| DNS Proxy | ☐ | |

- From any DHCPv6 Interfaces

**IP Configuration**

| Mode | Host |
|---|---|
| DNS Server 0 | From any DHCPv6 interfaces | |
| DNS Server 1 | No DNS server | |
| DNS Server 2 | No DNS server | |
| DNS Server 3 | No DNS server | |
| DNS Proxy | ☐ | |

- From this DHCPv6 Interfaces (VLAN1)

**IP Configuration**

| Mode | Host |
|---|---|
| DNS Server 0 | From this DHCPv6 interface | 1 |
| DNS Server 1 | No DNS server | |
| DNS Server 2 | No DNS server | |
| DNS Server 3 | No DNS server | |
| DNS Proxy | ☐ | |

➢ **DNS Proxy**

**IP Configuration**

| Mode | Host |
|---|---|
| DNS Server 0 | Configured IPv4 or IPv6 | 8.8.8.8 |
| DNS Server 1 | No DNS server | |
| DNS Server 2 | No DNS server | |
| DNS Server 3 | No DNS server | |
| DNS Proxy | ☑ | |

✓ **IP Interfaces**

➢ **VLAN**(This field is only available for input when creating a new interface.)

**IP Interfaces**

| Delete | VLAN | DHCPv4 | | | IPv4 | | DHCPv6 | | | IPv6 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Enable | Fallback | Current Lease | Address | Mask Length | Enable | Rapid Commit | Current Lease | Address | Mask Length |
| ☐ | 1 | ☐ | 0 | | 192.168.10.101 | 24 | ☐ | ☐ | | | |
| Delete | 2 | ☐ | 0 | | | | ☐ | ☐ | | | |

SOLTECH
INFONET INC.

➢ *DHCPv4*

- DHCPv4 fallback not set

**IP Interfaces**

| Delete | VLAN | DHCPv4 | | | IPv4 | | DHCPv6 | | | IPv6 | |
|--------|------|--------|----------|---------------|---------------|-------------|--------|--------------|---------------|---------|-------------|
| | | Enable | Fallback | Current Lease | Address | Mask Length | Enable | Rapid Commit | Current Lease | Address | Mask Length |
| ☐ | 1 | ☐ | 0 | | 192.168.10.101 | 24 | ☐ | ☐ | | | |
| ☐ | 2 | ☑ | 0 | | | | ☐ | ☐ | | | |

- DHCPv4 fallback setting.
  (After this period expires, a configured IPv4 address will be used as IPv4 interface address.)

**IP Interfaces**

| Delete | VLAN | DHCPv4 | | | IPv4 | | DHCPv6 | | | IPv6 | |
|--------|------|--------|----------|---------------|---------------|-------------|--------|--------------|---------------|---------|-------------|
| | | Enable | Fallback | Current Lease | Address | Mask Length | Enable | Rapid Commit | Current Lease | Address | Mask Length |
| ☐ | 1 | ☐ | 0 | | 192.168.10.101 | 24 | ☐ | ☐ | | | |
| ☐ | 2 | ☑ | 30 | | 2.2.2.2 | 24 | ☐ | ☐ | | | |

➢ *IPv4*

**IP Interfaces**

| Delete | VLAN | DHCPv4 | | | IPv4 | | DHCPv6 | | | IPv6 | |
|--------|------|--------|----------|---------------|---------------|-------------|--------|--------------|---------------|---------|-------------|
| | | Enable | Fallback | Current Lease | Address | Mask Length | Enable | Rapid Commit | Current Lease | Address | Mask Length |
| ☐ | 1 | ☐ | 0 | | 192.168.10.101 | 24 | ☐ | ☐ | | | |
| ☐ | 2 | ☐ | 0 | | 2.2.2.2 | 24 | ☐ | ☐ | | | |

Add Interface

✓ **IP Routes**

➢ *Add Route*

- Use Default gateway

**IP Routes**

| Delete | Network | Mask Length | Gateway | Next Hop VLAN |
|--------|---------|-------------|--------------|---------------|
| ☐ | 0.0.0.0 | 0 | 192.168.10.1 | 0 |

- Use Static gateway

**IP Routes**

| Delete | Network | Mask Length | Gateway | Next Hop VLAN |
|--------|---------|-------------|--------------|---------------|
| ☐ | 2.2.2.0 | 24 | 192.168.10.1 | 0 |

# EXAMPLE CLI CONFIGURATION

✓ **IP Configuration**

➢ *Mode*

- Mode Host

```
(config)# no ip routing
```

- Mode Router

```
(config)# ip routing
```

➢ **DNS Server**

- Configured IPv4 or IPv6

```
(config)# ip name-server <0-3> <ipv4_ucast>
(config)# ip name-server 0 8.8.8.8
```

```
(config)# ip name-server <0-3> <ipv6_ucast>
(config)# ip name-server 0 2001:4860:4860::8888
```

- From any DHCPv4 Interfaces

```
(config)# ip name-server <0-3> dhcp ipv4
(config)# ip name-server 0 dhcp ipv4
```

- From this DHCPv4 Interfaces

```
(config)# ip name-server <0-3> dhcp ipv4 interface vlan <vlan_id>
(config)# ip name-server 0 dhcp ipv4 interface vlan 1
```

- From any DHCPv6 Interfaces

```
(config)# ip name-server <0-3> dhcp ipv6
(config)# ip name-server 0 dhcp ipv6
```

- From this DHCPv6 Interfaces

```
(config)# ip name-server <0-3> dhcp ipv6 interface vlan <vlan_id>
(config)# ip name-server 0 dhcp ipv6 interface vlan 1
```

➢ **DNS Proxy**

```
(config)# ip dns proxy
```

✓ **IP Interfaces**

➢ **VLAN**

```
(config)# interface vlan <vlan_list>
(config)# interface vlan 1
```

➢ **DHCPv4**

- DHCPv4 fallback not set

```
(config)# interface vlan <vlan_list>

(config-if-vlan)# ip address dhcp
```

- DHCPv4 fallback setting.
  (After this period expires, a configured IPv4 address will be used as IPv4 interface address.)

```
(config)# interface vlan <vlan_list>
```

(config-if-vlan)# ip address dhcp fallback <ipv4_addr> <ipv4_netmask>
timeout <uint>
*(config-if-vlan)# ip address dhcp fallback 192.168.10.101 255.255.255.0*
*timeout 30*

➢ *IPv4*

(config)# interface vlan <vlan_list>

(config-if-vlan)# ip address <ipv4_addr> <ipv4_netmask>
*(config-if-vlan)# ip address 192.168.10.101 255.255.255.0*

✓ **IP Routes**

➢ *Add Route*

• Use Default gateway(Sending all packets to the gateway)

(config)# ip route 0.0.0.0 0.0.0.0 <ipv4_addr>
*(config)# ip route 0.0.0.0 0.0.0.0 192.168.10.1*

• Use Static gateway(Sending packets of the respective network subnet to the gateway)

(config)# ip route <ipv4_addr> <ipv4_netmask> <ipv4_addr>
*(config)# ip route 2.2.2.0 255.255.255.0 192.168.10.1*

## 6.1.1.3. System Time

WEB MENU Configuration>System>NTP

This page allows you to configure the Time.



### System Time Status

| Object | Description |
|---|---|
| **NTP Mode** | Indicates NTP status. |
| **System time** | Indicates the current time on the switch |

**\* When 'NTP Mode' is enable, 'Time Setting' will be disabled.**

**To enable 'Time Setting', Please set NTP mode on disable.**

### System Time Configuration

| Object | Description |
|---|---|
| **Time Setting** | This page is used to setup System Time Configuration.<br>**Year**　　　　Select the starting year.<br>**Month**　　　Select the starting month.<br>**Date**　　　　Select the starting date.<br>**Hours**　　　Select the starting hour.<br>**Minutes**　　Select the starting minute. |

**Buttons**

Apply : Click to apply changes.

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

NTP : Click to move to NTP setting page.

Refresh : Click to refresh the page.

## EXAMPLE WEB CONFIGURATION

✓ **System Time Configuration**

➢ *Time Setting*

- Year(2000~2037)
- Month(1~12)
- Date(1~31)
- Hours(0~23)
- Minutes(0~59)

| Time Setting | |
|---|---|
| Year | 2024 |
| Month | 1 (Jan) |
| Date | 1 |
| Hours | 0 |
| Minutes | 10 |

Click the Apply button

| NTP Mode | Disable |
|---|---|
| System time | 2024-01-01 T00:10:18 (Monday) |

## EXAMPLE CLI CONFIGURATION

✓ **System Time Configuration**

➢ *Time Setting*

- Year(2000~2037)
- Month(1~12)
- Date(1~31)
- Hours(0~23)
- Minutes(0~59)
- Seconds(0~59)

```
(config)# clock system-time set <d> <t>
<date>    Date yyyy/mm/dd, yyyy=1970-2037, mm=1-12, dd=1-31
<time>    Time HH:mm:ss, HH=0-23, mm=0-59, ss=0-59
(config)# clock system-time set 2024/01/01 00:10:00
```

SOLTECH
INFONET INC.

## 6.1.1.4. NTP

WEB MENU Configuration>System>NTP

Configure NTP on this page.

**NTP Configuration**

| Mode | Disabled ∨ |
|---|---|
| Server 1 | |
| Server 2 | |
| Server 3 | |
| Server 4 | |
| Server 5 | |

### NTP Configuration

| Object | Description |
|---|---|
| **Mode** | Indicates the NTP mode operation. Possible modes are:<br>Enabled: Enable NTP client mode operation.<br>Disabled: Disable NTP client mode operation.<br>(Need to configure Time Zone setting Configuration>System>Time) |
| **Server** | Provide the IPv4 or IPv6 address of a NTP server.<br>(Using DNS, Need to configure the DNS settings<br>Configuration>System>IP)<br>If NTP server is located in an external network you need to configure<br>the default gateway for IP Routes under Configuration>System>IP.) |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

## EXAMPLE WEB CONFIGURATION

✓ **NTP Configuration**

➢ *Mode*

• Enable

**NTP Configuration**

| Mode | Enabled |
|------|---------|
| Server 1 | |
| Server 2 | |
| Server 3 | |
| Server 4 | |
| Server 5 | |

• Disable

**NTP Configuration**

| Mode | Disabled |
|------|----------|
| Server 1 | |
| Server 2 | |
| Server 3 | |
| Server 4 | |
| Server 5 | |

➢ *Server*

• Use the IPv4 or IPv6 address of the NTP server

**NTP Configuration**

| Mode | Enabled |
|------|---------|
| Server 1 | 216.239.35.0 |
| Server 2 | |
| Server 3 | |
| Server 4 | |
| Server 5 | |

• Use the domain name of the NTP server

**NTP Configuration**

| Mode | Enabled |
|------|---------|
| Server 1 | time.google.com |
| Server 2 | |
| Server 3 | |
| Server 4 | |
| Server 5 | |

## EXAMPLE CLI CONFIGURATION

✓ **NTP Configuration**

➢ *Mode*

- Enable (NTP client mode operation is used.)

```
(config)# ntp
```

- Disable (NTP client mode operation is not used.)
```
(config)# no ntp
```

➢ *Server*

- NTP server configuration
```
(config)# ntp server <1-5> ip-address <domain_name>
<ipv4_ucast> <ipv6_ucast>
(config)# ntp server 1 ip-address 216.239.35.0
(config)# ntp server 1 ip-address time.google.com
```

## CHECK CONFIGURATION

✓ **Check Configuration**

You can verify the change at Information Monitor

➢ *WEB*

WEB MENU Monitor>System>Information.

➢ *CLI*
```
# show ntp status

NTP Mode : enabled
Idx    Server IP host address (a.b.c.d) or a host name string
---    --------------------------------------------------------

1      time.google.com
2
3
4
5
```

## 6.1.1.5. Time

WEB MENU Configuration>System>Time

This page allows you to configure the Time Zone.

**Time Zone Configuration**

| Time Zone Configuration | |
|---|---|
| Time Zone | (UTC+09:00) Seoul |
| Hours | 9 |
| Minutes | 0 |
| Acronym | ( 0 - 16 characters ) |

**Daylight Saving Time Configuration**

| Daylight Saving Time Mode | |
|---|---|
| Daylight Saving Time | Disabled |

| Start Time settings | |
|---|---|
| Month | Jan |
| Date | 1 |
| Year | 2014 |
| Hours | 0 |
| Minutes | 0 |
| **End Time settings** | |
| Month | Jan |
| Date | 1 |
| Year | 2097 |
| Hours | 0 |
| Minutes | 0 |
| **Offset settings** | |
| Offset | 1 (1 - 1439) Minutes |

### Time Zone Configuration

| Object | Description |
|---|---|
| **Time Zone** | Lists various Time Zones world wide. Select appropriate Time Zone. |
| **Hours** | Number of hours offset from UTC. The field only available when time zone manual setting. |
| **Minutes** | Number of minutes offset from UTC. The field only available when time zone manual setting. |
| **Acronym** | User can set the acronym of the time zone. |

### Daylight Saving Time Configuration

| Object | Description |
|---|---|
| **Daylight Saving Time** | This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. |
| **Week** | Select the starting and ending week number. |
| **Day/Date** | Select the starting and ending day/date. |

| Month | Select the starting and ending month. |
|---|---|
| Hours | Select the starting and ending hour. |
| Minutes | Select the starting and ending minute. |
| Offset | Enter the number of minutes to add during Daylight Saving Time. ( Range: 1 to 1439 ) |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

## EXAMPLE WEB CONFIGURATION

✓   **Time Zone Configuration**

➢   *Time Zone*

•   (UTC+09:00) Seoul

**Time Zone Configuration**

| Time Zone Configuration | | |
|---|---|---|
| Time Zone | (UTC+09:00) Seoul | |
| Hours | 9 | |
| Minutes | 0 | |
| Acronym | | ( 0 - 16 characters ) |

•   Manual Setting

**Time Zone Configuration**

| Time Zone Configuration | | |
|---|---|---|
| Time Zone | Manual Setting | |
| Hours | 7 | |
| Minutes | 10 | |
| Acronym | | ( 0 - 16 characters ) |

➢   *Acronym*

**Time Zone Configuration**

| Time Zone Configuration | | |
|---|---|---|
| Time Zone | (UTC+09:00) Seoul | |
| Hours | 9 | |
| Minutes | 0 | |
| Acronym | KOR_SEOUL | ( 0 - 16 characters ) |

✓   **Daylight Saving Time Configuration**

➢   *Daylight Saving Time*

•   Disable

**SOLTECH**
INFONET INC.

**Daylight Saving Time Configuration**

| Daylight Saving Time Mode | |
| --- | --- |
| Daylight Saving Time | Disabled |

| Start Time settings | |
| --- | --- |
| Month | Jan |
| Date | 1 |
| Year | 2014 |
| Hours | 0 |
| Minutes | 0 |

| End Time settings | |
| --- | --- |
| Month | Jan |
| Date | 1 |
| Year | 2097 |
| Hours | 0 |
| Minutes | 0 |

| Offset settings | | |
| --- | --- | --- |
| Offset | 1 | (1 - 1439) Minutes |

- Recurring

**Daylight Saving Time Configuration**

| Daylight Saving Time Mode | |
| --- | --- |
| Daylight Saving Time | Recurring |

| Start Time settings | |
| --- | --- |
| Week | 1 |
| Day | Mon |
| Month | Jun |
| Hours | 0 |
| Minutes | 0 |

| End Time settings | |
| --- | --- |
| Week | 4 |
| Day | Mon |
| Month | Aug |
| Hours | 0 |
| Minutes | 0 |

| Offset settings | | |
| --- | --- | --- |
| Offset | 1 | (1 - 1439) Minutes |

- Non-Recurring

**Daylight Saving Time Configuration**

| Daylight Saving Time Mode | |
| --- | --- |
| Daylight Saving Time | Non-Recurring |

| Start Time settings | |
| --- | --- |
| Month | May |
| Date | 1 |
| Year | 2023 |
| Hours | 0 |
| Minutes | 0 |

| End Time settings | |
| --- | --- |
| Month | Aug |
| Date | 1 |
| Year | 2023 |
| Hours | 0 |
| Minutes | 0 |

| Offset settings | | |
| --- | --- | --- |
| Offset | 1 | (1 - 1439) Minutes |

SOLTECH
INFONET INC.

## EXAMPLE CLI CONFIGURATION

✓ **Time Zone Configuration**

➢ *Time Zone*

- (UTC+09:00) Seoul

```
(config)# clock timezone '' <-23-23> <0-59> <0-9>
(config)# clock timezone '' 9 0 1
```

- Manual Setting

```
(config)# clock timezone '' <-23-23> <0-59> <0-9>
(config)# clock timezone '' 7 10 0
```

➢ *Acronym*

```
(config)# clock timezone <word16> <-23-23> <0-59> <0-9>
(config)# clock timezone KOR_SEOUL 9 0 1
```

✓ **Daylight Saving Time Configuration**

➢ *Daylight Saving Time*

- Disable

```
(config)# no clock summer-time
```

- Recurring

```
(config)# clock summer-time '' recurring <1-5> <1-7> <1-12> <hhmm>
<1-5> <1-7> <1-12> <hhmm> <1-1439>
(config)# clock summer-time '' recurring 1 1 6 00:00 4 1 8 00:00 60
```

- Non-Recurring

```
(config)# clock summer-time '' date <1-12> <1-31> <2000-2097>
<hhmm> <1-12> <1-31> <2000-2097> <hhmm> <1-1439>
(config)# clock summer-time '' date 5 1 2023 00:00 8 1 2023 00:00 60
```

# CHECK CONFIGURATION

✓ **Check Configuration**

You can verify the change at Information Monitor

✓ **Daylight Saving Time Monitor**

➢ *WEB*

You can verify the changes on the same page after saving

➢ *CLI*

```
# show clock detail

System Time: 2023-05-17T18:00:58+10:00
Timezone: Timezone Offset : 5401 ( 540 minutes)
Timezone Acronym : KOR_SEOUL
Daylight Saving Time Mode : Non-Recurring.
Daylight Saving Time Start Time Settings :
      Week: 0
      Day: 0
    * Month: 5
    * Date: 1
    * Year: 2023
    * Hour: 0
    * Minute: 0
Daylight Saving Time End Time Settings :
      Week: 0
      Day: 0
    * Month: 8
    * Date: 1
    * Year: 2023
    * Hour: 0
    * Minute: 0
Daylight Saving Time Offset : 60 (minutes)
```

## 6.1.1.6. Log

WEB MENU Configuration>System>Log

Configure System Log on this page.

**System Log Configuration**

| Server Mode | Disabled | ∨ |
|---|---|---|
| Server Address | | |
| Syslog Level | Informational | ∨ |

### System Log Configuration

| Object | Description |
|---|---|
| **Server Mode** | Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. Enabled: Enable server mode operation. Disabled: Disable server mode operation. |
| **Server Address** | Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a domain name. |
| **Syslog Level** | Indicates what kind of message will send to syslog server. Audit: Send the specific messages which severity code is less or equal than Audit. Error: Send the specific messages which severity code is less or equal than Error. Warning: Send the specific messages which severity code is less or equal than Warning. Notice: Send the specific messages which severity code is less or equal than Notice. Informational: Send the specific messages which severity code is less or equal than Informational. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

### EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>System>Log

✓ **System Log Configuration**

➢ *Server Mode*

• Disable

**System Log Configuration**

| Server Mode | Disabled | ∨ |
|---|---|---|
| Server Address | | |
| Syslog Level | Informational | ∨ |

- Enable

**System Log Configuration**

| Server Mode | Enabled |
|---|---|
| Server Address | |
| Syslog Level | Informational |

➢ *Server Address*

- IPv4 Address (PC Address)

**System Log Configuration**

| Server Mode | Enabled |
|---|---|
| Server Address | 192.168.10.130 |
| Syslog Level | Informational |

➢ *Syslog Level*

- Audit

**System Log Configuration**

| Server Mode | Enabled |
|---|---|
| Server Address | 192.168.10.130 |
| Syslog Level | Audit |

- Error

**System Log Configuration**

| Server Mode | Enabled |
|---|---|
| Server Address | 192.168.10.130 |
| Syslog Level | Error |

- Warning

**System Log Configuration**

| Server Mode | Enabled |
|---|---|
| Server Address | 192.168.10.130 |
| Syslog Level | Warning |

- Notice

**System Log Configuration**

| Server Mode | Enabled |
|---|---|
| Server Address | 192.168.10.130 |
| Syslog Level | Notice |

- Information

**System Log Configuration**

| Server Mode | Enabled |
|---|---|
| Server Address | 192.168.10.130 |
| Syslog Level | Informational |

## EXAMPLE CLI CONFIGURATION

✓ **System Log Configuration**

➢ *Server Mode*

SOLTECH
INFONET INC.

- Disable

```
(config)# no logging on
```

- Enable

```
(config)# logging on
```

➢ **Server Address**

- IPv4 Address (PC Address)

```
(config)# logging host <ipv4_ucast>
(config)# logging host 192.168.10.130
```

➢ **Syslog Level**

- Audit

```
(config)# logging level audit
```

- Error

```
(config)# logging level error
```

- Warning

```
(config)# logging level warning
```

- Notice

```
(config)# logging level notice
```

- Information

```
(config)# logging level informational
```

## 6.1.2. System Monitor

## 6.1.2.1. Information

WEB MENU Monitor>System>Information

The switch system information is provided here.

**System Information**

| | |
|---|---|
| **System** | |
| Contact | |
| Name | |
| Location | |
| **Hardware** | |
| MAC Address | 00-21-6d-00-00-00 |
| Device Serial | |
| **Time** | |
| System Date | 1970-01-02T06:16:20+09:00 |
| System Uptime | 0d 21:16:20 |
| **Software** | |
| Software Version | |
| Software Date | 2023-07-17T15:20:33+09:00 |
| **System Temperature** | |
| Current | 42.000 'C  (107.600 'F) |
| Minimum | 39.500 'C  (103.100 'F) |
| Maximum | 53.500 'C  (128.300 'F) |
| Average | 42.000 'C  (107.600 'F) |

**System Information**

| Object | Description |
|---|---|
| **System** | Displays system information for the switch. |
| **Contact** | Displays switch identification information. |
| **Name** | Displays switch Name. |
| **Location** | Displays switch Location. |
| **Hardware** | Displays Hardware information for the switch. |
| **MAC Address** | The MAC Address of this switch. |
| **Device Serial** | The Serial Number of this switch. |
| **Time** | Displays Time information for the switch. |
| **System Date** | The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any. |
| **System Uptime** | The period of time the device has been operational. |
| **Software** | Displays Software information for the switch. |
| **Software Version** | The software version of this switch. |
| **Software Data** | The date when the switch software was produced. |
| **System Temperature** | Displays Temperature information for the switch. |

| Current | Displays the current intenal templature of switch. |
|---------|----------------------------------------------------|
| Minimum | Displays the minimum intenal templature of switch. |
| Maximum | Displays the maximum intenal templature of switch. |
| Average | Displays the average intenal templature of switch. |

## EXAMPLE WEB MONITOR

WEB MENU Monitor>System>Information

### System Information

| System | |
|--------|--------------------------------|
| Contact | SOLTECH |
| Name | TESTSWITCH |
| Location | SOLTECH-LAB |
| **Hardware** | |
| MAC Address | 00-21-6d-00-00-00 |
| Device Serial | |
| **Time** | |
| System Date | 1970-01-02T05:59:39+09:00 |
| System Uptime | 0d 20:59:39 |
| **Software** | |
| Software Version | |
| Software Date | 2023-07-17T15:20:33+09:00 |
| **System Temperature** | |
| Current | 42.000 'C   (107.600 'F) |
| Minimum | 39.500 'C   (103.100 'F) |
| Maximum | 53.500 'C   (128.300 'F) |
| Average | 42.000 'C   (107.600 'F) |

## EXAMPLE CLI MONITOR

✓ **System Information**

```
TESTSWITCH# show version

# show version
MEMORY : Total=208355 KBytes, Free=181987 KBytes, Max=181905 Kbytes
FLASH : 0x40000000-0x40ffffff, 256 x 0x10000 blocks
MAC Address : 00-21-6d-00-00-00
Board Serial :
Previous Restart : Cool
System Contact : SOLTECH
System Name : TESTSWITCH
System Location : SOLTECH-LAB
System Time : 1970-01-02T07:24:10+09:00
System Uptime    : 21:24:10
```

SOLTECH
INFONET INC.

```
Active Image
------------
Image           : SFC8100BT.dat (primary)
Version         : OneImg_JAGUAR2 (standalone) build 5.0.3.0 by Soltech Corp.
Date            : 2023-07-21T14:21:27+09:00
Bank-Index       : Bank1

Alternate Image
---------------
Image           : SFC8100BT.dat (backup)
Version         : OneImg_JAGUAR2 (standalone) build 5.0.1.0 by Soltech Corp.
Date            : 2023-07-17T15:20:33+09:00
Bank-Index       : Bank0
```

```
TESTSWITCH# show system temperature status

   System Temperature Current: 39.500'C (103.100'F)
   System Temperature min: 36.000'C (96.800'F)
   System Temperature Max: 49.500'C (121.100'F)
   System Temperature Average: 39.500'C (103.100'F)
```

## 6.1.2.2. CPU Load

WEB MENU Monitor>System>CPU Load

This page displays the CPU load, using an SVG graph.
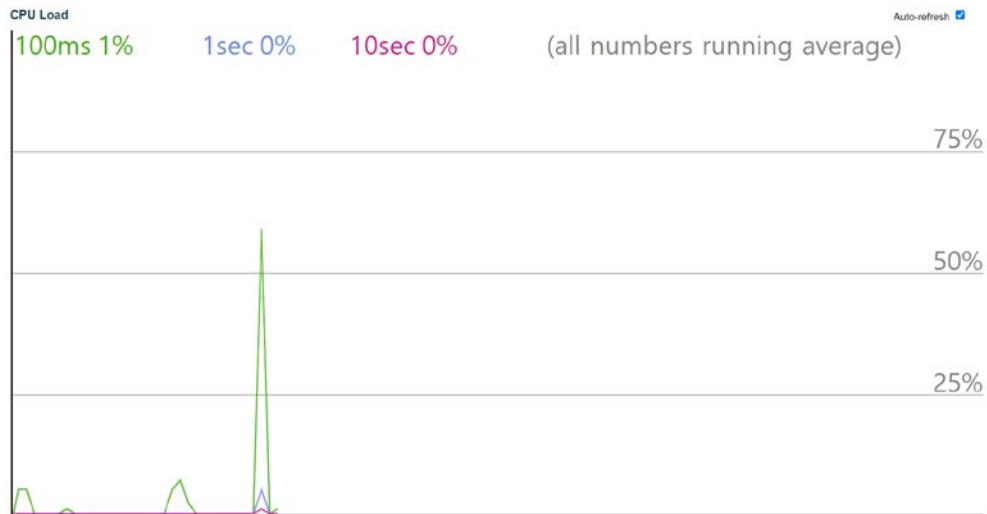


**Buttons**

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

### EXAMPLE WEB MONITOR

WEB MENU Monitor>System>CPU Load
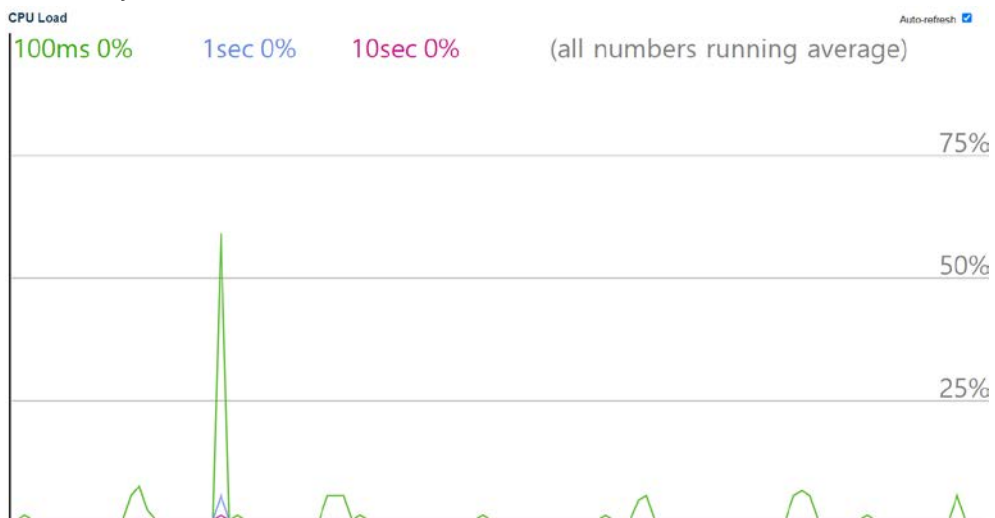


### EXAMPLE CLI MONITOR

```
# show system cpu status

    Average load in 100 ms: 2%
    Average load in 1 sec: 1%
    Average load in 10 sec: 0%
```

## 6.1.2.3. IP Status

WEB MENU Monitor>System>IP Status

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbor cache (ARP cache) status.

### IP Interfaces

| Interface | Type | Address | Status |
|-----------|------|---------|--------|
| OS:lo | LINK | 00-00-00-00-00-00 | <UP LOOPBACK RUNNING MULTICAST> |
| OS:lo | IPv4 | 127.0.0.1/8 | |
| OS:lo | IPv6 | fe80::1/64 | |
| OS:lo | IPv6 | ::1/128 | |
| VLAN1 | LINK | 00-21-6d-00-87-32 | <UP BROADCAST RUNNING MULTICAST> |
| VLAN1 | IPv4 | 192.168.10.101/24 | |
| VLAN1 | IPv6 | fe80::221:6dff:fe00:8732/64 | |

### IP Routes

| Network | Gateway | Status |
|---------|---------|--------|
| 127.0.0.1/32 | 127.0.0.1 | <UP HOST> |
| 224.0.0.0/4 | 127.0.0.1 | <UP> |
| ::1/128 | ::1 | <UP HOST> |

### Neighbour cache

| IP Address | Link Address |
|------------|--------------|
| 192.168.10.130 | VLAN1:c0-18-50-7e-50-56 |
| fe80::221:6dff:fe00:8732 | VLAN1:00-21-6d-00-87-32 |

**IP Interface**

| Object | Description |
|--------|-------------|
| Interface | The name of the interface. |
| Type | The address type of the entry. This may be LINK or IPv4. |
| Address | The current address of the interface (of the given type). |
| Status | The status flags of the interface (and/or address). |

**IP Routes**

| Object | Description |
|--------|-------------|
| Network | The destination IP network or host address of this route. |
| Gateway | The gateway address of this route. |
| Status | The status flags of the route. |

**Neighbour cache**

| Object | Description |
|--------|-------------|
| IP Address | The IP address of the entry. |
| Link Address | The Link (MAC) address for which a binding to the IP address given exist.. |

SOLTECH
INFONET INC.

**Buttons**

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

Refresh : Click to refresh the page immediately.

---

## EXAMPLE WEB MONITOR

### IP Interfaces

| Interface | Type | Address | Status |
|---|---|---|---|
| OS:lo | LINK | 00-00-00-00-00-00 | <UP LOOPBACK RUNNING MULTICAST> |
| OS:lo | IPv4 | 127.0.0.1/8 | |
| OS:lo | IPv6 | ::1/128 | |
| OS:lo | IPv6 | fe80::1/64 | |
| VLAN1 | LINK | 00-21-6d-00-87-32 | <UP BROADCAST RUNNING MULTICAST> |
| VLAN1 | IPv4 | 192.168.10.101/24 | |
| VLAN1 | IPv6 | fe80::221:6dff:fe00:8732/64 | |
| VLAN2 | LINK | 00-21-6d-00-87-32 | <UP BROADCAST RUNNING MULTICAST> |
| VLAN2 | IPv4 | 2.2.2.2/24 | |
| VLAN2 | IPv6 | fe80::221:6dff:fe00:8732/64 | |

### IP Routes

| Network | Gateway | Status |
|---|---|---|
| 0.0.0.0/0 | 192.168.10.1 | <UP GATEWAY HW_RT> |
| 3.3.3.0/24 | 192.168.10.1 | <UP GATEWAY HW_RT> |
| 127.0.0.1/32 | 127.0.0.1 | <UP HOST> |
| 224.0.0.0/4 | 127.0.0.1 | <UP> |
| ::1/128 | ::1 | <UP HOST> |

### Neighbour cache

| IP Address | Link Address |
|---|---|
| 192.168.10.130 | VLAN1:c0-18-50-7e-50-56 |
| fe80::221:6dff:fe00:8732 | VLAN1:00-21-6d-00-87-32 |
| fe80::221:6dff:fe00:8732 | VLAN2:00-21-6d-00-87-32 |

---

## EXAMPLE CLI MONITOR

✓ **IP Interfaces**

```
# show interface vlan

VLAN1
   LINK: 00-21-6d-00-87-32 Mtu:1500 <UP BROADCAST RUNNING MULTICAST>
   IPv4: 192.168.10.101/24 192.168.10.255
   IPv6: fe80::221:6dff:fe00:8732/64 <UP RUNNING>

VLAN2
   LINK: 00-21-6d-00-87-32 Mtu:1500 <UP BROADCAST RUNNING MULTICAST>
   IPv4: 2.2.2.2/24 2.2.2.255
   DHCP: State: FALLBACK
   IPv6: fe80::221:6dff:fe00:8732/64 <UP RUNNING>
```

SOLTECH
INFONET INC.

   ✓ **IP Routes**

```
# show ip route

0.0.0.0/0 via 192.168.10.1 <UP GATEWAY HW_RT>
2.2.2.0/24 via interface index 2 <UP HW_RT>
3.3.3.0/24 via 192.168.10.1 <UP GATEWAY HW_RT>
127.0.0.1/32 via 127.0.0.1 <UP HOST>
192.168.10.0/24 via interface index 1 <UP HW_RT>
224.0.0.0/4 via 127.0.0.1 <UP>
```

   ✓ **Neighbour cache**

```
# show ip arp

192.168.10.1 (Incomplete)
192.168.10.130 via VLAN1:c0-18-50-7e-50-56
```

```
# show ipv6 neighbor

fe80::221:6dff:fe00:8732 via VLAN1: 00-21-6d-00-87-32
Permanent/REACHABLE
fe80::221:6dff:fe00:8732 via VLAN2: 00-21-6d-00-87-32
Permanent/REACHABLE
```

## 6.1.2.4. Log

WEB MENU Configuration>System>Log

Configure System Log on this page.

**System Log Information**

| Level | All |
|---|---|
| Clear Level | All |

The total number of entries is 0 for the given level.

Start from ID 1 with 20 entries per page.

| ID | Level | Time | Message |
|---|---|---|---|
| *No entry exists* | | | |

**System Log Information**

| Object | Description |
|---|---|
| **Level** | Display the information from the system logs for the selected log level. |
| **Clear Level** | Delete the information from the system logs for the selected log level. |
| **ID** | The identification of the system log entry. |
| **Level** | The level of the system log entry.<br>Audit: The system log entry is belonged audit level.<br>Error: The system log entry is belonged error level.<br>Warning: The system log entry is belonged warning level.<br>Notice: The system log entry is belonged notice level.<br>Infomational: The system log entry is belonged information level.<br>All: All system log entry. |
| **Time** | The occurred time of the system log entry. |
| **Message** | The detail message of the system log entry. |

**Buttons**

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

Refresh : Updates the system log entries, starting from the current entry ID.

Clear : Flushes the selected log entries.

|<< : Updates the system log entries, starting from the first available entry ID.

<< : Updates the system log entries, ending at the last entry currently displayed.

>> : Updates the system log entries, starting from the last entry currently displayed

>>| : Updates the system log entries, ending at the last available entry ID.

# EXAMPLE WEB MONITOR

WEB MENU Configuration>System>Log

✓ **System Log Information**

**System Log Information**

| Level | All |
|-------|-----|
| Clear Level | All |

The total number of entries is 27 for the given level.

Start from ID `1` with `50` entries per page.

| ID | Level | Time | Message |
|----|-------|------|---------|
| 1 | Audit | 1970-01-01T00:00:00+00:00 | Audit Log Start, Image:[SFC8100G 5.0.0.4] |
| 2 | Info. | 1970-01-01T00:00:02+00:00 | SYS-BOOTING: Switch just made a cool boot. |
| 3 | Audit | 1970-01-01T00:00:02+00:00 | TELNET server started on port 23. |
| 4 | Notice | 1970-01-01T00:00:02+00:00 | LINK-UPDOWN: Intf. Vlan 1, changed state to down. |
| 5 | Audit | 1970-01-01T00:00:02+00:00 | Intf. Port:1 TEST Ok!!!, (CAP:0x0000303F) |
| 6 | Audit | 1970-01-01T00:00:02+00:00 | Intf. Port:2 TEST Ok!!!, (CAP:0x0000303F) |
| 7 | Audit | 1970-01-01T00:00:02+00:00 | Intf. Port:3 TEST Ok!!!, (CAP:0x0000303F) |
| 8 | Audit | 1970-01-01T00:00:02+00:00 | Intf. Port:4 TEST Ok!!!, (CAP:0x0000303F) |
| 9 | Audit | 1970-01-01T00:00:02+00:00 | Intf. Port:5 TEST Ok!!!, (CAP:0x048E1171) |
| 10 | Audit | 1970-01-01T00:00:02+00:00 | Intf. Port:6 TEST Ok!!!, (CAP:0x048E1171) |
| 11 | Audit | 1970-01-01T00:00:02+00:00 | Intf. Port:7 TEST Ok!!!, (CAP:0x048E1171) |
| 12 | Audit | 1970-01-01T00:00:02+00:00 | Intf. Port:8 TEST Ok!!!, (CAP:0x048E1171) |
| 13 | Audit | 1970-01-01T00:00:03+00:00 | SNMP server Stop. |
| 14 | Audit | 1970-01-01T00:00:03+00:00 | HTTP server started on port 80. |
| 15 | Notice | 1970-01-01T00:00:06+00:00 | LINK-UPDOWN: Intf. GigabitEthernet 1/4, changed state to up. |
| 16 | Notice | 1970-01-01T00:00:08+00:00 | LINK-UPDOWN: Intf. Vlan 1, changed state to up. |
| 17 | Audit | 1970-01-01T00:00:09+00:00 | SSH server started on port 22. |
| 18 | Audit | 1970-01-01T00:00:10+00:00 | HTTPs server started on port 443. |
| 19 | Audit | 1970-01-01T00:00:13+00:00 | User [admin] logged on Console |
| 20 | Notice | 1970-01-01T00:00:31+00:00 | LINK-UPDOWN: Intf. Vlan 1, changed state to up. |
| 21 | Audit | 1970-01-01T00:00:41+00:00 | User [admin] logged on HTTP |
| 22 | Notice | 1970-01-01T00:01:38+00:00 | LINK-UPDOWN: Intf. GigabitEthernet 1/2, changed state to up. |
| 23 | Notice | 1970-01-01T00:01:40+00:00 | LINK-UPDOWN: Intf. GigabitEthernet 1/2, changed state to down. |
| 24 | Notice | 1970-01-01T00:01:47+00:00 | LINK-UPDOWN: Intf. GigabitEthernet 1/2, changed state to up. |
| 25 | Notice | 1970-01-01T00:01:52+00:00 | LINK-UPDOWN: Intf. GigabitEthernet 1/2, changed state to down. |
| 26 | Notice | 1970-01-01T00:02:07+00:00 | LINK-UPDOWN: Intf. GigabitEthernet 1/1, changed state to up. |
| 27 | Notice | 1970-01-01T00:02:11+00:00 | LINK-UPDOWN: Intf. GigabitEthernet 1/1, changed state to down. |

➢ *Level*

• example notice

Select Notice> Click `Refresh` (Check only Notice)

**System Log Information**

| Level | Notice |
|-------|--------|
| Clear Level | All |

The total number of entries is 10 for the given level.

Start from ID `4` with `50` entries per page.

| ID | Level | Time | Message |
|----|-------|------|---------|
| 4 | Notice | 1970-01-01T00:00:02+00:00 | LINK-UPDOWN: Intf. Vlan 1, changed state to down. |
| 15 | Notice | 1970-01-01T00:00:06+00:00 | LINK-UPDOWN: Intf. GigabitEthernet 1/4, changed state to up. |
| 16 | Notice | 1970-01-01T00:00:08+00:00 | LINK-UPDOWN: Intf. Vlan 1, changed state to up. |
| 20 | Notice | 1970-01-01T00:00:31+00:00 | LINK-UPDOWN: Intf. Vlan 1, changed state to up. |
| 22 | Notice | 1970-01-01T00:01:38+00:00 | LINK-UPDOWN: Intf. GigabitEthernet 1/2, changed state to up. |
| 23 | Notice | 1970-01-01T00:01:40+00:00 | LINK-UPDOWN: Intf. GigabitEthernet 1/2, changed state to down. |
| 24 | Notice | 1970-01-01T00:01:47+00:00 | LINK-UPDOWN: Intf. GigabitEthernet 1/2, changed state to up. |
| 25 | Notice | 1970-01-01T00:01:52+00:00 | LINK-UPDOWN: Intf. GigabitEthernet 1/2, changed state to down. |
| 26 | Notice | 1970-01-01T00:02:07+00:00 | LINK-UPDOWN: Intf. GigabitEthernet 1/1, changed state to up. |
| 27 | Notice | 1970-01-01T00:02:11+00:00 | LINK-UPDOWN: Intf. GigabitEthernet 1/1, changed state to down. |

➢ *Clear Level*

• example notice

Select Notice> Click [Clear] (Delete only Notice)

**System Log Information**

| Level | All |
|---|---|
| Clear Level | Notice |

The total number of entries is 18 for the given level.

Start from ID [1] with [50] entries per page.

| ID | Level | Time | Message |
|---|---|---|---|
| 1 | Audit | 1970-01-01T00:00:00+00:00 | Audit Log Start, Image:[SFC8100G 5.0.0.4] |
| 2 | Info. | 1970-01-01T00:00:02+00:00 | SYS-BOOTING: Switch just made a cool boot. |
| 3 | Audit | 1970-01-01T00:00:02+00:00 | TELNET server started on port 23. |
| 5 | Audit | 1970-01-01T00:00:02+00:00 | Intf. Port:1 TEST Ok!!!, (CAP:0x0000303F) |
| 6 | Audit | 1970-01-01T00:00:02+00:00 | Intf. Port:2 TEST Ok!!!, (CAP:0x0000303F) |
| 7 | Audit | 1970-01-01T00:00:02+00:00 | Intf. Port:3 TEST Ok!!!, (CAP:0x0000303F) |
| 8 | Audit | 1970-01-01T00:00:02+00:00 | Intf. Port:4 TEST Ok!!!, (CAP:0x0000303F) |
| 9 | Audit | 1970-01-01T00:00:02+00:00 | Intf. Port:5 TEST Ok!!!, (CAP:0x048E1171) |
| 10 | Audit | 1970-01-01T00:00:02+00:00 | Intf. Port:6 TEST Ok!!!, (CAP:0x048E1171) |
| 11 | Audit | 1970-01-01T00:00:02+00:00 | Intf. Port:7 TEST Ok!!!, (CAP:0x048E1171) |
| 12 | Audit | 1970-01-01T00:00:02+00:00 | Intf. Port:8 TEST Ok!!!, (CAP:0x048E1171) |
| 13 | Audit | 1970-01-01T00:00:03+00:00 | SNMP server Stop. |
| 14 | Audit | 1970-01-01T00:00:03+00:00 | HTTP server started on port 80. |
| 17 | Audit | 1970-01-01T00:00:09+00:00 | SSH server started on port 22. |
| 18 | Audit | 1970-01-01T00:00:10+00:00 | HTTPs server started on port 443. |
| 19 | Audit | 1970-01-01T00:00:13+00:00 | User [admin] logged on Console |
| 21 | Audit | 1970-01-01T00:00:41+00:00 | User [admin] logged on HTTP |
| 28 | Audit | 1970-01-01T00:05:36+00:00 | User [admin] logouted on Console |

## EXAMPLE CLI MONITOR

✓ **System Log Information**

```
# show logging

Switch logging host mode is enabled
Switch logging host address is 192.168.10.130
Switch logging level is info.
Number of entries on Switch 1:
Audit: 18
Error: 0
Warning: 0
Notice: 4
Info.: 1
All: 23

ID   Level    Time                      Message
---- -------- ------------------------  --------------------------------

  1 Audit    1970-01-01T00:00:00+00:00 Audit Log Start, Image: [SFC8100G 5.0.0.4]
  2 Info.    1970-01-01T00:00:02+00:00 SYS-BOOTING: Switch just made a cool boot.
  3 Audit    1970-01-01T00:00:02+00:00 TELNET server started on port 23.
  4 Notice   1970-01-01T00:00:02+00:00 LINK-UPDOWN: Intf. Vlan 1, changed state to
down.
  5 Audit    1970-01-01T00:00:02+00:00 Intf. Port:1 TEST Ok!!!, (CAP:0x0000303F)
```

```
  6 Audit     1970-01-01T00:00:02+00:00  Intf. Port:2 TEST Ok!!!. (CAP:0x0000303F)
```

```
 22 Audit                               User admin logouted on HTTP
 23 Audit     1970-01-01T00:15:35+00:00 User [admin] logged on HTTP
```

➢ **Level**

- example notice

```
# show logging notice

Switch logging host mode is enabled
Switch logging host address is 192.168.10.130
Switch logging level is info.
Number of entries on Switch 1:
Audit: 18
Error: 0
Warning: 0
Notice: 4
Info.: 1
All: 23

ID  Level   Time                    Message

---- -------- ------------------------  -------------------------------

4  Notice  1970-01-01T00:00:02+00:00 LINK-UPDOWN: Intf. Vlan 1, changed state to down.
16 Notice  1970-01-01T00:00:06+00:00 LINK-UPDOWN: Intf. GigabitEthernet 1/4, changed state to up.
18 Notice  1970-01-01T00:00:08+00:00 LINK-UPDOWN: Intf. Vlan 1, changed state to up.
20 Notice  1970-01-01T00:00:35+00:00 LINK-UPDOWN: Intf. Vlan 1, changed state to up.
```

➢ **Clear Level**

- example notice

```
# clear logging notice

# show logging notice

Switch logging host mode is enabled
Switch logging host address is 192.168.10.130
Switch logging level is info.

Number of entries on Switch 1:
Audit: 18
Error: 0
Warning: 0
Notice: 0
Info.: 1
All: 19
```

## 6.1.2.5. Detailed Log

WEB MENU Configuration>System>Detailed Log

The switch system detailed log information is provided here.

**Detailed System Log Information**

ID [ 1 ]

**Message**

No system log entry

### Detailed System Log Information

| Object | Description |
|--------|-------------|
| ID | The ID (>= 1) of the system log entry. |
| Message | The detailed message of the system log entry. |

**Buttons**

Refresh : Updates the system log entry to the current entry ID.

|<< : Updates the system log entry to the first available entry ID.

<< : Updates the system log entry to the previous available entry ID.

>> : Updates the system log entry to the next available entry ID.

>>| : Updates the system log entry to the last available entry ID.

---

## EXAMPLE WEB MONITOR

---

WEB MENU Configuration>System>Detailed Log

✓ **Detailed System Log Information**

➢ *ID*

**Detailed System Log Information**

ID [ 1 ]

**Message**

| Level | Audit |
|-------|-------|
| Time | 1970-01-01T09:00:00+09:00 |
| Message | Audit Log Start, Image:[SFC6810BT 5.0.3.0] |

SOLTECH
INFONET INC.

## EXAMPLE CLI MONITOR

✓ **Detailed System Log Information**

➢ *ID*

```
# show logging <1-4294967295>

# show logging 1
Switch : 1
ID     : 1
Level  : Audit
Time   : 1970-01-01T09:00:00+09:00
Message:
Audit Log Start, Image:[SFC8100BT 5.0.3.0]
```

## 6.2. Green Ethernet

## 6.2.1. Green Ethernet Configuration

## 6.2.1.1. Port Power Savings

WEB MENU Configuration>Green Ethernet>Port Power Savings

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

**Port Power Savings Configuration**

Optimize EEE for [ Latency ⌄ ]

**Port Configuration**

| Port | ActiPHY | PerfectReach | EEE | EEE Urgent Queues | | | | | | | |
|------|---------|--------------|-----|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| * | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 2 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 3 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 4 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 5 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 6 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 7 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 8 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

### Port Power Saving Configuration

| Object | Description |
|--------|-------------|
| **Optimize EEE for** | The option is to configure the switch to optimize EEE.<br>Latency: The option is to minimize traffic latency.<br>Power: The option is to optimize power saving. |

### Port Configuration

| Object | Description |
|--------|-------------|
| **Port** | The switch port number of the logical port. |
| **ActiPHY** | ActiPHY works by lowering the power for a port when there is no link. |
| **PerfectReach** | PerfectReach works by determining the cable length and lowering the power for ports with short cables. |
| **EEE** | This controls whether EEE is enabled for this switch port.<br>EEE (Ethernet Energy Efficiency) is a feature that allows network devices in an Ethernet network to transition into a low-power sleep mode when they are idle, based on the actual traffic demand on the network. This helps reduce power consumption. |
| **EEE Urgent Queues** | Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted. |

### Buttons

[ Apply ] : Click to apply changes.

[ Apply&Save ] : Click to apply and save changes.

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

<div align="center">

## EXAMPLE WEB CONFIGURATION

</div>

WEB MENU Configuration>Green Ethernet>Port Power Savings

✓ **Port Power Saving Configuration**

➢ ***Optimize EEE for***

• Latency

**Port Power Savings Configuration**

Optimize EEE for  Latency

**Port Configuration**

| Port | ActiPHY | PerfectReach | EEE | EEE Urgent Queues |
|------|---------|--------------|-----|---|---|---|---|---|---|---|---|
|  |  |  |  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| * | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 2 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 3 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 4 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 5 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 6 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 7 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 8 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

• Power

**Port Power Savings Configuration**

Optimize EEE for  Power

**Port Configuration**

| Port | ActiPHY | PerfectReach | EEE | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|------|---------|--------------|-----|---|---|---|---|---|---|---|---|
| * | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 2 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 3 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 4 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 5 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 6 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 7 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 8 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

➢ ***ActiPHY***

**Port Power Savings Configuration**

Optimize EEE for  Power

**Port Configuration**

| Port | ActiPHY | PerfectReach | EEE | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|------|---------|--------------|-----|---|---|---|---|---|---|---|---|
| * | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 2 | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 3 | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 4 | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 5 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 6 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 7 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 8 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

<div align="center">SOLTECH<br>INFONET INC.</div>

➢ **PerfectReach**



➢ **EEE (Energy-Efficient Ethernet)**



➢ **EEE Urgent Queues**

# EXAMPLE CLI CONFIGURATION

✓ **Port Power Saving Configuration**

➢ *Optimize EEE for*

- Latency

```
(config)# no green-ethernet eee optimize-for-power
```

- Power

```
(config)# green-ethernet eee optimize-for-power
```

➢ *ActiPHY*

```
(config)# interface GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1
(config-if)# green-ethernet energy-detect
```

➢ *PerfectReach*

```
(config)# interface GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1
(config-if)# green-ethernet short-reach
```

➢ *EEE (Energy-Efficient Ethernet)*

```
(config)# interface GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1
(config-if)# green-ethernet eee
```

➢ *EEE Urgent Queues*

```
(config)# interface GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1
(config-if)# green-ethernet eee urgent-queues <range_list>
(config-if)# green-ethernet eee urgent-queues 1,7
(config-if)# green-ethernet eee urgent-queues 5-6
```

## 6.2.2. Green Ethernet Monitor

## 6.2.2.1. Port Power Savings

WEB MENU Monitor>Green Ethernet>Port Power Savings

This page provides the current status for EEE.

**Port Power Savings Status**

| Port | Link | EEE Cap | EEE Ena | LP EEE Cap | EEE In power save | ActiPhy Savings | PerfectReach Savings |
|------|------|---------|---------|------------|-------------------|-----------------|----------------------|
| 1 | ● | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 2 | ● | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 3 | ● | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 4 | ● | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ |
| 5 | ● | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 6 | ● | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 7 | ● | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 8 | ● | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

**Port Power Saving Status**

| Object | Description |
|--------|-------------|
| **Port** | This is the logical port number for this row. |
| **Link** | Shows if the link is up for the port (green = link up, red = link down). |
| **EEE cap** | Shows if the port is EEE capable. |
| **EEE Ena** | Shows if EEE is enabled for the port. |
| **LP EEE cap** | Shows if the link partner is EEE capable. |
| **EEE In power save** | Shows if the system is currently saving power due to EEE. |
| **Actiphy Savings** | Shows if the system is currently saving power due to ActiPhy. |
| **PerfectReach Savings** | Shows if the system is currently saving power due to PerfectReach. |

**Buttons**

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

Refresh : Click to refresh the page.

# EXAMPLE WEB MONITOR

✓ **Port Power Saving Status**

**Port Power Savings Status**

| Port | Link | EEE Cap | EEE Ena | LP EEE Cap | EEE In power save | ActiPhy Savings | PerfectReach Savings |
|------|------|---------|---------|------------|-------------------|-----------------|----------------------|
| 1 | 🔴 | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ |
| 2 | 🟢 | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ |
| 3 | 🔴 | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ |
| 4 | 🟢 | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ |
| 5 | 🔴 | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 6 | 🔴 | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 7 | 🔴 | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 8 | 🔴 | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

# EXAMPLE CLI MONITOR

✓ **Port Power Saving Status**

```
# show green-ethernet

Interface    Link  Energy-detect  Short-Reach  EEE Capable  EEE Enabled  LP EEE Capable   EEE In Power Save

---------------------- ---  --------  -----------  -----------  -----------  ----------------  ------------------
GigabitEthernet 1/1   No   Yes        No           Yes          Yes          No                No
GigabitEthernet 1/2   Yes  No         Yes          Yes          Yes          No                No
GigabitEthernet 1/3   No   Yes        No           Yes          Yes          No                No
GigabitEthernet 1/4   Yes  No         Yes          Yes          Yes          Yes               Yes
10GigabitEthernet 1/1 No   N/A        N/A          No           N/A          N/A               N/A
10GigabitEthernet 1/2 No   N/A        N/A          No           N/A          N/A               N/A
10GigabitEthernet 1/3 No   N/A        N/A          No           N/A          N/A               N/A
10GigabitEthernet 1/4 No   N/A        N/A          No           N/A          N/A               N/A
```

# 6.3. Ports

## 6.3.1. Ports Configuration

## 6.3.1.1. Ports

WEB MENU Configuration>Ports

Indicate general setting detail of switch and configure.



**Port Configuration**

| Object | Description |
|---|---|
| **Port** | This is the logical port number for this row. |
| **Description** | The description of the port. It is an ASCII string no longer than 256 characters. |
| **Link** | The current link state is displayed graphically. Green indicates the link is up and red that it is down. |
| **PHY** | Refers to the physical layer of the port. It is categorized as either UTP or SFP ports. For SFP ports, the maximum speed information of the inserted optical module is displayed. |
| **Speed – Current** | Provides the current link speed of the port. |
| **Speed – Configured** | Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are: Disabled - Disables the switch port operation. Auto - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner. 10Mbps HDX - Forces the port in 10Mbps half duplex mode. 10Mbps FDX - Forces the port in 10Mbps full duplex mode. 100Mbps HDX - Forces the port in 100Mbps half duplex mode. 100Mbps FDX - Forces the port in 100Mbps full duplex mode. 1Gbps FDX - Forces the port in 1Gbps full duplex 1Gbps C37 - Forces the port in 1Gbps CLAUSE37 Auto Negotiation 10Gbps FDX - Forces the port in 10Gbps full duplex 2.5Gbps FDX - Forces the Serdes port in 2.5Gbps full duplex mode. SFP_Auto_AMS - Automatically determines the speed of the SFP. Note: There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect some SFPs might not be detectable. The port is set in AMS mode. Cu port is set in Auto mode. 100-FX - SFP port in 100-FX speed. Cu port disabled. 1000-X - SFP port in 1000-X speed. Cu port disabled. |

| | |
|---|---|
| | Ports in AMS mode with 1000-X speed has Cu port preferred.<br>Ports in AMS mode with 1000-X speed has fiber port preferred.<br>Ports in AMS mode with 100-FX speed has fiber port preferred. |
| **Advertise Duplex** | When duplex is set as auto i.e auto negotiation, the port will only advertise the specified duplex as either Fdx or Hdx to the link partner. By default port will advertise all the supported duplexes if the Duplex is Auto. |
| **Advertise Speed** | When Speed is set as auto i.e auto negotiation, the port will only advertise the specified speeds (10M 100M 1G) to the link partner. By default port will advertise all the supported speeds if speed is set as Auto. |
| **Flow Control** | When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner.<br>When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto Negotiation.<br>Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.<br>NOTICE: The 100FX standard doesn't support Auto Negotiation, so when in 100FX mode the flow control capabilities will always be shown as "disabled". |
| **PFC** | When PFC (802.1Qbb Priority Flow Control) is enabled on a port then flow control on a priority level is enabled. Through the Priority field, range (one or more) of priorities can be configured, e.g. '0-3,7' which equals '0,1,2,3,7'. PFC is not supported through auto negotiation. PFC and Flowcontrol cannot both be enabled on the same port. |
| **Maximum Frame Size** | Enter the maximum frame size allowed for the switch port, including FCS. The range is 1518-10240 bytes. |
| **Excessive Collision Mode** | Configure port transmit collision behavior.<br>Discard: Discard frame after 16 collisions (default).<br>Restart: Restart backoff algorithm after 16 collisions. |
| **Frame Length Check** | Configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If "frame length check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actually payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch. Note: No drop counters count frames dropped due to frame length mismatch |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

## EXAMPLE WEB CONFIGURATION

✓ **Port Configuration**

➢ *Description*



➢ *Speed Configured*

Auto-negotiation is the default value, and other values are fixed. (speed, duplex)



➢ *Advertise Duplex*

For UTP ports, only Speed Auto can be configured, and Full duplex is prioritized and communicated to the link partner.



➢ *Advertise Speed*

For UTP ports, only Speed Auto can be configured, and the higher speed is prioritized and communicated to the link partner.

• Speed – AUTO (connected as 1G full duplex based on priority)

- Speed – AUTO excluding 1G(connected as 100M full duplex based on priority)



- Speed – AUTO excluding 1G, 100M(connected as 10M full duplex based on priority)



➢ **Flow Control**

- Flow Control Disable(default)



- Flow Control Enable

➢ **PFC**

• Enable



• Priority





➢ **Maximum Frame Size**

(1518~10240bytes)

➢ **Excessive Collision Mode(Apply only UTP)**

• Discard(default)



• Restart



➢ **Frame Length Check**



# EXAMPLE CLI CONFIGURATION

✓ **Port Configuration**

➢ **Description**

(config)# interface 10GigabitEthernet/ GigabitEthernet <port_type_list>
*(config)# interface GigabitEthernet 1/1*

(config-if)# description <line>
*(config-if) )# description H/W TEAM*

> ➢ *Speed Configured*
> Auto-negotiation is the default value, and other values are fixed. (speed, duplex)

```
(config)# interface 10GigabitEthernet/ GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# speed { 10g | 2500 | 1000-c37 | 1000 | 100 | 10 | auto { [ 10 ] [ 100 ]
[ 1000 ] } }
(config-if)# speed auto
(config-if)# speed 100

(config-if)# duplex <auto/full/half>
(config-if)# duplex auto
(config-if)# duplex full
```

> ➢ *Advertise Duplex*
> For UTP ports, only Speed Auto can be configured, and Full duplex is prioritized and
> communicated to the link partner.

```
(config)# interface GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# speed auto

(config-if)# duplex auto <full/half/cr>
(config-if)# duplex auto
(config-if)# duplex auto full
```

> ➢ *Advertise Speed*
> For UTP ports, only Speed Auto can be configured, and the higher speed is prioritized and
> communicated to the link partner.

```
(config)# interface GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# speed auto { [ 10 ] [ 100 ] [ 1000 ] } }
(config-if)# speed auto 10 100
(config-if)# speed auto 1000 100

(config-if)# duplex auto
```

> ➢ *Flow Control*

> • Flow Control Disable(default)

```
(config)# interface 10GigabitEthernet/GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# flowcontrol off
```

> • Flow Control Enable

```
(config)# interface 10GigabitEthernet/GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# flowcontrol on
```

SOLTECH
INFONET INC.

➢ **PFC**

•   Enable, Priority

```
(config)# interface 10GigabitEthernet/GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# priority-flowcontrol prio <0~7>
(config-if)# priority-flowcontrol prio 0-7
(config-if)# priority-flowcontrol prio 1,3,7
```

•   Disable, Priority

```
(config)# interface 10GigabitEthernet/GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)#no priority-flowcontrol prio <0~7>
(config-if)#no priority-flowcontrol prio 0-7
(config-if)#no priority-flowcontrol prio 1,3,7
```

➢ **Maximum Frame Size**
(1518~10240bytes)

```
(config)# interface 10GigabitEthernet/GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)#mtu 1518-10240
(config-if)#mtu 1518
(config-if)#mtu 10240
```

➢ **Excessive Collision Mode(Apply only UTP)**

•   Discard(default)

```
(config)# interface GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# no excessive-restart
```

•   Restart

```
(config)# interface GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# excessive-restart
```

➢ **Frame Length Check**

•   ***Enable***

```
(config)# interface 10GigabitEthernet/GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# frame-length-check
```

•   ***Disable***

```
(config)# interface 10GigabitEthernet/GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# no frame-length-check
```

# 6.3.2. Ports Monitor

## 6.3.2.1. State

WEB MENU Monitor>Ports>State

This page provides an overview of the current status of switch ports.
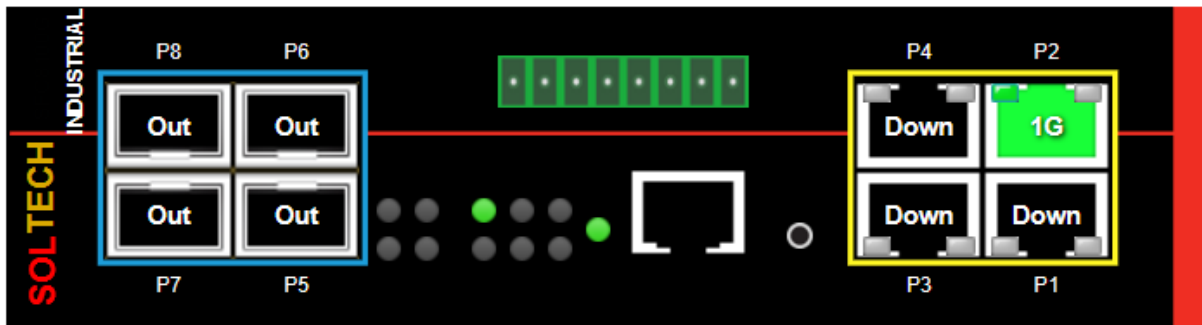


| State | Disabled | Down | Link (non-Max Speed) | Link (Max Speed) |
|---|---|---|---|---|
| **RJ-45 Ports** | | | | |
| **SFP Ports** | | | | |

| Info. | X (Disabled) | Out (Module-Out) | Down (Link Down) | 10M (Link 10m) | 100M (Link 100m) | 1G (Link 1G) | 2.5G (Link 2.5G) | 10G (Link 10G) | PoE (PoE) |
|---|---|---|---|---|---|---|---|---|---|

### Port State Overview

| Object | Description |
|---|---|
| **reset** | Change setting value into default value, if push it more than 2 seconds. If push it more than 10 seconds, all of setting value are changed into default value including IP(192.168.10.100). |
| **Power** | Turned on LED when power is supplied. |

**Buttons**

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

Refresh : Click to refresh the page.

## EXAMPLE WEB CONFIGURATION

WEB MENU Monitor>Ports>State
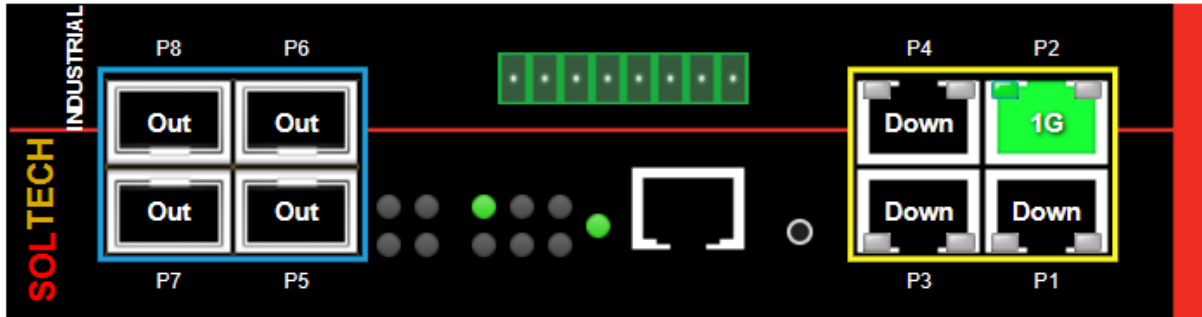


## EXAMPLE CLI CONFIGURATION

✓ **Port State Overview**

```
# show interface GigabitEthernet 1/1-4 status

Interface         Mode  Speed & Duplex  Flow Control  Max Frame  Excessive  Link     MAC-Addr
----------------------  -------  --------------  ------------  ---------  ---------  ---------  --------
GigabitEthernet 1/1  enabled  Auto        disabled     10240      Restart    100fdx  02:21:6D:60:D9:53
GigabitEthernet 1/2  enabled  Auto        disabled     10240      Discard    Down    06:21:6D:60:D9:53
GigabitEthernet 1/3  enabled  Auto        disabled     10240      Discard    Down    0A:21:6D:60:D9:53
GigabitEthernet 1/4  enabled  Auto        disabled     10240      Discard    Down    0E:21:6D:60:D9:53

# show interface 10GigabitEthernet 1/1-4 status

Interface         Mode  Speed & Duplex  Flow Control  Max Frame  Excessive  Link   MAC-Addr
----------------------  -------  --------------  ------------  ---------  ---------  ---------  --------
10GigabitEthernet 1/1  enabled  Auto        disabled     10240      Discard    Down   12:21:6D:60:D9:53
10GigabitEthernet 1/2  enabled  Auto        disabled     10240      Discard    Down   16:21:6D:60:D9:53
10GigabitEthernet 1/3  enabled  Auto        disabled     10240      Discard    Down   1A:21:6D:60:D9:53
10GigabitEthernet 1/4  enabled  Auto        disabled     10240      Discard    Down   1E:21:6D:60:D9:53
```

SOLTECH
INFONET INC.

## 6.3.2.2. Traffic Overview

WEB MENU Monitor>Ports>Traffic Overview

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

**Port Statistics Overview**

| Port | Description | Packets | | Bytes | | Errors | | Drops | | Filtered |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received |
| 1 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

### Port Statistics Overview

| Object | Description |
|---|---|
| **Port** | The logical port. Click number will navigate to the Detailed Statistics. |
| **Description** | Description of the port. |
| **Packets** | The number of received and transmitted packets per port. |
| **Bytes** | The number of received and transmitted bytes per port. |
| **Errors** | The number of frames received in error and the number of incomplete transmissions per port. |
| **Drops** | The number of frames discarded due to ingress or egress congestion. |
| **Filtered** | The number of received frames filtered by the forwarding process. |

**Buttons**

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

Refresh : Click to refresh the page immediately.

Clear : Clears the counters for all ports.

---

## EXAMPLE WEB MONITOR

---

WEB MENU Monitor>Ports>Traffic Overview

**Port Statistics Overview**

| Port | Description | Packets | | Bytes | | Errors | | Drops | | Filtered |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received |
| 1 | | 1215 | 486 | 232396 | 220964 | 0 | 0 | 0 | 0 | 148 |
| 2 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | | 1 | 4 | 64 | 256 | 0 | 0 | 0 | 0 | 0 |
| 4 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | | 2561 | 1 | 163904 | 64 | 0 | 0 | 0 | 0 | 0 |
| 6 | | 1783 | 4 | 114112 | 256 | 0 | 0 | 0 | 0 | 0 |
| 7 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | | 545 | 5 | 34880 | 320 | 0 | 0 | 0 | 0 | 0 |

SOLTECH
INFONET INC.

## EXAMPLE CLI MONITOR

✓ **Port Statistics Overview**

```
# show interface GigabitEthernet 1/1-4 statistics packets

Interface            Rx Packets          Tx Packets
---------------------  ------------------  ------------------
GigabitEthernet 1/1    4434                 2280
GigabitEthernet 1/2    0                    0
GigabitEthernet 1/3    1                    5
GigabitEthernet 1/4    0                    0

# show interface 10GigabitEthernet 1/1-4 statistics packets

Interface            Rx Packets          Tx Packets
---------------------  ------------------  ------------------
10GigabitEthernet 1/1   6929                 43
10GigabitEthernet 1/2   1783                 4
10GigabitEthernet 1/3   0                    0
10GigabitEthernet 1/4   545                  5
```

```
# show interface GigabitEthernet 1/1-4 statistics bytes

Interface            Rx Octets           Tx Octets
---------------------  ------------------  ------------------
GigabitEthernet 1/1    1015232              1238992
GigabitEthernet 1/2    0                    0
GigabitEthernet 1/3    64                   320
GigabitEthernet 1/4    0                    0

# show interface 10GigabitEthernet 1/1-4 statistics bytes

Interface            Rx Octets           Tx Octets
---------------------  ------------------  ------------------
10GigabitEthernet 1/1   443456               4008
10GigabitEthernet 1/2   114112               256
10GigabitEthernet 1/3   0                    0
10GigabitEthernet 1/4   34880                320
```

```
# show interface GigabitEthernet 1/1-4 statistics errors

Interface            Rx Errors           Tx Errors
---------------------  ------------------  ------------------
GigabitEthernet 1/1    3                    0
GigabitEthernet 1/2    0                    0
GigabitEthernet 1/3    0                    0
GigabitEthernet 1/4    0                    0

# show interface 10GigabitEthernet 1/1-4 statistics errors

Interface            Rx Errors           Tx Errors
---------------------  ------------------  ------------------
10GigabitEthernet 1/1   0                    0
10GigabitEthernet 1/2   0                    0
10GigabitEthernet 1/3   0                    0
10GigabitEthernet 1/4   0                    0
```

```
# show interface GigabitEthernet 1/1-4 statistics discards

Interface            Rx Discards        Tx Discards
---------------------- ------------------ ------------------
GigabitEthernet 1/1    0                 0
GigabitEthernet 1/2    0                 0
GigabitEthernet 1/3    0                 0
GigabitEthernet 1/4    0                 0

# show interface 10GigabitEthernet 1/1-4 statistics discards

Interface            Rx Discards        Tx Discards
---------------------- ------------------ ------------------
10GigabitEthernet 1/1   0                 0
10GigabitEthernet 1/2   0                 0
10GigabitEthernet 1/3   0                 0
10GigabitEthernet 1/4   0                 0
```

```
# show interface GigabitEthernet 1/1-4 statistics filtered

Interface            Rx Filtered
---------------------- ------------------
GigabitEthernet 1/1    1012
GigabitEthernet 1/2    0
GigabitEthernet 1/3    0
GigabitEthernet 1/4    0

# show interface 10GigabitEthernet 1/1-4 statistics filtered

Interface            Rx Filtered
---------------------- ------------------
10GigabitEthernet 1/1   0
10GigabitEthernet 1/2   0
10GigabitEthernet 1/3   0
10GigabitEthernet 1/4   0
```

SOLTECH
INFONET INC.

## 6.3.2.3. QoS Statistics

WEB MENU Monitor>Ports>QoS Statistics

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

**Queuing Counters**

| Port | Q0 Rx | Q0 Tx | Q1 Rx | Q1 Tx | Q2 Rx | Q2 Tx | Q3 Rx | Q3 Tx | Q4 Rx | Q4 Tx | Q5 Rx | Q5 Tx | Q6 Rx | Q6 Tx | Q7 Rx | Q7 Tx |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

### Queuing Counters

| Object | Description |
|---|---|
| Port | The logical port. Click number will navigate to the Detailed Statistics. |
| Qn | There are 8 QoS queues per port. Q0 is the lowest priority queue. |
| Rx/Tx | The number of received and transmitted packets per queue. |

**Buttons**

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

Refresh : Click to refresh the page immediately.

Clear : Clears the counters for all ports.

---

## EXAMPLE WEB MONITOR

---

WEB MENU Monitor>Ports>QoS Statistics

**Queuing Counters**

| Port | Q0 Rx | Q0 Tx | Q1 Rx | Q1 Tx | Q2 Rx | Q2 Tx | Q3 Rx | Q3 Tx | Q4 Rx | Q4 Tx | Q5 Rx | Q5 Tx | Q6 Rx | Q6 Tx | Q7 Rx | Q7 Tx |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 494 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 309 |
| 2 | 511 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 356 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 1 | 95 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 1323 | 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 2356 | 21 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

SOLTECH
INFONET INC.

# EXAMPLE CLI MONITOR

✓    **Queuing Counters**

```
#show interface GigabitEthernet 1/1-4 statistics priority

GigabitEthernet 1/1            Rx Priority queue  Tx Priority queue
-----------------------------------  -------------------  ------------------
Priority 0                     930               1
Priority 1                     0                 0
Priority 2                     0                 0
Priority 3                     0                 0
Priority 4                     0                 0
Priority 5                     0                 0
Priority 6                     0                 0
Priority 7                     0                 378

GigabitEthernet 1/2            Rx Priority queue  Tx Priority queue
-----------------------------------  -------------------  ------------------
Priority 0                     511               1
Priority 1                     0                 0
Priority 2                     0                 0
Priority 3                     0                 0
Priority 4                     0                 0
Priority 5                     0                 0
Priority 6                     0                 0
Priority 7                     0                 356

GigabitEthernet 1/3            Rx Priority queue  Tx Priority queue
-----------------------------------  -------------------  ------------------
Priority 0                     0                 0
Priority 1                     0                 0
Priority 2                     0                 0
Priority 3                     0                 0
Priority 4                     0                 0
Priority 5                     0                 0
Priority 6                     0                 0
Priority 7                     0                 0

GigabitEthernet 1/4            Rx Priority queue  Tx Priority queue
-----------------------------------  -------------------  ------------------
Priority 0                     1                 95
Priority 1                     0                 0
Priority 2                     0                 0
Priority 3                     0                 0
Priority 4                     0                 0
Priority 5                     0                 0
Priority 6                     0                 0
Priority 7                     0                 0

# show interface 10GigabitEthernet 1/1-4 statistics priority

10GigabitEthernet 1/1          Rx Priority queue    Tx Priority queue
-----------------------------------  -------------------  ------------------
Priority 0                     1323              12
Priority 1                     0                 0
Priority 2                     0                 0
Priority 3                     0                 0
```

```
Priority 4                    0               0
Priority 5                    0               0
Priority 6                    0               0
Priority 7                    0               0

10GigabitEthernet 1/2         Rx Priority queue    Tx Priority queue
------------------------------------- -------------------- ------------------
Priority 0                    0               0
Priority 1                    0               0
Priority 2                    0               0
Priority 3                    0               0
Priority 4                    0               0
Priority 5                    0               0
Priority 6                    0               0
Priority 7                    0               0


10GigabitEthernet 1/3         Rx Priority queue    Tx Priority queue
------------------------------------- -------------------- ------------------
Priority 0                    0               0
Priority 1                    0               0
Priority 2                    0               0
Priority 3                    0               0
Priority 4                    0               0
Priority 5                    0               0
Priority 6                    0               0
Priority 7                    0               0

10GigabitEthernet 1/4         Rx Priority queue    Tx Priority queue
------------------------------------- -------------------- ------------------
Priority 0                    2356            21
Priority 1                    0               0
Priority 2                    0               0
Priority 3                    0               0
Priority 4                    0               0
Priority 5                    0               0
Priority 6                    0               0
Priority 7                    0               0
```

## 6.3.2.4. QCL Status

WEB MENU Monitor>Ports>QCL Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined.
It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

**QoS Control List Status**

| User | QCE | Port | Frame Type | Action | | | | | | Conflict |
|------|-----|------|------------|--------|--------|--------|--------|--------|--------|----------|
| | | | | CoS | DPL | DSCP | PCP | DEI | Policy | |
| No entries | | | | | | | | | | |

**QoS Control List Status**

| Object | Description |
|--------|-------------|
| **User** | Indicates the QCL user. |
| **QCE** | Indicates the QCE id. |
| **Port** | Indicates the list of ports configured with the QCE. |
| **Frame Type** | Indicates the type of frame. <br> **Any** — Match any frame type. <br> **Ethernet** — Match EtherType frames. <br> **LLC** — Match (LLC) frames. <br> **SNAP** — Match (SNAP) frames. <br> **IPv4** — Match IPv4 frames. <br> **IPv6** — Match IPv6 frames. |
| **Action** | Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. <br> **CoS** — Classify Class of Service. <br> **DPL** — Classify Drop Precedence Level. <br> **DSCP** — Classify DSCP value. <br> **PCP** — Classify PCP value. <br> **DEI** — Classify DEI value. <br> **Policy** — Classify ACL Policy number. |
| **Conflict** | Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button. |

**Buttons**
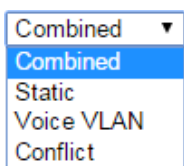
Combined ▼ / Combined / Static / Voice VLAN / Conflict : Select the QCL status from this drop down list.

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

SOLTECH
INFONET INC.

Resolve Conflict : Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.

Refresh : Click to refresh the page.

## 6.3.2.5. Detailed Statistics

WEB MENU Monitor>Ports>Detailed Statistics

This page provides detailed traffic statistics for a specific switch port.

(Use the port select box to select which switch port details to display.)

| Detailed Port Statistics  Port 1 | | Port 1 ⌄ Auto-refresh ☐ |
|---|---|---|

| Receive Total | | | Transmit Total | |
|---|---|---|---|---|
| Rx Packets | 0 | | Tx Packets | 0 |
| Rx Octets | 0 | | Tx Octets | 0 |
| Rx Unicast | 0 | | Tx Unicast | 0 |
| Rx Multicast | 0 | | Tx Multicast | 0 |
| Rx Broadcast | 0 | | Tx Broadcast | 0 |
| Rx Pause | 0 | | Tx Pause | 0 |
| **Receive Size Counters** | | | **Transmit Size Counters** | |
| Rx 64 Bytes | 0 | | Tx 64 Bytes | 0 |
| Rx 65-127 Bytes | 0 | | Tx 65-127 Bytes | 0 |
| Rx 128-255 Bytes | 0 | | Tx 128-255 Bytes | 0 |
| Rx 256-511 Bytes | 0 | | Tx 256-511 Bytes | 0 |
| Rx 512-1023 Bytes | 0 | | Tx 512-1023 Bytes | 0 |
| Rx 1024-1526 Bytes | 0 | | Tx 1024-1526 Bytes | 0 |
| Rx 1527- Bytes | 0 | | Tx 1527- Bytes | 0 |
| **Receive Queue Counters** | | | **Transmit Queue Counters** | |
| Rx Q0 | 0 | | Tx Q0 | 0 |
| Rx Q1 | 0 | | Tx Q1 | 0 |
| Rx Q2 | 0 | | Tx Q2 | 0 |
| Rx Q3 | 0 | | Tx Q3 | 0 |
| Rx Q4 | 0 | | Tx Q4 | 0 |
| Rx Q5 | 0 | | Tx Q5 | 0 |
| Rx Q6 | 0 | | Tx Q6 | 0 |
| Rx Q7 | 0 | | Tx Q7 | 0 |
| **Receive Error Counters** | | | **Transmit Error Counters** | |
| Rx Drops | 0 | | Tx Drops | 0 |
| Rx CRC/Alignment | 0 | | Tx Late/Exc. Coll. | 0 |
| Rx Undersize | 0 | | | |
| Rx Oversize | 0 | | | |
| Rx Fragments | 0 | | | |
| Rx Jabber | 0 | | | |
| Rx Filtered | 0 | | | |

### Detailed Port Statistics Port n

| Object | Description |
|---|---|
| Receive and Transmit Total | Display information about the total received and transmitted packets. |
| Rx and Tx Packets | The number of received and transmitted packets. |
| Rx and Tx Octets | The number of received and transmitted bytes. |
| Rx and Tx Unicast | The number of received and transmitted unicast packets. |
| Rx and Tx Multicast | The number of received and transmitted multicast packets. |
| Rx and Tx Broadcast | The number of received and transmitted broadcast packets. |
| Rx and Tx Pause | A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation. |
| Receive and Transmit Size Counters | The number of received and transmitted packets split into categories based on their respective frame sizes. |
| Receive and Transmit Queue Counters | The number of received and transmitted packets per input and output queue. |
| Receive and Transmit Error Counters | The number of received and transmitted packets, classified as errors. |
| Rx Drops | The number of frames dropped due to lack of receive buffers or egress congestion. |
| Rx CRC/Alignment | The number of frames received with CRC or alignment errors. |
| Rx Undersize | The number of short frames received with valid CRC. |
| Rx Oversize | The number of long frames received with valid CRC. |
| Rx Fragments | The number of short frames received with invalid CRC. |
| Rx Jabber | The number of long frames received with invalid CRC. |

SOLTECH
INFONET INC.

| Rx Filtered | The number of received frames filtered by the forwarding process. |
|---|---|
| Tx Drops | The number of frames dropped due to output buffer congestion. |
| Tx Late/Exc. | The number of frames dropped due to excessive or late collisions. |

**Buttons**

[Port 1 ▾] : Selecting a port to retrieve information about the desired port.

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

[Refresh] : Click to refresh the page immediately.

[Clear] : Clears the counters for the selected port.

---

## EXAMPLE WEB MONITOR

---

WEB MENU Monitor>Ports>Detailed Statistics

**Detailed Port Statistics  Port 1**                                                                                    [Port 1 ▾] Auto-refresh ☐

| Receive Total | | Transmit Total | |
|---|---|---|---|
| Rx Packets | 2624 | Tx Packets | 553 |
| Rx Octets | 351169 | Tx Octets | 102221 |
| Rx Unicast | 668 | Tx Unicast | 553 |
| Rx Multicast | 693 | Tx Multicast | 0 |
| Rx Broadcast | 1263 | Tx Broadcast | 0 |
| Rx Pause | 0 | Tx Pause | 0 |
| **Receive Size Counters** | | **Transmit Size Counters** | |
| Rx 64 Bytes | 1673 | Tx 64 Bytes | 308 |
| Rx 65-127 Bytes | 175 | Tx 65-127 Bytes | 70 |
| Rx 128-255 Bytes | 648 | Tx 128-255 Bytes | 71 |
| Rx 256-511 Bytes | 0 | Tx 256-511 Bytes | 56 |
| Rx 512-1023 Bytes | 128 | Tx 512-1023 Bytes | 26 |
| Rx 1024-1526 Bytes | 0 | Tx 1024-1526 Bytes | 22 |
| Rx 1527- Bytes | 0 | Tx 1527- Bytes | 0 |
| **Receive Queue Counters** | | **Transmit Queue Counters** | |
| Rx Q0 | 2624 | Tx Q0 | 0 |
| Rx Q1 | 0 | Tx Q1 | 0 |
| Rx Q2 | 0 | Tx Q2 | 0 |
| Rx Q3 | 0 | Tx Q3 | 0 |
| Rx Q4 | 0 | Tx Q4 | 0 |
| Rx Q5 | 0 | Tx Q5 | 0 |
| Rx Q6 | 0 | Tx Q6 | 0 |
| Rx Q7 | 0 | Tx Q7 | 553 |
| **Receive Error Counters** | | **Transmit Error Counters** | |
| Rx Drops | 0 | Tx Drops | 0 |
| Rx CRC/Alignment | 0 | Tx Late/Exc. Coll. | 0 |
| Rx Undersize | 0 | | |
| Rx Oversize | 0 | | |
| Rx Fragments | 0 | | |
| Rx Jabber | 0 | | |
| Rx Filtered | 651 | | |

---

## EXAMPLE CLI MONITOR

---

✓ **Detailed Port Statistics Port**

```
#show interface GigabitEthernet <port_type_list> statistics
# show interface GigabitEthernet 1/1 statistics

GigabitEthernet 1/1 Statistics:
Rx Packets:           2693    Tx Packets:           565
Rx Octets:          360643    Tx Octets:          104266
Rx Unicast:            683    Tx Unicast:           565
Rx Multicast:          717    Tx Multicast:           0
Rx Broadcast:         1293    Tx Broadcast:           0
Rx Pause:                0    Tx Pause:               0

Rx 64:                1714    Tx 64:                316
Rx 65-127:             177    Tx 65-127:             71
```

SOLTECH
INFONET INC.

```
Rx 128-255:                  672   Tx 128-255:              72
Rx 256-511:                    0   Tx 256-511:              57
Rx 512-1023:                 130   Tx 512-1023:             27
Rx 1024-1526:                  0   Tx 1024-1526:           22
Rx 1527-   :                   0   Tx 1527-   :             0

Rx Priority 0:              2693   Tx Priority 0:           0
Rx Priority 1:                 0   Tx Priority 1:           0
Rx Priority 2:                 0   Tx Priority 2:           0
Rx Priority 3:                 0   Tx Priority 3:           0
Rx Priority 4:                 0   Tx Priority 4:           0
Rx Priority 5:                 0   Tx Priority 5:           0
Rx Priority 6:                 0   Tx Priority 6:           0
Rx Priority 7:                 0   Tx Priority 7:         565

Rx Drops:                      0   Tx Drops:                0
Rx CRC/Alignment:              0   Tx Late/Exc. Coll.:      0
Rx Undersize:                  0
Rx Oversize:                   0
Rx Fragments:                  0
Rx Jabbers:                    0
Rx Filtered:                 675
```

```
#show interface 10GigabitEthernet <port_type_list> statistics
# show interface 10GigabitEthernet 1/1 statistics

10GigabitEthernet 1/1 Statistics:
Rx Packets:                 1323   Tx Packets:             12
Rx Octets:                 84672   Tx Octets:             768
Rx Unicast:                    0   Tx Unicast:              0
Rx Multicast:               1322   Tx Multicast:            0
Rx Broadcast:                  1   Tx Broadcast:           12
Rx Pause:                      0   Tx Pause:                0

Rx 64:                      1323   Tx 64:                  12
Rx 65-127:                     0   Tx 65-127:               0
Rx 128-255:                    0   Tx 128-255:              0
Rx 256-511:                    0   Tx 256-511:              0
Rx 512-1023:                   0   Tx 512-1023:             0
Rx 1024-1526:                  0   Tx 1024-1526:            0
Rx 1527-   :                   0   Tx 1527-   :             0

Rx Priority 0:              1323   Tx Priority 0:          12
Rx Priority 1:                 0   Tx Priority 1:           0
Rx Priority 2:                 0   Tx Priority 2:           0
Rx Priority 3:                 0   Tx Priority 3:           0
Rx Priority 4:                 0   Tx Priority 4:           0
Rx Priority 5:                 0   Tx Priority 5:           0
Rx Priority 6:                 0   Tx Priority 6:           0
Rx Priority 7:                 0   Tx Priority 7:           0
Rx Drops:                      0   Tx Drops:                0
Rx CRC/Alignment:              0   Tx Late/Exc. Coll.:      0
Rx Undersize:                  0
Rx Oversize:                   0
Rx Fragments:                  0
Rx Jabbers:                    0
Rx Filtered:                   0
```

## 6.4. DHCP

## 6.4.1. DHCP Configuration

## 6.4.1.1. Server Mode

WEB MENU Configuration>DHCP>Server>Mode

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

**DHCP Server Mode Configuration**

**Global Mode**

Mode | Disabled ▼

**VLAN Mode**

Delete | VLAN Range | Mode

Add VLAN Range

### DHCP Server Mode Configuration
#### Global Mode

| Object | Description |
|---|---|
| **Mode** | Configure the operation mode per system. Enabled: Enable DHCP server per system. Disabled: Disable DHCP server per system. |

#### VLAN Mode

| Object | Description |
|---|---|
| **VLAN Range** | Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. BUT, if the VLAN range contains only 1 VLAN ID, then you can just input it into either one of the first and second VLAN ID or both. On the other hand, if you want to disable existed VLAN range, then you can follow the steps. 1. press to add a new VLAN range. 2. input the VLAN range that you want to disable. 3. choose Mode to be Disabled. 4. press to apply the change. |
| **Mode** | Indicate the operation mode per VLAN. Enabled: Enable DHCP server per VLAN. Disabled: Disable DHCP server pre VLAN. |

SOLTECH
INFONET INC.

**Buttons**

Add VLAN Range : Click to add a new VLAN range.

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

## EXAMPLE WEB CONFIGURATION

✓ **Global Mode**

➤ *Mode*

• *Disable*

**DHCP Server Mode Configuration**

**Global Mode**

| Mode | Disabled ▾ |
|------|-----------|

**VLAN Mode**

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

Add VLAN Range

• *Enable*

**DHCP Server Mode Configuration**

**Global Mode**

| Mode | Enabled ▾ |
|------|----------|

**VLAN Mode**

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

Add VLAN Range

✓ **VLAN Mode**

➤ *Add VLAN Range*

• *Enable*

**DHCP Server Mode Configuration**

**Global Mode**

| Mode | Enabled ▾ |
|------|----------|

**VLAN Mode**

| Delete | VLAN Range | Mode |
|--------|-----------|------|
| Delete | 1 - 2 | Enabled ▾ |

Add VLAN Range

**DHCP Server Mode Configuration**

**Global Mode**

| Mode | Enabled ▾ |
|------|----------|

**VLAN Mode**

| Delete | VLAN Range | Mode |
|--------|-----------|------|
| | 1 - 2 | Enabled |

Add VLAN Range

SOLTECH
INFONET INC.

- *Disable*

**DHCP Server Mode Configuration**

**Global Mode**

| Mode | Enabled ⌄ |

**VLAN Mode**

| Delete | VLAN Range | Mode |
|--------|-----------|------|
| | 1 - 2 | Enabled |
| Delete | 1 - 2 | Disabled ⌄ |

Add VLAN Range

**DHCP Server Mode Configuration**

**Global Mode**

| Mode | Enabled ⌄ |

**VLAN Mode**

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

Add VLAN Range

---

## EXAMPLE CLI CONFIGURATION

---

✓ **Global Mode**

➢ *Mode*

- *Disable*

```
(config)# no ip dhcp server
```

- *Enable*

```
(config)# ip dhcp server
```

✓ **VLAN Mode**

➢ *Add VLAN Range*

- *Enable*

```
(config)# interface vlan <vlan_list>
(config)# interface vlan 1-2

(config-if-vlan)# ip dhcp server
```

- *Disable*

```
(config)# interface vlan <vlan_list>
(config)# interface vlan 1-2

(config-if-vlan)# no ip dhcp server
```

## 6.4.1.2. Server Excluded IP

WEB MENU Configuration>DHCP>Server>Excluded IP

This page configures excluded IP addresses.

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

**DHCP Server Excluded IP Configuration**

**Excluded IP Address**

| Delete | IP Range |
|--------|----------|

Add IP Range

### DHCP Server Excluded IP Configuration

### Excluded IP Address

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

### Buttons

`Add IP Range` : Click to add a new excluded IP range.

`Apply` : Click to apply changes.

`Apply&Save` : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

✓ **Excluded IP Address**

➢ *Add IP Range*

• *IP Range*

**DHCP Server Excluded IP Configuration**

**Excluded IP Address**

| Delete | IP Range | |
|--------|----------|---|
| Delete | 192.168.10.1 | - 192.168.10.101 |
| Delete | 192.168.10.103 | - 192.168.10.130 |

Add IP Range

**DHCP Server Excluded IP Configuration**

**Excluded IP Address**

| Delete | IP Range |
|--------|----------|
| ☐ | 192.168.10.1 - 192.168.10.101 |
| ☐ | 192.168.10.103 - 192.168.10.130 |

Add IP Range

**SOLTECH**
INFONET INC.

## EXAMPLE CLI CONFIGURATION

✓ **Excluded IP Address**

➢ *Add IP Range*

• *IP Range*

```
(config)# ip dhcp excluded-address <ipv4_addr> <ipv4_addr>
(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.101
(config)# ip dhcp excluded-address 192.168.10.103 192.168.10.130
```

## 6.4.1.3. Server Pool

WEB MENU Configuration>DHCP>Server>Pool

This page manages DHCP pools.

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

**DHCP Server Pool Configuration**

**Pool Setting**

| Delete | Name | Type | IP | Subnet Mask | Lease Time |
|--------|------|------|----|-----|------------|

Add New Pool

### DHCP Server Pool Configuration

### Pool Setting

| Object | Description |
|--------|-------------|
| **Name** | Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page. |
| **Type** | Display which type of the pool is.<br>Network: the pool defines a pool of IP addresses to service more than one DHCP client.<br>Host: the pool services for a specific DHCP client identified by client identifier or hardware address. |
| **IP** | Display network number of the DHCP address pool. |
| **Subnet Mask** | Display subnet mask of the DHCP address pool. |
| **Lease Time** | Display lease time of the pool. |

**Buttons**

Add New Pool : Click to add a new DHCP pool.

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

### DHCP Pool Configuration

This page configures all settings of a DHCP pool.

SOLTECH
INFONET INC.

## DHCP Pool Configuration

### Pool

| Object | Description |
|---|---|
| **Name** | Select a pool by pool name. |

### Setting

| Object | Description |
|---|---|
| **Pool Name** | Display the selected pool name. |
| **Type** | Specify which type of the pool is. Network: the pool defines a pool of IP addresses to service more than one DHCP client. Host: the pool services for a specific DHCP client identified by client identifier or hardware address. |
| **IP** | Specify network number of the DHCP address pool. |
| **Subnet Mask** | Specify subnet mask of the DHCP address pool. |

| | |
|---|---|
| **Lease Time** | Specify lease time that allows the client to request a lease time for the IP address.(If all are 0's, then it means the lease time is infinite.) |
| **Domain Name** | Specify domain name that client should use when resolving hostname via DNS. |
| **Broadcast Address** | Specify the broadcast address in use on the client's subnet. |
| **Default Router** | Specify a list of IP addresses for routers on the client's subnet. |
| **DNS Server** | Specify a list of Domain Name System name servers available to the client. |
| **NTP Server** | Specify a list of IP addresses indicating NTP servers available to the client. |
| **NetBIOS Node Type** | Specify NetBIOS node type option to allow Netbios over TCP/IP clients which are configurable to be configured as described in RFC 1001/1002. |
| **NetBIOS Scope** | Specify the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002. |
| **NetBIOS Name Server** | Specify a list of NBNS name servers listed in order of preference. |
| **NIS Domain Name** | Specify the name of the client's NIS domain. |
| **NIS Server** | Specify a list of IP addresses indicating NIS servers available to the client. |
| **Client Identifier** | Specify client's unique identifier to be used when the pool is the type of host. |
| **Hardware Address** | Specify client's hardware(MAC) address to be used when the pool is the type of host. |
| **Client Name** | Specify the name of client to be used when the pool is the type of host. |
| **Vendor/Class Identifier** | Specify to be used by DHCP client to optionally identify the vendor type and configuration of a DHCP client.<br>DHCP server will deliver the corresponding specific information to the client that sends vendor class identifier. |
| **Vendor/Specific Information** | Specify vendor specific information according to vendor class identifier. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>DHCP>Server>Pool

✓ **DHCP Server Pool Configuration**

➢ *Add New Pool*

SOLTECH
INFONET INC.

- ***Name***

**DHCP Server Pool Configuration**

**Pool Setting**

| Delete | Name | Type | IP | Subnet Mask | Lease Time |
|--------|------|------|----|-----|-----------|
| ☐ | DHCP_TEST | - | - | - | 1 days 0 hours 0 minutes |

Add New Pool

✓ **DHCP Pool Configuration**

➢ ***Type***

- ***Network***

**DHCP Pool Configuration**

**Pool**

Name  DHCP_TEST ▾

**Setting**

| Pool Name | DHCP_TEST |
|-----------|-----------|
| Type | Network ▾ |
| IP | 192.168.10.101 |
| Subnet Mask | 255.255.255.0 |
| Lease Time | 1 days (0-365) / 0 hours (0-23) / 0 minutes (0-59) |
| Domain Name | |
| Broadcast Address | |
| Default Router | 0.0.0.0 / 0.0.0.0 / 0.0.0.0 / 0.0.0.0 |
| DNS Server | 0.0.0.0 / 0.0.0.0 / 0.0.0.0 / 0.0.0.0 |
| NTP Server | 0.0.0.0 / 0.0.0.0 / 0.0.0.0 / 0.0.0.0 |
| NetBIOS Node Type | None ▾ |
| NetBIOS Scope | |
| NetBIOS Name Server | 0.0.0.0 / 0.0.0.0 / 0.0.0.0 / 0.0.0.0 |
| NIS Domain Name | 192.168.10.101 |
| NIS Server | 0.0.0.0 / 0.0.0.0 / 0.0.0.0 / 0.0.0.0 |
| Client Identifier | None ▾ |
| Hardware Address | |
| Client Name | |
| Vendor 1 Class Identifier | |
| Vendor 1 Specific Information | |
| Vendor 2 Class Identifier | |
| Vendor 2 Specific Information | |
| Vendor 3 Class Identifier | |
| Vendor 3 Specific Information | |
| Vendor 4 Class Identifier | |
| Vendor 4 Specific Information | |

SOLTECH
INFONET INC.

✓ **DHCP Server Pool Configuration**

➢ *Type*

• *Network*

**DHCP Server Pool Configuration**

**Pool Setting**

| Delete | Name | Type | IP | Subnet Mask | Lease Time |
|--------|------|------|-----|-------------|------------|
| ☐ | DHCP_TEST | Network | 192.168.10.101 | 255.255.255.0 | 1 days 0 hours 0 minutes |

Add New Pool

---

## EXAMPLE CLI CONFIGURATION

---

✓ **DHCP Server Pool Configuration**

➢ *Add New Pool*

• *Name*

```
(config)# ip dhcp pool <word32>
(config)# ip dhcp pool DHCP_TEST
```

✓ **DHCP Pool Configuration**

➢ *Type*

• *Network*

```
(config)# ip dhcp pool <word32>
(config)# ip dhcp pool DHCP_TEST

(config-dhcp-pool)# network <ipv4_ucast> <ipv4_netmask>
(config-dhcp-pool)# network 192.168.10.101 255.255.255.0
```

```
(config)# ip dhcp pool <word32>
(config)# ip dhcp pool DHCP_TEST

(config-dhcp-pool)# nis-domain-name <word128>
(config-dhcp-pool)# nis-domain-name 192.168.10.101
```

SOLTECH
INFONET INC.

## 6.4.1.4. Snooping

WEB MENU Configuration>DHCP>Snooping

Configure DHCP Snooping on this page.

**DHCP Snooping Configuration**

| Snooping Mode | Disabled ▾ |

**Port Mode Configuration**

| Port | Mode |
|------|------|
| * | <> ▾ |
| 1 | Trusted ▾ |
| 2 | Trusted ▾ |
| 3 | Trusted ▾ |
| 4 | Trusted ▾ |
| 5 | Trusted ▾ |
| 6 | Trusted ▾ |
| 7 | Trusted ▾ |
| 8 | Trusted ▾ |

### DHCP Snooping Configuration

| Object | Description |
|--------|-------------|
| **Snooping Mode** | Indicates the DHCP snooping mode operation.<br>Enabled: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.<br>Disabled: Disable DHCP snooping mode operation. |

### Port Mode Configuration

| Object | Description |
|--------|-------------|
| **Port** | The logical port. |
| **Mode** | Indicates the DHCP snooping port mode.<br>Trusted: Configures the port as trusted source of the DHCP messages.<br>Untrusted: Configures the port as untrusted source of the DHCP messages. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

## EXAMPLE WEB CONFIGURATION

✓   **DHCP Snooping Configuration**

➢   *Snooping Mode*

SOLTECH
INFONET INC.

- *Disable (Default)*

**DHCP Snooping Configuration**

| Snooping Mode | Disabled ⌄ |
|---|---|

**Port Mode Configuration**

| Port | Mode |
|---|---|
| * | <> ⌄ |
| 1 | Trusted ⌄ |
| 2 | Trusted ⌄ |
| 3 | Trusted ⌄ |
| 4 | Trusted ⌄ |
| 5 | Trusted ⌄ |
| 6 | Trusted ⌄ |
| 7 | Trusted ⌄ |
| 8 | Trusted ⌄ |

- *Enable*

**DHCP Snooping Configuration**

| Snooping Mode | Enabled ⌄ |
|---|---|

**Port Mode Configuration**

| Port | Mode |
|---|---|
| * | <> ⌄ |
| 1 | Trusted ⌄ |
| 2 | Trusted ⌄ |
| 3 | Trusted ⌄ |
| 4 | Trusted ⌄ |
| 5 | Trusted ⌄ |
| 6 | Trusted ⌄ |
| 7 | Trusted ⌄ |
| 8 | Trusted ⌄ |

✓ **Port Mode Configuration**

➢ *Mode*

- *Trusted (Default)*

**DHCP Snooping Configuration**

| Snooping Mode | Enabled ⌄ |
|---|---|

**Port Mode Configuration**

| Port | Mode |
|---|---|
| * | <> ⌄ |
| 1 | Trusted ⌄ |
| 2 | Trusted ⌄ |
| 3 | Trusted ⌄ |
| 4 | Trusted ⌄ |
| 5 | Trusted ⌄ |
| 6 | Trusted ⌄ |
| 7 | Trusted ⌄ |
| 8 | Trusted ⌄ |

**SOLTECH**
INFONET INC.

- ***Untrusted***

**DHCP Snooping Configuration**

| Snooping Mode | Enabled ▼ |
|---|---|

**Port Mode Configuration**

| Port | Mode |
|---|---|
| * | <> ▼ |
| 1 | Trusted ▼ |
| 2 | Untrusted ▼ |
| 3 | Trusted ▼ |
| 4 | Trusted ▼ |
| 5 | Trusted ▼ |
| 6 | Trusted ▼ |
| 7 | Trusted ▼ |
| 8 | Trusted ▼ |

## EXAMPLE CLI CONFIGURATION

✓ **DHCP Snooping Configuration**

➢ ***Snooping Mode***

- ***Disable (Default)***

```
(config)# no ip dhcp snooping
```

- ***Enable***

```
(config)# ip dhcp snooping
```

✓ **Port Mode Configuration**

➢ ***Mode***

- ***Trusted (Default)***

```
(config)# interface 10GigabitEthernet/GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/2

(config-if)# ip dhcp snooping trust
```

- ***Untrusted***

```
(config)# interface 10GigabitEthernet/GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/2

(config-if)# no ip dhcp snooping trust
```

SOLTECH
INFONET INC.

# 6.4.2. DHCP Monitor

## 6.4.2.1. Server Statistics

WEB MENU Monitor>DHCP>Server>Statistics

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

**DHCP Server Statistics**

**Database Counters**

| Pool | Excluded IP Address | Declined IP Address |
|------|---------------------|---------------------|
| 0    | 0                   | 0                   |

**Binding Counters**

| Automatic Binding | Manual Binding | Expired Binding |
|-------------------|----------------|-----------------|
| 0                 | 0              | 0               |

**DHCP Message Received Counters**

| DISCOVER | REQUEST | DECLINE | RELEASE | INFORM |
|----------|---------|---------|---------|--------|
| 0        | 0       | 0       | 0       | 0      |

**DHCP Message Sent Counters**

| OFFER | ACK | NAK |
|-------|-----|-----|
| 0     | 0   | 0   |

### DHCP Server Statistics

### Database Counters

| Object | Description |
|--------|-------------|
| **Pool** | Number of pools. |
| **Excluded IP Address** | Number of excluded IP address ranges. |
| **Declined IP Address** | Number of declined IP addresses. |

### Binding Counters

| Object | Description |
|--------|-------------|
| **Automatic Binding** | Number of bindings with network-type pools. |
| **Manual Binding** | Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type. |
| **Expired Binding** | Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings. |

### DHCP Message Received Counters

| Object | Description |
|--------|-------------|
| **DISCOVER** | Number of DHCP DISCOVER messages received. |
| **REQUEST** | Number of DHCP REQUEST messages received. |
| **DECLINE** | Number of DHCP DECLINE messages received. |
| **RELEASE** | Number of DHCP RELEASE messages received. |
| **INFORM** | Number of DHCP INFORM messages received. |

**DHCP Message Received Counters**

| Object | Description |
|--------|-------------|
| **OFFER** | Number of DHCP OFFER messages sent. |
| **ACK** | Number of DHCP ACK messages sent. |
| **NAK** | Number of DHCP NAK messages sent. |

**Buttons**

Auto-refresh ☐ : Check this box to refresh the page automatically.

Refresh : Click to refresh the page immediately.

Clear : Click to Clears DHCP Message Received Counters and DHCP Message Sent Counters.

# EXAMPLE WEB MONITOR

WEB MENU Monitor>DHCP>Server>Statistics

**DHCP Server Statistics**

**Database Counters**

| Pool | Excluded IP Address | Declined IP Address |
|------|---------------------|---------------------|
| 1 | 2 | 0 |

**Binding Counters**

| Automatic Binding | Manual Binding | Expired Binding |
|-------------------|----------------|-----------------|
| 1 | 0 | 0 |

**DHCP Message Received Counters**

| DISCOVER | REQUEST | DECLINE | RELEASE | INFORM |
|----------|---------|---------|---------|--------|
| 13 | 1 | 0 | 0 | 0 |

**DHCP Message Sent Counters**

| OFFER | ACK | NAK |
|-------|-----|-----|
| 1 | 1 | 0 |

# EXAMPLE CLI MONITOR

✓ **DHCP Server Statistics**

```
# show ip dhcp server statistics

Database Counters
=========================
 POOL             1
 Excluded IP       2
 Declined IP       0
=========================
Binding Counters
=========================
```

```
  Automatic          1
  Manual             0
  Expired            0
=========================
Message Received Counters
=========================
  DISCOVER          13
  REQUEST            1
  DECLINE            0
  RELEASE            0
  INFORM             0
=========================
Message Sent Counters
=========================
  OFFER              1
  ACK                1
  NAK                0
=========================
```

## 6.4.2.2. Server Binding

WEB MENU Monitor>DHCP>Server>Binding

This page displays bindings generated for DHCP clients.

**DHCP Server Binding IP**

**Binding IP Address**

| Delete | IP | Type | State | Pool Name | Server ID |
|--------|----|----|------|-----------|-----------|

**DHCP Server Binding IP**

**Binding IP Address**

| Object | Description |
|--------|-------------|
| **IP** | IP address allocated to DHCP client.<br>Click IP navigate to the detailed page. |
| **Type** | Type of binding. Possible types are Automatic, Manual, Expired. |
| **State** | State of binding. Possible states are Committed, Allocated, Expired |
| **Pool Name** | The pool that generates the binding. |
| **Server ID** | Server IP address to service the binding. |

**Buttons**

Auto-refresh ☐ : Check this box to refresh the page automatically.

Refresh : Click to refresh the page immediately.

Clear Selected : Click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to be Expired. If the selected binding is Expired, then it is freed.

Clear Automatic : Click to clear all Automatic bindings and Change them to Expired bindings.

Clear Manual : Click to clear all Manual bindings and Change them to Expired bindings.

Clear Expired : Click to clear all Expired bindings and free them.

SOLTECH
INFONET INC.

## DHCP Server Binding IP Data

WEB MENU Monitor>DHCP>Server>Binding

This page displays the detailed data of a binding.

**DHCP Server Binding IP Data**

**Binding**

| IP | 192.168.10.102 ∨ |

**Binding IP Data**

| IP | 192.168.10.102 |
|---|---|
| Type | Automatic |
| State | Committed |
| Pool Name | DHCP_TEST |
| Server ID | 192.168.10.101 |
| VLAN | 1 |
| Subnet Mask | 255.255.255.0 |
| Client ID Type | FQDN |
| Client ID Value | sfc8000 |
| MAC Address | 00-12-6d-12-00-05 |
| Lease Time | 1 days 0 hours 0 minutes 0 seconds |
| Will Expired in | 23 hours 20 minutes 45 seconds |

### DHCP Server Binding IP Data

#### Binding

| Object | Description |
|---|---|
| **IP** | IP address of the selected binding. |

#### Binding IP Data

| Object | Description |
|---|---|
| **IP** | IP address allocated to DHCP client. |
| **Type** | Type of binding. Possible types are Automatic, Manual, Expired. |
| **State** | State of binding. Possible states are Committed, Allocated, Expired. |
| **Pool Name** | The pool that generates the binding. |
| **Server ID** | Server IP address to service the binding. |
| **VLAN ID** | VLAN ID of the interface where the DHCP client is from. |
| **Subnet Mask** | Netmask of the interface where the DHCP client is from. |
| **Client ID Type** | Type of client identifier from DHCP client. Possible types are FQDN, MAC and -. |
| **Client ID Value** | Value of client identifier from DHCP client. |
| **MAC Address** | Hardware address from DHCP client. |
| **Lease Time** | The lease time of the binding. |
| **Will Expired in** | How much remaining time the binding will be expired. |

SOLTECH
INFONET INC.

## EXAMPLE WEB MONITOR

WEB MENU Monitor>DHCP>Server>Binding

**DHCP Server Binding IP**

**Binding IP Address**

| Delete | IP | Type | State | Pool Name | Server ID |
|--------|-----|------|-------|-----------|-----------|
| ☐ | 192.168.10.102 | Automatic | Committed | DHCP_TEST | 192.168.10.101 |

WEB MENU Monitor>DHCP>Server>Binding>Click IP

**DHCP Server Binding IP Data**

**Binding**

IP  192.168.10.102 ▼

**Binding IP Data**

| IP | 192.168.10.102 |
|----|-----------------|
| Type | Automatic |
| State | Committed |
| Pool Name | DHCP_TEST |
| Server ID | 192.168.10.101 |
| VLAN | 1 |
| Subnet Mask | 255.255.255.0 |
| Client ID Type | FQDN |
| Client ID Value | sfc8000 |
| MAC Address | 00-12-6d-12-00-05 |
| Lease Time | 1 days 0 hours 0 minutes 0 seconds |
| Will Expired in | 23 hours 2 minutes 53 seconds |

## EXAMPLE CLI MONITOR

✓ **DHCP Server Binding IP**

```
# show ip dhcp server binding

IP: 192.168.10.102
----------------------------------------------
  State is committed
  Binding type is automatic
  Pool name is DHCP_TEST
  Server ID is 192.168.10.101
  VLAN ID is 1
  Subnet mask is 255.255.255.0
  Client identifer is type of FQDN that is sfc8000
  Hardware address is 00:12:6d:12:00:05
  Lease time is 1 days 0 hours 0 minutes 0 seconds
  Expiration is in 23 hours 33 minutes 17 seconds
```

SOLTECH
INFONET INC.

## 6.4.2.3. Server Declined IP

WEB MENU Monitor>DHCP>Server>Declined IP

This page displays declined IP addresses.

**DHCP Server Declined IP**

**Declined IP Address**

**Declined IP**

### DHCP Server Declined IP

### Declined IP Address

| Object | Description |
|---|---|
| **Declined IP** | List of IP addresses declined. |

**Buttons**

Auto-refresh ☐ : Check this box to refresh the page automatically.

Refresh : Click to refresh the page immediately.

## EXAMPLE WEB MONITOR

WEB MENU Monitor>DHCP>Server>Declined IP

**DHCP Server Declined IP**

**Declined IP Address**

| Declined IP |
|---|
| 192.168.10.102 |

## EXAMPLE CLI MONITOR

✓ **DHCP Server Binding IP**

```
# show ip dhcp server declined-ip

Declined IP Address
    ------------------
0001  192.168.10.102
```

# 6.4.2.4. Snooping Table

WEB MENU Monitor>DHCP>Snooping Table

This page display the dynamic IP assigned information after DHCP Snooping mode is disabled.

All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except

for local VLAN interface IP addresses.

**Dynamic DHCP Snooping Table**

Start from MAC address 00-00-00-00-00-00 , VLAN 0 with 20 entries per page.

| MAC Address | VLAN ID | Source Port | IP Address | IP Subnet Mask | DHCP Server |
|---|---|---|---|---|---|
| No more entries | | | | | |

## Dynamic DHCP Snooping Table

| Object | Description |
|---|---|
| **MAC Address** | User MAC address of the entry. |
| **VLAN ID** | VLAN-ID in which the DHCP traffic is permitted. |
| **Source Port** | Switch Port Number for which the entries are displayed. |
| **IP Address** | User IP address of the entry. |
| **IP Subnet Mask** | User IP subnet mask of the entry. |
| **DHCP Server** | DHCP Server address of the entry. |

**Buttons**

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

Refresh : Refreshes the displayed table starting from the input fields.

Clear : Flushes all dynamic entries.

|<< : Updates the table starting from the first entry in the Dynamic DHCP snooping Table.

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

## EXAMPLE WEB MONITOR

WEB MENU Monitor>DHCP>Snooping Table

**Dynamic DHCP Snooping Table**

Start from MAC address `00-00-00-00-00-00` , VLAN `0` with `20` entries per page.

| MAC Address | VLAN ID | Source Port | IP Address | IP Subnet Mask | DHCP Server |
|---|---|---|---|---|---|
| 00-21-6d-05-f0-5c | 1 | 1 | 192.168.10.102 | 255.255.255.0 | 192.168.10.101 (Local) |

## EXAMPLE CLI MONITOR

✓  **Dynamic DHCP Snooping Table**

```
# show ip dhcp snooping table

Entry ID          : 1
MAC Address       : 00-21-6d-05-f0-5c
VLAN ID           : 1
Source Port       : GigabitEthernet 1/1
IP Address        : 192.168.10.102
IP Subnet Mask    : 255.255.255.0
DHCP Server Address: 192.168.10.101 (Local)
Total Entries Number : 1
```

## 6.4.2.5. Detailed Statistics

WEB MENU Monitor>DHCP>Detailed Statistics

This page provides statistics for DHCP snooping.

**DHCP Detailed Statistics  Port 1**

| Receive Packets | | Transmit Packets | |
|---|---|---|---|
| Rx Discover | 0 | Tx Discover | 0 |
| Rx Offer | 0 | Tx Offer | 0 |
| Rx Request | 0 | Tx Request | 0 |
| Rx Decline | 0 | Tx Decline | 0 |
| Rx ACK | 0 | Tx ACK | 0 |
| Rx NAK | 0 | Tx NAK | 0 |
| Rx Release | 0 | Tx Release | 0 |
| Rx Inform | 0 | Tx Inform | 0 |
| Rx Lease Query | 0 | Tx Lease Query | 0 |
| Rx Lease Unassigned | 0 | Tx Lease Unassigned | 0 |
| Rx Lease Unknown | 0 | Tx Lease Unknown | 0 |
| Rx Lease Active | 0 | Tx Lease Active | 0 |
| Rx Discarded Checksum Error | 0 | | |
| Rx Discarded from Untrusted | 0 | | |

### Dynamic Detailed Statistics Port n

| Object | Description |
|---|---|
| Rx and Tx Discover | The number of discover packets received and transmitted. |
| Rx and Tx Offer | The number of offer packets received and transmitted. |
| Rx and Tx Request | The number of request packets received and transmitted. |
| Rx and Tx Decline | The number of decline packets received and transmitted. |
| Rx and Tx ACK | The number of ACK packets received and transmitted. |
| Rx and Tx NAK | The number of NAK packets received and transmitted. |
| Rx and Tx Release | The number of release packets received and transmitted. |
| Rx and Tx Inform | The number of inform packets received and transmitted. |
| Rx and Tx Lease Query | The number of lease query packets received and transmitted. |
| Rx and Tx Lease Unassigned | The number of lease unassigned packets received and transmitted. |
| Rx and Tx Lease Unknown | The number of lease unknown packets received and transmitted. |
| Rx and Tx Lease Active | The number of lease active packets received and transmitted. |
| Rx Discarded checksum error | The number of discard packet that IP/UDP checksum is error. |
| Rx Discarded from Untrusted | The number of discarded packet that are coming from untrusted port. |

**Buttons**

Combined ▾ : The DHCP user select box determines which user is affected by clicking the buttons.

Port 1 ▾ : The port select box determines which port is affected by clicking the buttons.

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

Refresh : Click to refresh the page immediately.

Clear : Clears the counters for the selected port.

# EXAMPLE WEB MONITOR

WEB MENU Monitor>DHCP>Detailed Statistics

✓ **DHCP Detailed Statistics Port 1(Client/port1)**

**DHCP Detailed Statistics  Port 1**

| Receive Packets | | Transmit Packets | |
|---|---|---|---|
| Rx Discover | 35 | Tx Discover | 29 |
| Rx Offer | 0 | Tx Offer | 1 |
| Rx Request | 28 | Tx Request | 1 |
| Rx Decline | 0 | Tx Decline | 0 |
| Rx ACK | 1 | Tx ACK | 28 |
| Rx NAK | 0 | Tx NAK | 0 |
| Rx Release | 0 | Tx Release | 0 |
| Rx Inform | 0 | Tx Inform | 0 |
| Rx Lease Query | 0 | Tx Lease Query | 0 |
| Rx Lease Unassigned | 0 | Tx Lease Unassigned | 0 |
| Rx Lease Unknown | 0 | Tx Lease Unknown | 0 |
| Rx Lease Active | 0 | Tx Lease Active | 0 |
| Rx Discarded Checksum Error | 0 | | |
| Rx Discarded from Untrusted | 0 | | |

# EXAMPLE CLI MONITOR

✓ **DHCP Detailed Statistics Port 1(Client/port1)**

```
# show ip dhcp detailed statistics client/combined/normal-forward/relay/server/snooping
interface 10GigabitEthernet/GigabitEthernet <port_type_list>
# show ip dhcp detailed statistics client interface GigabitEthernet 1/1

GigabitEthernet 1/1 Statistics:
-------------------------------
Rx Discover:              0   Tx Discover:            29
Rx Offer:                 0   Tx Offer:               0
Rx Request:               0   Tx Request:             1
Rx Decline:               0   Tx Decline:             0
Rx ACK:                   1   Tx ACK:                 0
Rx NAK:                   0   Tx NAK:                 0
Rx Release:               0   Tx Release:             0
Rx Inform:                0   Tx Inform:              0
Rx Lease Query:           0   Tx Lease Query:         0
Rx Lease Unassigned:      0   Tx Lease Unassigned:    0
Rx Lease Unknown:         0   Tx Lease Unknown:       0
Rx Lease Active:          0   Tx Lease Active:        0
Rx Discarded checksum error:     0
```

## 6.5. Security

## 6.5.1. Switch Configuration

The product provides authentication capabilities for both local administrators and users, granting permissions based on account-specific privilege levels.

User Accounts and Permissions:
Multiple users can be created on the switch, identified by their usernames and corresponding privilege levels.

The permission levels for user access range from 1 to 15. A privilege level of 15 allows access to all groups and grants full control over the device. User privileges must be equal to or higher than the privilege level of the group. By default, privilege level 5 provides read-only access, while privilege level 10 grants read-write access to most groups. System maintenance tasks such as software uploads and factory default restoration require privilege level 15. Typically, administrator accounts have privilege level 15, regular user accounts have privilege level 10, and guest accounts have privilege level 5.

The names identifying the permission groups are referred to as group names. In most cases, permission level groups consist of a single module (e.g., LACP, RSTP, or QoS), but some may include more than one.

Each group has authentication privilege levels ranging from 1 to 15 for the following subgroups:

• Configuration read-only
• Configuration/Execution read-write
• Status/Statistics read-only
• Status/Statistics read-write (e.g., clear statistics)

Group privilege levels are used only in the web interface. CLI privilege levels function within each individual command. User privileges must be greater than or equal to the privilege level of the group.

## 6.5.1.1. Users

WEB MENU Configuration>Security>Switch>Users

This page provides an overview of the current users.
Currently the way to login as another user on the web server is to close and reopen the browser or use the "Logout" option in the top right corner.

**Users Configuration**

| User Name | Privilege Level |
|-----------|-----------------|
| admin     | 15              |

Add New User

## Users Configuration

| Object | Description |
|---|---|
| User Name | The name identifying the user. This is also a link to Add/Edit User. |
| Privilege Level | The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account. |

**Buttons**

Add New User : Click to add a new user.

When put the  Add New User  buttons, User setting page will be appeared.

## Add User

This page configures a user.

**Add User**

| User Settings | |
|---|---|
| User Name | |
| Password | |
| Password (again) | |
| Privilege Level | 0 |

## Add User

| Object | Description |
|---|---|
| User Name | A string identifying the user name that this entry should belong to. The allowed string length is 1 to 31. The valid user name allows letters, numbers and underscores. |
| Password | The password of the user. The allowed string length is 0 to 63. Any printable characters including space is accepted. In the case of products with security Switch, please refer to the "Information > Secure Information" section under the WEB menu for configuration. |
| Privilege Level | The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user |

SOLTECH
INFONET INC.

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

**Buttons**

`Apply` : Click to apply changes.

`Apply&Save` : Click to apply and save changes.

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

`Cancel` : Click to undo any changes made locally and return to the Users.

`Delete User` : Click to delete this user.

`Delete User Save` : Click to delete this user and save.

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>Security>Switch>Users

✓ **Users Configuration**

➢ *Add New User*

• *Add User (Click Add New User)*

**Add User**

| User Settings | |
|---|---|
| User Name | test |
| Password | •••••••••• |
| Password (again) | •••••••••• |
| Privilege Level | 10 |

**Users Configuration**

| User Name | Privilege Level |
|---|---|
| test | 10 |
| admin | 15 |

• *Edit User (Click User Name)*

**Edit User**

| User Settings | |
|---|---|
| User Name | test |
| Password | •••••••••••• |
| Password (again) | •••••••••• |
| Privilege Level | 9 |

**Users Configuration**

| User Name | Privilege Level |
|---|---|
| test | 9 |
| admin | 15 |

SOLTECH
INFONET INC.

## EXAMPLE CLI CONFIGURATION

✓ **Users Configuration**

    ➢    *Add New User*

        •    *Add User / Edit User*

```
(config)# username <word31> privilege <0-15> password unencrypted
(config)# username test privilege 10 password unencrypted

#: Please input a new password (plain): <line31>

#: Please input the new password AGAIN: <line31>
```

## 6.5.1.2. Privilege Levels

WEB MENU Configuration>Security>Switch>Privilege Level

This page provides an overview of the privilege levels.

**Privilege Level Configuration**

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

### Privilege Level Configuration

| Object | Description |
| --- | --- |
| Group Name | The name identifying the privilege group. In most cases, a privilege level group consists of a single module, but a few of them contains more than one. The following description defines these privilege level groups in details: |
| | **System** — Contact, Name, Location, Timezone, Daylight Saving Time, Log. |
| | **Security** — Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard. |
| | **IP** — Everything except 'ping'. |
| | **Port** — Everything except 'VeriPHY'. |
| | **Diagnostics** — 'ping' and 'VeriPHY'. |
| | **Maintenance** — CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. |

|  |  | Web- Users, Privilege Levels and everything in Maintenance. |
|  | Debug | Only present in CLI. |
| **Privilege Level** |  | Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>Security>Switch>Privilege Level

✓ **Privilege Level Configuration**



---

## EXAMPLE CLI CONFIGURATION

---

✓ **Privilege Level Configuration**

```
(config)# web privilege group {1} level {2} <0-15>
(config)# web privilege group DDMI level configRoPriv 6

{1}
Aggregation      DDMI            DHCP            DHCPv6_Client

Debug            Diagnostics     EPS             ERPS

ETH_LINK_OAM     Green_Ethernet    IP              IPMC_Snooping

LACP             LLDP            Loop_Protect      MAC_Table

MEP              MVR             Maintenance       NTP

POE              Ports           Private_VLANs     QoS

RMirror          Security          Spanning_Tree     System

VCL              VLAN_Translation   VLANs           Voice_VLAN

XXRP             sFlow

{2}
configRoPriv  configRwPriv  statusRoPriv  statusRwPriv
```

## 6.5.1.3. Auth Method

WEB MENU Configuration>Security>Switch>Auth Method

**Authentication Method Configuration**

| Client | Methods | | |
|---|---|---|---|
| console | local | no | no |
| telnet | local | no | no |
| ssh | local | no | no |
| http | local | no | no |

**Command Authorization Method Configuration**

| Client | Method | Cmd Lvl | Cfg Cmd |
|---|---|---|---|
| console | no | 0 | ☐ |
| telnet | no | 0 | ☐ |
| ssh | no | 0 | ☐ |

**Accounting Method Configuration**

| Client | Method | Cmd Lvl | Exec |
|---|---|---|---|
| console | no | | ☐ |
| telnet | no | | ☐ |
| ssh | no | | ☐ |

### Authentication Method Configuration

| Object | Description |
|---|---|
| **Authentication Method Configuration** | You can configure how a user is authenticated when they log into the switch via one of the management client interfaces. |
| **Client** | The management client for which the configuration below applies. |
| **Methods** | Method can be set to one of the following values:<br><br>**no** — Authentication is disabled and login is not possible.<br>**local** — Use the local user database on the switch for authentication.<br>**radius** — Use remote RADIUS server(s) for authentication.<br>**tacacs** — Use remote TACACS+ server(s) for authentication.<br>Methods that involves remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. (If a local configuration is available, you can still configure it directly even if the servers are not operational.) |

### Command Authorization Method Configuration

| Object | Description |
|---|---|
| **Command Authorization Method Configuration** | The command authorization section allows you to limit the CLI commands available to a user. |
| **Client** | The management client for which the configuration below applies. |
| **Method** | Method can be set to one of the following values:<br><br>**no** — Command authorization is disabled. User is granted access to CLI commands according to his privilege level.<br>**tacacs** — Use remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is |

| | |
|---|---|
| | granted access to CLI commands according to his privilege level. |
| **Cmd Lvl** | Authorize all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15. |
| **Cfg Cmd** | Also authorize configuration commands. |

## Accounting Method Configuration

| Object | Description |
|---|---|
| **Accounting Method Configuration** | The accounting section allows you to configure command and exec (login) accounting. |
| **Client** | The management client for which the configuration below applies. |
| **Method** | Method can be set to one of the following values:<br>**no**       Accounting is disabled.<br>**tacacs**    Use remote TACACS+ server(s) for accounting. |
| **Cmd Lvl** | Enable accounting of all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15.<br>Leave the field empty to disable command accounting. |
| **Exec** | Enable exec (login) accounting. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>Security>Switch>Auth Method

✓ **Authentication Method Configuration**

**Authentication Method Configuration**

| Client | Methods | | |
|---|---|---|---|
| console | tacacs | radius | local |
| telnet | no | no | no |
| ssh | tacacs | local | no |
| http | radius | tacacs | local |

✓ **Command Authorization Method Configuration**

**Command Authorization Method Configuration**

| Client | Method | Cmd Lvl | Cfg Cmd |
|---|---|---|---|
| console | tacacs | 15 | ☑ |
| telnet | tacacs | 10 | ☐ |
| ssh | no | 0 | ☐ |

SOLTECH
INFONET INC.

✓ **Accounting Method Configuration**

**Accounting Method Configuration**

| Client | Method | Cmd Lvl | Exec |
|--------|--------|---------|------|
| console | tacacs ˅ | 15 | ☑ |
| telnet | tacacs ˅ | 10 | ☐ |
| ssh | no ˅ | | ☐ |

# EXAMPLE CLI CONFIGURATION

✓ **Authentication Method Configuration**

```
(config)# aaa authentication login {1} {2}
(config)# aaa authentication login console tacacs radius local
(config)# aaa authentication login ssh tacacs local
(config)# aaa authentication login http radius tacacs local

(config)# no aaa authentication login {1}
(config)# no aaa authentication login telnet

{1}
Console  http  ssh  telnet

{2}
local  radius  tacacs
```

✓ **Command Authorization Method Configuration**

```
(config)# aaa authorization {1} tacacs commands <0-15> {2}
(config)# aaa authorization console tacacs commands 15 config-commands
(config)# aaa authorization telnet tacacs commands 10

(config)# no aaa authorization {1}
(config)# no aaa authorization ssh

{1}
console   ssh   telnet

{2}
config-commands   <cr>
```

✓ **Accounting Method Configuration**

```
(config)# aaa accounting {1} tacacs {2}
(config)# aaa accounting console tacacs commands 15 exec
(config)# aaa accounting telnet tacacs commands 10

(config)# no aaa accounting {1}
(config)# no aaa accounting ssh

{1}
console   ssh   telnet

{2}
commands <0-15>   exec
```

SOLTECH
INFONET INC.

## 6.5.1.4. Telnet

WEB MENU Configuration>Security>Switch>Telnet
Configure Telnet on this page.

**Telnet Configuration**

| Mode | Disabled ▼ |
|---|---|
| Port(TCP) | 23 |
| Max Connection | 1 |
| Fail Blocking Time(s) | 300 |

### Telnet Configuration

| Object | Description |
|---|---|
| **Mode** | Indicates the Telnet mode operation.<br>Enabled: Enable Telnet mode operation.<br>Disabled: Disable Telnet mode operation.(Default) |
| **Port(TCP)** | Enter the TCP port for Telnet access. |
| **Max Connection** | Number of clients accessible to the switch. |
| **Fail Blocking Time(s)** | Block time when logging in fails multiple times Valid values are restricted to 10 - 3600(S) seconds. |

**Buttons**

`Apply` : Click to apply changes.

`Apply&Save` : Click to apply and save changes.

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

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>Security>Switch>Telnet

✓ **Telnet Configuration**

➢ *Mode*

• *Enable | Disable*

**Telnet Configuration**

| Mode | Disabled ▼ |
|---|---|
| Port(TCP) | Disabled |
| | Enabled |
| Max Connection | |
| Fail Blocking Time(s) | 300 |

➢ *Port(TCP)*

• *Default 23*

| Mode | Enabled ▼ |
|---|---|
| Port(TCP) | 23 |
| Max Connection | 1 |
| Fail Blocking Time(s) | 300 |

➢ *Max Connection*

• *1 | 2 | 3 | 4*

| Mode | Enabled ▾ |
|---|---|
| Port(TCP) | 23 |
| Max Connection | 1 ▾ |
| Fail Blocking Time(s) | 1 |
| | 2 |
| | 3 |
| | 4 |

➢ **Fail Blocking Time(s)**

- **10~3600sec**

| Mode | Enabled ▾ |
|---|---|
| Port(TCP) | 23 |
| Max Connection | 1 ▾ |
| Fail Blocking Time(s) | 300 |

## EXAMPLE CLI CONFIGURATION

✓ **Telnet Configuration**

➢ **Mode**

- **Enable | Disable**

```
(config)# ip telnet
(config)# no ip telnet
```

➢ **Port(TCP)**

- **Default 23**

```
(config)# ip telnet port { <port> | default }
(config)# ip telnet port 23
(config)# ip telnet port default
```

➢ **Max Connection**

- **1 | 2 | 3 | 4**

```
(config)# ip telnet max-connection <connection_cnt>
(config)# ip telnet max-connection 2
(config)# ip telnet max-connection 1
```

➢ **Fail Blocking Time(s)**

- **10~3600sec**

```
(config)# ip telnet retry-block-time <block_time>
(config)# ip telnet retry-block-time 300
(config)# ip telnet retry-block-time 10
```

## 6.5.1.5. SSH

WEB MENU Configuration>Security>Switch>SSH
Configure SSH on this page.

**SSH Configuration**

| Mode | Enabled ▾ |
|---|---|
| Port(TCP) | 22 |
| Max Connection | 1 |
| Fail Blocking Time(s) | 300 |

### SSH Configuration

| Object | Description |
|---|---|
| **Mode** | Indicates the SSH mode operation.<br>Enabled: Enable SSH mode operation.<br>Disabled: Disable SSH mode operation. |
| **Port(TCP)** | TCP port number for SSH Service |
| **Max Connection** | Number of clients accessible to the switch. |
| **Fail Blocking Time(s)** | Block time when logging in fails multiple times Valid values are restricted to 10 - 3600(S) seconds |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>Security>Switch>SSH

✓ **SSH Configuration**

  ➢ *Mode*

    • *Enable | Disable*

| Mode | Enabled ▾ |
|---|---|
| Port(TCP) | Disabled |
| Max Connection | Enabled |
| Fail Blocking Time(s) | 300 |

  ➢ *Port(TCP)*

    • *1~65534 | 22(default)*

| Mode | Enabled ▾ |
|---|---|
| Port(TCP) | 22 |
| Max Connection | 1 |
| Fail Blocking Time(s) | 300 |

  ➢ *Max Connection*

    • *1 | 2 | 3 | 4*

SOLTECH
INFONET INC.

| Mode | Enabled ∨ |
|------|-----------|
| Port(TCP) | 22 |
| Max Connection | 1 ∨ |
| Fail Blocking Time(s) | **1** |
| | 2 |
| | 3 |
| | 4 |

➢ **Fail Blocking Time(s)**

- **10~3600sec**

| Mode | Enabled ∨ |
|------|-----------|
| Port(TCP) | 22 |
| Max Connection | 1 ∨ |
| Fail Blocking Time(s) | 300 |

## EXAMPLE CLI CONFIGURATION

✓ **SSH Configuration**

➢ **Mode**

- **Enable | Disable**

```
(config)# ip ssh
(config)# no ip ssh
```

➢ **Port(TCP)**

- **1~65534 | 22(default)**

```
(config)# ip ssh port { <port> | default }
(config)# ip ssh port 22
(config)# ip ssh port default
```

➢ **Max Connection**

- **1 | 2 | 3 | 4**

```
(config)# ip ssh max-connection <connection_cnt>
(config)# ip ssh max-connection 1
(config)# ip ssh max-connection 2
```

➢ **Fail Blocking Time(s)**

- **10~3600sec**

```
(config)# ip ssh retry-block-time <block_time>
(config)# ip ssh retry-block-time 10
(config)# ip ssh retry-block-time 300
```

SOLTECH
INFONET INC.

## 6.5.1.6. HTTPS

WEB MENU Configuration>Security>Switch>HTTPS

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

**HTTPS Configuration**

| Mode | Enabled |
| Automatic Redirect | Enabled |
| Certificate Maintain | None |
| Max Connection | 3 |
| Fail Blocking Time(s) | 300 |
| Certificate Status | Switch secure HTTP certificate is presented |

### HTTPS Configuration

| Object | Description |
|---|---|
| **Mode** | Indicate the HTTPS mode operation.<br>Enabled: Enabled HTTPS mode operation.<br>Disabled: Disabled HTTPS mode operation.(Web access may not be available.) |
| **Automatic Redirect** | Indicate the HTTPS redirect mode operation.<br>When HTTPS mode is enabled and the redirection mode is enabled, HTTP connections will be automatically redirected to HTTPS connections.<br>Enabled: Enable HTTPS redirect mode operation.<br>Disabled: Disable HTTPS redirect mode operation. |
| **Certificate Maintain** | The operation of certificate maintenance.<br>(The security device can only use this feature in CLI.)<br>None: No operation.<br>Delete: Delete the current certificate.<br>Upload: Upload a certificate PEM file.<br>(Possible methods are: Web Browser or URL.)<br>Generate: Generate a new self-signed RSA certificate. |
| **Certificate Pass Phrase** | Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.<br>(Select "Upload" in the "Certificate Maintain" section, it will be available.) |
| **Certificate Upload** | Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem<br>Notice that the RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificate, e.g. Firefox v37 and Chrome v39.<br>Possible methods are:<br>Web Browser: Upload a certificate via Web browser.<br>URL: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is<br>&lt;protocol&gt;://[&lt;username&gt;[:&lt;password&gt;]@]&lt;host&gt;[:&lt;port&gt;][/&lt;path&gt;]/&lt;file_name&gt;. For example,<br>*tftp://10.10.10.10/new_image_path/new_image.dat,*<br>*http://username:password@10.10.10.10:80/new_image_path/new_image.dat.*<br>A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score(_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not |

| | allowed. |
|---|---|
| **Certificate Status** | Display the current status of certificate on the switch. Switch secure HTTP certificate is presented. Switch secure HTTP certificate is not presented. Switch secure HTTP certificate is generating. |
| **Max Connection** | Number of clients accessible to the switch. |
| **Fail Blocking Time(s)** | Block time when logging in fails multiple times Valid values are restricted to 10 - 3600(S) seconds. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

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

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>Security>Switch>HTTPS

✓ **HTTPS Configuration**

    ➢ *Mode*

        • *Enable(default) | Disable*

| Mode | Enabled |
|---|---|
| Automatic Redirect | Disabled |
| Certificate Maintain | Enabled |
| Max Connection | 3 |
| Fail Blocking Time(s) | 300 |
| Certificate Status | Switch secure HTTP certificate is presented |

    ➢ *Automatic Redirect*

        • *Enable(default) | Disable*

| Mode | Enabled |
|---|---|
| Automatic Redirect | Enabled |
| Certificate Maintain | Disabled |
| Max Connection | Enabled |
| Fail Blocking Time(s) | 300 |
| Certificate Status | Switch secure HTTP certificate is presented |

    ➢ *Certificate Maintain*

        • *None(default) | Delete | Upload | Generate*

| Mode | Enabled |
|---|---|
| Automatic Redirect | Enabled |
| Certificate Maintain | None |
| Max Connection | None |
| Fail Blocking Time(s) | Delete |
| Certificate Status | Upload |
| | Generate |

    ➢ *Certificate Pass Phrase*

| Mode | Enabled |
|---|---|
| Automatic Redirect | Enabled |
| Certificate Maintain | Upload |
| Certificate Pass Phrase | •••••••• |
| Max Connection | 3 |
| Fail Blocking Time(s) | 300 |
| Certificate Upload | Web Browser |
| File Upload | 파일 선택 선택된 파일 없음 |
| Certificate Status | Switch secure HTTP certificate is presented |

➢ **Max Connection**

• **1 | 2 | 3 | 4**

| Mode | Enabled |
|---|---|
| Automatic Redirect | Enabled |
| Certificate Maintain | None |
| Max Connection | 3 |
| Fail Blocking Time(s) | 1 |
| Certificate Status | 2 |
| | 3 |
| | 4 |

➢ **Fail Blocking Time(s)**

• **10~3600sec**

| Mode | Enabled |
|---|---|
| Automatic Redirect | Enabled |
| Certificate Maintain | None |
| Max Connection | 3 |
| Fail Blocking Time(s) | 300 |
| Certificate Status | Switch secure HTTP certificate is presented |

➢ **Certificate Upload**

• **Web Browser | URL**

| Mode | Enabled |
|---|---|
| Automatic Redirect | Enabled |
| Certificate Maintain | Upload |
| Certificate Pass Phrase | •••••••• |
| Max Connection | 3 |
| Fail Blocking Time(s) | 300 |
| Certificate Upload | Web Browser |
| File Upload | Web Browser |
| Certificate Status | URL |

➢ **File Upload | URL**

| Mode | Enabled |
|---|---|
| Automatic Redirect | Enabled |
| Certificate Maintain | Upload |
| Certificate Pass Phrase | •••••••• |
| Max Connection | 3 |
| Fail Blocking Time(s) | 300 |
| Certificate Upload | Web Browser |
| File Upload | 파일 선택 선택된 파일 없음 |
| Certificate Status | Switch secure HTTP certificate is presented |

| Mode | Enabled |
|---|---|
| Automatic Redirect | Enabled |
| Certificate Maintain | Upload |
| Certificate Pass Phrase | •••••••• |
| Max Connection | 3 |
| Fail Blocking Time(s) | 300 |
| Certificate Upload | URL |
| URL | tftp://192.168.10.xxx/new_image_path/new_image.dat |
| Certificate Status | Switch secure HTTP certificate is presented |

SOLTECH
INFONET INC.

## EXAMPLE CLI CONFIGURATION

✓ **HTTPS Configuration**

➢ *Mode*

• *Enable(default) | Disable*

```
(config)# ip http secure-server
(config)# no ip http secure-server
```

➢ *Automatic Redirect*

• *Enable(default) | Disable*

```
(config)# ip http secure-redirect
(config)# no ip http secure-redirect
```

➢ *Certificate Maintain*

• *None | Delete | Generate | Upload*

➢ *Certificate Pass Phrase*

```
(config)# ip http secure-certificate { upload <url_file> [ pass-phrase <pass_phrase> ] |
delete | generate }
(config)# ip http secure-server
(config)# ip http secure-certificate delete
(config)# ip http secure-certificate generate
(config)# ip http secure-certificate upload
tftp://192.168.10.xxx/new_image_path/new_image.dat
(config)# ip http secure-certificate upload
tftp://192.168.10.xxx/new_image_path/new_image.dat pass-phrase password
```

➢ *Max Connection*

• *1 | 2 | 3 | 4*

```
(config)# ip http max-connection <connection_cnt>
(config)# ip http max-connection 1
(config)# ip http max-connection
```

➢ *Fail Blocking Time(s)*

• *10~3600sec*

```
(config)# ip http retry-block-time <block_time>
(config)# ip http retry-block-time 10
(config)# ip http retry-block-time 300
(config)# ip http retry-block-time 3600
```

## 6.5.1.7. Access Management

WEB MENU Configuration>Security>Switch>Access Management

Configure access management table on this page. The maximum number of entries is 16.

**Access Management Configuration**

| Mode | Disabled ✓ |

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

Add New Entry

### Access Management Configuration

| Object | Description |
|---|---|
| **Mode** | Indicates the access management mode operation.<br>Enabled: Enable access management mode operation.<br>Disabled: Disable access management mode operation. |
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **VLAN ID** | Indicates the VLAN ID for the access management entry. |
| **Start IP address** | Indicates the start IP address for the access management entry. |
| **End IP address** | Indicates the end IP address for the access management entry. |
| **HTTP/HTTPS** | Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry. |
| **SNMP** | Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry. |
| **TELNET/SSH** | Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry. |

**Buttons**

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

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>Security>Switch>Access Management

✓ **Access Management Configuration**

➢ *Mode*

SOLTECH
INFONET INC.

- **Disable(default)**

**Access Management Configuration**

| Mode | Disabled |

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

- **Enable**

**Access Management Configuration**

| Mode | Enabled |

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

➢ **Add New Entry**

**Access Management Configuration**

| Mode | Enabled |

| Delete | VLAN ID | Start IP Address | End IP Address | HTTP/HTTPS | SNMP | TELNET/SSH |
| --- | --- | --- | --- | --- | --- | --- |
| ☐ | 1 | 192.168.10.1 | 192.168.10.135 | ☑ | ☐ | ☑ |
| ☐ | 2 | 2.2.2.1 | 2.2.2.100 | ☐ | ☑ | ☐ |

# EXAMPLE CLI CONFIGURATION

✓ **Access Management Configuration**

➢ **Mode**

- **Disable(default)**

```
(config)# no access management
```

- **Enable**

```
(config)# access management
```

➢ **Add New Entry**

```
(config)# access management <1-16> <1-4095> <ipv4_addr> to <ipv4_addr> [1]
(config)# access management 1 1 192.168.10.1 to 192.168.10.135 web telnet
(config)# access management 2 2 2.2.2.1 to 2.2.2.100 snmp

[1}
all   snmp   telnet   web
```

## 6.5.1.8. SNMP

### 6.5.1.8.1. System

WEB MENU Configuration>Security>SNMP>System

Configure SNMP on this page

**SNMP System Configuration**

| Mode | Disabled |
|---|---|
| Version | SNMP v2c |
| Read Community | def_ro_pwd |
| Write Community | def_rw_pwd |
| Engine ID | 800007e5017f000001 |

#### SNMP System Configuration

| Object | Description |
|---|---|
| **Mode** | Indicates the SNMP mode operation. <br> Enabled: Enable SNMP mode operation. <br> Disabled: Disable SNMP mode operation. |
| **Version** | Indicates the SNMP supported version. <br> SNMP v1: Set SNMP supported version 1. <br> SNMP v2c: Set SNMP supported version 2c. <br> SNMP v3: Set SNMP supported version 3. |
| **Read Community** | Indicates the community read access string to permit access to SNMP agent. <br> (Only English alphabet letters and numbers., 0 to 255 characters.) <br> The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. <br> For Secure OS products, a minimum of 8 characters including uppercase letters, lowercase letters, and numbers is required. |
| **Write Community** | Indicates the community write access string to permit access to SNMP agent. <br> (Only English alphabet letters and numbers., 0 to 255 characters.) <br> The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. <br> For Secure OS products, a minimum of 8 characters including uppercase letters, lowercase letters, and numbers is required. |
| **Engine ID** | Indicates the SNMPv3 engine ID. <br> The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. <br> Change of the Engine ID will clear all original local users. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

SOLTECH
INFONET INC.

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>Security>SNMP>System

✓ **SNMP System Configuration**

➢ *Mode*

• *Disable(default)*

**SNMP System Configuration**

| Mode | Disabled |
|---|---|
| Version | SNMP v2c |
| Read Community | def_ro_pwd |
| Write Community | def_rw_pwd |
| Engine ID | 800007e5017f000001 |

• *Enable*

**SNMP System Configuration**

| Mode | Enabled |
|---|---|
| Version | SNMP v2c |
| Read Community | def_ro_pwd |
| Write Community | def_rw_pwd |
| Engine ID | 800007e5017f000001 |

➢ *Version*

**SNMP System Configuration**

| Mode | Enabled |
|---|---|
| Version | SNMP v1 |
| Read Community | def_ro_pwd |
| Write Community | def_rw_pwd |
| Engine ID | 800007e5017f000001 |

**SNMP System Configuration**

| Mode | Enabled |
|---|---|
| Version | SNMP v2c |
| Read Community | def_ro_pwd |
| Write Community | def_rw_pwd |
| Engine ID | 800007e5017f000001 |

**SNMP System Configuration**

| Mode | Enabled |
|---|---|
| Version | SNMP v3 |
| Read Community | def_ro_pwd |
| Write Community | def_rw_pwd |
| Engine ID | 800007e5017f000001 |

SOLTECH
INFONET INC.

➢ **Community(v1/v2c)**

• **Read Community**

**SNMP System Configuration**

| Mode | Enabled |
|---|---|
| Version | SNMP v2c |
| Read Community | test123 |
| Write Community | private |
| Engine ID | 800007e5017f000001 |

• **Write Community**

**SNMP System Configuration**

| Mode | Enabled |
|---|---|
| Version | SNMP v2c |
| Read Community | public |
| Write Community | test234 |
| Engine ID | 800007e5017f000001 |

➢ **Engine ID(v3)**

**SNMP System Configuration**

| Mode | Enabled |
|---|---|
| Version | SNMP v3 |
| Read Community | public |
| Write Community | private |
| Engine ID | 800007e5017f000002 |

➢ **Secure OS products**

**SNMP System Configuration**

| Mode | Enabled |
|---|---|
| Version | SNMP v2c |
| Read Community | Security1 |
| Write Community | Security2 |
| Engine ID | 800007e5017f000001 |

## EXAMPLE CLI CONFIGURATION

✓ **SNMP System Configuration**

➢ **Mode**

• **Disable(default)**

```
(config)# no snmp-server
```

SOLTECH
INFONET INC.

- ***Enable***

```
(config)# snmp-server
```

➢ ***Version***

```
(config)# snmp-server version {1}
(config)# snmp-server version v1

{1}
v1   v2c   v3
```

➢ ***Community(v1/v2c)***

- ***Read Community***

```
(config)# snmp-server community v2c <word255> ro
(config)# snmp-server community v2c test123 ro
```

- ***Write Community***

```
(config)# snmp-server community v2c <word255> rw
(config)# snmp-server community v2c test234 rw
```

➢ ***Engine ID(v3)***

```
(config)# snmp-server engine-id local <word10-64>
(config)# snmp-server engine-id local 800007e5017f000002
```

➢ ***Secure OS products***

```
(config)# snmp-server community v2c Security1 ro

(config)# snmp-server community v2c Security2 rw
```

## 6.5.1.8.2. Trap

WEB MENU Configuration>Security>SNMP>Trap

Configure SNMP trap on this page.

**Trap Configuration**

**Global Settings**

Mode [ Disabled v ]

**Trap Destination Configurations**

| Delete | Name | Enable | Version | Destination Address | Destination Port |

[ Add New Entry ]

### Trap Configuration

#### Global Setting

| Object | Description |
|--------|-------------|
| **Mode** | Indicates the trap mode operation. Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation. |

#### Trap Destination Configurations

| Object | Description |
|--------|-------------|
| **Name** | Indicates the trap Configuration's name. Indicates the trap destination's name. |
| **Enable** | Indicates the trap destination mode operation. Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation. |
| **Version** | Indicates the SNMP trap supported version. SNMPv1: Set SNMP trap supported version 1. SNMPv2c: Set SNMP trap supported version 2c. SNMPv3: Set SNMP trap supported version 3. |
| **Destination Address** | Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w'). And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash. Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'. |
| **Destination port** | Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535. |

SOLTECH
INFONET INC.

**Buttons**

Add New Entry : Click to add a new user.

(Clicking on the button will open the SNMP Trap Configuration window.)

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

## SNMP Trap Detailed Configuration

Configure trap detailed configuration on this page.

**SNMP Trap Configuration**

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

**SNMP Trap Event**

| System | ☐ * ☐ Warm Start                                                    ☐ Cold Start |
|---|---|
| Interface | Link up ⦿ none ◯ specific ◯ all switches<br>☐ *Link down ◯ none ◯ specific ◯ all switches<br>LLDP ⦿ none ◯ specific ◯ all switches |
| Authentication | ☐ * ☐ SNMP Authentication Fail |
| Switch | ☐ * ☐ STP                                                              ☐ RMON |

### SNMP Trap Configuration

| Object | Description |
|---|---|
| **Trap Config Name** | Indicates which trap Configuration's name for configuring. |
| **Trap Mode** | Indicates the SNMP mode operation.<br>Enabled: Enable SNMP mode operation.<br>Disabled: Disable SNMP mode operation. |
| **Trap Version** | Indicates the SNMP supported version.<br>SNMP v1: Set SNMP supported version 1.<br>SNMP v2c: Set SNMP supported version 2c.<br>SNMP v3: Set SNMP supported version 3. |
| **Trap Community** | Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126. |
| **Trap Destination Address** | Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').<br>And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, |

| | |
|---|---|
| | the first character must be an alpha character, and the first and last characters must not be a dot or a dash. |
| **Trap Destination port** | Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535. |
| **Trap Inform Mode** | Indicates the SNMP trap inform mode operation. Enabled: Enable SNMP trap inform mode operation. Disabled: Disable SNMP trap inform mode operation. |
| **Trap Inform Timeout** | Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147. |
| **Trap Inform Retry Times** | Indicates the SNMP trap inform retry times. The allowed range is 0 to 255. |
| **Trap Probe Security Engine ID** | Indicates the SNMP trap probe security engine ID mode of operation. Enabled: Enable SNMP trap probe security engine ID mode of operation. Disabled: Disable SNMP trap probe security engine ID mode of operation. |
| **Trap Security Engine ID** | Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. |
| **Trap Security Name** | Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled. |

**SNMP Trap Event**

| Object | Description |
|---|---|
| **System** | Enable/disable that the Interface group's traps. Warm Start: Enable/disable Warm Start trap. Cold Start: Enable/disable Cold Start trap. |
| **Interface** | Indicates that the Interface group's traps. (Indicates that the SNMP entity is permitted to generate authentication failure traps.) Link Up: Enable/disable Link up trap. Link Down: Enable/disable Link down trap. LLDP: Enable/disable LLDP trap. |
| **Authentication** | Indicates that the authentication group's traps. SNMP Authentication Fail : Enable/disable SNMP trap authentication failure trap. |
| **Switch** | Indicates that the Switch group's traps. STP: Enable/disable STP trap. RMON: Enable/disable RMON trap. |

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>Security>SNMP>Trap

✓ **Global Setting**

➤ *Mode*

• *Disable(default)*



• *Enable*



✓ **Trap Destination Configurations**

➤ *Add New Entry*

• *Use SNMP v1*

**Trap Configuration**

**Global Settings**

| Mode | Enabled ∨ |

**Trap Destination Configurations**

| Delete | Name | Enable | Version | Destination Address | Destination Port |
|--------|------|--------|---------|---------------------|------------------|
| ☐ | TEST-123 | Enabled | SNMPv1 | 192.168.10.130 | 162 |

- **Use SNMP v2c**

**SNMP Trap Configuration**

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

**SNMP Trap Event**

| System | ☐ * ☐ Warm Start | ☐ Cold Start |
|---|---|---|
| Interface | Link up ⦿ none ○ specific ○ all switches<br>☐ *Link down ⦿ none ○ specific ○ all switches<br>LLDP ⦿ none ○ specific ○ all switches | |
| Authentication | ☐ * ☐ SNMP Authentication Fail | |
| Switch | ☐ * ☐ STP | ☐ RMON |

**Trap Configuration**

**Global Settings**

| Mode | Enabled ∨ |

**Trap Destination Configurations**

| Delete | Name | Enable | Version | Destination Address | Destination Port |
|--------|------|--------|---------|---------------------|------------------|
| ☐ | TEST-123 | Enabled | SNMPv2c | 192.168.10.130 | 162 |

---

# EXAMPLE CLI CONFIGURATION

---

✓ **Global Setting**

➢ *Mode*

- *Disable(default)*

```
(config)# no snmp-server trap
```

- *Enable*

```
(config)# snmp-server trap
```

✓ **Trap Destination Configurations**

➢ *Add New Entry*

• *Use SNMP v1*

| |
|---|
| (config)# snmp-server host <word32><br>*(config)# snmp-server host TEST-123*<br><br>(config-snmps-host)# |
| (config-snmps-host)# shutdown |
| (config-snmps-host)# version {v1/v2/v3} <word255><br>*(config-snmps-host)# version v1 def_trap_pwd* |
| (config-snmps-host)# host { <v_ipv4_ucast> \| <v_word> } [ <udp_port> ] [ traps \| informs ]<br>*(config-snmps-host)# host 192.168.10.130 162* |
| (config-snmps-host)# traps [ authentication snmp-auth-fail ] [ system [ coldstart ] [ warmstart ] ] [ switch [ stp ] [ rmon ] ]<br>*(config-snmps-host)# traps authentication snmp-auth-fail system switch* |
| (config)# interface ( <port_type> [ <plist> ] )<br>*(config)# interface \**<br><br>(config-if)# snmp-server host <conf_name> traps [ linkup ] [ linkdown ] [ lldp ]<br>*(config-if)# snmp-server host TEST-123 traps linkup linkdown lldp* |

• *Use SNMP v2*

| |
|---|
| (config)# snmp-server host <word32><br>*(config)# snmp-server host TEST-123*<br><br>(config-snmps-host)# |
| (config-snmps-host)# shutdown |
| (config-snmps-host)# version {v1/v2/v3} <word255><br>*(config-snmps-host)# version v2 def_trap_pwd* |
| (config-snmps-host)# host { <v_ipv4_ucast> \| <v_word> } [ <udp_port> ] [ traps \| informs ]<br>*(config-snmps-host)# host 192.168.10.130 162 informs* |
| (config-snmps-host)# traps [ authentication snmp-auth-fail ] [ system [ coldstart ] [ warmstart ] ] [ switch [ stp ] [ rmon ] ]<br>*(config-snmps-host)# traps authentication snmp-auth-fail system switch* |
| (config-snmps-host)# informs retries <retries> timeout <timeout><br>*(config-snmps-host)# informs retries 5 timeout 3(default)* |
| (config)# interface ( <port_type> [ <plist> ] )<br>*(config)# interface \**<br><br>(config-if)# snmp-server host <conf_name> traps [ linkup ] [ linkdown ] [ lldp ]<br>*(config-if)# snmp-server host TEST-123 traps linkup linkdown lldp* |

## 6.5.1.8.3. Communities

WEB MENU Configuration>Security>SNMP>Communities

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

**SNMPv3 Community Configuration**

| Delete | Community | Source IP | Source Mask |
|--------|-----------|-----------|-------------|
| ☐ | def_ro_pwd | 0.0.0.0 | 0.0.0.0 |
| ☐ | def_rw_pwd | 0.0.0.0 | 0.0.0.0 |

### SNMPv3 Community Configuration

| Object | Description |
|--------|-------------|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Community** | Indicates the community access string to permit access to SNMPv3 agent. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string. (This entry is influences the Groups.) |
| **Source IP** | Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask. |
| **Source Mask** | Indicates the SNMP access source address mask. |

**Buttons**

`Add New Entry` : Click to add a new community entry.

`Apply` : Click to apply changes.

`Apply&Save` : Click to apply and save changes.

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

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>Security>SNMP>Communities

✓ **SNMPv3 Community Configuration**

➢ *Add New Entry*

**SNMPv3 Community Configuration**

| Delete | Community | Source IP | Source Mask |
|--------|-----------|-----------|-------------|
| ☐ | def_ro_pwd | 192.168.10.0 | 255.255.255.0 |
| ☐ | def_rw_pwd | 192.168.10.0 | 255.255.255.0 |

SOLTECH
INFONET INC.

## EXAMPLE CLI CONFIGURATION

✓ **SNMPv3 Community Configuration**

➢ *Add New Entry*

```
(config)# snmp-server community v3 <v3_comm> [<v_ipv4_addr> <v_ipv4_netmask>]
(config)# snmp-server community v3 def_ro_pwd 192.168.10.0 255.255.255.0
(config)# snmp-server community v3 def_rw_pwd 192.168.10.0 255.255.255.0
```

## 6.5.1.8.4. Users

WEB MENU Configuration>Security>SNMP>Users

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

**SNMPv3 User Configuration**

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

### SNMPv3 User Configuration

| Object | Description |
|--------|-------------|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Engine ID** | An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user. |
| **User Name** | A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. (This entry is influences the <u>Groups</u>.) |
| **Security Level** | Indicates the security model that this entry should belong to. **NoAuth, NoPriv**  No authentication and no privacy. **Auth, NoPriv**  Authentication and no privacy. **Auth, Priv**  Authentication and privacy. The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly. |
| **Authentication Protocol** | Indicates the authentication protocol that this entry should belong to. **None**  No authentication protocol. **SHA**  An optional flag to indicate that this user uses SHA authentication protocol. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly. |
| **Authentication Password** | A string identifying the authentication password phrase. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126. |
| **Privacy Protocol** | Indicates the privacy protocol that this entry should belong to. **None**  No privacy protocol. **AES**  An optional flag to indicate that this user uses AES authentication protocol. |

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

**Buttons**

[Add New Entry] : Click to add a new user entry.

[Apply] : Click to apply changes.

[Apply&Save] : Click to apply and save changes.

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

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>Security>SNMP>Users

✓ **SNMPv3 User Configuration**

➢ *Add New Entry*

• *NoAuth, NoPriv*

**SNMPv3 User Configuration**

| Delete | Engine ID | User Name | Security Level | Authentication Protocol | Authentication Password | Privacy Protocol | Privacy Password |
|---|---|---|---|---|---|---|---|
| ☑ | 800007e5017f000001 | TEST-123 | NoAuth, NoPriv | None | None | None | None |
| Delete | 800007e5017f000001 | TEST-123 | NoAuth, NoPriv ▾ | | | | |

• *Auth, NoPriv*

**SNMPv3 User Configuration**

| Delete | Engine ID | User Name | Security Level | Authentication Protocol | Authentication Password | Privacy Protocol | Privacy Password |
|---|---|---|---|---|---|---|---|
| ☑ | 800007e5017f000001 | default_user | NoAuth, NoPriv | None | None | None | None |
| Delete | 800007e5017f000001 | TEST-123 | Auth, NoPriv ▾ | SHA ▾ | •••••••••• | | |

SHA
SHA224
SHA256
SHA384
SHA512

• *Auth, Priv*

**SNMPv3 User Configuration**

| Delete | Engine ID | User Name | Security Level | Authentication Protocol | Authentication Password | Privacy Protocol | Privacy Password |
|---|---|---|---|---|---|---|---|
| ☑ | 800007e5017f000001 | default_user | NoAuth, NoPriv | None | None | None | None |
| Delete | 800007e5017f000001 | TEST-123 | Auth, Priv ▾ | SHA ▾ | •••••••••• | AES ▾ | •••••••••• |

AES
AES192
AES256

## EXAMPLE CLI CONFIGURATION

SOLTECH
INFONET INC.

✓ **SNMPv3 User Configuration**

➢ *Add New Entry*

• *NoAuth, NoPriv*

```
(config)# snmp-server user <username> engine-id <engineID>
(config)# snmp user TEST-123 engine-id 800007e5017f000001
```

• *Auth, NoPriv*

```
(config)# snmp-server user <username> engine-id <engineID> [ { sha | sha224 | sha256 |
sha384 | sha512 } <auth_passwd>
(config)# snmp user TEST-123 engine-id 800007e5017f000001 sha **********
```

• *Auth, Priv*

```
(config)# snmp-server user <username> engine-id <engineID> [ { sha | sha224 | sha256 |
sha384 | sha512 } <auth_passwd> [ priv { aes | aes192 | aes256 } <priv_passwd> ] ]
(config)# snmp user TEST-123 engine-id 800007e5017f000001 sha ********** priv aes
**********
```

## 6.5.1.8.5. Groups

WEB MENU Configuration>Security>SNMP>Groups

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

**SNMPv3 Group Configuration**

| Delete | Security Model | Security Name | Group Name |
|---|---|---|---|
| ☐ | usm | default_user | default_rw_group |

### SNMPv3 Group Configuration

| Object | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Security Model** | Indicates the security model that this entry should belong to.<br>**v1**        Reserved for SNMPv1.<br>**v2c**       Reserved for SNMPv2c.<br>**usm**       User-based Security Model (USM). |
| **Security Name** | A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.(This entry is influenced by the communities, users.) |
| **Group Name** | A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. (This entry is influences the Access.) |

**Buttons**

Add New Entry : Click to add a new group entry.

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>Security>SNMP>Groups

✓ **SNMPv3 Group Configuration**

➢ *Add New Entry*

• *v1*
  *(Security Name influenced by Communities)*

**SNMPv3 Group Configuration**

| Delete | Security Model | Security Name | Group Name |
|--------|----------------|---------------|------------|
| ☑ | usm | default_user | default_rw_group |
| Delete | v1 ▾ | public ▾ | default_ro_group |

public
private

- *v2c*
  *(Security Name influenced by Communities)*

**SNMPv3 Group Configuration**

| Delete | Security Model | Security Name | Group Name |
|--------|----------------|---------------|------------|
| ☑ | usm | default_user | default_rw_group |
| Delete | v2c ▾ | public ▾ | default_ro_group |

public
private

- *usm*
  *(Security Name influenced by Users)*

**SNMPv3 Group Configuration**

| Delete | Security Model | Security Name | Group Name |
|--------|----------------|---------------|------------|
| ☑ | usm | default_user | default_rw_group |
| Delete | usm ▾ | default_user ▾ | default_ro_group |

default_user

---

# EXAMPLE CLI CONFIGURATION

---

✓  **SNMPv3 Group Configuration**

➢  *Add New Entry*

- *v1*
  *(Security Name influenced by Communities)*

```
(config)# snmp-server security-to-group model { v1 | v2c | v3 } name <security_name>
group <group_name>
(config)# snmp-server security-to-group model v1 name public group default_ro_group
```

- *v2c*
  *(Security Name influenced by Communities)*

```
(config)# snmp-server security-to-group model { v1 | v2c | v3 } name <security_name>
group <group_name>
(config)# snmp-server security-to-group model v2c name public group default_ro_group
```

- *usm*
  *(Security Name influenced by Users)*

```
(config)# snmp-server security-to-group model { v1 | v2c | v3 } name <security_name>
group <group_name>
(config)# snmp-server security-to-group model v3 name default_user group
default_ro_group
```

SOLTECH
INFONET INC.

## 6.5.1.8.6. Views

WEB MENU Configuration>Security>SNMP>Views

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

**SNMPv3 View Configuration**

| Delete | View Name | View Type | OID Subtree |
|--------|-----------|-----------|-------------|
| ☐ | default_view | included ⌄ | .1 |

### SNMPv3 View Configuration

| Object | Description |
|--------|-------------|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **View Name** | A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. (This entry is influences the Access.) |
| **View Type** | Indicates the view type that this entry should belong to. **included** An optional flag to indicate that this view subtree should be included. **excluded** An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry. |
| **OID Subtree** | The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*). |

**Buttons**

Add New Entry : Click to add a new view entry.

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

## EXAMPLE WEB CONFIGURATION

✓ **SNMPv3 Group Configuration**

➢ *Add New Entry*

• *test_view(excluded SysName)*

**SNMPv3 View Configuration**

| Delete | View Name | View Type | OID Subtree |
|--------|-----------|-----------|-------------|
| ☐ | test_view | included ⌄ | .1 |
| ☐ | test_view | excluded ⌄ | .1.3.6.1.2.1.1.5.0 |

**SOLTECH**
INFONET INC.

## EXAMPLE CLI CONFIGURATION

✓ **SNMPv3 Group Configuration**

➢ *Add New Entry*

• *test_view(excluded SysName)*

```
(config)# snmp-server view <view_name> <oid_subtree> { include | exclude }
(config)# snmp-server view test_view .1 include
(config)# snmp-server view test_view .1.3.6.1.2.1.1.5.0 exclude
```

## 6.5.1.8.7. Access

WEB MENU Configuration>Security>SNMP>Access

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

**SNMPv3 Access Configuration**

| Delete | Group Name | Security Model | Security Level | Read View Name | Write View Name |
|--------|-----------|----------------|----------------|----------------|-----------------|

### SNMPv3 Access Configuration

| Object | Description |
|--------|-------------|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Group Name** | A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.(This entry is influenced by the Groups.) |
| **Security Model** | Indicates the security model that this entry should belong to. <br> **any** — Any security model accepted(v1\|v2c\|usm). <br> **v1** — Reserved for SNMPv1. <br> **v2** — Reserved for SNMPv2c. <br> **usm** — User-based Security Model (USM). |
| **Security Level** | Indicates the security model that this entry should belong to. <br> **NoAuth, NoPriv** No authentication and no privacy. <br> **Auth, NoPriv** Authentication and no privacy. <br> **Auth, Priv** Authentication and privacy. |
| **Read View Name** | The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. (This entry is influenced by the Views.) |
| **Write View Name** | The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. (This entry is influenced by the Views.) |

**Buttons**

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

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

## EXAMPLE WEB CONFIGURATION

✓ **SNMPv3 Access Configuration**

➤ *Add New Entry*

• *default_rw_group(test_view)*

**SNMPv3 Access Configuration**

| Delete | Group Name | Security Model | Security Level | Read View Name | Write View Name |
|--------|------------|----------------|----------------|----------------|-----------------|
| ☐ | default_rw_group | any | Auth, Priv | test_view ⌄ | test_view ⌄ |

## EXAMPLE CLI CONFIGURATION

✓ **SNMPv3 Access Configuration**

➤ *Add New Entry*

• *default_rw_group(test_view)*

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

## 6.5.2. Network Configuration

## 6.5.2.1. Limit Control

WEB MENU Configuration>Security>Network>Limit Control

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

You can set up port security aging for each system.

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

• None, Trap, Shutdown, Trap and Shutdown

Switches are configured based on the total number of MAC addresses brought in by all ports when a new MAC address is detected on a port with port security enabled. Since all ports draw from the same pool, there could be instances where the configured maximum cannot be assigned if the remaining ports have already utilized all available MAC addresses.

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

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

**Port Security Limit Control Configuration**

**System Configuration**

| Mode | Disabled |
|---|---|
| Aging Enabled | ☐ |
| Aging Period | 3600    seconds |

**Port Configuration**

| Port | Mode | Limit | Action | State | Re-open |
|---|---|---|---|---|---|
| * | <> | 4 | <> | | |
| 1 | Disabled | 4 | None | Disabled | Reopen |
| 2 | Disabled | 4 | None | Disabled | Reopen |
| 3 | Disabled | 4 | None | Disabled | Reopen |
| 4 | Disabled | 4 | None | Disabled | Reopen |
| 5 | Disabled | 4 | None | Disabled | Reopen |
| 6 | Disabled | 4 | None | Disabled | Reopen |
| 7 | Disabled | 4 | None | Disabled | Reopen |
| 8 | Disabled | 4 | None | Disabled | Reopen |

**Port Security Limit Control Configuration**

**System Configuration**

| Object | Description |
|---|---|
| **Mode** | Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled limit checks and corresponding actions are disabled. |
| **Aging Enabled** | If checked, secured MAC addresses are subject to aging as discussed under Aging Period. |
| **Aging Period** | If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, underlying port security will use the shorter requested aging period of all modules that use the functionality. (The Aging Period can be set to a number between 10 and 9,999,999 seconds.) |

**Port Configuration**

| Object | Description | | |
|---|---|---|---|
| **Port** | The port number to which the configuration below applies. | | |
| **Mode** | Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port. | | |
| **Limit** | The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The switch has a total number of MAC addresses and since all ports draw from the same pool, it is possible that a configured maximum cannot be granted if all available MAC addresses have already been used by the remaining ports. | | |
| **Action** | If MAC address Limit is reached, the switch can take one of the actions: | | |
| | **None** | Do not allow more than Limit MAC addresses on the port, but take no further action. | |
| | **Trap** | If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded. | |
| | **Shutdown** | If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port: 1) Boot the switch, 2) Disable and re-enable Limit Control on the port or the | |

| | | switch, <br> 3) Click the Reopen button. |
|---|---|---|
| | **Trap&Shutdown** | If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken. |
| **State** | This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values: | |
| | **Disabled** | Limit Control is either globally disabled or disabled on the port. |
| | **Ready** | The limit is not yet reached. This can be shown for all actions. |
| | **Limit Reached** | Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap. |
| | **Shutdown** | Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown. |
| **Re-open Button** | If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. <br> Note that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost. | |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

Refresh : Click to refresh the page. Note that non-committed changes will be lost.

## EXAMPLE WEB CONFIGURATION

✓ **System Configuration**

➢ *Mode*

• *Disabled*



• *Enabled*



➢ *Aging Enable*

- **Disabled**

**System Configuration**

| Mode | Enabled |
|---|---|
| Aging Enabled | ☐ |
| Aging Period | 3600    seconds |

- **Enabled**

**System Configuration**

| Mode | Enabled |
|---|---|
| Aging Enabled | ☑ |
| Aging Period | 3600    seconds |

➢ **Aging Period**
**(10 ~ 9,999,999 seconds)**

**System Configuration**

| Mode | Enabled |
|---|---|
| Aging Enabled | ☑ |
| Aging Period | 9999999    seconds |

✓ **Port Configuration**

➢ **Mode**

- **Disabled**

**Port Configuration**

| Port | Mode | Limit | Action | State | Re-open |
|---|---|---|---|---|---|
| * | <> | 4 | <> | | |
| 1 | Disabled | 4 | None | Disabled | Reopen |
| 2 | Disabled | 4 | None | Disabled | Reopen |
| 3 | Disabled | 4 | None | Disabled | Reopen |
| 4 | Disabled | 4 | None | Disabled | Reopen |
| 5 | Disabled | 4 | None | Disabled | Reopen |
| 6 | Disabled | 4 | None | Disabled | Reopen |
| 7 | Disabled | 4 | None | Disabled | Reopen |
| 8 | Disabled | 4 | None | Disabled | Reopen |

- **Enabled**

**Port Configuration**

| Port | Mode | Limit | Action | State | Re-open |
|---|---|---|---|---|---|
| * | <> | 4 | <> | | |
| 1 | Enabled | 4 | None | Ready | Reopen |
| 2 | Disabled | 4 | None | Disabled | Reopen |
| 3 | Disabled | 4 | None | Disabled | Reopen |
| 4 | Disabled | 4 | None | Disabled | Reopen |
| 5 | Disabled | 4 | None | Disabled | Reopen |
| 6 | Disabled | 4 | None | Disabled | Reopen |
| 7 | Disabled | 4 | None | Disabled | Reopen |
| 8 | Disabled | 4 | None | Disabled | Reopen |

➢ **Limit (1 ~ 1024 MAC address)**

**Port Configuration**

| Port | Mode | Limit | Action | State | Re-open |
|---|---|---|---|---|---|
| * | <> | 1024 | <> | | |
| 1 | Enabled | 1024 | None | Ready | Reopen |
| 2 | Disabled | 4 | None | Disabled | Reopen |
| 3 | Disabled | 4 | None | Disabled | Reopen |
| 4 | Disabled | 4 | None | Disabled | Reopen |
| 5 | Disabled | 4 | None | Disabled | Reopen |
| 6 | Disabled | 4 | None | Disabled | Reopen |
| 7 | Disabled | 4 | None | Disabled | Reopen |
| 8 | Disabled | 4 | None | Disabled | Reopen |

➢   *Action*

•   *None | Trap | Shutdown | Trap&Shutdown*

**Port Configuration**

| Port | Mode | Limit | Action | State | Re-open |
|---|---|---|---|---|---|
| * | <> | 1024 | <> | | |
| 1 | Enabled | 1024 | Shutdown | Disabled | Reopen |
| 2 | Disabled | 4 | None | Disabled | Reopen |
| 3 | Disabled | 4 | Trap | Disabled | Reopen |
| 4 | Disabled | 4 | Shutdown / Trap & Shutdown | Disabled | Reopen |
| 5 | Disabled | 4 | None | Disabled | Reopen |
| 6 | Disabled | 4 | None | Disabled | Reopen |
| 7 | Disabled | 4 | None | Disabled | Reopen |
| 8 | Disabled | 4 | None | Disabled | Reopen |

---

## EXAMPLE CLI CONFIGURATION

---

✓   **System Configuration**

➢   *Mode*

•   *Disabled*

```
(config)# no port-security
```

•   *Enabled*

```
(config)# port-security
```

➢   *Aging Enable*

•   *Disabled*

```
(config)# no port-security aging
```

•   *Enabled*

```
(config)# port-security aging
```

•   *Aging Period*
    *(10 ~ 9,999,999 seconds)*

```
(config)# port-security aging time <v_10_to_9999999>
(config)# port-security aging time 9999999
```

✓ **Port Configuration**

➢ *Mode*

• *Disabled*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# no port-security
```

• *Enabled*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# port-security
```

➢ *Limit (1 ~ 1024 MAC address)*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# port-security maximum [ <v_1_to_1024> ]
(config-if)# port-security maximum 1024
```

➢ *Action*

• *None | Trap | Shutdown | Trap&Shutdown*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# port-security violation { protect | trap | trap-shutdown | shutdown }
(config-if)# port-security violation protect
(config-if)# port-security violation trap
(config-if)# port-security violation shutdown
(config-if)# port-security violation trap-shutdown
```

## 6.5.2.2. ACL

ACL (Access Control List) is composed of ACE (Access Control Entry) entries that specify individual users or groups allowed access to specific traffic entities such as processes or programs. ACE parameters vary depending on the selected frame type.

Each accessible traffic entity includes an identifier for its corresponding ACL. Permissions determine whether specific traffic entities have access rights.

Implementing ACLs can become highly complex, for instance, when prioritizing ACEs for various scenarios. In networking, ACLs represent lists of service ports or network service offerings available on hosts or servers. Each service has a list of allowed host or server entries for service usage. ACLs are typically configured to control inbound traffic, and in this context, ACLs share similarities with firewalls.

There are three configurable sections related to manual ACL configuration.

ACL configuration displays ACEs in a top-to-bottom priority manner, from highest (top) to lowest (bottom). Incoming frames hit only one ACE, even if multiple matching ACEs exist. The first matching ACE performs the action (permit/deny) for that frame, and the associated counter increments. ACEs can be associated with all combinations of incoming port and policy (value/mask pair). Once ACE policies are created, they can be linked with port groups as part of ACL port configuration. Multiple parameters can be configured with ACEs.

ACL port configuration is used to assign policy IDs to incoming ports, useful for grouping ports to follow the same traffic rules. Traffic policies are generated in ACL configuration. For each incoming port, the following traffic attributes can be set:

• Action

• Rate Limiter

• Port Redirection

• Mirroring

• Logging

• Termination

The management interface allows you to enable forwarding (Permit) or deny forwarding (Deny) on a port, determining whether traffic is allowed to pass through. The default action is Permit.

ACEs are applied only if frames do not match and pass through ACE matches. In this case, the counter associated with that port increases. There can be up to 16 different ACL rate limiters. Rate limiter IDs can be assigned to ACE(s) or incoming port(s).

ACEs are configured with multiple parameters, which vary depending on the selected frame type. Incoming ports must select the next frame type chosen for ACE. Different parameter options are displayed based on the chosen frame type. Supported frame types include:

- Any

- Configurable Ethernet types

- ARP

- IPv4

- IPv6

MAC-based filtering and IP protocol-based filtering can be achieved through configuration based on the appropriate frame type selection.

## 6.5.2.2.1. Ports

WEB MENU Configuration>Security>Network>ACL>Ports

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



### ACL Ports Configuration

| Object | Description |
|---|---|
| **Port** | The logical port for the settings contained in the same row. |
| **Policy ID** | Select the policy to apply to this port.<br>The allowed values are 0 through 255. The default value is 0. |
| **Action** | Select whether forwarding is permitted ("Permit") or denied ("Deny").<br>The default value is "Permit". |

| Rate Limiter ID | Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled". |
|---|---|
| Port Redirect | Select which port frames are redirected on. The allowed values are Disabled or a specific port number. The default value is "Disabled". (It can't be set when action is permitted.) |
| Mirror | Specify the mirror operation of this port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is "Disabled". |
| Logging | Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC. The allowed values are: Enabled: Frames received on the port are stored in the System Log. Disabled: Frames received on the port are not logged. The default value is "Disabled". Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited. |
| Shutdown | Specify the port shut down operation of this port. The allowed values are: Enabled: If a frame is received on the port, the port will be disabled. Disabled: Port shut down is disabled. The default value is "Disabled". Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags). |
| State | Specify the port state of this port. The allowed values are: Enabled: To reopen ports by changing the volatile port configuration of the ACL user module. Disabled: To close ports by changing the volatile port configuration of the ACL user module. The default value is "Enabled". |
| Counter | Counts the number of frames that match this ACE. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

Refresh : Click to refresh the page.

Clear : Click to clear the counters.

---

# EXAMPLE WEB CONFIGURATION

---

✓ **ACL Ports Configuration**

    ➢ *Policy ID*

        • *0~255(default 0)*

| Port | Policy ID | Action | Rate Limiter ID | Port Redirect | Mirror | Logging | Shutdown | State | Counter |
|---|---|---|---|---|---|---|---|---|---|
| * | 255 | <> | <> | Disabled / Port 1 / Port 2 | <> | <> | <> | <> | * |
| 1 | 255 | Permit | Disabled | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |

    ➢ *Action*

        • *Permit(default) | Deny*

SOLTECH
INFONET INC.

| Port | Policy ID | Action | Rate Limiter ID | Port Redirect | Mirror | Logging | Shutdown | State | Counter |
|---|---|---|---|---|---|---|---|---|---|
| * | 0 | <> | <> | Disabled / Port 1 / Port 2 | <> | <> | <> | <> | * |
| 1 | 0 | Permit / Deny / Permit | Disabled | Disabled / Port 1 / Port 2 / Disabled | Disabled | Disabled | Disabled | Enabled | 0 |

➢ **Rate Limiter ID**

• **Disabled | 1~16**

| Port | Policy ID | Action | Rate Limiter ID | Port Redirect | Mirror | Logging | Shutdown | State | Counter |
|---|---|---|---|---|---|---|---|---|---|
| * | 0 | <> | <> | Disabled / Port 1 / Port 2 | <> | <> | <> | <> | * |
| 1 | 0 | Permit | 1 / Disabled | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 2 | 0 | Permit | 1 / 2 / 3 | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 30741 |
| 3 | 0 | Permit | 4 / 5 / 6 | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 16713 |
| 4 | 0 | Permit | 7 / 8 / 9 | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 5 | 0 | Permit | 10 / 11 / 12 | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 6 | 0 | Permit | 13 / 14 / 15 / 16 | Disabled / Port 1 / Port 2 / Disabled | Disabled | Disabled | Disabled | Enabled | 0 |

➢ **Port Redirect (Need Action Deny)**

• **Disabled(default) | Port Number**

| Port | Policy ID | Action | Rate Limiter ID | Port Redirect | Mirror | Logging | Shutdown | State | Counter |
|---|---|---|---|---|---|---|---|---|---|
| * | 0 | <> | <> | Disabled / Port 1 / Port 2 | <> | <> | <> | <> | * |
| 1 | 0 | Deny | Disabled | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |

➢ **Mirror**

• **Disabled(default) | Enabled**

| Port | Policy ID | Action | Rate Limiter ID | Port Redirect | Mirror | Logging | Shutdown | State | Counter |
|---|---|---|---|---|---|---|---|---|---|
| * | 0 | <> | <> | Disabled / Port 1 / Port 2 | <> | <> | <> | <> | * |
| 1 | 0 | Permit | Disabled | Disabled / Port 1 / Port 2 / Disabled | Disabled / Disabled / Enabled | Disabled | Disabled | Enabled | 0 |

➢ **Logging**

• **Disabled(default) | Enabled**

| Port | Policy ID | Action | Rate Limiter ID | Port Redirect | Mirror | Logging | Shutdown | State | Counter |
|---|---|---|---|---|---|---|---|---|---|
| * | 0 | <> | <> | Disabled / Port 1 / Port 2 | <> | <> | <> | <> | * |
| 1 | 0 | Permit | Disabled | Disabled / Port 1 / Port 2 / Disabled | Disabled | Disabled / Disabled / Enabled | Disabled | Enabled | 0 |

➢ **Shutdown**

• **Disabled(default) | Enabled**

| Port | Policy ID | Action | Rate Limiter ID | Port Redirect | Mirror | Logging | Shutdown | State | Counter |
|------|-----------|--------|-----------------|---------------|--------|---------|----------|-------|---------|
| * | 0 | <> | <> | Disabled / Port 1 / Port 2 | <> | <> | <> | <> | * |
| 1 | 0 | Permit | Disabled | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled / Disabled / Enabled | Enabled | 0 |
|  |  |  |  | Disabled |  |  |  |  |  |

➢ **State**

• **Enabled(default) | Disabled**

| Port | Policy ID | Action | Rate Limiter ID | Port Redirect | Mirror | Logging | Shutdown | State | Counter |
|------|-----------|--------|-----------------|---------------|--------|---------|----------|-------|---------|
| * | 0 | <> | <> | Disabled / Port 1 / Port 2 | <> | <> | <> | <> | * |
| 1 | 0 | Permit | Disabled | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled / Disabled / Enabled | 0 |
|  |  |  |  | Disabled |  |  |  |  |  |

---

## EXAMPLE CLI CONFIGURATION

---

✓ **ACL Ports Configuration**

➢ **Policy ID**

• **0~255(default 0)**

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# access-list policy <policy_id>
(config-if)# access-list policy 255
```

➢ **Action**

• **Permit(default) | Deny**

```
(config-if)# access-list action { permit | deny }
(config-if)# access-list action deny
```

➢ **Rate Limiter ID**

• **Disabled(default) | 1~16**

```
(config-if)# no access-list rate-limiter
```

```
(config-if)# access-list rate-limiter <rate_limiter_id>
(config-if)# access-list rate-limiter 16

<rate_limiter_id> = <1-16>
```

➢ **Port Redirect (Need Action Deny)**

• **Disabled(default) | Port Number**

```
(config-if)# no access-list redirect
```

```
(config-if)# access-list redirect interface { <port_type> <port_type_id> | ( <port_type>
[ <port_type_list> ] ) }
(config-if)# access-list redirect interface GigabitEthernet 1/4
```

➢ *Mirror*

• *Disabled(default) | Enabled*

```
(config-if)# no access-list mirror
```

```
(config-if)# access-list mirror
```

➢ *Logging*

• *Disabled(default) | Enabled*

```
(config-if)# no access-list logging
```

```
(config-if)# access-list logging
```

➢ *Shutdown*

• *Disabled(default) | Enabled*

```
(config-if)# no access-list shutdown
```

```
(config-if)# access-list shutdown
```

➢ *State*

• *Enabled(default) | Disabled*

```
(config-if)# access-list port-state
```

```
(config-if)# no access-list port-state
```

## 6.5.2.2.2. Rate Limiters

WEB MENU Configuration>Security>Network>ACL>Rate Limiters

Configure the rate limiter for the ACL of the switch.

**ACL Rate Limiter Configuration**

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

### ACL Ports Configuration

| Object | Description |
|---|---|
| **Rate Limiter ID** | The rate limiter ID for the settings contained in the same row and its range is 1 to 16. |
| **Rate** | The valid rate is 0 ~ 5,000,000 in pps or 0 ~ 10,000,000 in kbps. |
| **Unit** | Specify the rate unit.(pps: packets per second, kbps: Kbits per second.) |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

✓ **ACL Rate Limiter Configuration**

➢ *Rate*

• *0 ~ 5,000,000pps or 0 ~ 10,000,000kbps*

SOL TECH
INFONET INC.

**ACL Rate Limiter Configuration**

| Rate Limiter ID | Rate | Unit |
|---|---|---|
| * | 5000000 | <> |
| 1 | 5000000 | pps |
| 2 | 10000000 | kbps |
| 3 | 10 | pps |
| 4 | 10 | pps |
| 5 | 10 | pps |
| 6 | 10 | pps |
| 7 | 10 | pps |
| 8 | 10 | pps |
| 9 | 10 | pps |
| 10 | 10 | pps |
| 11 | 10 | pps |
| 12 | 10 | pps |
| 13 | 10 | pps |
| 14 | 10 | pps |
| 15 | 10 | pps |
| 16 | 10 | pps |

## EXAMPLE CLI CONFIGURATION

✓ **ACL Rate Limiter Configuration**

➢ *Rate*

• *0 ~ 5,000,000pps or 0 ~ 10,000,000kbps*

```
(config)# access-list rate-limiter [ <rate_limiter_list> ] { 10pps <pps10_rate> | 25kbps
<kpbs25_rate> }
(config)# access-list rate-limiter <1-16> 10pps <0-500000>
(config)# access-list rate-limiter 1 10pps 500000
```

```
(config)# access-list rate-limiter [ <rate_limiter_list> ] { 10pps <pps10_rate> | 25kbps
<kpbs25_rate> }
(config)# access-list rate-limiter <1-16> 25kbps <0-400000>
(config)# access-list rate-limiter 2 25kbps 400000
```

SOLTECH
INFONET INC.

## 6.5.2.2.3. Access Control List Configuration

WEB MENU Configuration>Security>Network>ACL>Access Control List

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 512 on each switch.

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

**Access Control List Configuration**

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

### Access Control List Configuration

| Object | Description |
|--------|-------------|
| **ACE** | Indicates the ACE ID. |
| **Ingress Port** | Indicates the ingress port of the ACE. Possible values are:<br>All: The ACE will match all ingress port.<br>Port: The ACE will match a specific ingress port. |
| **Policy / Bitmask** | Indicates the policy number and bitmask of the ACE. |
| **Frame Type** | Indicates the frame type of the ACE.<br>**Any** The ACE will match any frame type.<br>**EType** The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.<br>**ARP** The ACE will match ARP/RARP frames.<br>**IPv4** The ACE will match all IPv4 frames.<br>**IPv4/ICMP** The ACE will match IPv4 frames with ICMP protocol.<br>**IPv4/UDP** The ACE will match IPv4 frames with UDP protocol.<br>**IPv4/TCP** The ACE will match IPv4 frames with TCP protocol.<br>**IPv4/Other** The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.<br>**IPv6** The ACE will match all IPv6 standard frames. |
| **Action** | Indicates the forwarding action of the ACE.<br>**Permit** Frames matching the ACE may be forwarded and learned.<br>**Deny** Frames matching the ACE are dropped.<br>**Filter** Frames matching the ACE are filtered. |
| **Rate Limiter** | Indicates the rate limiter number of the ACE. The allowed range is 1 to 16.<br>When Disabled is displayed, the rate limiter operation is disabled. |
| **Port Redirect** | Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled. |
| **Mirror** | Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port.<br>Enabled: Frames received on the port are mirrored.<br>Disabled: Frames received on the port are not mirrored. |

| Counter | Indicates the number of times the ACE was hit by a frame. |
|---|---|
| **Modification Buttons** | You can modify each ACE in the table using the following buttons: |

| | | |
|---|---|---|
| ⊕ | | Inserts a new ACE before the current row. Clicking on it will navigate to the ACE configuration page. |
| ⊜ | | Edits the ACE row. |
| ⬆ | | Moves the ACE up the list. (Priority Increase) |
| ⬇ | | Moves the ACE down the list. (Priority decrease) |
| ⊗ | | Deletes the ACE. |
| ⊕ | | The lowest plus sign adds a new entry at the bottom of the ACE listings.(Lowest Priority) |

**Buttons**

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

Refresh : Click to refresh the page;

Clear : Click to clear the counters.

Remove All : Click to remove all ACEs.

## ACE Configuration

Configure an ACE (Access Control Entry) on this page.

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

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

**ACE Configuration**

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

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

**VLAN Parameters**

| 802.1Q Tagged | Any |
|---|---|
| VLAN ID Filter | Any |
| Tag Priority | Any |

### ACE Configuration

| Object | Description |
|---|---|
| **Ingress Port** | Select the ingress port for which this ACE applies. All: The ACE applies to all port. Port n: The ACE applies to this port number. |
| **Policy Filter** | Specify the policy number filter for this ACE. Any: No policy filter is specified. |

SOLTECH
INFONET INC.

| | Specific: If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears. |
|---|---|
| **Policy Value** | When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 255. |
| **Policy Bitmask** | When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0xff. |
| **Frame Type** | Select the frame type for this ACE.<br><table><tr><td>**Any**</td><td>Any frame can match this ACE.</td></tr><tr><td>**Ethernet Type**</td><td>Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal) and the value should not be equal to 0x800(IPv4), 0x806(ARP) or 0x86DD(IPv6).</td></tr><tr><td>**ARP**</td><td>Only ARP frames can match this ACE. (0x806)</td></tr><tr><td>**IPv4**</td><td>Only IPv4 frames can match this ACE. (0x800)</td></tr><tr><td>**IPv6**</td><td>Only IPv6 frames can match this ACE. (0x86DD)</td></tr></table> |
| **Action** | Specify the action to take with a frame that hits this ACE.<br><table><tr><td>**Permit**</td><td>The frame that hits this ACE is granted permission for the ACE operation.</td></tr><tr><td>**Deny**</td><td>The frame that hits this ACE is dropped.</td></tr><tr><td>**Filter**</td><td>Frames matching the ACE are filtered.</td></tr></table> |
| **Rate Limiter** | Specify the rate limiter in number of base units. The allowed range is 1 to 16. Disabled indicates that the rate limiter operation is disabled. |
| **Port Redirect** | Frames that hit the ACE are redirected to the port number specified here. The rate limiter will affect these ports. The allowed range is the same as the switch port number range. Disabled indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when action is permitted. |
| **Mirror** | Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port.<br>Enabled: Frames received on the port are mirrored.<br>Disabled: Frames received on the port are not mirrored. |
| **Logging** | Specify the logging operation of the ACE.<br>Enabled: Frames matching the ACE are stored in the System Log.<br>Disabled: Frames matching the ACE are not logged.<br>Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited. |
| **Shutdown** | Specify the port shut down operation of the ACE.<br>Enabled: If a frame matches the ACE, the ingress port will be disabled.<br>Disabled: Port shut down is disabled for the ACE.<br>Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags). |
| **Counter** | The counter indicates the number of times the ACE was hit by a frame. |
| **MAC Parameters** | Configure MAC settings for ACE<br>(Only displayed when the frame type is Ethernet Type or ARP.) |
| **SMAC Filter** | Specify the source MAC filter for this ACE.<br>Any: No SMAC filter is specified.<br>Specific: If you want to filter a specific source MAC address with this ACE |
| **SMAC Value** | When "Specific" is selected for the SMAC filter, you can enter a specific |

| | source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value |
|---|---|
| **DMAC Filter** | Specify the destination MAC filter for this ACE. |
| | **Any** No DMAC filter is specified. |
| | **MC** Frame must be multicast. |
| | **BC** Frame must be broadcast. |
| | **UC** Frame must be unicast. |
| | **Specific** To filter a specific destination MAC address with this ACE. |
| **DMAC Value** | When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value. |
| **VLAN Parameters** | Configure VLAN settings for ACE |
| **802.1Q Tagged** | Specify whether frames can hit the action according to the 802.1Q tagged. |
| | **Any** Any value is allowed. |
| | **Enabled** Tagged frame only. |
| | **Disabled** Untagged frame only. |
| **VLAN ID Filter** | Specify the VLAN ID filter for this ACE. |
| | **Any** No VLAN ID filter is specified. |
| | **Specific** If you want to filter a specific VLAN ID with this ACE |
| **VLAN ID** | When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value. |
| **Tag Priority** | Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7 or range 0-1, 2-3, 4-5, 6-7, 0-3 and 4-7. The value Any means that no tag priority is specified. |
| **ARP Parameters** | Configure ARP settings for ACE (The ARP parameters can be configured when Frame Type "ARP" is selected.) |
| **ARP/RARP** | Specify the available ARP/RARP opcode (OP) flag for this ACE. |
| | **Any** No ARP/RARP OP flag is specified. |
| | **ARP** Frame must have ARP opcode set to ARP. |
| | **RARP** Frame must have RARP opcode set to RARP. |
| | **Other** Frame has unknown ARP/RARP Opcode flag. |
| **Request/Reply** | Specify the available Request/Reply opcode (OP) flag for this ACE. |
| | **Any** No Request/Reply OP flag is specified. |
| | **Request** Frame must have ARP Request or RARP Request OP flag set. |
| | **Reply** Frame must have ARP Reply or RARP Reply OP flag. |
| **Sender IP Filter** | Specify the sender IP filter for this ACE. |
| | **Any** No sender IP filter is specified. |
| | **Host** Sender IP filter is set to Host. |
| | **Network** Sender IP filter is set to Network. |
| **Sender IP Address** | When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation. |
| **Sender IP Mask** | When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation. |
| **Target IP Filter** | Specify the target IP filter for this specific ACE. |
| | **Any** No target IP filter is specified. |
| | **Host** Target IP filter is set to Host. |
| | **Network** Target IP filter is set to Network. |

| Target IP Address | When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation. |
|---|---|
| Target IP Mask | When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation. |
| ARP Sender MAC Match | Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.<br>**0**    ARP frames where SHA is not equal to the SMAC address.<br>**1**    ARP frames where SHA is equal to the SMAC address.<br>**Any** Any value is allowed. |
| RARP Target MAC Match | Specify whether frames can hit the action according to their target hardware address field (THA) settings.<br>**0**    RARP frames where THA is not equal to the target MAC address.<br>**1**    RARP frames where THA is equal to the target MAC address.<br>**Any** Any value is allowed. |
| IP/Ethernet Length | Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.<br>**0**    ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).<br>**1**    ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).<br>**Any** Any value is allowed. |
| IP | Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.<br>**0**    ARP/RARP frames where the HLD is not equal to Ethernet (1).<br>**1**    ARP/RARP frames where the HLD is equal to Ethernet (1).<br>**Any** Any value is allowed. |
| Ethernet | Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.<br>**0**    ARP/RARP frames where the PRO is not equal to IP (0x800).<br>**1**    ARP/RARP frames where the PRO is equal to IP (0x800).<br>**Any** Any value is allowed. |
| IP Parameters | Configure IPv4 settings for ACE. The IP parameters can be configured when Frame Type "IPv4" is selected. |
| IP Protocol Filter | Specify the IP protocol filter for this ACE.<br>**Any**    No IP protocol filter is specified<br>**Specific** Select Specific if you want to filter a specific IP protocol with this ACE.<br>**ICMP**    Select ICMP to filter IPv4 ICMP protocol frames.<br>**UDP**    Select UDP to filter IPv4 UDP protocol frames.<br>**TCP**    Select TCP to filter IPv4 TCP protocol frames. |
| IP Protocol Value | When "Specific" is selected for the IP protocol value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value. |
| IP TTL | Specify the Time-to-Live settings for this ACE.<br>**zero**    IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.<br>**non-zero** IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.<br>**Any**    Any value is allowed. |
| IP Fragment | Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG |

| | | | |
|---|---|---|---|
| | OFFSET) field for an IPv4 frame. | | |
| | **No** | IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry. | |
| | **Yes** | IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry. | |
| | **Any** | Any value is allowed. | |
| **IP Option** | Specify the options flag setting for this ACE. | | |
| | **No** | IPv4 frames where the options flag is set must not be able to match this entry. | |
| | **Yes** | IPv4 frames where the options flag is set must be able to match this entry. | |
| | **Any** | Any value is allowed. | |
| **SIP Filter** | Specify the source IP filter for this ACE. | | |
| | **Any** | No source IP filter is specified. | |
| | **Host** | Source IP filter is set to Host. | |
| | **Network** | Source IP filter is set to Network. | |
| **SIP Address** | When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation. | | |
| **SIP Mask** | When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation. | | |
| **DIP Filter** | Specify the destination IP filter for this ACE. | | |
| | **Any** | No destination IP filter is specified. | |
| | **Host** | Destination IP filter is set to Host. | |
| | **Network** | Destination IP filter is set to Network. | |
| **DIP Address** | When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation. | | |
| **DIP Mask** | When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation. | | |
| **IPv6 Parameters** | Configure IPv6 settings for ACE. The IPv6 parameters can be configured when Frame Type "IPv6" is selected. | | |
| **Next Header Filter** | Specify the IPv6 next header filter for this ACE. | | |
| | **Any** | No IPv6 next header filter is specified | |
| | **Specific** | Select Specific if you want to filter a specific IPv6 next header filter with this ACE. | |
| | **ICMP** | Select ICMP to filter IPv6 ICMP protocol frames. | |
| | **UDP** | Select UDP to filter IPv6 UDP protocol frames. | |
| | **TCP** | Select TCP to filter IPv6 TCP protocol frames. | |
| **Next Header Value** | When "Specific" is selected for the IPv6 next header value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IPv6 protocol value. | | |
| **SIP Filter** | Specify the source IPv6 filter for this ACE. | | |
| | **Any** | No source IPv6 filter is specified. | |
| | **Specific** | Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear. | |
| **SIP Address** | When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address. | | |
| **SIP BitMask** | When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address. Notice the usage of bitmask, if the binary bit value is "0", it | | |

| | means this bit is "don't-care". The real matched pattern is [sipv6_address & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFFE(bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule. | |
|---|---|---|
| **Hop Limit** | Specify the hop limit settings for this ACE. | |
| | **Zero** | IPv6 frames with a hop limit field greater than zero must not be able to match this entry. |
| | **non-zero** | IPv6 frames with a hop limit field greater than zero must be able to match this entry. |
| | **Any** | Any value is allowed. |
| **ICMP Parameters** | Configure ICMP settings for ACE. | |
| **ICMP Type Filter** | Specify the ICMP filter for this ACE. | |
| | **Any** | No ICMP filter is specified. |
| | **Specific** | If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. |
| **ICMP Type Value** | When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP value. | |
| **ICMP Code Filter** | Specify the ICMP code filter for this ACE. | |
| | **Any** | No ICMP code filter is specified. |
| | **Specific** | If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. |
| **ICMP Code Value** | When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value. | |
| **TCP/UDP Parameters** | Configure TCP/UDP settings for ACE. | |
| **TCP/UDP Source Filter** | Specify the TCP/UDP source filter for this ACE. | |
| | **Any** | No TCP/UDP source filter is specified. |
| | **Specific** | If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. |
| | **Range** | If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. |
| **TCP/UDP Source No.** | When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value. | |
| **TCP/UDP Source Range** | When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value. | |
| **TCP/UDP Destination Filter** | Specify the TCP/UDP destination filter for this ACE. | |
| | **Any** | No TCP/UDP destination filter is specified |
| | **Specific** | If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. |
| | **Range** | If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. |
| **TCP/UDP Destination Number** | When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value. | |

| TCP/UDP Destination Range | When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value. |
|---|---|
| **TCP FIN** | Specify the TCP "No more data from sender" (FIN) value for this ACE. |
| | **0** TCP frames where the FIN field is set must not be able to match this entry. |
| | **1** TCP frames where the FIN field is set must be able to match this entry. |
| | **Any** Any value is allowed. |
| **TCP SYN** | Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE. |
| | **0** TCP frames where the SYN field is set must not be able to match this entry. |
| | **1** TCP frames where the SYN field is set must be able to match this entry. |
| | **Any** Any value is allowed. |
| **TCP RST** | Specify the TCP "Reset the connection" (RST) value for this ACE. |
| | **0** TCP frames where the RST field is set must not be able to match this entry. |
| | **1** TCP frames where the RST field is set must be able to match this entry. |
| | **Any** Any value is allowed. |
| **TCP PSH** | Specify the TCP "Push Function" (PSH) value for this ACE. |
| | **0** TCP frames where the PSH field is set must not be able to match this entry. |
| | **1** TCP frames where the PSH field is set must be able to match this entry. |
| | **Any** Any value is allowed. |
| **TCP ACK** | Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE. |
| | **0** TCP frames where the ACK field is set must not be able to match this entry. |
| | **1** TCP frames where the ACK field is set must be able to match this entry. |
| | **Any** Any value is allowed. |
| **TCP URG** | Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE. |
| | **0** TCP frames where the URG field is set must not be able to match this entry. |
| | **1** TCP frames where the URG field is set must be able to match this entry. |
| | **Any** Any value is allowed. |
| **Ethernet Type Parameters** | Configure Ethernet Type settings for ACE. The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected. |
| **EtherType Filter** | Specify the Ethernet type filter for this ACE. |
| | **Any** No EtherType filter is specified |
| | **Specific** If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. |
| **Ethernet Type Value** | When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits |

| | |
|---|---|
| | this ACE matches this EtherType value. |

**Buttons**

`Apply` : Click to apply changes.

`Apply&Save` : Click to apply and save changes.

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

`Cancel` : Return to the previous page.

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>Security>Network>ACL>Access Control List

Example) Deny frames based on the source MAC address from PORT1.

**Access Control List Configuration**

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

✓   **Access Control List Configuration**

➢   ***Add ACE to end of list***

•   ⊕

✓   **ACE Configuration**

**ACE Configuration**

| Ingress Port | All / Port 1 / Port 2 / Port 3 / Port 4 |
|---|---|
| Policy Filter | Any |
| Frame Type | Ethernet Type |

| Action | Deny |
|---|---|
| Rate Limiter | Disabled |
| Port Redirect | Disabled / Port 1 / Port 2 / Port 3 / Port 4 |
| Mirror | Disabled |
| Logging | Disabled |
| Shutdown | Disabled |
| Counter | 0 |

**MAC Parameters**

| SMAC Filter | Specific |
|---|---|
| SMAC Value | 00-21-6d-05-f0-5c |
| DMAC Filter | Any |

**VLAN Parameters**

| 802.1Q Tagged | Any |
|---|---|
| VLAN ID Filter | Any |
| Tag Priority | Any |

**Ethernet Type Parameters**

| EtherType Filter | Any |
|---|---|

✓   **Access Control List Configuration**

**Access Control List Configuration**

| ACE | Ingress Port | Policy / Bitmask | Frame Type | Action | Rate Limiter | Port Redirect | Mirror | Counter |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | Any | EType | Deny | Disabled | Disabled | Disabled | 21 |

## EXAMPLE CLI CONFIGURATION

Example) Deny frames based on the source MAC address from PORT1.

```
(config)# access-list ace <ace_id> [1]
(config)# access-list ace 1 ingress interface GigabitEthernet 1/1 frame-type etype smac
00-21-6d-05-f0-5c action deny

[1]

action       dmac-type      frame-type    ingress      logging

mirror       next           policy        rate-limiter  redirect

shutdown     tag            tag-priority  vid           <cr>

[ action { permit | deny | filter interface <port_type> <fliter_port_list> } } ]

[ dmac-type { unicast | multicast | broadcast | any}

[ ingress { interface ( <port_type> [ <ingress_port_list> ] ) | any } ]

[ logging [ disable ] ]

[ mirror [ disable ] ]

[ next { <ace_id_next> | last } ]

[ policy <policy ID> [ policy-bitmask <policy_bitmask> ] ]

[ rate-limiter { <rate_limiter_id> | disable } ]

[ redirect { interface { ( <port_type> [ <redirect_port_list> ] ) } | disable } ]

[ shutdown [ disable ] ]

[ tag { tagged | untagged | any } ]

[ tag-priority { <tag_priority> | 0-1 | 2-3 | 4-5 | 6-7 | 0-3 | 4-7 | any } ]

[ vid { <vid> | any } ]

[ shutdown [ disable ] ]

[ frame-type { any | etype [ etype-value { <etype_value> | any } ] [ smac { <etype_smac> |
any } ] [ dmac { <etype_dmac> | any } ] | arp [ sip { <arp_sip> | any } ] [ dip { <arp_dip> |
any } ] [ smac { <arp_smac> | any } ] [ arp-opcode { arp | rarp | other | any } ] [ arp-flag
[ arp-request { <arp_flag_request> | any } ] [ arp-smac { <arp_flag_smac> | any } ] [ arp-
tmac { <arp_flag_tmac> | any } ] [ arp-len { <arp_flag_len> | any } ] [ arp-ip <arp_flag_ip>
| any } ] [ arp-ether { <arp_flag_ether> | any } ] ]
 | ipv4 [ sip { <sipv4> | any } ] [ dip { <dipv4> | any } ] [ ip-protocol { <ipv4_protocol> |
any } ] [ ip-flag [ ip-ttl { <ip_flag_ttl> | any } ] [ ip-options { <ip_flag_options> | any } ]
[ ip-fragment { <ip_flag_fragment> | any } ] ] | ipv4-icmp [ sip { <sipv4_icmp> | any } ]
[ dip { <dipv4_icmp> | any } ] [ icmp-type { <icmpv4_type> | any } ] [ icmp-code
{ <icmpv4_code> | any } ] [ ip-flag [ ip-ttl { <ip_flag_icmp_ttl> | any } ] [ ip-options
{ <ip_flag_icmp_options> | any } ] [ ip-fragment { <ip_flag_icmp_fragment> | any } ] ] |
ipv4-udp [ sip { <sipv4_udp> | any } ] [ dip { <dipv4_udp> | any } ] [ sport
{ <sportv4_udp_start> [ to <sportv4_udp_end> ] | any } ] [ dport { <dportv4_udp_start>
[ to <dportv4_udp_end> ] | any } ] [ ip-flag [ ip-ttl { <ip_flag_udp_ttl> | any } ] [ ip-
options { <ip_flag_udp_options> | any } ] [ ip-fragment { <ip_flag_udp_fragment> |
any } ] ] | ipv4-tcp [ sip { <sipv4_tcp> | any } ] [ dip { <dipv4_tcp> | any } ] [ sport
```

```
{ <sportv4_tcp_start> [ to <sportv4_tcp_end> ] | any } ] [ dport { <dportv4_tcp_start> [ to
<dportv4_tcp_end> ] | any } ] [ ip-flag [ ip-ttl { <ip_flag_tcp_ttl> | any } ] [ ip-options
{ <ip_flag_tcp_options> | any } ] [ ip-fragment { <ip_flag_tcp_fragment> | any } ] ] [ tcp-
flag [ tcp-fin { <tcpv4_flag_fin> | any } ] [ tcp-syn { <tcpv4_flag_syn> | any } ] [ tcp-rst
{ <tcpv4_flag_rst> | any } ] [ tcp-psh { <tcpv4_flag_psh> | any } ] [ tcp-ack
{ <tcpv4_flag_ack> | any } ] [ tcp-urg { <tcpv4_flag_urg> | any } ] ] | ipv6 [ next-header
{ <next_header> | any } ] [ sip { <sipv6> [ sip-bitmask <sipv6_bitmask> ] | any } ] [ hop-
limit { <hop_limit> | any } ] | ipv6-icmp [ sip { <sipv6_icmp> [ sip-bitmask
<sipv6_bitmask_icmp> ] | any } ] [ icmp-type { <icmpv6_type> | any } ] [ icmp-code
{ <icmpv6_code> | any } ] [ hop-limit { <hop_limit_icmp> | any } ] | ipv6-udp [ sip
{ <sipv6_udp> [ sip-bitmask <sipv6_bitmask_udp> ] | any } ] [ sport
{ <sportv6_udp_start> [ to <sportv6_udp_end> ] | any } ] [ dport { <dportv6_udp_start>
[ to <dportv6_udp_end> ] | any } ] [ hop-limit { <hop_limit_udp> | any } ] | ipv6-tcp [ sip
{ <sipv6_tcp> [ sip-bitmask <sipv6_bitmask_tcp> ] | any } ] [ sport { <sportv6_tcp_start>
[ to <sportv6_tcp_end> ] | any } ] [ dport { <dportv6_tcp_start> [ to <dportv6_tcp_end> ]
| any } ] [ hop-limit { <hop_limit_tcp> | any } ] [ tcp-flag [ tcp-fin { <tcpv6_flag_fin> |
any } ] [ tcp-syn { <tcpv6_flag_syn> | any } ] [ tcp-rst { <tcpv6_flag_rst> | any } ] [ tcp-psh
{ <tcpv6_flag_psh> | any } ] [ tcp-ack { <tcpv6_flag_ack> | any } ] [ tcp-urg
{ <tcpv6_flag_urg> | any } ] ] } ]
```

## 6.5.2.3. IP Source Guard

### 6.5.2.3.1. Configuration

WEB MENU Configuration>Security>Network>IP Source Guard>Configuration

This page provides IP Source Guard related configuration.

**IP Source Guard Configuration**

Mode | Disabled ∨

[ Translate dynamic to static ]

**Port Mode Configuration**

| Port | Mode | Max Dynamic Clients |
|------|------|---------------------|
| * | <> ∨ | <> ∨ |
| 1 | Disabled ∨ | Unlimited ∨ |
| 2 | Disabled ∨ | Unlimited ∨ |
| 3 | Disabled ∨ | Unlimited ∨ |
| 4 | Disabled ∨ | Unlimited ∨ |
| 5 | Disabled ∨ | Unlimited ∨ |
| 6 | Disabled ∨ | Unlimited ∨ |
| 7 | Disabled ∨ | Unlimited ∨ |
| 8 | Disabled ∨ | Unlimited ∨ |

### IP Source Guard Configuration

| Object | Description |
|--------|-------------|
| **Mode of IP Source Guard Configuration** | Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled. |

### Port Mode Configuration

| Object | Description |
|--------|-------------|
| **Port Mode Configuration** | Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port. |
| **Max Dynamic Clients** | Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port. |

**Buttons**

[ Apply ] : Click to apply changes.

[ Apply&Save ] : Click to apply and save changes.

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

[ Translate dynamic to static ] : Click to translate all dynamic entries to static entries.

SOLTECH
INFONET INC.

## EXAMPLE WEB CONFIGURATION

✓ **IP Source Guard Configuration**

  ➢ *Mode*

   • *Disable | Enable*

**IP Source Guard Configuration**

| Mode | Disabled ⌄ |
|------|------------|
|      | Disabled   |
| Translate | Enabled | static |

✓ **Port Mode Configuration**

  ➢ *Mode*

   • *Disable | Enable*

**Port Mode Configuration**

| Port | Mode | Max Dynamic Clients |
|------|------|---------------------|
| * | <> ⌄ | <> ⌄ |
| 1 | Disabled ⌄ | Unlimited ⌄ |
| 2 | Disabled | Unlimited ⌄ |
| 3 | Enabled | Unlimited ⌄ |
| 4 | Disabled ⌄ | Unlimited ⌄ |
| 5 | Disabled ⌄ | Unlimited ⌄ |
| 6 | Disabled ⌄ | Unlimited ⌄ |
| 7 | Disabled ⌄ | Unlimited ⌄ |
| 8 | Disabled ⌄ | Unlimited ⌄ |

  ➢ *Max Dynamic Clients*

   • *0 | 1 | 2 | Unlimited*

**Port Mode Configuration**

| Port | Mode | Max Dynamic Clients |
|------|------|---------------------|
| * | <> ⌄ | <> ⌄ |
| 1 | Enabled ⌄ | Unlimited ⌄ |
| 2 | Disabled ⌄ | 0 |
| 3 | Disabled ⌄ | 1 |
| 4 | Disabled ⌄ | 2 |
| 5 | Disabled ⌄ | Unlimited |
| 6 | Disabled ⌄ | Unlimited ⌄ |
| 7 | Disabled ⌄ | Unlimited ⌄ |
| 8 | Disabled ⌄ | Unlimited ⌄ |

## EXAMPLE CLI CONFIGURATION

✓ **IP Source Guard Configuration**

  ➢ *Mode*

- ● ***Disable | Enable***

```
(config)# no ip verify source

(config)# ip verify source
```

✓ **Port Mode Configuration**

➢ ***Mode***

- ● ***Disable | Enable***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# no ip verify source

(config-if)# ip verify source
```

➢ ***Max Dynamic Clients***

- ● ***0 | 1 | 2 | Unlimited***

```
(config-if)# ip verify source limit <cnt_var>
(config-if)# ip verify source limit <0-2>
(config-if)# ip verify source limit 0
(config-if)# ip verify source limit 1
(config-if)# ip verify source limit 2

(config-if)# no ip verify source limit
```

## 6.5.2.3.2. Static Table

WEB MENU Configuration>Security>Network>IP Source Guard>Static Table

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



### Static IP Source Guard Table

| Object | Description |
|---|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| Port | The logical port for the settings. |
| VLAN ID | The vlan id for the settings. |
| IP Address | Allowed Source IP address. |
| MAC address | Allowed Source MAC address. |

**Buttons**

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

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

✓ **Static IP Source Guard Table**

➢ *Add New Entry*

• *Port | VLAN ID(Port VLAN) | IP Address | MAC address*

## EXAMPLE CLI CONFIGURATION

✓ **Static IP Source Guard Table**

➢ *Add New Entry*

• *Port | VLAN ID(Port VLAN) | IP Address | MAC address*

```
(config)# ip source binding interface <port_type> <in_port_type_id> <vlan_var>
<ipv4_var> <mac_var>
(config)# ip source binding interface GigabitEthernet 1/1 1 192.168.10.100 00-21-6D-05-
F0-5C
```

# 6.5.2.4. ARP Inspection

## 6.5.2.4.1. Port Configuration

WEB MENU Configuration>Security>Network>ARP Inspection>Port Configuration

This page provides ARP Inspection related configuration.

**ARP Inspection Configuration**

| Mode | Disabled v |

[ Translate dynamic to static ]

**Port Mode Configuration**

| Port | Mode | Check VLAN | Log Type |
|------|------|-----------|----------|
| * | <> v | <> v | <> v |
| 1 | Disabled v | Disabled v | None v |
| 2 | Disabled v | Disabled v | None v |
| 3 | Disabled v | Disabled v | None v |
| 4 | Disabled v | Disabled v | None v |
| 5 | Disabled v | Disabled v | None v |
| 6 | Disabled v | Disabled v | None v |
| 7 | Disabled v | Disabled v | None v |
| 8 | Disabled v | Disabled v | None v |

### ARP Inspection Configuration

| Object | Description |
|--------|-------------|
| **Mode** | Enable the Global ARP Inspection or disable the Global ARP Inspection. |

### ARP Inspection Configuration

| Object | Description |
|--------|-------------|
| **Port** | The logical port for the settings. |
| **Mode** | Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. <br> **Enable** Enable ARP Inspection operation. <br> **Disable** Disable ARP Inspection operation. |
| **Check VLAN** | If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". <br> The default setting of "Check VLAN" is disabled. <br> (Please configure the list of VLANs to be inspected in the VLAN Configuration settings.) <br> **Enable** Enable Check VLAN operation. The log type of ARP Inspection will refer to the VLAN setting. <br> **Disable** Disable Check VLAN operation. The log type of ARP Inspection will refer to the port setting. |
| **Log Type** | Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. <br> **None** Log nothing. <br> **Deny** Log denied entries. <br> **Permit** Log permitted entries. <br> **All** Log all entries. |

SOLTECH
INFONET INC.

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

Translate dynamic to static : Click to translate all dynamic entries to static entries.

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>Security>Network>ARP Inspection>Port Configuration

✓ **ARP Inspection Configuration**

➢ *Mode*

• *Disable | Enable*



✓ **Port Mode Configuration**

➢ *Mode*

• *Disable | Enable*



➢ *Check VLAN*

• *Disable | Enable*

➢ **Log Type**

- **None | Deny | Permit | All**

**Port Mode Configuration**

| Port | Mode | Check VLAN | Log Type |
|------|------|-----------|----------|
| * | <> | <> | <> |
| 1 | Enabled | Disabled | None |
| 2 | Disabled | Disabled | None |
| 3 | Disabled | Disabled | Deny |
| 4 | Disabled | Disabled | Permit |
| 5 | Disabled | Disabled | All |
| 6 | Disabled | Disabled | None |
| 7 | Disabled | Disabled | None |
| 8 | Disabled | Disabled | None |

---

# EXAMPLE CLI CONFIGURATION

---

✓ **ARP Inspection Configuration**

➢ **Mode**

- **Disable | Enable**

```
(config)# no ip arp inspection
```

```
(config)# ip arp inspection
```

✓ **Port Mode Configuration**

➢ **Mode**

- **Disable | Enable**

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# ip arp inspection trust
```

```
(config)# no ip arp inspection trust
```

➢ **Check VLAN**

- **Disable | Enable**

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# no ip arp inspection check-vlan
```

```
(config-if)# ip arp inspection check-vlan
```

➢ **Log Type**

- **None | Deny | Permit | All**

SOLTECH
INFONET INC.

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# no ip arp inspection logging
```

```
(config-if)# ip arp inspection logging { deny | permit | all }
(config-if)# ip arp inspection logging deny
```

## 6.5.2.4.2. VLAN Configuration

WEB MENU Configuration>Security>Network>ARP Inspection>VLAN Configuration

This page provides ARP Inspection related configuration.

**VLAN Mode Configuration**

Start from VLAN `1` with `20` entries per page.

| Delete | VLAN ID | Log Type |

Add New Entry

### VLAN Mode Configuration

| Object | Description |
|---|---|
| **VLAN Mode Configuration** | Specify ARP Inspection is enabled on which VLANs.<br>First, you have to enable the port setting on Port configuration.<br>Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port.<br>Second, you can specify which VLAN will be inspected on this page.<br>The log type also can be configured on per VLAN setting.<br>**None**   Log nothing.<br>**Deny**   Log denied entries.<br>**Permit**   Log permitted entries.<br>**All**   Log all entries. |

### Buttons

`Refresh` : Click to refresh the page immediately.

`Apply` : Click to apply changes.

`Apply&Save` : Click to apply and save changes.

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

`|<<` : Updates the table starting from the first entry in the ARP Inspection VLAN table.

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

`Add New Entry` : Click to add a new VLAN to the ARP Inspection VLAN table.

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>Security>Network>ARP Inspection>VLAN Configuration

✓ **VLAN Mode Configuration**

➢ *Add New Entry*

• *VLAN ID(1~4095)*

**VLAN Mode Configuration**

Start from VLAN [1] with [20] entries per page.

| Delete | VLAN ID | Log Type |
|--------|---------|----------|
| Delete | 4095 | None ∨ |

[Add New Entry]

- *Log Type( None | Deny | Permit | All )*

**VLAN Mode Configuration**

Start from VLAN [1] with [20] entries per page.

| Delete | VLAN ID | Log Type |
|--------|---------|----------|
| Delete | 4095 | None ∨ |

None
Deny
Permit
All

[Add New Entry]

---

## EXAMPLE CLI CONFIGURATION

---

✓ **VLAN Mode Configuration**

➢ *Add New Entry*

- *VLAN ID(1~4095)*

```
(config)# ip arp inspection vlan <in_vlan_list>
(config)# ip arp inspection vlan 4095
```

- *Log Type( None | Deny | Permit | All )*

```
(config)# no ip arp inspection vlan <in_vlan_list> logging
(config)# no ip arp inspection vlan 4095 logging
```

```
(config)# ip arp inspection vlan <in_vlan_list> logging { deny | permit | all }
(config)# ip arp inspection vlan 4095 logging deny
(config)# ip arp inspection vlan 4095 logging permit
(config)# ip arp inspection vlan 4095 logging all
```

## 6.5.2.4.3. Static Table

WEB MENU Configuration>Security>Network>ARP Inspection>Static Table

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

**Static ARP Inspection Table**

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

Add New Entry

**Static ARP Inspection Table**

| Object | Description |
|--------|-------------|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Port** | The logical port for the settings. |
| **VLAN ID** | The vlan id for the settings. |
| **MAC Address** | Allowed Source MAC address in ARP request packets. |
| **IP Address** | Allowed Source IP address in ARP request packets. |

**Buttons**

Add New Entry : Click to add a new entry to the Static ARP Inspection table.

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>Security>Network>ARP Inspection>Static Table

✓ **Static ARP Inspection Table**

➢ *Add New Entry*

• *Example*

**Static ARP Inspection Table**

| Delete | Port | VLAN ID | MAC Address | IP Address |
|--------|------|---------|-------------|------------|
| Delete | 4 ▾ | 1 | 00-21-6d-05-f0-5c | 192.168.10.100 |

Add New E
1
2
3
4
5
6
7
8

## EXAMPLE CLI CONFIGURATION

✓ **Static ARP Inspection Table**

➢ *Add New Entry*

• *Example*

```
(config)# ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var>
<mac_var> <ipv4_var>
(config)# ip arp inspection entry interface GigabitEthernet 1/4 1 00-21-6d-05-f0-5c
192.168.10.100
```

## 6.5.2.4.4. Dynamic Table

WEB MENU Configuration>Security>Network>ARP Inspection>Dynamic Table

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

**Dynamic ARP Inspection Table**

Start from Port 1 ∨ , VLAN 1 , MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

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

### Dynamic ARP Inspection Table

| Object | Description |
|--------|-------------|
| **Port** | Switch Port Number for which the entries are displayed. |
| **VLAN ID** | VLAN-ID in which the ARP traffic is permitted. |
| **MAC Address** | User MAC address of the entry. |
| **IP Address** | User IP address of the entry. |
| **Translate to Static** | Select the checkbox to translate the entry to static entry. |

**Buttons**

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

Refresh : Refreshes the displayed table starting from the input fields.

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

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

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

## 6.5.3. AAA Configuration

AAA allows for common server configurations including Timeout, Retransmit, Secret Key, NAS IP Address, NAS IPv6 Address, NAS Identifier, and Dead Time parameters. The software supports configuration of RADIUS and TACACS+ servers.

RADIUS servers use the inherently untrusted UDP protocol by design. To handle lost frames, the timeout interval is divided into three equal sub-intervals. If no response is received within a sub-interval, the request is retransmitted. This algorithm allows the RADIUS server to be queried up to three times before being considered dead.

Dead Time, which can be set as a number between 0 to 3600 seconds, is the duration during which the switch does not send new requests to a server that did not respond to the previous request. This prevents the switch from continuously attempting to connect to a server it has already determined to be non-responsive. Dead Time can be set to a value greater than 0, but this feature is only applicable when multiple servers are configured.

Authentication is the process of verifying access to the switch's management interface for users. The RADIUS authentication server is used for granting access rights to both the NAS module and the switch's management interface. The RADIUS accounting server is used only by the NAS module.

TACACS+ is an access control network protocol for routers, network access servers, and other network computing devices. TACACS+ authentication, authorization, and accounting management are supported by the software. The CLI interface is only supported in the initial version for configuring TACACS+ authentication and accounting mechanisms.

## 6.5.3.1. Radius

WEB MENU Configuration>Security>AAA>RADIUS

This page allows you to configure the RADIUS servers

**RADIUS Server Configuration**

**Global Configuration**

| Timeout | 5 | seconds |
|---|---|---|
| Retransmit | 3 | times |
| Deadtime | 0 | minutes |
| Key | | |
| NAS-IP-Address | | |
| NAS-IPv6-Address | | |
| NAS-Identifier | | |

**Server Configuration**

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

Add New Server

**RADIUS Server Configuration**

SOLTECH
INFONET INC.

### Global Configuration

| Object | Description |
|---|---|
| Timeout | Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request. |
| Retransmit | Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead. |
| Deadtime | Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. |
| Key | The secret key - up to 63 characters long - shared between the RADIUS server and the switch. |
| NAS-IP-Address (Attribute 4) | The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used. |
| NAS-IPv6-Address (Attribute 95) | The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used. |
| NAS-Identifier (Attribute 32) | The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet. |

### Server Configuration

| Object | Description |
|---|---|
| Delete | To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save. |
| Hostname | The IP address or hostname of the RADIUS server. |
| Auth Port | The UDP port to use on the RADIUS server for authentication. Set to 0 to disable authentication. |
| Acct Port | The UDP port to use on the RADIUS server for accounting. Set to 0 to disable accounting. |
| Timeout | This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value. |
| Retransmit | This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value. |
| Key | This optional setting overrides the global key. Leaving it blank will use the global key. |

**Buttons**

Add New Server : Click Add New Server to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported.

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

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

SOLTECH
INFONET INC.

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>Security>AAA>RADIUS

✓ **Global Configuration**

➢ *Timeout(3sec)*

**Global Configuration**

| | | |
|---|---|---|
| Timeout | 3 | seconds |
| Retransmit | 3 | times |
| Deadtime | 0 | minutes |
| Key | | |
| NAS-IP-Address | | |
| NAS-IPv6-Address | | |
| NAS-Identifier | | |

➢ *Retransmit(5times)*

**Global Configuration**

| | | |
|---|---|---|
| Timeout | 3 | seconds |
| Retransmit | 5 | times |
| Deadtime | 0 | minutes |
| Key | | |
| NAS-IP-Address | | |
| NAS-IPv6-Address | | |
| NAS-Identifier | | |

➢ *Deadtime(2minutes)*

**Global Configuration**

| | | |
|---|---|---|
| Timeout | 3 | seconds |
| Retransmit | 5 | times |
| Deadtime | 2 | minutes |
| Key | | |
| NAS-IP-Address | | |
| NAS-IPv6-Address | | |
| NAS-Identifier | | |

➢ *Key (Radius server secret key)*

**Global Configuration**

| | | |
|---|---|---|
| Timeout | 5 | seconds |
| Retransmit | 3 | times |
| Deadtime | 2 | minutes |
| Key | •••••••••••••••••••••••••• | |
| NAS-IP-Address | | |
| NAS-IPv6-Address | | |
| NAS-Identifier | | |

➢ *Add New Server*

**Server Configuration**

| Delete | Hostname | Auth Port | Acct Port | Timeout | Retransmit | Key |
|---|---|---|---|---|---|---|
| ☐ | 192.168.10.251 | 1812 | 1813 | | | |

## EXAMPLE CLI CONFIGURATION

✓ **Global Configuration**

➢ *Timeout(3sec)*

```
(config)# radius-server timeout <seconds>
(config)# radius-server timeout 3
```

➢ *Retransmit(5times)*

```
(config)# radius-server retransmit <retries>
(config)# radius-server retransmit 5
```

➢ *Deadtime(2minutes)*

```
(config)# radius-server deadtime <minutes>
(config)# radius-server deadtime 2
```

➢ *Key (Radius server secret key)*

```
(config)# radius-server key [ <key> ]
(config)# radius-server key radius11
```

➢ *Add New Server*

```
(config)# radius-server host <host_name> [ auth-port <auth_port> ] [ acct-port
<acct_port> ] [ timeout <seconds> ] [ retransmit <retries> ] [ key <key> ]
(config)# radius-server host 192.168.10.251 auth-port 1812 acct-port 1813
```

## 6.5.3.2. TACACS+

WEB MENU Configuration>Security>AAA>TACACS+

This page allows you to configure the TACACS+ servers.

**TACACS+ Server Configuration**

**Global Configuration**

| | | |
|---|---|---|
| Timeout | 5 | seconds |
| Deadtime | 0 | minutes |
| Key | | |

**Server Configuration**

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

Add New Server

### TACACS+ Server Configuration

#### Global Configuration

| Object | Description |
|---|---|
| Timeout | Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead. |
| Deadtime | Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. |
| Key | The secret key - up to 63 characters long - shared between the TACACS+ server and the switch. |

#### Server Configuration

| Object | Description |
|---|---|
| Delete | To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save. |
| Hostname | The IP address or hostname of the TACACS+ server. |
| Port | The TCP port to use on the TACACS+ server for authentication. |
| Timeout | This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value. |
| Key | This optional setting overrides the global key. Leaving it blank will use the global key. |

**Buttons**

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

Delete : can be used to undo the addition of the new server.

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

SOLTECH
INFONET INC.

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>Security>AAA>TACACS+

✓ **Global Configuration**

➢ *Timeout(3sec)*

**Global Configuration**

| Timeout | 3 | seconds |
|---------|---|---------|
| Deadtime | 0 | minutes |
| Key | | |

➢ *Deadtime(2minutes)*

**Global Configuration**

| Timeout | 3 | seconds |
|---------|---|---------|
| Deadtime | 2 | minutes |
| Key | | |

➢ *Key (Tacacs+ server secret key)*

**Global Configuration**

| Timeout | 3 | seconds |
|---------|---|---------|
| Deadtime | 2 | minutes |
| Key | •••••••••••••••••••••••• | |

➢ *Add New Server*

**Server Configuration**

| Delete | Hostname | Port | Timeout | Key |
|--------|----------|------|---------|-----|
| ☐ | 192.168.10.251 | 49 | | |

## EXAMPLE CLI CONFIGURATION

✓ **Global Configuration**

➢ *Timeout(3sec)*

```
(config)# tacacs-server timeout <seconds>
(config)# tacacs-server timeout 3
```

➢ *Deadtime(2minutes)*

```
(config)# tacacs-server deadtime <minutes>
(config)# tacacs-server deadtime 2
```

SOLTECH
INFONET INC.

➢ *Key (Tacacs+ server secret key)*

```
(config)# tacacs-server key [ <key> ]
(config)# tacacs-server key tacacs11
```

➢ *Add New Server*

```
(config)# tacacs-server host <host_name> [ port <port> ] [ timeout <seconds> ] [ key <key> ]
(config)# tacacs-server host 192.168.10.251 port 49
```

## 6.5.4. Access Management Statistics Monitor

WEB MENU Monitor>Security>Access Management Statistics

This page provides statistics for access management.

**Access Management Statistics**

| Interface | Received Packets | Allowed Packets | Discarded Packets |
|---|---|---|---|
| HTTP | 0 | 0 | 0 |
| HTTPS | 0 | 0 | 0 |
| SNMP | 0 | 0 | 0 |
| TELNET | 0 | 0 | 0 |
| SSH | 0 | 0 | 0 |

### Access Management Statistics

| Object | Description |
|---|---|
| **Interface** | The interface type through which the remote host can access the switch. |
| **Received Packets** | Number of received packets from the interface when access management mode is enabled. |
| **Allowed Packets** | Number of allowed packets from the interface when access management mode is enabled. |
| **Discarded Packets** | Number of discarded packets from the interface when access management mode is enabled. |

**Buttons**

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

Refresh : Click to refresh the page immediately.

Clear : Clear all statistics.

---

## EXAMPLE WEB MONITOR

---

WEB MENU Monitor>Security>Access Management Statistics

**Access Management Statistics**

| Interface | Received Packets | Allowed Packets | Discarded Packets |
|---|---|---|---|
| HTTP | 0 | 0 | 0 |
| HTTPS | 183 | 183 | 0 |
| SNMP | 6 | 0 | 6 |
| TELNET | 122 | 122 | 0 |
| SSH | 85 | 85 | 0 |

---

## EXAMPLE CLI MONITOR

---

➢ *Access Management Statistics*

```
# show access management statistics
```

SOLTECH
INFONET INC.

```
Access Management Statistics:
----------------------------
HTTP     Receive:        0    Allow:        0    Discard:        0
HTTPS    Receive:      201    Allow:      201    Discard:        0
SNMP     Receive:       26    Allow:        0    Discard:       26
TELNET   Receive:      124    Allow:      124    Discard:        0
SSH      Receive:       89    Allow:       89    Discard:        0
```

# 6.5.5. Network Monitor

## 6.5.5.1. Port Security

### 6.5.5.1.1. Switch

WEB MENU Monitor>Security>Network>Port Security>Switch

This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

**Port Security Switch Status**

**User Module Legend**

| User Module Name | Abbr |
|---|---|
| Limit Control | L |
| Voice VLAN | V |

**Port Status**

| Port | Users | State | MAC Count Current | MAC Count Limit |
|---|---|---|---|---|
| 1 | -- | Disabled | - | - |
| 2 | -- | Disabled | - | - |
| 3 | -- | Disabled | - | - |
| 4 | -- | Disabled | - | - |
| 5 | -- | Disabled | - | - |
| 6 | -- | Disabled | - | - |
| 7 | -- | Disabled | - | - |
| 8 | -- | Disabled | - | - |

**Port Security Switch Status**

**User Module Legend**

| Object | Description |
|---|---|
| User Module Legend | The legend shows all user modules that may request Port Security services. |
| User Module Name | The full name of a module that may request Port Security services. |
| Abbr | A one-letter abbreviation of the user module. This is used in the Users column in the port status table. |

**User Module Legend**

| Object | Description |
|---|---|
| Port Status | The table has one row for each port on the switch and a number of columns |
| Port | The port number for which the status applies. Click the port number to see the status for this particular port. |

| Users | Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security. |
|---|---|
| State | Shows the current state of the port. It can take one of four values:<br>Disabled: No user modules are currently using the Port Security service.<br>Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.<br>Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.<br>Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page. |
| MAC Count<br><br>(Current, Limit) | The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.<br>If no user modules are enabled on the port, the Current column will show a dash (-).<br>If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-). |

**Buttons**

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

Refresh : Click to refresh the page immediately.

## EXAMPLE WEB MONITOR

WEB MENU Monitor>Security>Network>Port Security>Switch

✓    **Port Security Switch Status**

**Port Security Switch Status**

**User Module Legend**

| User Module Name | Abbr |
|------------------|------|
| Limit Control    | L    |
| Voice VLAN       | V    |

**Port Status**

| Port | Users | State | MAC Count | |
|------|-------|-------|-----------|---|
|      |       |       | Current | Limit |
| 1 | L- | Limit Reached | 5 | 4 |
| 2 | -- | Disabled | - | - |
| 3 | -- | Disabled | - | - |
| 4 | -- | Disabled | - | - |
| 5 | -- | Disabled | - | - |
| 6 | -- | Disabled | - | - |
| 7 | -- | Disabled | - | - |
| 8 | -- | Disabled | - | - |

## EXAMPLE CLI MONITOR

✓    **Port Security Switch Status**

```
# show port-security switch [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security switch

Users:
L = Limit Control
V = Voice VLAN
Interface             Users  State         MAC Cnt
---------------------- -----  ------------- -------
GigabitEthernet 1/1    L-     Limit Reached     5
GigabitEthernet 1/2    --     No users          0
GigabitEthernet 1/3    --     No users          0
GigabitEthernet 1/4    --     No users          0
10GigabitEthernet 1/1  --     No users          0
10GigabitEthernet 1/2  --     No users          0
10GigabitEthernet 1/3  --     No users          0
10GigabitEthernet 1/4  --     No users          0
```

SOLTECH
INFONET INC.

## 6.5.5.1.2. Port

WEB MENU Monitor>Security>Network>Port Security>Port

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

**Port Security Port Status  Port 1**

| MAC Address | VLAN ID | State | Time of Addition | Age/Hold |
|---|---|---|---|---|
| No MAC addresses attached | | | | |

### Port Security Port Status Port n

| Object | Description |
|---|---|
| **MAC Address & VLAN ID** | The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating *"No MAC addresses attached"* is displayed. |
| **State** | Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic. |
| **Time of Addition** | Shows the date and time when this MAC address was first seen on the port. |
| **Age/Hold** | If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise, a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown. |

**Buttons**

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

Refresh : Click to refresh the page immediately.

## EXAMPLE WEB MONITOR

WEB MENU Monitor>Security>Network>Port Security>Switch

✓ **Port Security Switch Status**

**Port Security Port Status  Port 1**

| MAC Address | VLAN ID | State | Time of Addition | Age/Hold |
|---|---|---|---|---|
| c0-18-50-d9-aa-2d | 1 | Blocked | 1970-01-01T09:25:21+09:00 | 85 |
| 70-5d-cc-f2-65-66 | 1 | Forwarding | 1970-01-01T09:20:21+09:00 | - |
| 00-21-6d-00-05-e3 | 1 | Forwarding | 1970-01-01T09:20:21+09:00 | - |
| 00-12-6d-00-06-04 | 1 | Forwarding | 1970-01-01T09:20:21+09:00 | - |
| 64-e5-99-68-23-98 | 1 | Forwarding | 1970-01-01T09:20:21+09:00 | - |

## EXAMPLE CLI MONITOR

✓ **Port Security Switch Status**

```
# show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security port interface GigabitEthernet 1/1

GigabitEthernet 1/1
-------------------
MAC Address       VID  State      Added                     Age/Hold Time
----------------- ---- ---------- ------------------------- -------------
58-86-94-f7-2f-79   1  Blocked    1970-01-01T09:30:21+09:00        171
70-5d-cc-f2-65-66   1  Forwarding 1970-01-01T09:20:21+09:00        N/A
00-21-6d-00-05-e3   1  Forwarding 1970-01-01T09:20:21+09:00        N/A
00-12-6d-00-06-04   1  Forwarding 1970-01-01T09:20:21+09:00        N/A
64-e5-99-68-23-98   1  Forwarding 1970-01-01T09:20:21+09:00        N/A
```

**SOLTECH**
INFONET INC.

## 6.5.5.2. ACL Status

WEB MENU Monitor>Security>Network>ACL Status

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 512 on each switch.

**ACL Status**

| User | ACE | Frame Type | Action | Rate Limiter | Mirror | CPU | Counter | Conflict |
|------|-----|------------|--------|--------------|--------|-----|---------|----------|
| No entries | | | | | | | | |

### ACL Status

| Object | Description |
|--------|-------------|
| **User** | Indicates the ACL user. |
| **ACE** | Indicates the ACE ID on local switch. |
| **Frame Type** | Indicates the frame type of the ACE. <br> **Any** The ACE will match any frame type. <br> **EType** The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. <br> **ARP** The ACE will match ARP/RARP frames. <br> **IPv4** The ACE will match all IPv4 frames. <br> **IPv4/ICMP** The ACE will match IPv4 frames with ICMP protocol. <br> **IPv4/UDP** The ACE will match IPv4 frames with UDP protocol. <br> **IPv4/TCP** The ACE will match IPv4 frames with TCP protocol. <br> **IPv4/Other** The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. <br> **IPv6** The ACE will match all IPv6 standard frames. |
| **Action** | Indicates the forwarding action of the ACE. <br> **Permit** Frames matching the ACE may be forwarded and learned. <br> **Deny** Frames matching the ACE are dropped. <br> **Filter** Frames matching the ACE are filtered. |
| **Rate Limiter** | Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled. |
| **CPU** | Forward packet that matched the specific ACE to CPU. |
| **Counter** | The counter indicates the number of times the ACE was hit by a frame. |
| **Conflict** | Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations. |

**Buttons**

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

Refresh : Click to refresh the page.

 : The select box determines which ACL user is affected by clicking the buttons.

---

## EXAMPLE WEB MONITOR

---

WEB MENU Monitor>Security>Network>ACL Status

**ACL Status**

| User | ACE | Frame Type | Action | Rate Limiter | Mirror | CPU | Counter | Conflict |
|------|-----|-----------|--------|-------------|--------|-----|---------|----------|
| static | 1 | EType | Deny | Disabled | Disabled | No | 4 | No |

---

## EXAMPLE CLI MONITOR

---

✓ **ACL Status**

```
# show access-list ace-status [ static ] [ link-oam ] [ loop-protect ] [ dhcp ] [ arp-
inspection ] [ mep ] [ ipmc ] [ ip-source-guard ] [ conflicts ]
# show access-list ace-status

User
----
S   : static
IPSG: ipSourceGuard
IPMC: ipmc
MEP : mep
ARPI: arpInspection
DHCP: dhcp
LOOP: loopProtect
LOAM: linkOam
?   : S-Ring
User ID   Frame  Action Rate L.  Mirror   CPU    Counter Conflict
---- --   -----  ------ -------- -------- ------ ------- -------
S   1    EType  Deny   Disabled Disabled No        29 No
Switch 1 access-list ace number: 1
```

## 6.5.5.3. ARP Inspection

WEB MENU Monitor>Security>Network>ARP Inspection

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

**Dynamic ARP Inspection Table**

Start from Port 1 ▾ , VLAN 1 , MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

| Port | VLAN ID | MAC Address | IP Address |
|------|---------|-------------|------------|
| No more entries |

**Dynamic ARP Inspection Table**

| Object | Description |
|--------|-------------|
| **Port** | Switch Port Number for which the entries are displayed. |
| **VLAN ID** | VLAN-ID in which the ARP traffic is permitted. |
| **MAC Address** | User MAC address of the entry. |
| **IP Address** | User IP address of the entry. |

**Buttons**

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

Refresh : Refreshes the displayed table starting from the input fields.

Clear : Flushes all dynamic entries.

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

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

## EXAMPLE WEB MONITOR

WEB MENU Monitor>Security>Network>ARP Inspection

**Dynamic ARP Inspection Table**                                    Auto-refresh ☐ Refresh |<< >>

Start from Port 1 ▾ , VLAN 1 , MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

| Port | VLAN ID | MAC Address | IP Address |
|------|---------|-------------|------------|
| No more entries |

## EXAMPLE CLI MONITOR

✓ **Dynamic ARP Inspection Table**

```
# show ip arp inspection entry
```

## 6.5.5.4. IP Source Guard

WEB MENU Monitor>Security>Network>IP Source Guard

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

**Dynamic IP Source Guard Table**

Start from [Port 1 ▼] , VLAN [1] and IP address [0.0.0.0] with [20] entries per page.

| Port | VLAN ID | IP Address | MAC Address |
|------|---------|------------|-------------|
| No more entries | | | |

**Dynamic IP Source Guard Table**

| Object | Description |
|--------|-------------|
| **Port** | Switch Port Number for which the entries are displayed. |
| **VLAN ID** | VLAN-ID in which the IP traffic is permitted. |
| **IP Address** | User IP address of the entry. |
| **MAC Address** | Source MAC address. |

**Buttons**

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

[Refresh] : Refreshes the displayed table starting from the input fields.

[Clear] : Flushes all dynamic entries.

[|<<] : Updates the table starting from the first entry in the Dynamic IP Source Guard Table.

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

---

### EXAMPLE WEB MONITOR

WEB MENU Monitor>Security>Network>IP Source Guard

**Dynamic IP Source Guard Table**

Start from [Port 1 ▼] , VLAN [1] and IP address [0.0.0.0] with [20] entries per page.

| Port | VLAN ID | IP Address | MAC Address |
|------|---------|------------|-------------|
| No more entries | | | |

---

### EXAMPLE CLI MONITOR

---

✓   **Dynamic IP Source Guard Table**

```
# show ip source binding
```

# 6.5.6. AAA Monitor

# 6.5.6.1. RADIUS Overview

WEB MENU Monitor>Security>AAA>RADIUS Overview

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

**RADIUS Server Status Overview**

| # | IP Address | Authentication Port | Authentication Status |
|---|---|---|---|
| 1 | | | Disabled |
| 2 | | | Disabled |
| 3 | | | Disabled |
| 4 | | | Disabled |
| 5 | | | Disabled |

## RADIUS Server Status Overview

| Object | Description |
|---|---|
| **#** | The RADIUS server number. Click to navigate to detailed statistics for this server. |
| **IP Address** | The IP address of this server. |
| **Authentication Port** | UDP port number for authentication. |
| **Authentication Status** | The current status of the server. <br> **Disabled** — The server is disabled. <br> **Not Ready** — The server is enabled, but IP communication is not yet up and running. <br> **Ready** — The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. <br> **Dead (X seconds left)** — Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled. |

**Buttons**

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

Refresh : Click to refresh the page immediately.

## 6.5.6.2. RADIUS Details

WEB MENU Monitor>Security>AAA>RADIUS Details

This page provides detailed statistics for a particular RADIUS server.

**RADIUS Authentication Statistics for Server #1**

| Receive Packets | | Transmit Packets | |
|---|---|---|---|
| Access Accepts | 0 | Access Requests | 0 |
| Access Rejects | 0 | Access Retransmissions | 0 |
| Access Challenges | 0 | Pending Requests | 0 |
| Malformed Access Responses | 0 | Timeouts | 0 |
| Bad Authenticators | 0 | | |
| Unknown Types | 0 | | |
| Packets Dropped | 0 | | |
| **Other Info** | | | |
| IP Address | | | |
| State | | | Disabled |
| Round-Trip Time | | | 0 ms |

### RADIUS Authentication Statistics for Server #n

| Object | Description |
|---|---|
| **RADIUS Authentication Statistics** | The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.<br>Use the server select box to switch between the backend servers to show details for. |
| **Packet Counters** | RADIUS authentication server packet counter. There are seven receive and four transmit counters. |
| | **Access Accepts** — The number of RADIUS Access-Accept packets (valid or invalid) received from the server. |
| | **Access Rejects** — The number of RADIUS Access-Reject packets (valid or invalid) received from the server. |
| | **Access Challenges** — The number of RADIUS Access-Challenge packets (valid or invalid) received from the server. |
| | **Malformed Access Responses** — The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses. |
| | **Bad Authenticators** — The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server. |
| | **Unknown Types** — The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped. |
| | **Packets Dropped** — The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason. |
| | **Access Requests** — The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions. |
| | **Access Retransmissions** — The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server. |
| | **Pending Requests** — The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission. |
| | **Timeouts** — The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout. |

| **Other Info** | This section contains information about the state of the server and the latest round-trip time. | |
| --- | --- | --- |
| | **IP Address** | IP address and UDP port for the authentication server in question. |
| | **State** | The number of RADIUS Access-Reject packets (valid or invalid) received from the server. |
| | **Round-Trip Time** | The number of RADIUS Access-Challenge packets (valid or invalid) received from the server. |

**Buttons**

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

Refresh : Click to refresh the page immediately.

Clear : Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

# 6.6. Aggregation

## 6.6.1. Static Configuration

WEB MENU Configuration>Aggregation>Static

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



### Aggregation Mode Configuration

#### Hash Code Contributors

| Object | Description |
|---|---|
| Source MAC Address | The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled. |
| Destination MAC Address | The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled. |
| IP Address | The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled. |
| TCP/UDP Port Number | The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled. |

### Aggregation Group Configuration

| Object | Description |
|---|---|
| Group ID | Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port. |
| Port Members | Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group. |

#### Buttons

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>Aggregation>Static

✓ **Aggregation Mode Configuration**

➢ *Hash Code Contributors*

• *Source MAC Address(Check)*

• *Destination MAC Address(Uncheck)*

• *IP Address(Check)*

• *TCP/UDP Port Number(Check)*

**Aggregation Mode Configuration**

| Hash Code Contributors | |
|---|---|
| Source MAC Address | ☑ |
| Destination MAC Address | ☐ |
| IP Address | ☑ |
| TCP/UDP Port Number | ☑ |

✓ **Aggregation Group Configuration**

➢ *Group ID*

➢ *Port Members*

**Aggregation Group Configuration**

| Group ID | Port Members | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Normal | ○ | ○ | ○ | ○ | ● | ● | ● | ● |
| 1 | ● | ● | ○ | ○ | ○ | ○ | ○ | ○ |
| 2 | ○ | ○ | ● | ● | ○ | ○ | ○ | ○ |
| 3 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| 4 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

## EXAMPLE CLI CONFIGURATION

✓ **Aggregation Mode Configuration**

    ➢ *Hash Code Contributors*

        • *Source MAC Address(Check)*

        • *Destination MAC Address(Uncheck)*

        • *IP Address(Check)*

        • *TCP/UDP Port Number(Check)*

```
(config)# aggregation mode { [ smac ] [ dmac ] [ ip ] [ port ] }*1
(config)# aggregation mode smac ip port
```

✓ **Aggregation Group Configuration**

    ➢ *Group ID*

    ➢ *Port Members*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1-2
(config)# interface GigabitEthernet 1/3-4

(config-if)# aggregation group <v_uint>
(config-if)# aggregation group 1
(config-if)# aggregation group 2
```

# 6.6.2. LACP Configuration

WEB MENU Configuration>Aggregation>LACP

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

**LACP Port Configuration**

| Port | LACP Enabled | Key | | Role | Timeout | Prio |
|------|------|------|------|------|------|------|
| * | ☐ | <> | | <> | <> | 32768 |
| 1 | ☐ | Auto | | Active | Fast | 32768 |
| 2 | ☐ | Auto | | Active | Fast | 32768 |
| 3 | ☐ | Auto | | Active | Fast | 32768 |
| 4 | ☐ | Auto | | Active | Fast | 32768 |
| 5 | ☐ | Auto | | Active | Fast | 32768 |
| 6 | ☐ | Auto | | Active | Fast | 32768 |
| 7 | ☐ | Auto | | Active | Fast | 32768 |
| 8 | ☐ | Auto | | Active | Fast | 32768 |

## LACP Port Configuration

| Object | Description |
|--------|-------------|
| **Port** | The switch port number. |
| **LACP Enabled** | Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner. |
| **Key** | The Key value incurred by the port, range 1-65535 . The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot. |
| **Role** | The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to). |
| **Timeout** | The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet. |
| **Prio** | The Prio controls the priority of the port, range 1-65535. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

# EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>Aggregation>LACP

✓ **LACP Port Configuration**

➢ *LACP Enable*

• *Enable(1~2 Port)*

**LACP Port Configuration**

| Port | LACP Enabled | Key | | Role | Timeout | Prio |
|------|------|------|------|------|------|------|
| * | ☐ | <> | | <> | <> | 32768 |
| 1 | ☑ | Auto | | Active | Fast | 32768 |
| 2 | ☑ | Auto | | Active | Fast | 32768 |
| 3 | ☐ | Auto | | Active | Fast | 32768 |
| 4 | ☐ | Auto | | Active | Fast | 32768 |
| 5 | ☐ | Auto | | Active | Fast | 32768 |
| 6 | ☐ | Auto | | Active | Fast | 32768 |
| 7 | ☐ | Auto | | Active | Fast | 32768 |
| 8 | ☐ | Auto | | Active | Fast | 32768 |

➢ *Key*

• *Auto | Specific(1~65535)*

**LACP Port Configuration**

| Port | LACP Enabled | Key | | Role | Timeout | Prio |
|------|------|------|------|------|------|------|
| * | ☐ | <> | | <> | <> | 32768 |
| 1 | ☑ | Auto | | Active | Fast | 32768 |
| 2 | ☑ | Auto / Specific | | Active | Fast | 32768 |
| 3 | ☐ | Auto | | Active | Fast | 32768 |
| 4 | ☐ | Auto | | Active | Fast | 32768 |
| 5 | ☐ | Auto | | Active | Fast | 32768 |
| 6 | ☐ | Auto | | Active | Fast | 32768 |
| 7 | ☐ | Auto | | Active | Fast | 32768 |
| 8 | ☐ | Auto | | Active | Fast | 32768 |

**LACP Port Configuration**

| Port | LACP Enabled | Key | | Role | Timeout | Prio |
|------|------|------|------|------|------|------|
| * | ☐ | <> | | <> | <> | 32768 |
| 1 | ☑ | Specific | 65535 | Active | Fast | 32768 |
| 2 | ☑ | Specific | 65535 | Active | Fast | 32768 |
| 3 | ☐ | Auto | | Active | Fast | 32768 |
| 4 | ☐ | Auto | | Active | Fast | 32768 |
| 5 | ☐ | Auto | | Active | Fast | 32768 |
| 6 | ☐ | Auto | | Active | Fast | 32768 |
| 7 | ☐ | Auto | | Active | Fast | 32768 |
| 8 | ☐ | Auto | | Active | Fast | 32768 |

SOLTECH
INFONET INC.

➢ **Role**

- **Active | Passive**

**LACP Port Configuration**

| Port | LACP Enabled | Key | | Role | Timeout | Prio |
|------|-------------|------|------|------|---------|------|
| * | ☐ | <> | | <> | <> | 32768 |
| 1 | ☑ | Specific | 65535 | Active | Fast | 32768 |
| 2 | ☑ | Specific | 65535 | Passive | Fast | 32768 |
| 3 | ☐ | Auto | | Active | Fast | 32768 |
| 4 | ☐ | Auto | | Active | Fast | 32768 |
| 5 | ☐ | Auto | | Active | Fast | 32768 |
| 6 | ☐ | Auto | | Active | Fast | 32768 |
| 7 | ☐ | Auto | | Active | Fast | 32768 |
| 8 | ☐ | Auto | | Active | Fast | 32768 |

➢ **Timeout**

- **Fast | Slow**

**LACP Port Configuration**

| Port | LACP Enabled | Key | | Role | Timeout | Prio |
|------|-------------|------|------|------|---------|------|
| * | ☐ | <> | | <> | <> | 32768 |
| 1 | ☑ | Specific | 65535 | Active | Fast | 32768 |
| 2 | ☑ | Specific | 65535 | Active | Fast / Slow | 32768 |
| 3 | ☐ | Auto | | Active | | 32768 |
| 4 | ☐ | Auto | | Active | Fast | 32768 |
| 5 | ☐ | Auto | | Active | Fast | 32768 |
| 6 | ☐ | Auto | | Active | Fast | 32768 |
| 7 | ☐ | Auto | | Active | Fast | 32768 |
| 8 | ☐ | Auto | | Active | Fast | 32768 |

➢ **Prio**

- **1~65535**

**LACP Port Configuration**

| Port | LACP Enabled | Key | | Role | Timeout | Prio |
|------|-------------|------|------|------|---------|------|
| * | ☑ | <> | 65535 | <> | <> | 1 |
| 1 | ☑ | Specific | 65535 | Active | Fast | 1 |
| 2 | ☑ | Specific | 65535 | Active | Fast | 65535 |
| 3 | ☐ | Auto | | Active | Fast | 32768 |
| 4 | ☐ | Auto | | Active | Fast | 32768 |
| 5 | ☐ | Auto | | Active | Fast | 32768 |
| 6 | ☐ | Auto | | Active | Fast | 32768 |
| 7 | ☐ | Auto | | Active | Fast | 32768 |
| 8 | ☐ | Auto | | Active | Fast | 32768 |

**SOLTECH**
INFONET INC.

## EXAMPLE CLI CONFIGURATION

✓  **LACP Port Configuration**

  ➢  *LACP Enable*

   •  *Enable(1~2 Port)*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1-2

(config-if)# lacp
```

  ➢  *Key*

   •  *Auto | Specific(1~65535)*

```
(config-if)# lacp key { <v_1_to_65535> | auto }
(config-if)# lacp key auto
(config-if)# lacp key 65535
```

  ➢  *Role*

   •  *Active | Passive*

```
(config-if)# lacp role { active | passive }
(config-if)# lacp role active
(config-if)# lacp role passive
```

  ➢  *Timeout*

   •  *Fast | Slow*

```
(config-if)# lacp timeout { fast | slow }
(config-if)# lacp timeout fast
(config-if)# lacp timeout slow
```

  ➢  *Prio*

   •  *1~65535*

```
(config-if)# lacp port-priority <v_1_to_65535>
(config-if)# lacp port-priority 1
(config-if)# lacp port-priority 65535
```

# 6.6.3. Static Monitor

WEB MENU Monitor>Aggregation>Static

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

**Aggregation Status**

| Aggr ID | Name | Type | Speed | Configured Ports | Aggregated Ports |
|---------|------|------|-------|------------------|------------------|
| No aggregation groups | | | | | |

### Aggregation Status

| Object | Description |
|--------|-------------|
| **Aggr ID** | The Aggregation ID associated with this aggregation instance. |
| **Name** | Name of the Aggregation group ID. |
| **Type** | Type of the Aggregation group(Static or LACP). |
| **Speed** | Speed of the Aggregation group. |
| **Configured ports** | Configured member ports of the Aggregation group. |
| **Aggregated ports** | Aggregated member ports of the Aggregation group. |

**Buttons**

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

Refresh : Click to refresh the page immediately.

---

## EXAMPLE WEB MONITOR

WEB MENU Monitor>Aggregation>Static

**Aggregation Status**

| Aggr ID | Name | Type | Speed | Configured Ports | Aggregated Ports |
|---------|------|------|-------|------------------|------------------|
| 1 | LLAG1 | Static | 1G | GigabitEthernet 1/1-2 | none |
| 2 | LLAG2 | Static | Undefined | GigabitEthernet 1/3-4 | none |

---

## EXAMPLE CLI MONITOR

✓ **Aggregation Status**

```
# show aggregation
# Aggr ID  Name    Type    Speed   Configured Ports   Aggregated Ports
-------  ------  ------  --------  -------------------------------------------------------------------
  1       LLAG1   Static  1G        GigabitEthernet 1/1-2    none
  2       LLAG2   Static  Undefined GigabitEthernet 1/3-4    none
```

# 6.6.4. LACP Monitor

## 6.6.4.1. System Status

WEB MENU Monitor>Aggregation>LACP>System Status

This page provides a status overview for all LACP instances.

**LACP System Status**

| Aggr ID | Partner System ID | Partner Key | Partner Prio | Last Changed | Local Ports |
|---------|-------------------|-------------|--------------|--------------|-------------|
| *No ports enabled or no existing partners* | | | | | |

### LACP System Status

| Object | Description |
|--------|-------------|
| **Aggr ID** | The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id' |
| **Partner System ID** | The system ID (MAC address) of the aggregation partner. |
| **Partner Key** | The Key that the partner has assigned to this aggregation ID. |
| **Partner Prio** | The priority assigned to the Aggregation ID partner. |
| **Last changed** | The time since this aggregation changed. |
| **Local Ports** | Shows which ports are a part of this aggregation for this switch. |

**Buttons**

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

Refresh : Click to refresh the page immediately.

## EXAMPLE WEB MONITOR

WEB MENU Monitor>Aggregation>LACP>System Status

**LACP System Status**

| Aggr ID | Partner System ID | Partner Key | Partner Prio | Last Changed | Local Ports |
|---------|-------------------|-------------|--------------|--------------|-------------|
| LLAG1 | 00-21-6d-00-00-00 | 3 | 32768 | 0d 00:28:57 | 1,2 |

## EXAMPLE CLI MONITOR

✓ **LACP System Status**

```
# show lacp neighbor
Aggr ID  Partner System ID  Partner Prio  Partner Key  Last Changed
-------  -----------------  ------------  -----------  ------------
1        00:21:6d:00:00:00  32768         3            00:35:08
Port                State    Key    Aggr ID  Partner Port  Partner Port Prio
------------------  -------- -----  -------  ------------  -----------------
Gi 1/1              enabled  3      1        1             32768
Gi 1/2              enabled  3      1        2             32768
```

## 6.6.4.2. Port Status

WEB MENU Monitor>Aggregation>LACP>Port Status

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

**LACP Status**

| Port | LACP | Key | Aggr ID | Partner System ID | Partner Port | Partner Prio |
|------|------|-----|---------|-------------------|--------------|--------------|
| 1 | No | - | - | - | - | - |
| 2 | No | - | - | - | - | - |
| 3 | No | - | - | - | - | - |
| 4 | No | - | - | - | - | - |
| 5 | No | - | - | - | - | - |
| 6 | No | - | - | - | - | - |
| 7 | No | - | - | - | - | - |
| 8 | No | - | - | - | - | - |

### LACP Status

| Object | Description |
|--------|-------------|
| **Port** | The switch port number. |
| **LACP** | 'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled. |
| **Key** | The key assigned to this port. Only ports with the same key can aggregate together. |
| **Aggr ID** | The Aggregation ID assigned to this aggregation group. |
| **Partner System ID** | The partner's System ID (MAC address). |
| **Partner Port** | The partner's port number connected to this port. |
| **Partner Prio** | The partner's port priority. |

**Buttons**

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

[ Refresh ] : Click to refresh the page immediately.

### EXAMPLE WEB MONITOR

WEB MENU Monitor>Aggregation>LACP>Port Status

**LACP Status**

| Port | LACP | Key | Aggr ID | Partner System ID | Partner Port | Partner Prio |
|------|------|-----|---------|-------------------|--------------|--------------|
| 1 | Yes | 3 | LLAG1 | 00-12-6d-00-06-a9 | 1 | 32768 |
| 2 | Yes | 3 | LLAG1 | 00-12-6d-00-06-a9 | 2 | 32768 |
| 3 | No | - | - | - | - | - |
| 4 | No | - | - | - | - | - |
| 5 | No | - | - | - | - | - |
| 6 | No | - | - | - | - | - |
| 7 | No | - | - | - | - | - |
| 8 | No | - | - | - | - | - |

**SOLTECH**
INFONET INC.

EXAMPLE CLI MONITOR

✓ **LACP Status**

```
# show lacp neighbor
Aggr ID  Partner System ID  Partner Prio  Partner Key  Last Changed
-------  -----------------  ------------  -----------  ------------
1        00:21:6d:00:00:00  32768         3            00:35:08
Port                State     Key    Aggr ID  Partner Port  Partner Port Prio
------------------  --------  -----  -------  ------------  -----------------
Gi 1/1              enabled   3      1        1             32768
Gi 1/2              enabled   3      1        2             32768
```

# 6.6.4.3. Port Statistics

WEB MENU Monitor>Aggregation>LACP>Port Statistics

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

**LACP Statistics**

| Port | LACP Received | LACP Transmitted | Discarded | |
|------|---------------|------------------|-----------|------|
|      |               |                  | Unknown | Illegal |
| 1 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 |

**LACP Statistics**

| Object | Description |
|--------|-------------|
| **Port** | The switch port number. |
| **LACP Received** | Shows how many LACP frames have been received at each port. |
| **LACP Transmitted** | Shows how many LACP frames have been sent from each port. |
| **Discarded** | Shows how many unknown or illegal LACP frames have been discarded at each port. |

**Buttons**

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

Refresh : Click to refresh the page immediately.

Clear : Clear all statistics.

WEB MENU Monitor>Aggregation>LACP>Port Statistics

SOLTECH
INFONET INC.

**LACP Statistics**

| Port | LACP Received | LACP Transmitted | Discarded | |
|------|---------------|------------------|-----------|---|
| | | | Unknown | Illegal |
| 1 | 113 | 113 | 0 | 0 |
| 2 | 114 | 113 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 |

## EXAMPLE CLI MONITOR

✓ **LACP Statistics**

```
# show lacp statistics

Port                 Rx Frames  Tx Frames  Rx Unknown  Rx Illegal
-------------------- ---------- ---------- ---------- ----------
Gi 1/1               491        491        0           0
Gi 1/2               491        491        0           0
```

# 6.7. Loop Protection

## 6.7.1. Loop Protection Configuration

WEB MENU Configuration>Loop protection

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



**Loop Protection Configuration**

**General Settings**

**Global Configuration**

| Object | Description |
|---|---|
| **Enable Loop Protection** | Controls whether loop protections is enabled (as a whole). |
| **Transmission Time** | The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds. Default value is 5 seconds. |
| **Shutdown Time** | The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart). Default value is 180 seconds. |

**Port Configuration**

| Object | Description |
|---|---|
| **Port** | The switch port number of the port. |
| **Enable** | Controls whether loop protection is enabled on this switch port. |
| **Action** | Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log or Log Only. |

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

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>Loop protection

&#10003; **General Settings**

&#10003; **Global Configuration**

&#10148; *Enable Loop Protection*

&bull; *Disable | Enable*



&#10148; *Transmission Time*

&bull; *5sec (1~10)*

&#10148; *Shutdown Time*

&bull; *180sec (0~604800)*



&#10003; **Port Configuration**

&#10148; *Enable*

&bull; *Enable(default) | Disable*

➢   **Action**

•   **Shudown Port(default) | Shutdown Port and Log | Log Only**



➢   **Tx Mode**

•   **Enable(default) | Disable**

## EXAMPLE CLI CONFIGURATION

✓ **General Settings**

✓ **Global Configuration**

➢ *Enable Loop Protection*

• *Disable | Enable*

```
(config)# no loop-protect
(config)# loop-protect
```

➢ *Transmission Time*

• *5sec (1~10)*

```
(config)# loop-protect transmit-time <t>
(config)# loop-protect transmit-time 5
```

➢ *Shutdown Time*

• *180sec (0~604800)*

```
(config)# loop-protect shutdown-time <t>
(config)# loop-protect shutdown-time 180
```

✓ **Port Configuration**

➢ *Enable*

• *Enable(default) | Disable*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/3

(config-if)# loop-protect
(config-if)# no loop-protect
```

➢ *Action*

• *Shudown Port(default) | Shutdown Port and Log | Log Only*

```
(config-if)# loop-protect action { [ shutdown ] [ log ] }*1
(config-if)# loop-protect action shutdown
(config-if)# loop-protect action shutdown log
(config-if)# loop-protect action log
```

➢ *Tx Mode*

• *Enable(default) | Disable*

```
(config-if)# loop-protect tx-mode
(config-if)# no loop-protect tx-mode
```

# 6.7.2. Loop Protection Monitor

WEB MENU Configuration>Loop Protection

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

**Loop Protection Status**

| Port | Action | Transmit | Loops | Status | Loop | Time of Last Loop |
|------|--------|----------|-------|--------|------|-------------------|
| 1 | Shutdown | Enabled | 0 | Up | - | - |
| 2 | Shutdown | Enabled | 0 | Down | - | - |
| 3 | Shutdown | Enabled | 0 | Up | - | - |
| 4 | Shutdown | Enabled | 0 | Down | - | - |
| 5 | Shutdown | Enabled | 0 | Down | - | - |
| 6 | Shutdown | Enabled | 0 | Down | - | - |
| 7 | Shutdown | Enabled | 0 | Down | - | - |
| 8 | Shutdown | Enabled | 0 | Down | - | - |

## Loop Protection Status

| Object | Description |
|--------|-------------|
| **Port** | The switch port number of the logical port. |
| **Action** | The currently configured port action. |
| **Transmit** | The currently configured port transmit mode. |
| **Loops** | The number of loops detected on this port. |
| **Status** | The current loop protection status of the port. |
| **Loop** | Whether a loop is currently detected on the port. |
| **Time of Last Loop** | The time of the last loop event detected. |

**Buttons**

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

Refresh : Click to refresh the page immediately.

## EXAMPLE WEB MONITOR

WEB MENU Configuration>Loop Protection

**Loop Protection Status**

| Port | Action | Transmit | Loops | Status | Loop | Time of Last Loop |
|------|--------|----------|-------|--------|------|-------------------|
| 1 | Shutdown | Enabled | 5 | Down | - | 1970-01-07T14:20:22+09:00 |
| 2 | Shutdown | Enabled | 17 | Down | - | 1970-01-07T14:17:30+09:00 |
| 3 | Shutdown | Enabled | 11 | Up | - | 1970-01-07T14:22:55+09:00 |
| 4 | Shutdown | Enabled | 4 | Down | - | 1970-01-07T14:14:20+09:00 |
| 5 | Shutdown | Enabled | 1 | Down | - | 1970-01-07T14:15:43+09:00 |
| 6 | Shutdown | Enabled | 1 | Down | - | 1970-01-07T14:18:41+09:00 |
| 7 | Shutdown | Enabled | 2 | Down | - | 1970-01-07T14:20:07+09:00 |
| 8 | Shutdown | Enabled | 3 | Down | - | 1970-01-07T14:19:49+09:00 |

SOLTECH
INFONET INC.

## EXAMPLE CLI MONITOR

✓ **Loop Protection Status**

```
# show loop-protect interface *
Loop Protection Configuration
======================================
Loop Protection   : Enable
Transmission Time : 5 sec
Shutdown Time     : 180 sec


GigabitEthernet 1/1
-----------------------------
    Loop protect mode is enabled.
    Action is shutdown.
    Transmit mode is enabled.
    No loop.
    The number of loops is 5.
    Time of last loop is at 1970-01-07T14:20:22+09:00
    Status is down.


GigabitEthernet 1/2
-----------------------------
    Loop protect mode is enabled.
    Action is shutdown.
    Transmit mode is enabled.
    No loop.
    The number of loops is 17.
    Time of last loop is at 1970-01-07T14:17:30+09:00
    Status is down.

......
```

# 6.8. Spanning Tree

## 6.8.1. Spanning Tree Configuration

### 6.8.1.1. Bridge Setting

WEB MENU Configuration>Spanning Tree>Bridge Setting

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



**STP Bridge Configuration**

**Basic Settings**

| Object | Description |
|---|---|
| **Protocol Version** | The MSTP / RSTP / STP protocol version setting. Valid values are STP, RSTP and MSTP. |
| **Bridge Priority** | Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge. |
| **Hello Time** | The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds, default is 2 seconds. Note: Changing this parameter from the default value is not recommended, and may have adverse effects on your network. |
| **Forward Delay** | The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds. |
| **Max Age** | The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, *and* Max Age must be <= (FwdDelay-1)*2. |
| **Maximum Hop Count** | This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops. |
| **Transmit Hold Count** | The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second. |

**Advanced Settings**

| Object | Description |
|---|---|
| **Edge Port BPDU** | Control whether a port explicitly configured as Edge will transmit and receive BPDUs. |

| Filtering | |
|---|---|
| Edge Port BPDU Guard | Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology. |
| Port Error Recovery | Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot. |
| Port Error Recovery Timeout | The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours). |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>Spanning Tree>Bridge Setting

✓ **STP Bridge Configuration**

➢ *Basic Settings*

• *Protocol Version (STP | RSTP | MSTP)*



• *Bridge Priority (Default 32768)*



• *Hello Time(Default 2, 1~10)*

- *Forward Delay(Default 15, 4~30sec)*

- *Max Age (Default 20, 6~40sec)*

- *Maximum Hop Count(Default 20, 6~40sec)*

- *Transmit Hold Count(Default 6, 1~10sec)*

| Basic Settings | |
| --- | --- |
| Protocol Version | MSTP |
| Bridge Priority | 32768 |
| Hello Time | 2 |
| Forward Delay | 15 |
| Max Age | 20 |
| Maximum Hop Count | 20 |
| Transmit Hold Count | 6 |

➢ *Advanced Settings*

- *Edge Port BPDU Filtering*

- *Edge Port BPDU Guard*

- *Port Error Recovery (30-86400)*

| Advanced Settings | |
| --- | --- |
| Edge Port BPDU Filtering | ☐ |
| Edge Port BPDU Guard | ☐ |
| Port Error Recovery | ☐ |
| Port Error Recovery Timeout | |

---

## EXAMPLE CLI CONFIGURATION

---

✓ **STP Bridge Configuration**

  ➢ *Basic Settings*

    - *Protocol Version(STP | RSTP | MSTP)*

```
(config)# spanning-tree mode {stp | rstp | mstp}
(config)# spanning-tree mode stp
```

    - *Bridge Priority(Default 32768)*

```
(config)# spanning-tree mst <instance> priority <prio>
(config)# spanning-tree mst 0 priority 32768
```

    - *Hello Time(Default 2, 1~10)*

```
(config)# spanning-tree mst hello-time <hellotime>
(config)# spanning-tree mst hello-time 2
```

    - *Forward Delay(Default 15, 4~30sec)*

```
(config)# spanning-tree mst forward-time <fwdtime>
(config)# spanning-tree mst forward-time 15
```

- • **Max Age (Default 20, 6~40sec)**

```
(config)# spanning-tree mst max-age <maxage>
(config)# spanning-tree mst max-age 20
```

- • **Maximum Hop Count(Default 20, 6~40sec)**

```
(config)# spanning-tree mst max-hops <maxhops>
(config)# spanning-tree mst max-hops 20
```

- • **Transmit Hold Count(Default 6, 1~10sec)**

```
(config)# spanning-tree transmit hold-count <holdcount>
(config)# spanning-tree transmit hold-count 6
```

➢ **Advanced Settings**

- • **Edge Port BPDU Filtering**

```
(config)# spanning-tree edge bpdu-filter
```

- • **Edge Port BPDU Guard**

```
(config)# spanning-tree edge bpdu-guard
```

- • **Port Error Recovery (30-86400)**

```
(config)# spanning-tree recovery interval <interval>
```

## 6.8.1.2. MSTI Mapping

WEB MENU Configuration>Spanning Tree>MSTI Mapping

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

**MSTI Configuration**

Add VLANs separated by spaces or comma.

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

Configuration Identification

| Configuration Name | 00-21-6d-00-00-00 |
| Configuration Revision | 0 |

MSTI Mapping

| MSTI | VLANs Mapped |
|---|---|
| MSTI1 | |
| MSTI2 | |
| MSTI3 | |
| MSTI4 | |
| MSTI5 | |
| MSTI6 | |
| MSTI7 | |

### MSTI Configuration

### Configuration Identification

| Object | Description |
|---|---|
| **Configuration Identification** | Configuration Identification refers to a value used to identify changes in the MSTP (Multiple Spanning Tree Protocol) configuration. |
| **Configuration Name** | The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters. |
| **Configuration Revision** | The revision of the MSTI configuration named above. This must be an integer between 0 and 65535. |

### MSTI Mapping

| Object | Description |
|---|---|
| **MSTI Mapping** | MSTI Mapping refers to the process of defining the mapping between VLANs (Virtual LANs) and MSTIs (Multiple Spanning Tree Instances) in the context of MSTP (Multiple Spanning Tree Protocol). |
| **MSTI** | The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. |
| **VLANs Mapped** | The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

## EXAMPLE WEB CONFIGURATION

✓ **MSTI Configuration**

➢ *Configuration Identification*

• *Configuration Name*

| Configuration Identification | |
|---|---|
| Configuration Name | MSTP1 |
| Configuration Revision | 0 |

• *Configuration Revision(0~65535)*

| Configuration Identification | |
|---|---|
| Configuration Name | MSTP1 |
| Configuration Revision | 65535 |

➢ *MSTI Mapping*

• *VLANs Mapped*

| MSTI | VLANs Mapped |
|---|---|
| MSTI1 | 1-10,4094 |
| MSTI2 | |
| MSTI3 | |
| MSTI4 | |
| MSTI5 | |
| MSTI6 | |
| MSTI7 | |

## EXAMPLE CLI CONFIGURATION

✓ **MSTI Configuration**

➢ *Configuration Identification*

SOLTECH
INFONET INC.

- *   **Configuration Name | Revision(0~65535)**

```
(config)# spanning-tree mst name <name> revision <v_0_to_65535>
(config)# spanning-tree mst name MSTP1 revision 65535
```

➢  **MSTI Mapping**

- *   **VLANs Mapped**

```
(config)# spanning-tree mst <instance> vlan <v_vlan_list>
(config)# spanning-tree mst 1 vlan 1-10,4094
```

## 6.8.1.3. MSTI Priorities

WEB MENU Configuration>Spanning Tree>MSTI Priorities

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

**MSTI Configuration**

**MSTI Priority Configuration**

| MSTI | Priority |
|------|----------|
| * | <> |
| CIST | 32768 |
| MSTI1 | 32768 |
| MSTI2 | 32768 |
| MSTI3 | 32768 |
| MSTI4 | 32768 |
| MSTI5 | 32768 |
| MSTI6 | 32768 |
| MSTI7 | 32768 |

**MSTI Configuration**

**MSTI Priority Configuration**

| Object | Description |
|--------|-------------|
| **MSTI** | The bridge instance. The CIST is the *default* instance, which is always active. |
| **Priority** | Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a *Bridge Identifier*. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

### EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>Spanning Tree>MSTI Priorities

✓ **MSTI Configuration**

➢ *MSTI Priority Configuration*

• *MSTI(0-7)*

• *Priority(Default 32768)*

SOLTECH
INFONET INC.

MSTI Configuration

---

## EXAMPLE CLI CONFIGURATION

---

✓ **MSTI Configuration**

➢ *MSTI Priority Configuration*

• *MSTI(0-7)*

• *Priority(Default 32768)*

```
(config)# spanning-tree mst <instance> priority <prio>
(config)# spanning-tree mst 1 priority 0
(config)# spanning-tree mst 1 priority 61440
```

## 6.8.1.4. CIST Ports

WEB MENU Configuration>Spanning Tree>CIST Ports

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well. This page contains settings for physical and aggregated ports.

**CIST Aggregated Port Configuration**

| Port | STP Enabled | Path Cost | Priority | Admin Edge | Auto Edge | Restricted Role | Restricted TCN | BPDU Guard | Point-to-point |
|------|-------------|-----------|----------|------------|-----------|------|-----|------------|----------------|
| - | ☐ | Auto ▾ | 128 ▾ | Non-Edge ▾ | ☐ | ☐ | ☐ | ☐ | Forced True ▾ |

**CIST Normal Port Configuration**

| Port | STP Enabled | Path Cost | Priority | Admin Edge | Auto Edge | Restricted Role | Restricted TCN | BPDU Guard | Point-to-point |
|------|-------------|-----------|----------|------------|-----------|------|-----|------------|----------------|
| * | ☐ | <> ▾ | <> ▾ | <> ▾ | ☐ | ☐ | ☐ | ☐ | <> ▾ |
| 1 | ☐ | Auto ▾ | 128 ▾ | Non-Edge ▾ | ☐ | ☐ | ☐ | ☐ | Auto ▾ |
| 2 | ☐ | Auto ▾ | 128 ▾ | Non-Edge ▾ | ☐ | ☐ | ☐ | ☐ | Auto ▾ |
| 3 | ☐ | Auto ▾ | 128 ▾ | Non-Edge ▾ | ☐ | ☐ | ☐ | ☐ | Auto ▾ |
| 4 | ☐ | Auto ▾ | 128 ▾ | Non-Edge ▾ | ☐ | ☐ | ☐ | ☐ | Auto ▾ |
| 5 | ☐ | Auto ▾ | 128 ▾ | Non-Edge ▾ | ☐ | ☐ | ☐ | ☐ | Auto ▾ |
| 6 | ☐ | Auto ▾ | 128 ▾ | Non-Edge ▾ | ☐ | ☐ | ☐ | ☐ | Auto ▾ |
| 7 | ☐ | Auto ▾ | 128 ▾ | Non-Edge ▾ | ☐ | ☐ | ☐ | ☐ | Auto ▾ |
| 8 | ☐ | Auto ▾ | 128 ▾ | Non-Edge ▾ | ☐ | ☐ | ☐ | ☐ | Auto ▾ |

**STP CIST Port Configuration**

**CIST Aggregated Port Configuration**

**CIST Normal Port Configuration**

| Object | Description |
|--------|-------------|
| **Port** | The switch port number of the logical STP port. |
| **STP Enabled** | Controls whether STP is enabled on this switch port. |
| **Path Cost** | Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000. |
| **Priority** | Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). |
| **operEdge (state flag)** | Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status. |
| **AdminEdge** | Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized) |
| **AutoEdge** | Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not. |
| **Restricted Role** | If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard. |

SOLTECH
INFONET INC.

| | |
|---|---|
| **Restricted TCN** | If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently. |
| **BPDU Guard** | If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well. |
| **Point-to-Point** | Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>Spanning Tree>CIST Ports

✓ **CIST Aggregated Port Configuration**

✓ **CIST Normal Port Configuration**

➢ *STP Enabled*

• *Enable | Disable*



➢ *Path Cost*

• *Auto | Specific(1~200,000,000)*

➢ **Priority**

• *0|16|32|48|64|80|96|112|128|144|160|176|192|208|224|240*



➢ **Admin Edge**

• *Non-Edge | Edge*



➢ **Auto Edge**

• *Enable | Disable*



➢ **Restricted Role**

• *Enable | Disable*



➢ **Restricted TCN**

• *Enable | Disable*

> ➢ **BPDU Guard**

- **Enable | Disable**

**CIST Aggregated Port Configuration**

| Port | STP Enabled | Path Cost | | Priority | Admin Edge | Auto Edge | Restricted Role | TCN | BPDU Guard | Point-to-point |
|------|-------------|-----------|---|----------|------------|-----------|-----------------|-----|------------|----------------|
| - | ☑ | Auto ▾ | | 128 ▾ | Non-Edge ▾ | ☑ | ☐ | ☐ | ☑ | Forced True ▾ |

> ➢ **Point-to-Point**

- **Forced True | Forced False | Auto**

**CIST Aggregated Port Configuration**

| Port | STP Enabled | Path Cost | | Priority | Admin Edge | Auto Edge | Restricted Role | TCN | BPDU Guard | Point-to-point |
|------|-------------|-----------|---|----------|------------|-----------|-----------------|-----|------------|----------------|
| - | ☑ | Auto ▾ | | 128 ▾ | Non-Edge ▾ | ☑ | ☐ | ☐ | ☐ | Forced True ▾ |

Forced True
Forced False
Auto

**CIST Normal Port Configuration**

---

# EXAMPLE CLI CONFIGURATION

---

✓ **CIST Aggregated Port Configuration**

✓ **CIST Normal Port Configuration**

> ➢ **STP Enabled**

- **Enable | Disable**

```
(config)# spanning-tree aggregation

(config-stp-aggr)# spanning-tree

(config-stp-aggr)# no spanning-tree

(config)# interface ( <port_type> [ <plist> ] )
(config)# interface *

(config-if)# spanning-tree

(config-if)# no spanning-tree
```

> ➢ **Path Cost**

- **Auto | Specific(1~200,000,000)**

```
(config-stp-aggr)# spanning-tree mst 0 cost { <cost> | auto }
(config-stp-aggr)# spanning-tree mst 0 cost auto
(config-stp-aggr)# spanning-tree mst 0 cost 200000000

(config-if)# spanning-tree mst 0 cost { <cost> | auto }
(config-if)# spanning-tree mst 0 cost auto
(config-if)# spanning-tree mst 0 cost 200000000
```

> ➢ *Priority*

> • *0|16|32|48|64|80|96|112|128|144|160|176|192|208|224|240*

```
(config-stp-aggr)# spanning-tree mst 0 port-priority <prio>
(config-stp-aggr)# spanning-tree mst 0 port-priority 128

(config-if)# spanning-tree mst 0 port-priority <prio>
(config-if)# spanning-tree mst 0 port-priority 128
```

> ➢ *Admin Edge*

> • *Non-Edge | Edge*

```
(config-stp-aggr)# no spanning-tree edge

(config-stp-aggr)# spanning-tree edge

(config-if)# no spanning-tree edge

(config-if)# spanning-tree edge
```

> ➢ *Auto Edge*

> • *Enable | Disable*

```
(config-stp-aggr)# spanning-tree auto-edge

(config-stp-aggr)# no spanning-tree auto-edge

(config-if)# spanning-tree auto-edge

(config-if)# no spanning-tree auto-edge
```

> ➢ *Restricted Role*

> • *Enable | Disable*

```
(config-stp-aggr)# spanning-tree restricted-role

(config-stp-aggr)# no spanning-tree restricted-role

(config-if)# spanning-tree restricted-role

(config-if)# no spanning-tree restricted-role
```

> ➢ *Restricted TCN*

> • *Enable | Disable*

```
(config-stp-aggr)# spanning-tree restricted-tcn

(config-stp-aggr)# no spanning-tree restricted-tcn

(config-if)# spanning-tree restricted-tcn

(config-if)# no spanning-tree restricted-tcn
```

SOLTECH
INFONET INC.

> ➤ *BPDU Guard*

- *Enable | Disable*

```
(config-stp-aggr)# spanning-tree bpdu-guard

(config-stp-aggr)# no spanning-tree bpdu-guard

(config-if)# spanning-tree bpdu-guard

(config-if)# no spanning-tree bpdu-guard
```

> ➤ *Point-to-Point*

- *Forced True | Forced False | Auto*

```
(config-stp-aggr)# spanning-tree link-type point-to-point

(config-stp-aggr)# spanning-tree link-type shared

(config-stp-aggr)# spanning-tree link-type auto

(config-if)# spanning-tree link-type point-to-point

(config-if)# spanning-tree link-type shared

(config-if)# spanning-tree link-type auto
```

## 6.8.1.5. MSTI Ports

WEB MENU Configuration>Spanning Tree>MSTI Ports

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well. An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.
This page contains MSTI port settings for physical and aggregated ports.

**MSTI Port Configuration**

**Select MSTI**

MST1 ✓ Get

### MSTI Port Configuration

| Object | Description |
|---|---|
| **Select MSTI** | Select the MSTI instance to configure. Once selected, click the "GET" button to display the configuration page. |

**Buttons**

Get : Click to retrieve settings for a specific MSTI.

### MSTI Port Configuration

When click 'Get' button, the next page will be displayed for MSTI setting.
This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well. An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.
This page contains MSTI port settings for physical and aggregated ports.

**MST1 MSTI Port Configuration**

**MSTI Aggregated Ports Configuration**

| Port | Path Cost | Priority |
|---|---|---|
| - | Auto | 128 |

**MSTI Normal Ports Configuration**

| Port | Path Cost | Priority |
|---|---|---|
| * | <> | <> |
| 1 | Auto | 128 |
| 2 | Auto | 128 |
| 3 | Auto | 128 |
| 4 | Auto | 128 |
| 5 | Auto | 128 |
| 6 | Auto | 128 |
| 7 | Auto | 128 |
| 8 | Auto | 128 |

SOLTECH
INFONET INC.

**MSTn MSTI Port Configuration**

**MSTI Aggregated Ports Configuration**

**MSTI Normal Ports Configuration**

| Object | Description |
|---|---|
| Port | The switch port number of the corresponding STP CIST (and MSTI) port. |
| Path Cost | Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000. |
| Priority | Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>Spanning Tree>MSTI Ports

✓ **MSTI Port Configuration**

➢ *Select MSTI*

**MSTI Port Configuration**

Select the MST to configure and Click 'Get' button

✓ **MSTn MSTI Port Configuration**

✓ **MSTI Aggregated Ports Configuration**

✓ **MSTI Normal Ports Configuration**

➢ *Path Cost*

- **Auto | Specific(1~200,000,000)**



➢ **Priority**

- **0|16|32|48|64|80|96|112|128|144|160|176|192|208|224|240**



---

## EXAMPLE CLI CONFIGURATION

---

✓ **MSTI Port Configuration**

- **Select MSTI**

  **mst <instance> (CIST=0, MSTI1=1, MSTI2=2, …, MSTI7=7)**

✓ **MSTn MSTI Port Configuration**

✓ **MSTI Aggregated Ports Configuration**

✓ **MSTI Normal Ports Configuration**

➢ **Path Cost**

- **Auto | Specific(1~200,000,000)**

```
(config)# spanning-tree aggregation

(config-stp-aggr)# spanning-tree mst <instance> cost { <cost> | auto }
(config-stp-aggr)# spanning-tree mst 1 cost auto
```

```
(config-stp-aggr)# spanning-tree mst 1 cost 200000000

(config)# interface ( <port_type> [ <plist> ] )
(config)# interface *

(config-if)# spanning-tree mst <instance> cost { <cost> | auto }
(config-if)# spanning-tree mst 1 cost auto
(config-if)# spanning-tree mst 1 cost 200000000
```

> ➢  *Priority*

   • **0|16|32|48|64|80|96|112|128|144|160|176|192|208|224|240**

```
(config-stp-aggr)# spanning-tree mst <instance> port-priority <prio>
(config-stp-aggr)# spanning-tree mst 1 port-priority 128

(config-if)# spanning-tree mst <instance> port-priority <prio>
(config-if)# spanning-tree mst 1 port-priority 128
```

# 6.8.2. Spanning Tree Monitor

# 6.8.2.1. Bridge Status

WEB MENU Monitor>Spanning Tree>Bridge Status

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

**STP Bridges**

| MSTI | Bridge ID | Root | | | Topology | Topology |
| | | ID | Port | Cost | Flag | Change Last |
|------|-----------|-----|------|------|----------|-------------|
| CIST | 32768.00-21-6D-00-00-00 | 32768.00-21-6D-00-00-00 | - | 0 | Steady | - |

The displayed table contains a row for each STP bridge instance, where the column displays the following information

## STP Bridges

| Object | Description |
|--------|-------------|
| **MSTI** | The Bridge Instance. This is also a link to the STP Detailed Bridge Status. |
| **Bridge ID** | The Bridge ID of this Bridge instance. |
| **Root ID** | The Bridge ID of the currently elected root bridge. |
| **Root Port** | The switch port currently assigned the *root* port role. |
| **Root Cost** | Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge. |
| **Topology Flag** | The current state of the Topology Change Flag of this Bridge instance. |
| **Topology Change Last** | The time since last Topology Change occurred. |

**Buttons**

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

Refresh : Click to refresh the page immediately.

## STP Detailed Bridge Status

This page provides detailed information on a single STP bridge instance, along with port state for all active ports associated.

**STP Detailed Bridge Status**

**STP Bridge Status**

| Bridge Instance | CIST |
|-----------------|------|
| Bridge ID | 32768.00-21-6D-00-00-00 |
| Root ID | 32768.00-21-6D-00-00-00 |
| Root Cost | 0 |
| Root Port | - |
| Regional Root | 32768.00-21-6D-00-00-00 |
| Internal Root Cost | 0 |
| Topology Flag | Steady |
| Topology Change Count | 0 |
| Topology Change Last | - |

**CIST Ports & Aggregations State**

| Port | Port ID | Role | State | Path Cost | Edge | Point-to-Point | Uptime |
|------|---------|------|-------|-----------|------|----------------|--------|
| *No ports or aggregations active* | | | | | | | |

## STP Detailed Bridge Status

| Object | Description |
|---|---|
| STP Bridge Status | This entry shows the state of the STP bridge instance. |
| Bridge Instance | The Bridge instance - CIST, MST1, ... |
| Bridge ID | The Bridge ID of this Bridge instance. |
| Root ID | The Bridge ID of the currently elected root bridge. |
| Root Port | The switch port currently assigned the root port role. |
| Root Cost | Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge. |
| Regional Root | The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (For the CIST instance only). |
| Internal Root Cost | The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (For the CIST instance only). |
| Topology Flag | The current state of the Topology Change Flag of this Bridge instance. |
| Topology Change Count | The number of times where the topology change flag has been set (during a one-second interval). |
| Topology Change Last | The time passed since the Topology Flag was last set. |

## CIST Ports & Aggregations State

| Object | Description |
|---|---|
| CIST Ports & Aggregations State | This entry shows the state of the CIST (Common and Internal Spanning Tree) ports and aggregations. |
| Port | The switch port number of the logical STP port. |
| Port ID | The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port. |
| Role | The current STP port role. The port role can be one of the following values: Alternate Port, Backup Port, Root Port, Designated Port. |
| State | The current STP port state. The port state can be one of the following values: Discarding, Learning, Forwarding. |
| Path Cost | The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value. |
| Edge | The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop. |
| Point-to-Point | The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state. |
| Uptime | The time since the bridge port was last initialized. |

**Buttons**

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

Refresh : Click to refresh the page immediately.

---

## EXAMPLE WEB MONITOR

---

SOLTECH
INFONET INC.

WEB MENU Monitor>Spanning Tree>Bridge Status

✓ **STP Bridges**

**STP Bridges**

| MSTI | Bridge ID | Root | | | Topology Flag | Topology Change Last |
|------|-----------|------|------|------|---------------|----------------------|
| | | ID | Port | Cost | | |
| CIST | 32768.00-21-6D-00-00-00 | 32768.00-21-6D-00-00-00 | - | 0 | Steady | - |
| MSTI1 | 32769.00-21-6D-00-00-00 | 32769.00-21-6D-00-00-00 | - | 0 | Steady | - |

When you click on MSTI, the STP Detailed Bridge Status window will open.

✓ **STP Detailed Bridge Status**

✓ **CIST Ports & Aggregations State**

**STP Detailed Bridge Status**

| STP Bridge Status | |
|-------------------|--|
| Bridge Instance | CIST |
| Bridge ID | 32768.00-21-6D-00-00-00 |
| Root ID | 32768.00-21-6D-00-00-00 |
| Root Cost | 0 |
| Root Port | - |
| Regional Root | 32768.00-21-6D-00-00-00 |
| Internal Root Cost | 0 |
| Topology Flag | Steady |
| Topology Change Count | 0 |
| Topology Change Last | - |

**CIST Ports & Aggregations State**

| Port | Port ID | Role | State | Path Cost | Edge | Point-to-Point | Uptime |
|------|---------|------|-------|-----------|------|----------------|--------|
| 2 | 128:002 | DesignatedPort | Forwarding | 20000 | Yes | Yes | 0d 00:46:47 |

---

## EXAMPLE CLI MONITOR

---

✓ **STP Bridges**

✓ **STP Detailed Bridge Status**

✓ **CIST Ports & Aggregations State**

```
# show spanning-tree

CIST Bridge STP Status
Bridge ID    : 32768.00-21-6D-00-00-00
Root ID      : 32768.00-21-6D-00-00-00
Root Port    : -
Root PathCost: 0
Regional Root: 32768.00-21-6D-00-00-00
Int. PathCost: 0
Max Hops     : 20
TC Flag      : Steady
TC Count     : 0
TC Last      : -
```

SOLTECH
INFONET INC.

```
Port       Port Role       State       Pri  PathCost  Edge  P2P  Uptime
---------  --------------  ----------  ---  --------  ----  ---  -------------
Gi 1/2     DesignatedPort  Forwarding  128    20000   Yes   Yes  0d 01:32:52

MSTI1 Bridge STP Status
Bridge ID    : 32769.00-21-6D-00-00-00
Root ID      : 32769.00-21-6D-00-00-00
Root Port    : -
Root PathCost: 0
TC Flag      : Steady
TC Count     : 0
TC Last      : -
Gi 1/2     DesignatedPort  Forwarding  128    20000   Yes   Yes  0d 01:31:56
```

## 6.8.2.2. Port Status

WEB MENU Monitor>Spanning Tree>Port Status

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

**STP Port Status**

| Port | CIST Role | CIST State | Uptime |
|------|-----------|------------|--------|
| 1 | Non-STP | Forwarding | - |
| 2 | Non-STP | Forwarding | - |
| 3 | Non-STP | Forwarding | - |
| 4 | Non-STP | Forwarding | - |
| 5 | Non-STP | Forwarding | - |
| 6 | Non-STP | Forwarding | - |
| 7 | Non-STP | Forwarding | - |
| 8 | Non-STP | Forwarding | - |

### STP Port Status

| Object | Description |
|--------|-------------|
| **Port** | The switch port number of the logical STP port. |
| **CIST Role** | The current STP port role of the CIST port. The port role can be one of the following values: Alternate Port, Backup Port, Root Port, Designated Port, Disabled. |
| **CIST State** | The current STP port state of the CIST port. The port state can be one of the following values: Discarding, Learning, Forwarding. |
| **Uptime** | The time since the bridge port was last initialized. |

**Buttons**

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

Refresh : Click to refresh the page immediately.

---

## EXAMPLE WEB MONITOR

---

WEB MENU Monitor>Spanning Tree>Port Status

✓ **STP Port Status**

**STP Port Status**

| Port | CIST Role | CIST State | Uptime |
|------|-----------|------------|--------|
| 1 | Disabled | Discarding | - |
| 2 | DesignatedPort | Forwarding | 0d 01:55:34 |
| 3 | Disabled | Discarding | - |
| 4 | Disabled | Discarding | - |
| 5 | Disabled | Discarding | - |
| 6 | Disabled | Discarding | - |
| 7 | Disabled | Discarding | - |
| 8 | Disabled | Discarding | - |
| 9 | Disabled | Discarding | - |
| 10 | Disabled | Discarding | - |
| 11 | Disabled | Discarding | - |
| 12 | Disabled | Discarding | - |

## EXAMPLE CLI MONITOR

✓ **STP Port Status**

```
# show spanning-tree mst 0 int *

Mst    Port        Port Role        State      Pri PathCost Edge P2P  Uptime
-----  ---------  --------------  ----------  --- -------- ---- ---  -------------
CIST   Gi 1/2     DesignatedPort  Forwarding  128    20000  Yes   Yes  0d 02:49:51
```

## 6.8.2.3. Port Statistics

WEB MENU Monitor>Spanning Tree>Port Statistics

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

**STP Statistics**

| Port | Transmitted | | | | Received | | | | Discarded | |
|------|------|------|-----|-----|------|------|-----|-----|---------|---------|
| | MSTP | RSTP | STP | TCN | MSTP | RSTP | STP | TCN | Unknown | Illegal |
| No ports enabled | | | | | | | | | | |

### STP Statistics

| Object | Description |
|--------|-------------|
| **Port** | The switch port number of the logical STP port. |
| **MSTP** | The number of MSTP BPDU's received/transmitted on the port. |
| **RSTP** | The number of RSTP BPDU's received/transmitted on the port. |
| **STP** | The number of legacy STP Configuration BPDU's received/transmitted on the port. |
| **TCN** | The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port. |
| **Discarded Unknown** | The number of unknown Spanning Tree BPDU's received (and discarded) on the port. |
| **Discarded Illegal** | The number of illegal Spanning Tree BPDU's received (and discarded) on the port. |

**Buttons**

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

Refresh : Click to refresh the page immediately.

Clear : Click to reset the counters.

---

## EXAMPLE WEB MONITOR

---

WEB MENU Monitor>Spanning Tree>Port Statistics

✓ **STP Statistics**

**STP Statistics**

| Port | Transmitted | | | | Received | | | | Discarded | |
|------|------|------|-----|-----|------|------|-----|-----|---------|---------|
| | MSTP | RSTP | STP | TCN | MSTP | RSTP | STP | TCN | Unknown | Illegal |
| 2 | 5666 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

---

## EXAMPLE CLI MONITOR

---

✓ **STP Port Status**

```
# show spanning-tree detailed interface *

Port      Rx MSTP  Tx MSTP  Rx RSTP  Tx RSTP  Rx STP  Tx STP  Rx TCN  Tx TCN  Rx Ill.  Rx Unk.
--------- -------- -------- -------- -------- ------- ------- ------- ------- ----------- ------ --
  Gi 1/2         0     6668        0        0       0       0       0       0         0        0
```

## 6.9. IPMC Profile

## 6.9.1. Profile Table Configuration

WEB MENU Configuration>IPMC Profile>Profile Table

This page provides IPMC Profile related configurations.

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

**IPMC Profile Configurations**

Global Profile Mode  Disabled ⌄

**IPMC Profile Table Setting**

| Delete | Profile Name | Profile Description | Rule |

Add New IPMC Profile

### IPMC Profile Configurations

| Object | Description |
|---|---|
| **Global Profile Mode** | Enable/Disable the Global IPMC Profile. System starts to do filtering based on profile settings only when the global profile mode is enabled. |

### IPMC Profile Table Setting

| Object | Description |
|---|---|
| **Delete** | Check to delete the entry. The designated entry will be deleted during the next save. |
| **Profile Name** | The name used for indexing the profile table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present. |
| **Profile Description** | Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile. No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence. |
| **Rule** | When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons. : List the rules associated with the designated profile. : Adjust the rules associated with the designated profile. |

### Buttons

Add New IPMC Profile : Click to add new IPMC profile. Specify the name and configure the new entry.

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

**IPMC Profile Rule Settings Table**

Clicking the 👁 button will bring up the list page.

Clicking the ⓔ button will bring up the settings page.

This page provides the filtering rule settings for a specific IPMC profile. It displays the configured rule entries in precedence order. First rule entry has highest priority in lookup, while the last rule entry has lowest priority in lookup.

**IPMC Profile [TestProfileName1] Rule Settings (In Precedence Order)**

| Profile Name & Index | Entry Name | Address Range | Action | Log | |
|---|---|---|---|---|---|

Add Last Rule

### IPMC Profile [Profile Name] Rule Settings (In precedence Order)

| Object | Description |
|---|---|
| **Profile Name** | The name of the designated profile to be associated. This field is not editable. |
| **Entry Name** | The name used in specifying the address range used for this rule.<br>Only the existing profile address entries will be chosen in the selected box. This field is not allowed to be selected as none ("-") while the Rule Settings Table is committed. |
| **Address Range** | The corresponding address range of the selected profile entry. This field is not editable and will be adjusted automatically according to the selected profile entry. |
| **Action** | Indicates the learning action upon receiving the Join/Report frame that has the group address matches the address range of the rule.<br>Permit: Group address matches the range specified in the rule will be learned.<br>Deny: Group address matches the range specified in the rule will be dropped. |
| **Log** | Indicates the logging preference upon receiving the Join/Report frame that has the group address matches the address range of the rule.<br>Enable: Corresponding information of the group address, that matches the range specified in the rule, will be logged.<br>Disable: Corresponding information of the group address, that matches the range specified in the rule, will not be logged. |
| **Rule Management Buttons** | You can manage rules and the corresponding precedence order by using the following buttons:<br>⊕: Insert a new rule before the current entry of rule.<br>⊗: Delete the current entry of rule.<br>⬆: Moves the current entry of rule up in the list.<br>⬇: Moves the current entry of rule down in the list. |

**Buttons**

Add Last Rule : Click to add a new rule in the end of the specific profile's rule list. Specify the address entry and configure the new entry.

Commit : Click to commit rule changes for the designated profile.

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

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>IPMC Profile>Profile Table

✓ **IPMC Profile Configuration**

SOLTECH
INFONET INC.

➢ **Global Profile Mode**

• **Enable |** *Disable*

**IPMC Profile Configurations**

| Global Profile Mode | Enabled ▼ |
|---|---|
| | Disabled |
| | Enabled |

✓ **IPMC Profile Table Setting**

➢ **Add New IPMC Profile**

**IPMC Profile Table Setting**

| Delete | Profile Name | Profile Description | Rule |
|---|---|---|---|
| Delete | | | 👁 ⊚ |

➢ **Profile Name**

• *Maximum 16 alphabetic and numeric characters.*

➢ **Profile Description**

• *Maximum 64 alphabetic and numeric characters.*

| Delete | Profile Name | Profile Description | Rule |
|---|---|---|---|
| ☐ | TestProfileName1 | Test-Profile_Name | 👁 ⓔ |

Click ⓔ button for setting Edit Profile [Profile Name] Rule

✓ **IPMC Profile [Profile Name] Rule Settings (In precedence Order)**

➢ **Add Last Rule**

**IPMC Profile [TestProfileName1] Rule Settings (In Precedence Order)**

| Profile Name & Index | Entry Name | Address Range | Action | Log | |
|---|---|---|---|---|---|
| TestProfileName1    1 | - ▼ | ~ | Deny ▼ | Disable ▼ | ⊕⊙ ⊗⊙ |

➢ **Entry Name**

• Select Entry (Settings required in the Address Entry.)

**IPMC Profile [TestProfileName1] Rule Settings (In Precedence Order)**

| Profile Name & Index | Entry Name | Address Range | Action | Log | |
|---|---|---|---|---|---|
| TestProfileName1    1 | - ▼ | ~ | Deny ▼ | Disable ▼ | ⊕⊙ ⊗⊙ |
| Add Last Rule | - | | | | |
| | TestEntry1 | | | | |

➢ **Action**

• Deny | **Permit**

SOLTECH
INFONET INC.

> ➢ **Log**

- Disable | **Enable**



Click Commit button to commit rule changes for the designated profile.

Click 👁 button to view Profile [Profile Name] Rule



---

## EXAMPLE CLI CONFIGURATION

---

✓ **IPMC Profile Configuration**

> ➢ *Global Profile Mode*

- *Enable |* Disable

```
(config)# ipmc profile
(config)# no ipmc profile
```

✓ **IPMC Profile Table Setting**

> ➢ *Add New IPMC Profile*

> ➢ *Profile Name*

- *Maximum 16 alphabetic and numeric characters.*

```
(config)# ipmc profile <word16>
(config)# ipmc profile TestProfileName1
```

> ➢ *Profile Description*

- *Maximum 64 alphabetic and numeric characters.*

```
(config)# ipmc profile <word16>
(config)# ipmc profile TestProfileName1
```

```
(config-ipmc-profile)# description <line64>
(config-ipmc-profile)# description Test-Profile_Name
```

✓ **IPMC Profile [Profile Name] Rule Settings (In precedence Order)**

➢ *Add Last Rule*

➢ *Entry Name*

• Select Entry (Settings required in the Address Entry.)

➢ *Action*

• Deny | **Permit**

➢ *Log*

• Disable | **Enable**

```
(config)# ipmc profile <word16>
(config)# ipmc profile TestProfileName1
(config-ipmc-profile)# range <entry_name> { permit | deny } [ log ] [ next <next_entry> ]
(config-ipmc-profile)# range TestEntry1 permit log
(config-ipmc-profile)# range TestEntry1 permit
(config-ipmc-profile)# range TestEntry1 deny log
(config-ipmc-profile)# range TestEntry1 deny
```

Click 👁 button to view Profile [Profile Name] Rule

```
# show ipmc profile [ <profile_name> ] [ detail ]
(config)# ipmc profile
(config)# ipmc profile detail
```

# 6.9.2. Address Entry Configuration

WEB MENU Configuration>IPMC Profile>Address Entry

This page provides address range settings used in IPMC profile.

The address entry is used to specify the address range that will be associated with IPMC Profile.

It is allowed to create at maximum 128 address entries in the system.

**IPMC Profile Address Configuration**

Navigate Address Entry Setting in IPMC Profile by [20] entries per page.

| Delete | Entry Name | Start Address | End Address |

Add New Address (Range) Entry

## IPMC Profile Address Configuration

| Object | Description |
|---|---|
| **Delete** | Check to delete the entry.<br>The designated entry will be deleted during the next save. |
| **Entry Name** | The name used for indexing the address entry table.<br>Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.<br>This entry is used in the Profile Table. |
| **Start Address** | The starting IPv4/IPv6 Multicast Group Address that will be used as an address range. |
| **End Address** | The ending IPv4/IPv6 Multicast Group Address that will be used as an address range. |

**Buttons**

Add New Address (Range) Entry : Click to add new address range. Specify the name and configure the addresses.

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

Refresh : Refreshes the displayed table starting from the input fields.

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

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

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>IPMC Profile>Address Entry

  ✓   **IPMC Profile Address Configuration**

    ➢   *Add New Address(Range) Entry*

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

    ➢   *Entry Name*

- *Maximum 16 alphabetic and numeric characters*

➢ **Start Address**

- *IPv4/IPv6 Multicast Group Address(ex IPv4-224.0.0.0~239.255.255.255)*

➢ **End Address**

- *IPv4/IPv6 Multicast Group Address(ex IPv4-224.0.0.0~239.255.255.255)*

| Delete | Entry Name | Start Address | End Address |
|--------|------------|---------------|-------------|
| ☐ | TestEntry1 | 224.0.0.0 | 224.0.0.1 |

## EXAMPLE CLI CONFIGURATION

✓ **IPMC Profile Address Configuration**

➢ **Add New Address(Range) Entry**

➢ **Entry Name**

- *Maximum 16 alphabetic and numeric characters*

➢ **Start Address**

- *IPv4/IPv6 Multicast Group Address(ex IPv4-224.0.0.0~239.255.255.255)*

➢ **End Address**

- *IPv4/IPv6 Multicast Group Address(ex IPv4-224.0.0.0~239.255.255.255)*

```
(config)# ipmc range <entry_name> { <v_ipv4_mcast> [ <v_ipv4_mcast_1> ] | <v_ipv6_mcast>
[ <v_ipv6_mcast_1> ] }
(config)# ipmc range TestEntry1 224.0.0.0 224.0.0.1
```

SOLTECH
INFONET INC.

# 6.10. IPMC

## 6.10.1. IGMP Snooping Configuration

## 6.10.1.1. Basic Configuration

WEB MENU Configuration>IPMC>IGMP Snooping>Basic Configuration

This page provides IGMP Snooping related configuration.

**IGMP Snooping Configuration**

| Global Configuration | |
|---|---|
| Snooping Enabled | ☐ |
| Unregistered IPMCv4 Flooding Enabled | ☑ |
| IGMP SSM Range | 232.0.0.0 / 8 |
| Leave Proxy Enabled | ☐ |
| Proxy Enabled | ☐ |

**Port Related Configuration**

| Port | Router Port | Fast Leave | Throttling |
|---|---|---|---|
| * | ☐ | ☐ | <> |
| 1 | ☐ | ☐ | unlimited |
| 2 | ☐ | ☐ | unlimited |
| 3 | ☐ | ☐ | unlimited |
| 4 | ☐ | ☐ | unlimited |
| 5 | ☐ | ☐ | unlimited |
| 6 | ☐ | ☐ | unlimited |
| 7 | ☐ | ☐ | unlimited |
| 8 | ☐ | ☐ | unlimited |
| 9 | ☐ | ☐ | unlimited |
| 10 | ☐ | ☐ | unlimited |

### IGMP Snooping Configuration

### Global Configuration

| Object | Description |
|---|---|
| **Snooping Enabled** | Enable the Global IGMP Snooping. |
| **Unregistered IPMCv4 Flooding Enabled** | Enable unregistered IPMCv4 traffic flooding.<br>The flooding control takes effect only when IGMP Snooping is enabled.<br>When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting. |
| **IGMP SSM Range** | SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.<br>Assign valid IPv4 multicast address as prefix with a prefix length (from 4 to 32) for the range. |
| **Leave Proxy Enabled** | Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side. |
| **Proxy Enabled** | Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side. |

SOLTECH
INFONET INC.

**Port Related Configuration**

| Object | Description |
|---|---|
| **Router Port** | Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.<br>If an aggregation member port is selected as a router port, the whole aggregation will act as a router port. |
| **Fast Leave** | Enable the fast leave on the port.<br>System will remove group record and stop forwarding data upon receiving the leave message without sending last member query messages.<br>It is recommended to enable this feature only when a single IGMPv2 host is connected to the specific port. |
| **Throttling** | Enable to limit the number of multicast groups to which a switch port can belong. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>IPMC>IGMP Snooping>Basic Configuration

✓ **IGMP Snooping Configuration**

✓ **Global Configuration**

  ➢ *Snooping Enabled*

   • **Enable |** *Disable*

  ➢ *Unregistered IPMCv4 Flooding Enabled*

   • *Enable |* **Disable**

  ➢ *IGMP SSM Range*

   • **224.0.0.0~239.255.255.255 / 4~32**

  ➢ *Leave Proxy Enable*

   • **Enable |** *Disable*

  ➢ *Proxy Enable*

   • *Enable |* **Disable**

**IGMP Snooping Configuration**

| Global Configuration | |
|---|---|
| Snooping Enabled | ☑ |
| Unregistered IPMCv4 Flooding Enabled | ☐ |
| IGMP SSM Range | 232.0.0.0    / 8 |
| Leave Proxy Enabled | ☑ |
| Proxy Enabled | ☐ |

✓ **Port Related Configuration**

➢ *Router Port*

• **Checked |** *Unchecked*

➢ *Fast Leave*

• **Checked |** *Unchecked*

➢ *Throttling*

• **Unlimited(default) |** *1~10*

**Port Related Configuration**

| Port | Router Port | Fast Leave | Throttling |
|---|---|---|---|
| * | ☑ | ☐ | <> |
| 1 | ☑ | ☐ | unlimited |
| 2 | ☐ | ☑ | unlimited |
| 3 | ☐ | ☐ | unlimited |
| 4 | ☐ | ☐ | unlimited |
| 5 | ☐ | ☐ | unlimited |
| 6 | ☐ | ☐ | unlimited |
| 7 | ☐ | ☐ | unlimited |
| 8 | ☐ | ☐ | unlimited |
| 9 | ☐ | ☐ | unlimited |
| 10 | ☐ | ☐ | unlimited |

# EXAMPLE CLI CONFIGURATION

✓ **IGMP Snooping Configuration**

✓ **Global Configuration**

➢ *Snooping Enabled*

• **Enable |** *Disable*

```
(config)# ip igmp snooping
(config)# no ip igmp snooping
```

➢ *Unregistered IPMCv4 Flooding Enabled*

• *Enable |* **Disable**

```
(config)# ip igmp unknown-flooding
(config)# no ip igmp unknown-flooding
```

> ➢ *IGMP SSM Range*

  • *224.0.0.0~239.255.255.255 / 4~32*

```
(config)# ip igmp ssm-range <v_ipv4_mcast> <ipv4_prefix_length>
(config)# ip igmp ssm-range 232.0.0.0 8
```

> ➢ *Leave Proxy Enable*

  • *Enable |* *Disable*

```
(config)# ip igmp host-proxy leave-proxy
(config)# no ip igmp host-proxy leave-proxy
```

> ➢ *Proxy Enable*

  • *Enable |* *Disable*

```
(config)# ip igmp host-proxy
(config)# no ip igmp host-proxy
```

✓ **Port Related Configuration**

> ➢ *Router Port*

  • *Checked |* *Unchecked*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# ip igmp snooping mrouter
(config-if)# no ip igmp snooping mrouter
```

> ➢ *Fast Leave*

  • *Checked |* *Unchecked*

```
(config-if)# ip igmp snooping immediate-leave
(config-if)# no ip igmp snooping immediate-leave
```

> ➢ *Throttling*

  • *Unlimited(default) |* *1~10*

```
(config-if)# no ip igmp snooping max-groups
(config-if)# ip igmp snooping max-groups <throttling>
(config-if)# ip igmp snooping max-groups 10
```

# 6.10.1.2. VLAN Configuration

WEB MENU Configuration>IPMC>IGMP Snooping>VLAN Configuration

**IGMP Snooping VLAN Configuration**

Start from VLAN 1 with 20 entries per page.

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

Add New IGMP VLAN

## IGMP Snooping VLAN Configuration

### Navigating the IGMP Snooping VLAN Table

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the next closest VLAN Table match.

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

### IGMP Snooping VLAN Table Columns

| Object | Description |
|---|---|
| **Delete** | Check to delete the entry. The designated entry will be deleted during the next save. |
| **VLAN ID** | The VLAN ID of the entry. |
| **IGMP Snooping Enabled** | Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping. |
| **Querier Election** | Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier. |
| **Querier Address** | Define the IPv4 address as source address used in IP header for IGMP Querier election.When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1. |
| **Compatibility** | Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto. |
| **PRI** | Priority of Interface. It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0. |
| **RV** | Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255, default robustness variable value is 2. |
| **QI** | Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds. |
| **QRI** | Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code |

|  | inserted into the periodic General Queries.<br>The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds). |
|---|---|
| **LLQI (LMQI for IGMP)** | Last Member Query Interval.<br>The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count.<br>The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second). |
| **URI** | Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group.<br>The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second. |

**Buttons**

Refresh : Refreshes the displayed table starting from the "VLAN" input fields.

|<< : Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

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

Add New IGMP VLAN : Click to add new IGMP VLAN. Specify the VID and configure the new entry. Click "Save".

The specific IGMP VLAN starts working after the corresponding static VLAN is also created.

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>IPMC>IGMP Snooping>VLAN Configuration

✓ **IGMP Snooping VLAN Configuration**

➢ ***Add New IGMP VLAN***

**IGMP Snooping VLAN Configuration**

Start from VLAN 1 with 20 entries per page.

| Delete | VLAN ID | Snooping Enabled | Querier Election | Querier Address | Compatibility | PRI | RV | QI (sec) | QRI (0.1 sec) | LLQI (0.1 sec) | URI (sec) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Delete |  | ☐ | ☑ | 0.0.0.0 | IGMP-Auto | 0 | 2 | 125 | 100 | 10 | 1 |

Add New IGMP VLAN

➢ ***VLAN ID***

• ***VLAN ID 1****(1~4095)*

➢ ***Snooping Enabled***

• ***Enable*** *| Disable*

➢ ***Querier Election***

• ***Enable*** *| Disable*

➢ ***Querier Address***

SOLTECH
INFONET INC.

- *0.0.0.0(no setting) | 192.168.10.1(setting)*

➢ **Compatibility**

- **IGMP-Auto** | *Forced IGMPv1 | Forced IGMPv2 | Forced IGMPv3*

➢ **PRI**

- **0***(0~7)*

➢ **RV**

- **2***(1~255)*

➢ **QI(sec)**

- **125***(1~31744)*

➢ **QRI(0.1sec)**

- **100***(0~31744)*

➢ **LLQI(0.1sec)**

- **10***(0~31744)*

➢ **URI(sec)**

- **1***(0~31744)*

**IGMP Snooping VLAN Configuration**

Start from VLAN `1` with `20` entries per page.

| Delete | VLAN ID | Snooping Enabled | Querier Election | Querier Address | Compatibility | PRI | RV | QI (sec) | QRI (0.1 sec) | LLQI (0.1 sec) | URI (sec) |
|--------|---------|------------------|------------------|-----------------|---------------|-----|-----|----------|---------------|----------------|-----------|
| Delete | 1 | ☑ | ☑ | 0.0.0.0 | IGMP-Auto | 0 | 2 | 125 | 100 | 10 | 1 |

# EXAMPLE CLI CONFIGURATION

✓ **IGMP Snooping VLAN Configuration**

 ➢ *VLAN ID*

 • *VLAN ID 1(1~4095)*

```
(config)# ip igmp snooping vlan <v_vlan_list>
(config)# ip igmp snooping vlan 1
```

 ➢ *Snooping Enabled*

 • *Enable | Disable*

```
(config)# interface vlan <vlist>
(config)# interface vlan 1

(config-if-vlan)# ip igmp snooping
(config-if-vlan)# no ip igmp snooping
```

 ➢ *Querier Election*

 • *Enable | Disable*

```
(config-if-vlan)# ip igmp snooping querier election
(config-if-vlan)# no ip igmp snooping querier election
```

 ➢ *Querier Address*

 • *0.0.0.0(no setting) | 192.168.10.100(setting)*

```
(config-if-vlan)# ip igmp snooping querier address <v_ipv4_ucast>
(config-if-vlan)# no ip igmp snooping querier address
(config-if-vlan)# ip igmp snooping querier address 192.168.10.1
```

 ➢ *Compatibility*

 • *IGMP-Auto | Forced IGMPv1 | Forced IGMPv2 | Forced IGMPv3*

```
(config-if-vlan)# ip igmp snooping compatibility { auto | v1 | v2 | v3 }
(config-if-vlan)# ip igmp snooping compatibility auto
(config-if-vlan)# ip igmp snooping compatibility v1
(config-if-vlan)# ip igmp snooping compatibility v2
(config-if-vlan)# ip igmp snooping compatibility v3
```

 ➢ *PRI*

 • *0(0~7)*

```
(config-if-vlan)# ip igmp snooping priority <cos_priority>
(config-if-vlan)# ip igmp snooping priority 0
```

➢ **RV**

- **2***(1~255)*

```
(config-if-vlan)# ip igmp snooping robustness-variable <ipmc_rv>
(config-if-vlan)# ip igmp snooping robustness-variable 2
```

➢ **QI(sec)**

- **125***(1~31744)*

```
(config-if-vlan)# ip igmp snooping query-interval <ipmc_qi>
(config-if-vlan)# ip igmp snooping query-interval 125
```

➢ **QRI(0.1sec)**

- **100***(0~31744)*

```
(config-if-vlan)# ip igmp snooping query-max-response-time <ipmc_qri>
(config-if-vlan)# ip igmp snooping query-max-response-time 100
```

➢ **LLQI(0.1sec)**

- **10***(0~31744)*

```
(config-if-vlan)# ip igmp snooping last-member-query-interval <ipmc_lmqi>
(config-if-vlan)# ip igmp snooping last-member-query-interval 10
```

➢ **URI(sec)**

- **1***(0~31744)*

```
(config-if-vlan)# ip igmp snooping unsolicited-report-interval <ipmc_uri>
(config-if-vlan)# ip igmp snooping unsolicited-report-interval 1
```

## 6.10.1.3. Port Filtering Profile

WEB MENU Configuration>IPMC>IGMP Snooping>Port Filtering Profile



**IGMP Snooping Port Filtering Profile Configuration**

| Object | Description |
|---|---|
| **Port** | The logical port for the settings. |
| **Filtering Profile** | Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button |
| **Profile Management Button** | You can inspect the rules of the designated profile by using the following button.  : List the rules associated with the designated profile. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

### EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>IPMC>IGMP Snooping>Port Filtering Profile

✓ **IGMP Snooping VLAN Configuration**

➢ *Filtering Profile*

• *Select the IPMC Profile*

**IGMP Snooping Port Filtering Profile Configuration**

| Port | Filtering Profile |
|------|-------------------|
| 1 | - |
| 2 | - |
| 3 | TestProfileName1 |
| 4 | - |
| 5 | - |
| 6 | - |
| 7 | - |
| 8 | - |
| 9 | - |
| 10 | - |

➢ *Profile Management Button*

● *Click button to view Profile [Profile Name] Rule*

**IPMC Profile [TestProfileName1] Rule Settings (In Precedence Order)**

| Profile Name & Index | | Entry Name | Address Range | Action | Log |
|----------------------|---|-----------|---------------|--------|-----|
| TestProfileName1 | 1 | TestEntry1 | 224.0.0.0 ~ 224.0.0.1 | Permit | Enable |

# EXAMPLE CLI CONFIGURATION

✓ **IGMP Snooping VLAN Configuration**

➢ **Filtering Profile**

● *Select the IPMC Profile*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# ip igmp snooping filter <profile_name>
(config-if)# ip igmp snooping filter TestProfileName1
```

➢ **Profile Management Button**

● *Click button to view Profile [Profile Name] Rule*

```
# show ipmc profile [ <profile_name> ] [ detail ]
# show ipmc profile
IPMC Profile is now enabled to start filtering.
Profile: TestProfileName1 (In IGMP Mode)
Description: Test-Profile_Name
HEAD-> TestEntry1 (Permit the following range and log the matched entry)
Start Address: 224.0.0.0
End Address  : 224.0.0.1

# show ipmc profile detail
IGMP will permit and log matched address between [224.0.0.0 <-> 224.0.0.1]
IGMP will deny matched address between [224.0.0.2 <-> 239.255.255.255]
MLD will deny matched address between [ff00:: <-> ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff]
```

SOLTECH
INFONET INC.

# 6.10.2. IGMP Snooping Monitor

## 6.10.2.1. Status

WEB MENU Monitor>IPMC>IGMC Snooping>Status

This page provides IGMP Snooping status.

**IGMP Snooping Status**

**Statistics**

| VLAN ID | Querier Version | Host Version | Querier Status | Queries Transmitted | Queries Received | V1 Reports Received | V2 Reports Received | V3 Reports Received | V2 Leaves Received |
|---|---|---|---|---|---|---|---|---|---|

**Router Port**

| Port | Status |
|---|---|
| 1 | - |
| 2 | - |
| 3 | - |
| 4 | - |
| 5 | - |
| 6 | - |
| 7 | - |
| 8 | - |
| 9 | - |
| 10 | - |

### IGMP Snooping Status

#### Statistics

| Object | Description |
|---|---|
| **VLAN ID** | The VLAN ID of the entry. |
| **Querier Version** | Working Querier Version currently. |
| **Host Version** | Working Host Version currently. |
| **Querier Status** | Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled. |
| **Queries Transmitted** | The number of Transmitted Queries. |
| **Queries Received** | The number of Received Queries. |
| **V1 Reports Received** | The number of Received V1 Reports. |
| **V2 Reports Received** | The number of Received V2 Reports. |
| **V3 Reports Received** | The number of Received V3 Reports. |
| **V2 Leaves Received** | The number of Received V2 Leaves. |

#### Router Port

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

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

Both denote the specific port is configured or learnt to be a router port.

| Object | Description |
|---|---|
| **Port** | Switch port number |

| Status | Indicate whether specific port is a router port or not. |
|---|---|

**Buttons**

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

[Refresh] : Click to refresh the page immediately.

[Clear] : Clears all Statistics counters.

## EXAMPLE WEB MONITOR

WEB MENU Monitor>IPMC>IGMC Snooping>Status

✓ **IGMP Snooping Status**

✓ **Statistics**

✓ **Router Port**

**IGMP Snooping Status**

**Statistics**

| VLAN ID | Querier Version | Host Version | Querier Status | Queries Transmitted | Queries Received | V1 Reports Received | V2 Reports Received | V3 Reports Received | V2 Leaves Received |
|---|---|---|---|---|---|---|---|---|---|
| 1 | v3 | v3 | ACTIVE | 1 | 0 | 0 | 0 | 0 | 0 |

**Router Port**

| Port | Status |
|---|---|
| 1 | Static |
| 2 | - |
| 3 | - |
| 4 | - |
| 5 | - |
| 6 | - |
| 7 | - |
| 8 | - |
| 9 | - |
| 10 | - |

## EXAMPLE CLI MONITOR

✓ **IGMP Snooping Status**

✓ **Statistics**

```
# show ip igmp snooping
IGMP Snooping is enabled to start snooping IGMP control plane.
Switch-1 IGMP Interface Status
IGMP snooping VLAN 1 interface is enabled.
Querier status is ACTIVE
RX IGMP Query:0 V1Join:0 V2Join:0 V3Join:5 V2Leave:0
TX IGMP Query:6 / (Source) Specific Query:0
Compatibility:IGMP-Auto / Querier Version:Default / Host Version:Version 3
```

✓ **Router Port**

```
# show ip igmp snooping mrouter
IGMP Snooping is enabled to start snooping IGMP control plane.
Switch-1 IGMP Router Port Status
Gi 1/1: Static Router Port
```

## 6.10.2.2. Groups Information

WEB MENU Monitor>IPMC>IGMC Snooping>Groups Information

Entries in the IGMP Group Table are shown on this page.

The IGMP Group Table is sorted first by VLAN ID, and then by group.

**IGMP Snooping Group Information**

Start from VLAN [1] and group address [224.0.0.0] with [20] entries per page.

| VLAN ID | Groups | Port Members 1 2 3 4 5 6 7 8 9 10 |
|---------|--------|-----------------------------------|
| No more entries | | |

**IGMP Snooping Group Information**

| Object | Description |
|--------|-------------|
| **VLAN ID** | VLAN ID of the group. |
| **Groups** | Group address of the group displayed. |
| **Port Members** | Ports under this group. |

**Buttons**

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

Refresh : Refreshes the displayed table starting from the input fields.

|<< : Updates the table, starting with the first entry in the IGMP Group Table.

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

## EXAMPLE WEB MONITOR

WEB MENU Monitor>IPMC>IGMC Snooping>Groups Information

&#10003;    **IGMP Snooping Group Information**

**IGMP Snooping Group Information**

Start from VLAN [1] and group address [224.0.0.0] with [20] entries per page.

| VLAN ID | Groups | Port Members 1 2 3 4 5 6 7 8 9 10 |
|---------|--------|-----------------------------------|
| 1 | 239.255.255.250 | ✓ |

## EXAMPLE CLI MONITOR

&#10003;    **IGMP Snooping Group Information**

```
# show ip igmp snooping group-database
IGMP Snooping is enabled to start snooping IGMP control plane.
IGMP Group Database
Switch-1 IGMP Group Table
239.255.255.250 is registered on VLAN 1
Port Members: Gi 1/2
Switch-1 IGMP Group Count: 1
```

SOLTECH
INFONET INC.

## 6.10.2.3. IPv4 SFM Information

WEB MENU Monitor>IPMC>IGMC Snooping>IPv4 SFM Information

Entries in the IGMP SFM Information Table are shown on this page.
The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

**IGMP SFM Information**

Start from VLAN `1` and Group `224.0.0.0` with `20` entries per page.

| VLAN ID | Group | Port | Mode | Source Address | Type | Hardware Filter/Switch |
|---|---|---|---|---|---|---|
| No more entries | | | | | | |

### IGMP SFM Information

| Object | Description |
|---|---|
| **VLAN ID** | VLAN ID of the group. |
| **Group** | Group address of the group displayed. |
| **Port** | Switch port number. |
| **Mode** | Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude. |
| **Source Address** | IP Address of the source. Currently, the maximum number of IPv4 source address for filtering (per group) is 8. When there is no any source filtering address, the text "None" is shown in the Source Address field. |
| **Type** | Indicates the Type. It can be either Allow or Deny. |
| **Hardware Filter/Switch** | Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not. |

**Buttons**

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

Refresh : Refreshes the displayed table starting from the input fields.

|<< : Updates the table starting from the first entry in the IGMP SFM Information Table.

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

## EXAMPLE WEB MONITOR

WEB MENU Monitor>IPMC>IGMC Snooping>IPv4 SFM Information

✓ **IGMP SFM Information**

**IGMP SFM Information**

Start from VLAN `1` and Group `224.0.0.0` with `20` entries per page.

| VLAN ID | Group | Port | Mode | Source Address | Type | Hardware Filter/Switch |
|---|---|---|---|---|---|---|
| 1 | 239.255.255.250 | 2 | Exclude | None | Deny | Yes |

## EXAMPLE CLI MONITOR

✓ **IGMP SFM Information**

```
# show ip igmp snooping group-database sfm-information detail
IGMP Snooping is enabled to start snooping IGMP control plane.
(IGMP proxy for LEAVE mechanism is active)
Multicast streams destined to unregistered IGMP groups will be flooding.
Groups in range 232.0.0.0/8 follow IGMP SSM registration service model.
IGMP Group Database
Switch-1 IGMP Group Table
239.255.255.250 is registered on VLAN 1
Port Members: Gi 1/2
Hardware Switch: Yes
Gi 1/2 Mode is Exclude (Filter Timer: 151)
Deny Source Address: None
Switch-1 IGMP Group Count: 1
```

# 6.11. LLDP

## 6.11.1. LLDP Configuration

### 6.11.1.1. LLDP

WEB MENU Configuration>LLDP>LLDP

This page allows the user to inspect and configure the current LLDP interface settings.

**LLDP Configuration**

**LLDP Parameters**

| | | |
|---|---|---|
| Tx Interval | 30 | seconds |
| Tx Hold | 4 | times |
| Tx Delay | 2 | seconds |
| Tx Reinit | 2 | seconds |

**LLDP Interface Configuration**

| Interface | Mode | CDP aware | Port Descr | Sys Name | Sys Descr | Sys Capa | Mgmt Addr |
|---|---|---|---|---|---|---|---|
| * | <> | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/1 | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/2 | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/3 | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/4 | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/1 | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/2 | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/3 | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/4 | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |

## LLDP Configuration

### LLDP Parameters

| Object | Description |
|---|---|
| **Tx Interval** | The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds. |
| **Tx Hold** | Each LLDP frame contains information about how long time the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times. |
| **Tx Delay** | If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds. |
| **Tx Reinit** | When a interface is disabled, LLDP is disabled or the switch is rebooted, a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the number of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds. |

### LLDP Interface Configuration

| Object | Description |
|---|---|
| **Interface** | The switch interface name of the logical LLDP interface. |
| **Mode** | Select LLDP mode.<br>    **Rx only**      The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed. |

| | | |
|---|---|---|
| | **Tx only** | The switch will drop LLDP information received from neighbors, but will send out LLDP information. |
| | **Disabled** | The switch will not send out LLDP information, and will drop LLDP information received from neighbors. |
| | **Enabled** | The switch will send out LLDP information, and will analyze LLDP information received from neighbors. |
| **CDP Aware** | Select CDP awareness.<br>The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the interface is enabled.<br>Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.<br>CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.<br>CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbor's table.<br>CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.<br>CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.<br>Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.<br>If all interfaces have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one interface has CDP awareness enabled all CDP frames are terminated by the switch.<br>Note: When CDP awareness on an interface is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded. | |
| **Port Descr** | When checked the "port description" is included in LLDP information transmitted. | |
| **Sys Name** | When checked the "system name" is included in LLDP information transmitted. | |
| **Sys Descr** | When checked the "system description" is included in LLDP information transmitted. | |
| **Sys Capa** | When checked the "system capability" is included in LLDP information transmitted. | |
| **Mgmt Addr** | When checked the "management address" is included in LLDP information transmitted. | |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>LLDP>LLDP

- ✓ **LLDP Configuration**
- ✓ **LLDP Parameters**

  - ➢ *Tx Interval*

    - • *5~32768 sec(30sec)*

  - ➢ *Tx Hold*

- **•** ***2~10 times(4times)***

➢ ***Tx Delay***

- **•** ***1~8192 sec(2sec)***

➢ ***Tx Delay***

- **•** ***1~10 sec(2sec)***

**LLDP Parameters**

| Tx Interval | 30 | seconds |
|---|---|---|
| Tx Hold | 4 | times |
| Tx Delay | 2 | seconds |
| Tx Reinit | 2 | seconds |

✓ **LLDP Interface Configuration**

➢ ***Mode***

- **•** ***Disabled | Enabled(default) | Rx Only | Tx Only***

**LLDP Interface Configuration**

|  |  |  | Optional TLVs |  |  |  |  |
|---|---|---|---|---|---|---|---|
| Interface | Mode | CDP aware | Port Descr | Sys Name | Sys Descr | Sys Capa | Mgmt Addr |
| * | <> | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/1 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/2 | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/3 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/4 | Rx only / Tx only | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/5 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/6 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/7 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/8 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/1 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/2 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/3 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/4 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |

➢ ***CDP aware***

- **•** ***Disabled(default) | Enabled***

**LLDP Interface Configuration**

|  |  |  | Optional TLVs |  |  |  |  |
|---|---|---|---|---|---|---|---|
| Interface | Mode | CDP aware | Port Descr | Sys Name | Sys Descr | Sys Capa | Mgmt Addr |
| * | <> | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/1 | Enabled | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/2 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/3 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/4 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/5 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/6 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/7 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/8 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/1 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/2 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/3 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/4 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |

➢ ***Optional TLVs***

**SOLTECH**
INFONET INC.

➢ **Port Descr**

•   **Disabled | Enabled(default)**

**LLDP Interface Configuration**

| Interface | Mode | CDP aware | Optional TLVs | | | | |
|---|---|---|---|---|---|---|---|
| | | | Port Descr | Sys Name | Sys Descr | Sys Capa | Mgmt Addr |
| * | <> | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/1 | Enabled | ☐ | ☐ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/2 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/3 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/4 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/5 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/6 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/7 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/8 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/1 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/2 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/3 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/4 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |

➢ **Sys Name**

•   **Disabled | Enabled(default)**

**LLDP Interface Configuration**

| Interface | Mode | CDP aware | Optional TLVs | | | | |
|---|---|---|---|---|---|---|---|
| | | | Port Descr | Sys Name | Sys Descr | Sys Capa | Mgmt Addr |
| * | <> | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/1 | Enabled | ☐ | ☑ | ☐ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/2 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/3 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/4 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/5 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/6 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/7 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/8 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/1 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/2 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/3 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/4 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |

➢ **Sys Descr**

•   **Disabled | Enabled(default)**

**LLDP Interface Configuration**

| Interface | Mode | CDP aware | Optional TLVs | | | | |
|---|---|---|---|---|---|---|---|
| | | | Port Descr | Sys Name | Sys Descr | Sys Capa | Mgmt Addr |
| * | <> | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/1 | Enabled | ☐ | ☑ | ☑ | ☐ | ☑ | ☑ |
| GigabitEthernet 1/2 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/3 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/4 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/5 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/6 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/7 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/8 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/1 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/2 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/3 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/4 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |

➢ **Sys Capa**

•   **Disabled | Enabled(default)**

SOLTECH
INFONET INC.

**LLDP Interface Configuration**

| Interface | Mode | CDP aware | Optional TLVs | | | | |
|---|---|---|---|---|---|---|---|
| | | | Port Descr | Sys Name | Sys Descr | Sys Capa | Mgmt Addr |
| * | <> | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/1 | Enabled | ☐ | ☑ | ☑ | ☑ | ☐ | ☑ |
| GigabitEthernet 1/2 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/3 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/4 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/5 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/6 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/7 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/8 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/1 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/2 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/3 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/4 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |

➢ *Mgmt Addr*

  • *Disabled | Enabled(default)*

**LLDP Interface Configuration**

| Interface | Mode | CDP aware | Optional TLVs | | | | |
|---|---|---|---|---|---|---|---|
| | | | Port Descr | Sys Name | Sys Descr | Sys Capa | Mgmt Addr |
| * | <> | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/1 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☐ |
| GigabitEthernet 1/2 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/3 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/4 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/5 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/6 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/7 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/8 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/1 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/2 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/3 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/4 | Enabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |

## EXAMPLE CLI CONFIGURATION

✓ **LLDP Configuration**

✓ **LLDP Parameters**

  ➢ *Tx Interval*

    • *5~32768 sec(30sec)*

```
(config)# lldp timer <val>
(config)# lldp timer 30
```

  ➢ *Tx Hold*

    • *2~10 times(4times)*

```
(config)# lldp holdtime <val>
(config)# lldp holdtime 4
```

  ➢ *Tx Delay*

SOLTECH
INFONET INC.

- **1~8192 sec(2sec)**

```
(config)# lldp transmission-delay <val>
(config)# lldp transmission-delay 2
```

> **Tx Delay**

- **1~10 sec(2sec)**

```
(config)# lldp transmission-delay <val>
(config)# lldp reinit 2
```

✓ **LLDP Interface Configuration**

> **Mode**

- **Disabled | Enabled(default) | Rx Only | Tx Only**

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# lldp receive
(config-if)# lldp transmit
Enabled
(config-if)# lldp receive
(config-if)# lldp transmit
Disabled
(config-if)# no lldp receive
(config-if)# no lldp transmit
Rx Only
(config-if)# lldp receive
(config-if)# no lldp transmit
Tx Only
(config-if)# no lldp receive
(config-if)# lldp transmit
```

> **CDP aware**

- **Disabled(default) | Enabled**

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# lldp cdp-aware
```

> **Optional TLVs**

> **Port Descr**

- **Disabled | Enabled(default)**

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# lldp tlv-select port-description
```

> ### *Sys Name*

- #### *Disabled | Enabled(default)*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# lldp tlv-select system-name
```

> ### *Sys Descr*

- #### *Disabled | Enabled(default)*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# lldp tlv-select system-description
```

> ### *Sys Capa*

- #### *Disabled | Enabled(default)*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# lldp tlv-select system-capabilities
```

> ### *Mgmt Addr*

- #### *Disabled | Enabled(default)*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# lldp tlv-select management-address
```

## 6.11.1.2. LLDP-MED

WEB MENU Configuration>LLDP>LLDP-MED

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

**LLDP-MED Configuration**

**Fast Start Repeat Count**

| Fast start repeat count | 4 |

**Transmit TLVs**

| Interface | Capabilities | Policies | Location | PoE |
|---|---|---|---|---|
| * | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/1 | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/2 | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/3 | ☑ | ☑ | ☑ | ☑ |
| GigabitEthernet 1/4 | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/1 | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/2 | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/3 | ☑ | ☑ | ☑ | ☑ |
| 10GigabitEthernet 1/4 | ☑ | ☑ | ☑ | ☑ |

**Coordinates Location**

| Latitude | 0 | ° | North | Longitude | 0 | ° | East | Altitude | 0 | Meters | Map Datum | WGS84 |

**Civic Address Location**

| Country code | | State | | County | |
|---|---|---|---|---|---|
| City | | City district | | Block (Neighborhood) | |
| Street | | Leading street direction | | Trailing street suffix | |
| Street suffix | | House no. | | House no. suffix | |
| Landmark | | Additional location info | | Name | |
| Zip code | | Building | | Apartment | |
| Floor | | Room no. | | Place type | |
| Postal community name | | P.O. Box | | Additional code | |

**Emergency Call Service**

| Emergency Call Service | |

**Policies**

| Delete | Policy ID | Application Type | Tag | VLAN ID | L2 Priority | DSCP |
|---|---|---|---|---|---|---|
| | | | No entries present | | | |

[Add New Policy]

### LLDP-MED Configuration

### Fast Start Repeat Count

| Object | Description |
|---|---|
| **Fast start repeat count** | Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.<br>With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs |

|  | in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated interface. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors.<br><br>Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.<br><br>It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links. |
|---|---|

**Transmit TLVs**

| Object | Description |
|---|---|
| Transmit TLVs | It is possible to select which LLDP-MED information that shall be transmitted to the neighbors. When the checkbox is checked the information is included in the frame transmitted to the neighbor. |
| Interface | The interface name to which the configuration applies. |
| Capabilities | When checked the switch's capabilities is included in LLDP-MED information transmitted. |
| Policies | When checked the configured policies for the interface is included in LLDP-MED information transmitted. |
| Location | When checked the configured location information for the switch is included in LLDP-MED information transmitted. |
| PoE | When checked the configured PoE (Power Over Ethernet) information for the interface is included in LLDP-MED information transmitted. |

**Coordinates Location**

| Object | Description |
|---|---|
| Coordinates Location | This section is dedicated to configuring the coordinates for a switch. |
| Latitude | Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator. |
| Longitude | Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian. |
| Altitude | Altitude SHOULD be normalized to within -2097151.9 to 2097151.9 with a maximum of 1 digit.<br>It is possible to select between two altitude types (floors or meters).<br>Meters: Representing meters of Altitude defined by the vertical datum specified.<br>Floors: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 |

| | |
|---|---|
| | represents the floor level associated with ground level at the main entrance. |
| **Map Datum** | The Map Datum is used for the coordinates given in these options:<br>WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.<br>NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).<br>NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean. |

**Civic Address Location**

| Object | Description |
|---|---|
| **Civic Address Location** | IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). The total number of characters for the combined civic address information must not exceed 250 characters.<br>A couple of notes to the limitation of 250 characters.<br>1) A non-empty civic address location will use 2 extra characters in addition to the civic address location text.<br>2) The 2 letter country code is not part of the 250 characters limitation. |
| **Country code** | The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US. |
| **State** | National subdivisions (state, canton, region, province, prefecture). |
| **County** | County, parish, gun (Japan), district. |
| **City** | City, township, shi (Japan) - Example: Copenhagen. |
| **City district** | City division, borough, city district, ward, chou (Japan). |
| **Block (Neighborhood)** | Neighborhood, block. |
| **Street** | Street - Example: Poppelvej. |
| **Leading street direction** | Leading street direction - Example: N. |
| **Trailing street suffix** | Trailing street suffix - Example: SW. |
| **Street suffix** | Street suffix - Example: Ave, Platz. |
| **House no.** | House number - Example: 21. |
| **House no. suffix** | House number suffix - Example: A, 1/2. |
| **Landmark** | Landmark or vanity address - Example: Columbia University. |
| **Additional location info** | Additional location info - Example: South Wing. |
| **Name** | Name (residence and office occupant) - Example: Flemming Jahn. |
| **Zip code** | Postal/zip code - Example: 2791. |
| **Building** | Building (structure) - Example: Low Library. |
| **Apartment** | Unit (Apartment, suite) - Example: Apt 42. |
| **Floor** | Floor - Example: 4. |
| **Room no.** | Room number - Example: 450F. |

| Place type | Place type - Example: Office. |
|---|---|
| Postal community name | Postal community name - Example: Leonia. |
| P.O. Box | Post office box (P.O. BOX) - Example: 12345. |
| Additional code | Additional code - Example: 1320300003. |

**Emergency Call Service**

| Object | Description |
|---|---|
| Emergency Call Service | Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA. ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling. |

**Policies**

| Object | Description |
|---|---|
| Policies | Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service. Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services The network policy attributes advertised are: 1. Layer 2 VLAN ID (IEEE 802.1Q-2003) 2. Layer 2 priority value (IEEE 802.1D-2004) 3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474) This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are: 1. Voice 2. Guest Voice 3. Softphone Voice 4. Video Conferencing 5. Streaming Video 6. Control / Signaling (conditionally support a separate network policy for the media types above) A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration. It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN. |
| Delete | Check to delete the policy. It will be deleted during the next save. |
| Policy ID | ID for the policy. This is auto generated and shall be used when selecting the policies |

| | that shall be mapped to the specific interfaces. |
|---|---|
| **Application Type** | Intended use of the application types:<br>1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.<br>2. Voice Signaling (conditional) - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.<br>3. Guest Voice - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.<br>4. Guest Voice Signaling (conditional) - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.<br>5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.<br>6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.<br>7. Streaming Video - for use by broadcast or multicast-based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.<br>8. Video Signaling (conditional) - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy. |
| **Tag** | Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN.<br>Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance. Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003. |
| **VLAN ID** | VLAN identifier (VID) for the interface as defined in IEEE 802.1Q-2003. |
| **L2 Priority** | L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004. |
| **DSCP** | DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 |

| | through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475. |
|---|---|

### Adding a new policy

| Object | Description |
|---|---|
| **Adding a new policy** | Click Add New Policy to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Save".<br>The number of policies supported is 32 |
| **Policies Interface Configuration** | Every interface may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or interface configuration. |
| **Interface** | The interface name to which the configuration applies. |
| **Policy Id** | The set of policies that shall apply to a given interface. The set of policies is selected by check marking the checkboxes that corresponds to the policies. |

**Buttons**

`Add New Policy` : Click  to add a new policy.

`Apply` : Click to apply changes.

`Apply&Save` : Click to apply and save changes.

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

# 6.11.2. LLDP Monitor

## 6.11.2.1. Neighbors

WEB MENU Monitor>LLDP>Neighbors

This page provides a status overview for all LLDP neighbors.

**LLDP Neighbor Information**

| LLDP Remote Device Summary | | | | | | |
|---|---|---|---|---|---|---|
| Local Interface | Chassis ID | Port ID | Port Description | System Name | System Capabilities | Management Address |
| No neighbor information found | | | | | | |

### LLDP Neighbor Information

The displayed table contains a row for each interface on which an LLDP neighbor is detected. The columns hold the following information.

| Object | Description |
|---|---|
| **Local Interface** | The interface on which the LLDP frame was received. |
| **Chassis ID** | The Chassis ID is the identification of the neighbor's LLDP frames. |
| **Port ID** | The Port ID is the identification of the neighbor port. |
| **Port Description** | Port Description is the port description advertised by the neighbor unit. |
| **System Name** | System Name is the name advertised by the neighbor unit. |
| **System Capabilities** | System Capabilities describes the neighbor unit's capabilities.<br>1. Other<br>2. Repeater<br>3. Bridge<br>4. WLAN Access Point<br>5. Router<br>6. Telephone<br>7. DOCSIS cable device<br>8. Station only<br>9. Reserved<br>When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-). |
| **Management Address** | Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address. |

**Buttons**

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

Refresh : Click to refresh the page.

## EXAMPLE WEB CONFIGURATION

WEB MENU Monitor>LLDP>Neighbors

✓ **LLDP Neighbor Information**

**LLDP Neighbor Information**

| LLDP Remote Device Summary | | | | | | |
|---|---|---|---|---|---|---|
| Local Interface | Chassis ID | Port ID | Port Description | System Name | System Capabilities | Management Address |
| GigabitEthernet 1/8 | 00-21-6D-01-02-03 | 5 | GigabitEthernet 1/5 | SFC8000GHP | Bridge(+) | 172.30.1.30 (IPv4) |

## EXAMPLE CLI CONFIGURATION

✓ **LLDP Neighbor Information**

```
# show lldp neighbors
Local Interface    : GigabitEthernet 1/8
Chassis ID         : 00-21-6D-01-02-03
Port ID            : 5
Port Description   : GigabitEthernet 1/5
System Name        : SFC8000GHP
System Description : SFC8000GHP 2.4.0.1 2023-10-11T11:11:42+09:00
System Capabilities : Bridge(+)
Management Address  : 172.30.1.30 (IPv4)
PoE Type           : PSE Device
PoE Source         : Primary Power Source
PoE Power          : 0.0 [W]
PoE Priority       : Low Priority
```

SOLTECH
INFONET INC.

## 6.11.2.2. LLDP-MED Neighbors

WEB MENU Monitor>LLDP>LLDP-MED Neighbors

This page provides a status overview of all LLDP-MED neighbors.

**LLDP-MED Neighbor Information**

| Local Interface |
|---|
| No LLDP-MED neighbor information found |

### LLDP-MED Neighbor Information

The displayed table contains a row for each interface on which an LLDP neighbor is detected. This function applies to VoIP devices which support LLDP-MED. The columns hold the following information.

| Object | Description |
|---|---|
| **Interface** | The interface on which the LLDP frame was received. |
| **Device Type** | LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices. <br><br>LLDP-MED Network Connectivity Device Definition <br>LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies: <br>1. LAN Switch/Router <br>2. IEEE 802.1 Bridge <br>3. IEEE 802.3 Repeater (included for historical reasons) <br>4. IEEE 802.11 Wireless Access Point <br>5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method. <br><br>LLDP-MED Endpoint Device Definition <br>LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework. <br><br>Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following. <br><br>Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I). <br><br>LLDP-MED Generic Endpoint (Class I) <br>The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057. Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management. <br><br>LLDP-MED Media Endpoint (Class II) <br>The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a |

| | |
|---|---|
| | particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar. Discovery services defined in this class include media-type-specific network layer policy discovery.<br><br>LLDP-MED Communication Endpoint (Class III)<br>The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.<br>Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management. |
| **LLDP-MED Capabilities** | LLDP-MED Capabilities describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are:<br>1. LLDP-MED capabilities<br>2. Network Policy<br>3. Location Identification<br>4. Extended Power via MDI – PSE<br>5. Extended Power via MDI – PD<br>6. Inventory<br>7. Reserved |
| **Application Type** | Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device.<br>The possible application types are shown below.<br>1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.<br>2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media.<br>3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.<br>4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.<br>5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.<br>6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.<br>7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.<br>8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media. |
| **Policy** | Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device.<br>Unknown: The network policy for the specified application type is currently unknown.<br>Defined: The network policy is defined (known). |
| **TAG** | TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN.<br>Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.<br>Tagged: The device is using the IEEE 802.1Q tagged frame format. |
| **VLAN ID** | VLAN ID is the VLAN identifier (VID) for the interface as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress interface is used instead. |
| **Priority** | Priority is the Layer 2 priority to be used for the specified application type. One of the |

| | eight priority levels (0 through 7). |
|---|---|
| **DSCP** | DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63). |
| **Auto-negotiation** | Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner. |
| **Auto-negotiation status** | Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation. |
| **Auto-negotiation Capabilities** | Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities. |

**Buttons**

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

Refresh : Click to refresh the page.

## 6.11.2.3. EEE

WEB MENU Monitor>LLDP>EEE

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

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

**LLDP Neighbors EEE Information**

| Local Interface | Tx Tw | Rx Tw | Fallback Receive Tw | Echo Tx Tw | Echo Rx Tw | Resolved Tx Tw | Resolved Rx Tw | EEE in Sync |
|---|---|---|---|---|---|---|---|---|
| | | | | No LLDP EEE information found | | | | |

### LLDP Neighbors EEE Information

The displayed table contains a row for each interface.

If the interface does not supports EEE, then it displays as "EEE not supported for this interface".

If EEE is not enabled on particular interface, then it displays as "EEE not enabled for this interface".

If the link partner doesn't supports EEE, then it displays as "Link partner is not EEE capable".

The columns hold the following information.

| Object | Description |
|---|---|
| **Local Interface** | The interface at which LLDP frames are received or transmitted. |
| **Tx Tw** | The link partner's maximum time that transmit path can hold-off sending data after dissertation of LPI. |
| **Rx Tw** | The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep. |
| **Fallback Receive Tw** | The link partner's fallback receive Tw. A receiving link partner may inform the transmitter of an alternate desired Tw sys Tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw sys Tx. |
| **Echo Tx Tw** | The link partner's Echo Tx Tw value. The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information. |
| **Echo Rx Tw** | The link partner's Echo Rx Tw value. |
| **Resolved Tx Tw** | The resolved Tx Tw for this link. Note : NOT the link partner The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP). |
| **Resolved Rx Tw** | The resolved Rx Tw for this link. Note : NOT the link partner The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP). |
| **EEE in Sync** | Shows whether the switch and the link partner have agreed on wake times. Red - Switch and link partner have not agreed on wakeup times. |

SOLTECH
INFONET INC.

| | Green - Switch and link partner have agreed on wakeup times. |
|---|---|

**Buttons**

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

Refresh : Click to refresh the page.

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Monitor>LLDP>EEE

    ✓    **LLDP Neighbors EEE Information**

**LLDP Neighbors EEE Information**

| Local Interface | Tx Tw | Rx Tw | Fallback Receive Tw | Echo Tx Tw | Echo Rx Tw | Resolved Tx Tw | Resolved Rx Tw | EEE in Sync |
|---|---|---|---|---|---|---|---|---|
| GigabitEthernet 1/8 | | | | EEE not enabled for this interface | | | | |

---

## EXAMPLE CLI CONFIGURATION

---

    ✓    **LLDP Neighbors EEE Information**

```
# show lldp eee
Local Interface      : GigabitEthernet 1/8
EEE not enabled for this interface
```

## 6.11.2.4. Port Statistics

WEB MENU Monitor>LLDP>Port Statistics

This page provides an overview of all LLDP traffic.

**LLDP Global Counters**

Auto-refresh ⌷

| Global Counters | |
|---|---|
| Clear global counters | ☑ |
| Neighbor entries were last changed | 1970-01-01T09:00:00+09:00 (166049 secs. ago) |
| Total Neighbors Entries Added | 0 |
| Total Neighbors Entries Deleted | 0 |
| Total Neighbors Entries Dropped | 0 |
| Total Neighbors Entries Aged Out | 0 |

**LLDP Statistics Local Counters**

| Local Interface | Tx Frames | Rx Frames | Rx Errors | Frames Discarded | TLVs Discarded | TLVs Unrecognized | Org. Discarded | Age-Outs | Clear |
|---|---|---|---|---|---|---|---|---|---|
| * | * | * | * | * | * | * | * | * | ☑ |
| GigabitEthernet 1/1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| GigabitEthernet 1/2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| GigabitEthernet 1/3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| GigabitEthernet 1/4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| 10GigabitEthernet 1/1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| 10GigabitEthernet 1/2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| 10GigabitEthernet 1/3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| 10GigabitEthernet 1/4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |

### LLDP Global Counters

| Object | Description |
|---|---|
| **Global Counters** | Global counters are counters that refer to the whole switch |
| **Clear global counters** | If checked the global counters are cleared when CLEAR is pressed. |
| **Neighbor entries were last changed** | Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected. |
| **Total Neighbors Entries Added** | Shows the number of new entries added since switch reboot. |
| **Total Neighbors Entries Deleted** | Shows the number of new entries deleted since switch reboot. |
| **Total Neighbors Entries Dropped** | Shows the number of LLDP frames dropped due to the entry table being full. |
| **Total Neighbors Entries Aged Out** | Shows the number of entries deleted due to Time-To-Live expiring. |

### LLDP Statistics Local Counters

| Object | Description |
|---|---|
| **Local Counters** | Local counters refer to per interface counters for the currently selected switch. |
| **Local Interface** | The interface on which LLDP frames are received or transmitted. |
| **Tx Frames** | The number of LLDP frames transmitted on the interface. |
| **Rx Frames** | The number of LLDP frames received on the interface. |
| **Rx Errors** | The number of received LLDP frames containing some kind of error. |
| **Frames Discarded** | If a LLDP frame is received on a interface, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when |

SOLTECH
INFONET INC.

| | the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given interface's link is down, an LLDP shutdown frame is received, or when the entry ages out. |
|---|---|
| **TLVs Discarded** | Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded. |
| **TLVs Unrecognized** | The number of well-formed TLVs, but with an unknown type value. |
| **Org. Discarded** | If LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted. |
| **Age-Outs** | Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented. |
| **Clear** | If checked the counters for the specific interface are cleared when Clear is pressed. |

**Buttons**

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

Refresh : Click to refresh the page.

Clear : Clears the local counters. All counters (including global counters) are cleared upon reboot.

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Monitor>LLDP>Port Statistics

✓ **LLDP Global Counters**

✓ **LLDP Statistics Local Counters**

**LLDP Global Counters**

| Global Counters | |
|---|---|
| Clear global counters | ☑ |
| Neighbor entries were last changed | 1970-01-01T13:44:54+09:00 (89711 secs. ago) |
| Total Neighbors Entries Added | 23 |
| Total Neighbors Entries Deleted | 22 |
| Total Neighbors Entries Dropped | 0 |
| Total Neighbors Entries Aged Out | 8 |

**LLDP Statistics Local Counters**

| Local Interface | Tx Frames | Rx Frames | Rx Errors | Frames Discarded | TLVs Discarded | TLVs Unrecognized | Org. Discarded | Age-Outs | Clear |
|---|---|---|---|---|---|---|---|---|---|
| * | * | * | * | * | * | * | * | * | ☑ |
| GigabitEthernet 1/1 | 135 | 2668 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| GigabitEthernet 1/2 | 263 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| GigabitEthernet 1/3 | 1470 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| GigabitEthernet 1/4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| GigabitEthernet 1/5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| GigabitEthernet 1/6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| GigabitEthernet 1/7 | 19 | 25 | 0 | 0 | 0 | 0 | 0 | 2 | ☑ |
| GigabitEthernet 1/8 | 3300 | 3054 | 0 | 0 | 0 | 0 | 0 | 4 | ☑ |
| 10GigabitEthernet 1/1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| 10GigabitEthernet 1/2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| 10GigabitEthernet 1/3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| 10GigabitEthernet 1/4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |

SOLTECH
INFONET INC.

# EXAMPLE CLI CONFIGURATION

✓    **LLDP Global Counters**

✓    **LLDP Statistics Local Counters**

```
# show lldp statistics
LLDP global counters
Neighbor entries was last changed at 1970-01-01T13:44:54+09:00  (90116 secs. ago).
Total Neighbors Entries Added    23.
Total Neighbors Entries Deleted  22.
Total Neighbors Entries Dropped  0.
Total Neighbors Entries Aged Out 8.

LLDP local counters
                   Rx        Tx        Rx        Rx        Rx TLV    Rx TLV    Rx TLV
Interface          Frames    Frames    Errors    Discards  Errors    Unknown   Organiz.  Aged
---------          ------    ------    ------    --------  ------    -------   --------  ----

GigabitEthernet 1/1    2668    135     0         0         0         0         0         0
GigabitEthernet 1/2    0       263     0         0         0         0         0         0
GigabitEthernet 1/3    0       1483    0         0         0         0         0         0
GigabitEthernet 1/4    0       0       0         0         0         0         0         0
GigabitEthernet 1/5    0       0       0         0         0         0         0         0
GigabitEthernet 1/6    0       0       0         0         0         0         0         0
GigabitEthernet 1/7    25      19      0         0         0         0         0         2
GigabitEthernet 1/8    3067    3314    0         0         0         0         0         4
10GigabitEthernet 1/1  0       0       0         0         0         0         0         0
10GigabitEthernet 1/2  0       0       0         0         0         0         0         0
10GigabitEthernet 1/3  0       0       0         0         0         0         0         0
10GigabitEthernet 1/4  0       0       0         0         0         0         0         0
```

## 6.12. PoE

## 6.12.1. PoE Configuration

WEB MENU Configuration>PoE

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

1. AF/AT supported model

**Power Over Ethernet Configuration**

| Reserved Power determined by | ◉ Class | ○ LLDP-MED |
|---|---|---|
| Power Management Mode | ◉ Actual Consumption | ○ Reserved Power |
| Capacitor Detection | ◉ Disabled | ○ Enabled |

**PoE Power Supply Configuration**

| Primary Power Supply [W] |
|---|
| 240 |

**PoE Port Configuration**

| Port | Enable | PoE Mode | Priority | PD Alive | PD Reset |
|---|---|---|---|---|---|
| * | ☑ | <> | <> | ☐ | ☐ |
| 1 | ☑ | PoE+ | Low | ☐ | ☐ |
| 2 | ☑ | PoE+ | Low | ☐ | ☐ |
| 3 | ☑ | PoE+ | Low | ☐ | ☐ |
| 4 | ☑ | PoE+ | Low | ☐ | ☐ |
| 5 | ☑ | PoE+ | Low | ☐ | ☐ |
| 6 | ☑ | PoE+ | Low | ☐ | ☐ |
| 7 | ☑ | PoE+ | Low | ☐ | ☐ |
| 8 | ☑ | PoE+ | Low | ☐ | ☐ |

2. AF/AT/BT supported model

**Power Over Ethernet Configuration**

| Reserved Power determined by | ◉ Class | ○ LLDP-MED |
|---|---|---|
| Power Management Mode | ◉ Actual Consumption | ○ Reserved Power |
| Capacitor Detection | ○ Disabled | ○ Enabled |

**PoE Power Supply Configuration**

| Primary Power Supply [W] |
|---|
| 240 |

**PoE Port Configuration**

| Port | Enable | PoE Mode | Priority | PD Alive | PD Reset | PSE Detect |
|---|---|---|---|---|---|---|
| * | ☑ | <> | <> | ☐ | ☐ | ☑ |
| 1 | ☑ | 4p Type4 90w / 2p Type3 30w | Low | ☐ | ☐ | ☑ |
| 2 | ☑ | 4p Type4 90w / 2p Type3 30w | Low | ☐ | ☐ | ☑ |
| 3 | ☑ | 4p Type4 90w / 2p Type3 30w | Low | ☐ | ☐ | ☑ |
| 4 | ☑ | 4p Type4 90w / 2p Type3 30w | Low | ☐ | ☐ | ☑ |
| 5 | ☑ | 2p Type2 30w | Low | ☐ | ☐ | ☑ |
| 6 | ☑ | 2p Type2 30w | Low | ☐ | ☐ | ☑ |
| 7 | ☑ | 2p Type2 30w | Low | ☐ | ☐ | ☑ |
| 8 | ☑ | 2p Type2 30w | Low | ☐ | ☐ | ☑ |

SOLTECH
INFONET INC.

### Power Over Ethernet Configuration

| Object | Description |
|---|---|
| **Reserved Power determined by** | There are two modes for configuring how the ports/PDs may reserve power. <br><br> **Class** In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. <br><br> **LLDP-MED** This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode. <br><br> For all modes: If a port uses more power than the reserved power for the port, the port is shut down. |
| **Power Management Mode** | There are 2 modes for configuring when to shut down the ports. <br><br> **Actual Consumption** In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down. <br><br> **Reserved Power** In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply. |
| **Capacitor Detection** | Controls capacitor detection for legacy PD devices.(Enabled only in AT Model) <br><br> **Disabled** This feature is disabled. <br><br> **Enabled** This feature is enabled. |

### Power Supply Configuration

| Object | Description |
|---|---|
| **Power Source** | For being able to determine the amount of power the PD may use, it must be defined what amount of power a power source can deliver. It varies based on the number of ports and models. |

### Port Configuration

| Object | Description |
|---|---|
| **Port** | This is the logical port number for this row. <br> Ports that are not PoE-capable are grayed out and thus impossible to configure PoE for. |
| **Enable** | This is the area for configuring the usage of PoE functionality. |
| **PoE Mode** | The PoE Mode represents the PoE operating mode for the port. <br> 1. AF/AT Model <br><br> **PoE** Enables PoE IEEE 802.3af (Class 3 PDs limited to 15.4W) <br><br> **PoE+** Enables PoE+ IEEE 802.3at (Class 4 PDs limited to 30W) |

SOLTECH
INFONET INC.

| Object | Description |
|---|---|
| **PoE Mode** | 2. AF/AT/BT Model<br>PoE mode terminology<br><br>4p — Model utilizing 4Pair Matrix<br>2p — Model utilizing 2Pair Matrix<br>W — The maximum power wattage that the switch can provide.<br>Type — Type1 - Class1~3(Class 3 PDs limited to 15.4W)<br>        Type2 - Class4(Class 4 PDs limited to 30W)<br>        Type3 – Class5~6(Class 6 PDs limited to 60W)<br>        Type4 – Class7~8(Class 8 PDs limited to 90W)<br>Non Compliant — Non-standard PDs, use in case of PD operation failure after standard mode implementation<br>Legacy — Activation of Capacitor Detection<br><br>Example for IEEE802.3bt Type Port<br>4p Type4 90w / 2p Type3 30w<br>4p Type3 60w / 2p Type3 30w<br>4p Type3 30w / 2p Type3 30w<br>4p Type3 15w / 2p Type3 15w<br>4p Type2 30w / 2p Type2 30w<br>4p Type4 Non Compliant 90w / 2p Type3 Non Compliant 30w [Legacy]<br>4p Type4 Non Compliant 60w / 2p Type3 Non Compliant 30w [Legacy]<br>4p Type4 Non Compliant 30w / 2p Type3 Non Compliant 30w [Legacy]<br>4p Type4 Non Compliant 15w / 2p Type3 BT Non Compliant 15w [Legacy]<br>4p Type4 Non Compliant 90w / 2p Type3 Non Compliant 30w class0 = 4pair [Legacy]<br>4p Type4 Non Compliant 60w / 2p Type3 Non Compliant 30w class0 = 4pair [Legacy]<br>4p Type4 Non Compliant PoH 90w / 2p Type4 Non Compliant PoH 45w<br>4p Type3 Non Compliant Special 60w / 2p Type3 Compliant Special 30w [Legacy]<br>4p Type3 Non Compliant CDP 60w / 2p Type3 Non Compliant CDP 30w [Legacy]<br>4p Type2 Non Compliant 60w / 2p Type2 Non Compliant 30w<br>4p 4 class events 60w / 2p 3 class events 30w [Legacy]<br>4p Type4 Non Compliant PoH 90w / 2p Type3 Non Compliant PoH 45w [Legacy]<br>4p All Classes Non Compliant PoH 90w / 2p All Classes Non Compliant PoH 45w [Legacy]<br>4p Type3 60w / 2p Type3 30w [Legacy]<br>4p Type4 Non Compliant Spec 90w / 2p Type3 Non Compliant Spec 45w [Legacy]<br><br>Example for IEEE802.3at Type Port<br>2p Type3 30w<br>2p Type3 15w<br>2p Type2 30w<br>2p Type3 Non Compliant 30w [Legacy]<br>2p Type3 BT Non Compliant 15w [Legacy]<br>2p Type3 Non Compliant 30w class0 = 4pair [Legacy]<br>2p Type3 Non Compliant 30w class0 = 4pair [Legacy]<br>2p Type4 Non Compliant PoH 45w<br>2p Type3 Compliant Special 30w [Legacy]<br>2p Type3 Non Compliant CDP 30w [Legacy]<br>2p Type2 Non Compliant 30w<br>2p 3 class events 30w Legacy [Legacy]<br>2p Type3 Non Compliant PoH 45w [Legacy]<br>2p All Classes Non Compliant PoH 45w [Legacy]<br>2p Type3 30w [Legacy]<br>2p Type3 Non Compliant Spec 45w [Legacy] |
| **Priority** | Priority represents the priority of the port. There are three power priority levels: "Low," "High," and "Critical."<br>In case the remote devices require more power than the power supply can deliver, the ports will be shut down starting from the port with the lowest priority. If multiple ports have the same priority, the port with the highest port number will be shut down first. |
| **PD Alive** | The PD Alive feature monitors the status of PD devices. If a PD device is not functioning properly, it will be automatically restarted. |
| **PD Reset** | The PD reset function restarts the PD device.(Remote PD device recovery function.) |
| **PSE Detect** | The PSE Detect detects devices connected to PoE ports.If the connected device is a PSE device (e.g., L2 switch), change the PoE status to Disable. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>PoE>Configuration

- ✓ **Power Over Ethernet Configuration**

    - ➢ *Reserved Power Determined by*

        - • *Class(default) | LLDP-MED*

    - ➢ *Power Management Mode*

        - • *Actual Consumption(default) | Reserved Power*

    - ➢ *Capacitor Detection(only AF/AT Model)*

        - • *Disabled(default) | Enabled*

**Power Over Ethernet Configuration**

| Reserved Power determined by | ◉ Class | ○ LLDP-MED |
|---|---|---|
| Power Management Mode | ◉ Actual Consumption | ○ Reserved Power |
| Capacitor Detection | ◉ Disabled | ○ Enabled |

- ✓ **PoE Power Supply Configuration**

    - ➢ *Primary Power Supply*

        - • *Power Source (Different for each Model)*

**PoE Power Supply Configuration**

| Primary Power Supply [W] |
|---|
| 240 |

✓ **PoE Port Configuration**

**AF/AT Model**

➢ *Enable | Disable*

**PoE Port Configuration**

| Port | Enable | PoE Mode | Priority | PD Alive | PD Reset |
|------|--------|----------|----------|----------|----------|
| * | ☑ | <> ∨ | <> ∨ | ☐ | ☐ |
| 1 | ☐ | PoE+ ∨ | Low ∨ | ☐ | ☐ |
| 2 | ☑ | PoE+ ∨ | Low ∨ | ☐ | ☐ |
| 3 | ☑ | PoE+ ∨ | Low ∨ | ☐ | ☐ |
| 4 | ☑ | PoE+ ∨ | Low ∨ | ☐ | ☐ |
| 5 | ☑ | PoE+ ∨ | Low ∨ | ☐ | ☐ |
| 6 | ☑ | PoE+ ∨ | Low ∨ | ☐ | ☐ |
| 7 | ☑ | PoE+ ∨ | Low ∨ | ☐ | ☐ |
| 8 | ☑ | PoE+ ∨ | Low ∨ | ☐ | ☐ |

➢ *PoE Mode*

• *PoE | PoE+*

**PoE Port Configuration**

| Port | Enable | PoE Mode | Priority | PD Alive | PD Reset |
|------|--------|----------|----------|----------|----------|
| * | ☑ | <> ∨ | <> ∨ | ☐ | ☐ |
| 1 | ☐ | PoE+ ∨ | Low ∨ | ☐ | ☐ |
| 2 | ☑ | PoE+ ∨ | Low ∨ | ☐ | ☐ |
| 3 | ☑ | PoE | Low ∨ | ☐ | ☐ |
| 4 | ☑ | PoE+ | Low ∨ | ☐ | ☐ |
| 5 | ☑ | PoE+ ∨ | Low ∨ | ☐ | ☐ |
| 6 | ☑ | PoE+ ∨ | Low ∨ | ☐ | ☐ |
| 7 | ☑ | PoE+ ∨ | Low ∨ | ☐ | ☐ |
| 8 | ☑ | PoE+ ∨ | Low ∨ | ☐ | ☐ |

➢ *Priority*

• *Low | High | Critical*

**PoE Port Configuration**

| Port | Enable | PoE Mode | Priority | PD Alive | PD Reset |
|------|--------|----------|----------|----------|----------|
| * | ☑ | <> ∨ | <> ∨ | ☐ | ☐ |
| 1 | ☐ | PoE+ ∨ | Low ∨ | ☐ | ☐ |
| 2 | ☑ | PoE+ ∨ | Low ∨ | ☐ | ☐ |
| 3 | ☑ | PoE+ ∨ | Low | ☐ | ☐ |
| 4 | ☑ | PoE+ ∨ | High | ☐ | ☐ |
| 5 | ☑ | PoE+ ∨ | Critical | ☐ | ☐ |
| 6 | ☑ | PoE+ ∨ | Low ∨ | ☐ | ☐ |
| 7 | ☑ | PoE+ ∨ | Low ∨ | ☐ | ☐ |
| 8 | ☑ | PoE+ ∨ | Low ∨ | ☐ | ☐ |

SOLTECH
INFONET INC.

➢ **PD Alive**



➢ **PD Reset**



## AF/AT/BT Model

➢ **Enable | Disable**



➢ **PoE Mode**

• **AF/AT/BT Port**

• **AF/AT Port**

| Port | Enable | PoE Mode | Priority | PD Alive | PD Reset | PSE Detect |
|------|--------|----------|----------|----------|----------|------------|
| * | ☑ | <> ▼ | <> ▼ | ☐ | ☐ | ☑ |
| 1 | ☐ | 4p Type4 90w / 2p Type3 30w ▼ | Low ▼ | ☐ | ☐ | ☑ |
| 2 | ☑ | 4p Type4 90w / 2p Type3 30w ▼ | Low ▼ | ☐ | ☐ | ☑ |
| 3 | ☑ | 4p Type4 90w / 2p Type3 30w ▼ | Low ▼ | ☐ | ☐ | ☑ |
| 4 | ☑ | 4p Type4 90w / 2p Type3 30w ▼ | Low ▼ | ☐ | ☐ | ☑ |
| 5 | ☑ | 2p Type2 30w ▼ | Low ▼ | ☐ | ☐ | ☑ |
| 6 | ☑ | 2p Type3 30w | Low ▼ | ☐ | ☐ | ☑ |
| 7 | ☑ | 2p Type3 15w | Low ▼ | ☐ | ☐ | ☑ |
| 8 | ☑ | 2p Type2 30w | Low ▼ | ☐ | ☐ | ☑ |

2p Type3 Non Compliant 30w [Legacy]
2p Type3 BT Non Compliant 15w [Legacy]
2p Type3 Non Compliant 30w class0 = 4pair [Legacy]
2p Type3 Non Compliant 30w class0 = 4pair [Legacy]
2p Type4 Non Compliant PoH 45w
2p Type3 Compliant Special 30w [Legacy]
2p Type3 Non Compliant CDP 30w [Legacy]
2p Type2 Non Compliant 30w
2p 3 class events 30w Legacy [Legacy]
2p Type3 Non Compliant PoH 45w [Legacy]
2p All Classes Non Compliant PoH 45w [Legacy]
2p Type3 30w [Legacy]
2p Type3 Non Compliant Spec 45w [Legacy]

➢ **Priority(Low | High | Critical)**

| Port | Enable | PoE Mode | Priority | PD Alive | PD Reset | PSE Detect |
|------|--------|----------|----------|----------|----------|------------|
| * | ☑ | <> ▼ | <> ▼ | ☐ | ☐ | ☑ |
| 1 | ☑ | 4p Type4 90w / 2p Type3 30w ▼ | Low ▼ | ☐ | ☐ | ☑ |
| 2 | ☑ | 4p Type4 90w / 2p Type3 30w ▼ | Low ▼ | ☐ | ☐ | ☑ |
| 3 | ☑ | 4p Type4 90w / 2p Type3 30w ▼ | High | ☐ | ☐ | ☑ |
| 4 | ☑ | 4p Type4 90w / 2p Type3 30w ▼ | Critical | ☐ | ☐ | ☑ |
| 5 | ☑ | 2p Type2 30w ▼ | Low ▼ | ☐ | ☐ | ☑ |
| 6 | ☑ | 2p Type2 30w ▼ | Low ▼ | ☐ | ☐ | ☑ |
| 7 | ☑ | 2p Type2 30w ▼ | Low ▼ | ☐ | ☐ | ☑ |
| 8 | ☑ | 2p Type2 30w ▼ | Low ▼ | ☐ | ☐ | ☑ |

➢ **PD Alive(Enable | Disable)**

➢ **PD Reset(Enable | Disable)**

➢ **PSE Detect(Enable | Disable)**

| Port | Enable | PoE Mode | Priority | PD Alive | PD Reset | PSE Detect |
|------|--------|----------|----------|----------|----------|------------|
| * | ☑ | <> ▼ | <> ▼ | ☐ | ☐ | ☑ |
| 1 | ☑ | 4p Type4 90w / 2p Type3 30w ▼ | Low ▼ | ☑ | ☑ | ☑ |
| 2 | ☑ | 4p Type4 90w / 2p Type3 30w ▼ | Low ▼ | ☐ | ☐ | ☑ |
| 3 | ☑ | 4p Type4 90w / 2p Type3 30w ▼ | Low ▼ | ☐ | ☐ | ☑ |
| 4 | ☑ | 4p Type4 90w / 2p Type3 30w ▼ | Low ▼ | ☐ | ☐ | ☑ |
| 5 | ☑ | 2p Type2 30w ▼ | Low ▼ | ☐ | ☐ | ☑ |
| 6 | ☑ | 2p Type2 30w ▼ | Low ▼ | ☐ | ☐ | ☑ |
| 7 | ☑ | 2p Type2 30w ▼ | Low ▼ | ☐ | ☐ | ☑ |
| 8 | ☑ | 2p Type2 30w ▼ | Low ▼ | ☐ | ☐ | ☑ |

---

# EXAMPLE CLI CONFIGURATION

---

✓ **Power Over Ethernet Configuration**

➢ **Reserved Power Determined by**

• **Class(default) | LLDP-MED**

➢ **Power Management Mode**

• **Actual Consumption(default) | Reserved Power**

SOLTECH
INFONET INC.

```
(config)# poe management mode class-consumption
(config)# poe management mode class-reserved-power
(config)# poe management mode lldp-consumption
(config)# poe management mode lldp-reserved-power
```

> ➢ *Capacitor Detection*

> • *Disabled(default) | Enabled*

```
(config)# no poe capacitor-detect
(config)# poe capacitor-detect
```

✓ **PoE Power Supply Configuration**

> ➢ *Primary Power Supply*

> • *Power Source(Different for each Model)*

```
(config)# poe supply sid <v_1_to_2000>
(config)# poe supply sid 240
```

✓ **PoE Port Configuration**

> ➢ *Enable | Disable*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# poe enable
(config-if)# poe disable
```

> ➢ *PoE Mode*

> • *PoE | PoE+| BT*

```
AT/AF모델
(config-if)# poe mode { standard | plus }
(config-if)# poe mode standard
(config-if)# poe mode plus

BT모델
(config-if)# poe mode bt <bt_mode>
<0x0-0xFF>   0x00:BT_4P_90W_2P_30W
             0x02:BT_4P_30W_2P_30W
             0x03:BT_4P_15W_2P_15W
             009:4P_AS_2P_AT_30W_2P_AT_30W
             0x10:BT_4P_90W_2P_30W_L_DET
             0x11:BT_4P_60W_2P_30W_L_DET
             0x12:BT_4P_30W_2P_30W_L_DET
             0x13:BT_4P_15W_2P_15W_L_DET
             0x14:BT_4P_90W_2P_30W_L_DET_SP_C0
             0x15:BT_4P_60W_2P_30W_L_DET_SP_C0
             0x20:4P_90W_2P_45W_POH_IEEE_DET
             0x21:BT_4P_PRE_60W_2P_PRE_30W_L_DET
             0x22:4P_60W_2P_30W_L_DET
             0x23:BT_4P_PRE_60W_2P_PRE_30W_IEEE_DET
```

```
0x24:4P_4_FIN_60W_2P_3_FIN_30W_L_DET
0x25:BT_4P_POH_LIKE_90W_2P_POE_LIKE_45W_L_DET
0x26:4P_90W_2P_45W_POE_L_DET
0x27:BT_4P_60W_2P_30W_L_DET_SP_C4 0x30:BT_4P_90W_2P_45W_L_DET
```

➢ *Priority*

- *Low | High | Critical*

```
(config-if)# poe priority { low | high | critical }
(config-if)# poe priority low
(config-if)# poe priority high
(config-if)# poe priority critical
```

➢ *PD Alive*

```
(config-if)# poe pd-alive { enable | disable }
(config-if)# poe pd-alive enable
(config-if)# poe pd-alive disable
```

➢ *PD Reset*

```
(config-if)# poe pd-reset { enable | disable }
(config-if)# poe pd-reset enable
(config-if)# poe pd-reset disable
```

➢ *PSE Detect*

```
(config-if)# poe pse-detect { enable | disable }
(config-if)# poe pse-detect enable
(config-if)# poe pse-detect disable
```

## 6.12.2. Power off Scheduler

WEB MENU Configuration>PoE>Power off scheduler

This page allows users to configure time slots during which PoE will not be utilized for each port.



After setting up system time or NTP, use PoE Power Off Scheduler. If not set, the PoE Power Off Scheduler will not function correctly.

### PoE Power Off Scheduler

| Object | Description |
|---|---|
| **Port** | This is the logical port number. |
| **Enable** | Select the port(s) to apply PoE deactivation. When checked, day and time settings will be enabled. |
| | **Enable** — Select the days and times to deactivate PoE. |
| | **Disable** — PoE is always activate. |
| **Every, Sun, Mon, Tue, Wed, Thu, Fri, Sat** | Select the days to set PoE deactivation. The settings will repeat every week. |
| **Start Time** | This is the start time for PoE deactivation. It will only operate on the selected days. |
| **End Time** | This is the end time for PoE deactivation. It will only operate on the selected days. If set earlier than the Start Time, it will end at the configured time on the next day of the selected days. |
| **Description** | This displays the configured time for PoE deactivation. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

### EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>PoE>Power off scheduler

✓ **PoE Power Off Scheduler**

➢ *Enable*

**PoE Power Off Scheduler**

| Port | Enable | Every | SUN | MON | TUE | WED | THU | FRI | SAT | Start Time | ~ | End Time | Description |
|------|--------|-------|-----|-----|-----|-----|-----|-----|-----|------------|---|----------|-------------|
| * | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ◇∨ ◇∨ | | ◇∨ ◇∨ | |
| 1 | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | 00:00 ~ 24:00 & 00:00 ~ 00:00 |
| 2 | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | 00:00 ~ 24:00 & 00:00 ~ 00:00 |
| 3 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | |
| 4 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | |
| 5 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | |
| 6 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | |
| 7 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | |
| 8 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | |

➢ *Every, Sun, Mon, Tue, Wed, Thu, Fri, Sat*

**PoE Power Off Scheduler**

| Port | Enable | Every | SUN | MON | TUE | WED | THU | FRI | SAT | Start Time | ~ | End Time | Description |
|------|--------|-------|-----|-----|-----|-----|-----|-----|-----|------------|---|----------|-------------|
| * | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ◇∨ ◇∨ | | ◇∨ ◇∨ | |
| 1 | ☑ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | 00:00 ~ 24:00 & 00:00 ~ 00:00 |
| 2 | ☑ | ☐ | ☐ | ☑ | ☐ | ☑ | ☐ | ☑ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | 00:00 ~ 24:00 & 00:00 ~ 00:00 |
| 3 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | |
| 4 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | |
| 5 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | |
| 6 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | |
| 7 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | |
| 8 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | |

➢ *Start Time, End Time*

• *00:00~23:59*

**PoE Power Off Scheduler**

| Port | Enable | Every | SUN | MON | TUE | WED | THU | FRI | SAT | Start Time | ~ | End Time | Description |
|------|--------|-------|-----|-----|-----|-----|-----|-----|-----|------------|---|----------|-------------|
| * | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ◇∨ ◇∨ | | ◇∨ ◇∨ | |
| 1 | ☑ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 8∨h 0∨m | ~ | 16∨h 0∨m | 08:00 ~ 16:00 |
| 2 | ☑ | ☐ | ☐ | ☑ | ☐ | ☑ | ☐ | ☑ | ☐ | 20∨h 0∨m | ~ | 4∨h 0∨m | 20:00 ~ 24:00 & 00:00 ~ 04:00 |
| 3 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | |
| 4 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | |
| 5 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | |
| 6 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | |
| 7 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | |
| 8 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | 0∨h 0∨m | ~ | 0∨h 0∨m | |

## EXAMPLE CLI CONFIGURATION

✓ **PoE Power Off Scheduler**

➢ *Enable*

➢ *Every, Sun, Mon, Tue, Wed, Thu, Fri, Sat*

➢ *Start Time, End Time*

• *00:00~23:59*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1
(config)# interface GigabitEthernet 1/2

(config-if)# poe scheduler [ mode { disable | enable } ] [ day { [ Every-day ] [ SUN ] [ MON ] [ TUE ]
[ WED ] [ THU ] [ FRI ] [ SAT ] } ] [ start-time <has_start_hour> <has_start_min> ] [ end-time
<has_end_hour> <has_end_min> ]
(config-if)# poe scheduler mode enable day Every-day start-time 8 0 end-time 16 0
(config-if)# poe scheduler mode enable day MON WED FRI start-time 20 0 end-time 4 0
```

SOLTECH
INFONET INC.

## 6.12.3. PoE Monitor

WEB MENU Monitor>PoE

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

**Power Over Ethernet Status**

| Local Port | PD class | Power Requested | Power Allocated | Power Used | Current Used | Priority | Port Status |
|---|---|---|---|---|---|---|---|
| 1 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 2 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 3 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 4 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 5 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 6 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 7 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 8 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF |
| Total | | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | | |

### Power Over Ethernet Status

| Object | Description |
|---|---|
| **Local Port** | This is the logical port number. The last row displays the sum of all ports. |
| **PD Class** | Each PD(Power Device) is classified according to a class that defines the maximum power the PD will use. The PD Class displays the class of the PD. Class 0: Max. power 15.4 W Class 1: Max. power 4.0 W Class 2: Max. power 7.0 W Class 3: Max. power 15.4 W Class 4: Max. power 30.0 W |
| **Power Requested** | The Power Requested displays the requested amount of power the PD wants to be reserved. |
| **Power Allocated** | The Power Allocated displays the power provided by the PSE (Power Sourcing Equipment) to the PD. |
| **Power Used** | The Power Used displays the actual power consumed by the PD. |
| **Current Used** | The Current Used displays the actual current consumed by the PD. |
| **Priority** | The Priority displays the priority assigned by the user to the PoE port. |
| **Port Status** | The Port Status displays the current status of the PoE port. Each port is separated, and the meanings of the statements are as follows: |

| | |
|---|---|
| PoE turned ON | PD is connected to the PoE port and is currently operating. |
| PoE turned OFF | The PoE port is turned off due to the connected device not being a PD (Power Device) and therefore not receiving power delivery. |
| PoE turned OFF  - PoE disabled | The PoE port is turned off due to the user setting it as disabled in the PoE configurations. |
| PoE turned OFF  - Power budget exceeded | The PoE port is turned off due to the PSE (Power Sourcing Equipment) |

|  | | exceeding its maximum power limit. |
|  | PoE turned OFF - PD overload | The PoE port is turned off due to the power usage exceeding the available allocation for the port. |
|  | PoE turned OFF - High temperature | The PoE port is turned off due to high PSE (Power Sourcing Equipment) temperature. |
|  | No PD detected | No device is connected to the PoE port. |

**PoE average total power [W]**

AVG [W]  0
100%

75%

50%

25%
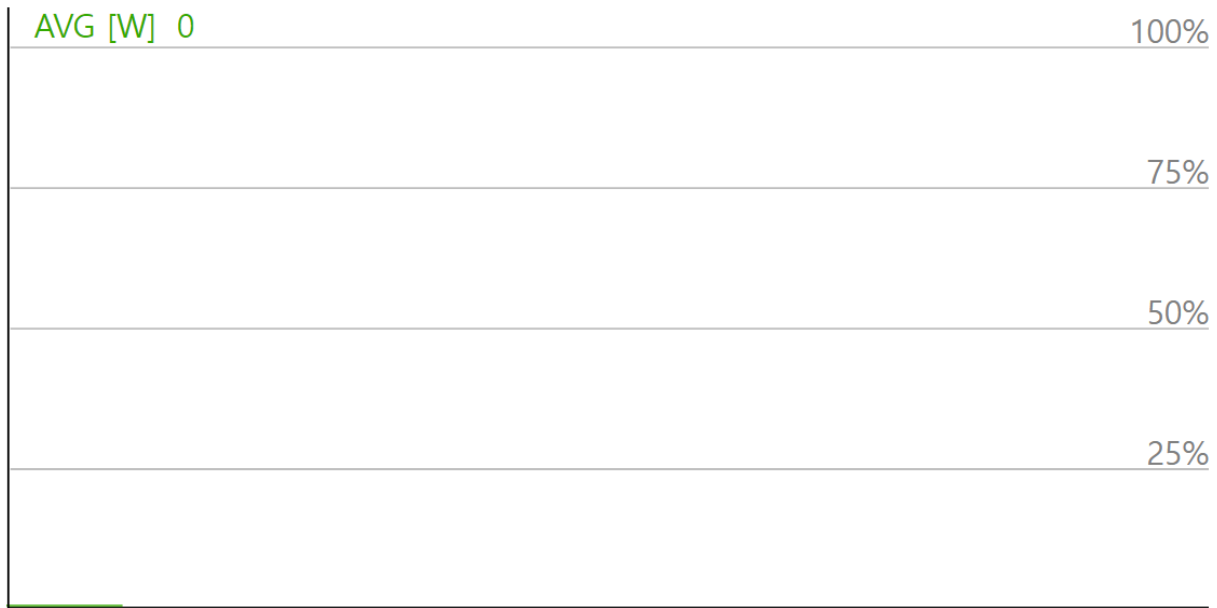
## Poe average total power

| Object | Description |
|---|---|
| **AVG [W]** | "AVG" displays the average value of the current PoE power usage from the PSE (Power Sourcing Equipment). The unit is in watts (W). |
| **Graph** | This is a graph depicting the average power consumption. The X-axis spans the entire day, while the Y-axis, scaled to 100%, represents the equipment's maximum power capacity. In other words, it displays the average power consumption over a maximum of one day from the present moment. |

**Buttons**

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

Refresh : Click to refresh the page.

SOLTECH
INFONET INC.

# 6.13. EPS

## 6.13.1. EPS Configuration

WEB MENU Configuration>EPS

The Ethernet (Linear) Protection Switch instances are configured here.

**Ethernet Protection Switching**

| Delete | EPS ID | Domain | Architecture | W Flow | P Flow | W SF MEP | P SF MEP | APS MEP | Alarm |

Add New EPS    Apply&Save    Apply    Reset

### Ethernet Protection Switching

| Object | Description |
|---|---|
| **Delete** | This box is used to mark an EPS for deletion in next Save operation. |
| **EPS ID** | The ID of the EPS. Click on the ID of an EPS to enter the configuration page. The range is 1-100. |
| **Domain** | Port: This will create a EPS in the Port Domain. 'W/P Flow' is a Port. |
| **Architecture** | **1+1**      This will create a 1+1 EPS. <br> **1:1**      This will create a 1:1 EPS. |
| **W Flow** | The working flow for the EPS - See 'Domain'. |
| **P Flow** | The protecting flow for the EPS - See 'Domain'. |
| **W SF MEP** | The working Signal Fail reporting MEP. |
| **P SF MEP** | The protecting Signal Fail reporting MEP. |
| **APS MEP** | The APS PDU handling MEP. |
| **Alarm** | There is an active alarm on the EPS. |

### Buttons

Add New EPS : Click to add a new EPS entry.

Refresh : Click to refresh the page immediately.

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

### EPS Configuration

Click on the ID of an EPS to enter the configuration page.

This page allows the user to inspect and configure the current EPS Instance.

**EPS Configuration**

**Instance Data**

| EPS ID | Domain | Architecture | W Flow | P Flow | W SF MEP | P SF MEP | APS MEP |
|--------|--------|--------------|--------|--------|----------|----------|---------|
| 1 | Port | 1+1 | 1 | 2 | 1 | 2 | 2 |

**Instance Configuration**

| Protection Type | APS | Revertive | WTR Time | Hold Off Time |
|-----------------|-----|-----------|----------|---------------|
| Unidirectional ▾ | ☐ | ☐ | 300 | 0 |

**Instance Command**

| Command |
|---------|
| None ▾ |

**Instance State**

| Protection State | W Flow | P Flow | Transmit APS r/b | Receive APS r/b | Architecture Mismatch | APS On Working | Switching Incomplete | No Aps Received |
|------------------|--------|--------|------------------|-----------------|-----------------------|----------------|----------------------|-----------------|
| Disabled | OK | OK | NR Null/Null | NR Null/Null | 🟢 | 🟢 | 🟢 | 🟢 |

## EPS Configuration

### Instance Data

| Object | Description |
|--------|-------------|
| **EPS ID** | The ID of the EPS. |
| **Domain** | See help on EPS create WEB. |
| **Architecture** | See help on EPS create WEB. |
| **W Flow** | See help on EPS create WEB. |
| **P Flow** | See help on EPS create WEB. |
| **W SF MEP** | See help on EPS create WEB. |
| **P SF MEP** | See help on EPS create WEB. |
| **APS MEP** | See help on EPS create WEB. |

### Instance Configuration

| Object | Description | |
|--------|-------------|---|
| **Protection Type** | Unidirectional | EPS in the two ends can select traffic from different working/protecting flow. This is only possible in case of 1+1. |
| | **Bidirectional** | EPS in the two ends is selecting traffic from the same working/protecting flow. This requires APS enabled. This is mandatory for 1:1 |
| **APS** | The Automatic Protection Switching protocol can be enabled/disabled. This is mandatory for 1:1. | |
| **Revertive** | The revertive switching to working flow can be enabled/disabled. | |
| **WTR Time** | The Wait To Restore timing value to be used in revertive switching. Range is 1 to 720 seconds. | |
| **Hold Off Time** | The timing value to be used to make persistent check on Signal Fail before switching. This is in 100 ms. and the max value is 100 (10 sec). | |

### Instance Command

| Object | Description | |
|--------|-------------|---|
| **Command** | None | There is no active local command on this instance. |
| | Clear | The active local command will be cleared. |
| | Lock Out | This EPS is locked to working (not active). In case of 1:N (more than one EPS with same protecting flow) - when one EPS switch to protecting flow, other EPS is enforced this command |
| | Forced Switch | Forced switch to protecting. |
| | Manual Switch P | Manual switch to protecting. |

SOLTECH
INFONET INC.

| | | |
|---|---|---|
| | Manual Switch W | Manual switch to working. This is only allowed in case of 'non-revertive' mode |
| | Exercise | Exercise of the protocol - not traffic effecting. This is only allowed in case of 'Bidirectional' protection type |
| | Freeze | This EPS is locally freezed - ignoring all input. |
| | Lock Out Local | This EPS is locally "locked out" - ignoring local SF detected on working. |

**Instance State**

| Object | Description | |
|---|---|---|
| **Protection State** | EPS state according to State Transition Tables in G.8031. | |
| **W Flow** | OK | State of working flow is ok |
| | SF | State of working flow is Signal Fail |
| | SD | State of working flow is Signal Degrade (for future use) |
| **P Flow** | OK | State of protecting flow is ok |
| | SF | State of protecting flow is Signal Fail |
| | SD | State of protecting flow is Signal Degrade (for future use) |
| **Transmit APS r/b** | The transmitted APS according to State Transition Tables in G.8031. | |
| **Receive APS r/b** | The received APS according to State Transition Tables in G.8031. | |
| **Architecture Mismatch** | The architecture indicated in the received APS does not match the locally configured. | |
| **APS on working** | APS is received on the working flow. | |
| **Switching Incomplete** | Traffic is not selected from the same flow instance in the two ends. | |
| **No APS Received** | APS PDU is not received from the other end. | |

**Buttons**

Refresh : Click to refresh the page immediately.

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

✓ **Ethernet Protection Switching**

➤ *Add New EPS*

**Ethernet Protection Switching**

| Delete | EPS ID | Domain | Architecture | W Flow | P Flow | W SF MEP | P SF MEP | APS MEP | Alarm |
|---|---|---|---|---|---|---|---|---|---|
| Delete | 1 | Port ∨ | 1+1 ∨ | 1 | 1 | 1 | 1 | 1 | |

- *EPS ID (1~100)*

- *Domain(Port)*

- *Architecture(1+1 | 1:1)*

- *W Flow(MEP instance number)*

- *P Flow(MEP instance number)*

- *W SF MEP(MEP instance number)*

- *P SF MEP(MEP instance number)*

- *APS MEP(MEP instance number | Not W Flow)*

- *Alarm*

| Delete | EPS ID | Domain | Architecture | W Flow | P Flow | W SF MEP | P SF MEP | APS MEP | Alarm |
|---|---|---|---|---|---|---|---|---|---|
| ☐ | 1 | Port | 1:1 | 1 | 2 | 1 | 2 | 2 | 🔴 |

*Click EPS ID*

- ✓ **EPS Configuration**
- ✓ **Instance Data**

| EPS ID | Domain | Architecture | W Flow | P Flow | W SF MEP | P SF MEP | APS MEP |
|---|---|---|---|---|---|---|---|
| 1 | Port | 1:1 | 1 | 2 | 1 | 2 | 2 |

- ✓ **Instance Configuration**

  - *Protection Type (Unidirectional | Bidirectional)*

  - *APS*

  - *Revertive*

  - *WTR Time(1~720)*

  - *Hold Off Time(0~100 10sec)*

    *1+1 Unidirectional*

| Protection Type | APS | Revertive | WTR Time | Hold Off Time |
|---|---|---|---|---|
| Unidirectional ▾ | ☐ | ☐ | 300 | 0 |

    Unidirectional
    Bidirectional

    *1+1 Bidirectional*

| Protection Type | APS | Revertive | WTR Time | Hold Off Time |
|---|---|---|---|---|
| Bidirectional ▾ | ☑ | ☑ | 300 | 0 |

    *1:1*

| Protection Type | APS | Revertive | WTR Time | Hold Off Time |
|---|---|---|---|---|
| Bidirectional | ✓ | ☑ | 300 | 0 |

- ✓ **Instance Command**

  - *None | Clear | Lock Out | Forced Switch | Manual Switch P | Manual Switch W | Exercise | Freeze | Lock Out Local*

| Command |
|---|
| None ▾ |

    None
    Clear
    Lock Out
    Forced Switch
    Manual Switch P
    Manual Switch W
    Exercise
    Freeze
    Lock Out Local

SOLTECH
INFONET INC.

✓ **Instance State**

- *Protection State*

- *W Flow*

- *P Flow*

- *Transmit APS r/b*

- *Receive APS r/b*

- *Architecture Mismatch*

- *APS On Working*

- *Switching Incomplete*

- *No APS Received*

| Protection State | W Flow | P Flow | Transmit APS r/b | Receive APS r/b | Architecture Mismatch | APS On Working | Switching Incomplete | No Aps Received |
|---|---|---|---|---|---|---|---|---|
| SfW | SF | OK | SFw Normal/Normal | SFw Normal/Normal | 🟢 | 🟢 | 🟢 | 🟢 |

## EXAMPLE CLI CONFIGURATION

✓ **Ethernet Protection Switching**

➢ *Add New EPS*

- *EPS ID (1~100)*

- *Domain(Port)*

- *Architecture(1+1 | 1:1)*

- *W Flow(MEP instance number)*

- *P Flow(MEP instance number)*

```
(config)# eps <inst> domain { port | tunnel-tp | pw } architecture { 1plus1 | 1for1 } work-flow
{ <flow_w> | <port_type> <port_w> } protect-flow { <flow_p> | <port_type> <port_p> }
(config)# eps 1 domain port architecture 1for1 work-flow GigabitEthernet 1/1 protect-flow
GigabitEthernet
```

- *W SF MEP(MEP instance number)*

- *P SF MEP(MEP instance number)*

- *APS MEP(MEP instance number | Not W Flow )*

```
(config)# eps <inst> mep-work <mep_w> mep-protect <mep_p> mep-aps <mep_aps>
(config)# eps 1 mep-work 1 mep-protect 2 mep-aps 2
```

✓ **EPS Configuration**

✓ **Instance Configuration**

- *Protection Type (Unidirectional | Bidirectional)*

SOLTECH
INFONET INC.

*1+1 Unidirectional*
*1+1 Bidirectional*

- *APS*

```
(config)# eps <inst> 1plus1 { bidirectional | { unidirectional [ aps ] } }
(config)# eps 1 1plus1 bidirectional
(config)# eps 1 1plus1 unidirectional
(config)# eps 1 1plus1 unidirectional aps
```

- *Revertive*

- *WTR Time(1~720)*

```
(config)# eps <inst> revertive { 10s | 30s | 5m | 6m | 7m | 8m | 9m | 10m | 11m | 12m | { wtr-value
<wtr_value> } }
(config)# eps 1 revertive 10s
(config)# eps 1 revertive wtr-value 10
(config)# eps 1 revertive 12m
(config)# eps 1 revertive wtr-value 720
```

- *Hold Off Time(0~100 10sec)*

```
(config)# eps <inst> holdoff <hold>
(config)# eps 1 holdoff 100
(config)# eps 1 holdoff 1
(config)# eps 1 holdoff 0
```

✓ **Instance Command**

- *None | Clear | Lock Out | Forced Switch | Manual Switch P | Manual Switch W | Exercise | Freeze | Lock Out Local*

```
(config)# eps <inst> command { lockout | forced | manualp | manualw | exercise | freeze |
lockoutlocal }
(config)# no eps 1 command
(config)# eps 1 command lockout
```

## 6.14. MEP

## 6.14.1. MEP Configuration

WEB MENU Configuration>MEP

The Maintenance Entity Point instances are configured here.

**Maintenance Entity Point**

| Delete | Instance | Domain | Mode | Direction | Residence Port | Level | Flow Instance | Tagged VID | This MAC | Alarm |
|---|---|---|---|---|---|---|---|---|---|---|

Add New MEP

### Maintenance Entity Point

| Object | Description |
|---|---|
| **Delete** | This box is used to mark a MEP for deletion in next Save operation. |
| **Instance** | The ID of the MEP. Click on the ID of a MEP to enter the configuration page. The range is from 1 through 100. |
| **Domain** | Port: This is a MEP in the Port Domain. |
| **Mode** | MEP: This is a Maintenance Entity End Point.<br>MIP: This is a Maintenance Entity Intermediate Point. |
| **Direction** | Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.<br>Up: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'. |
| **Residence Port** | The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member. |
| **Level** | The MEG level of this MEP. |
| **Flow Instance** | The MEP is related to this flow - See 'Domain'.<br>This is not relevant and not shown in case of Port MEP. |
| **Tagged VID** | Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.<br>EVC MEP: This is not used.<br>VLAN MEP: This is not used.<br>EVC MIP: On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active. |
| **This MAC** | The MAC of this MEP - can be used by other MEP when unicast is selected (Info only). |
| **Alarm** | There is an active alarm on the MEP. |

**Buttons**

Add New MEP : Click to add a new MEP entry.

Refresh : Click to refresh the page immediately.

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

SOLTECH
INFONET INC.

## MEP Configuration

This page allows the user to inspect and configure the current MEP Instance.



### Instance Data

| Object | Description |
|---|---|
| MEP Instance | The ID of the MEP. |
| Domain | See help on MEP create WEB. |
| Mode | See help on MEP create WEB. |
| Direction | See help on MEP create WEB. |
| Residence Port | See help on MEP create WEB. |
| Flow Instance | See help on MEP create WEB. |
| Tagged VID | See help on MEP create WEB. |
| This MAC | See help on MEP create WEB. |

### Instance Configuration

| Object | Description |
|---|---|
| Level | See help on MEP create WEB. |
| Format | This is the configuration of the two possible Maintenance Association Identifier formats.<br>**ITU ICC**: This is defined by ITU (Y1731 Fig. A3). 'Domain Name' is not used. 'MEG id' must be max. 13 char.<br>**IEEE String**: This is defined by IEEE (802.1ag Section 21.6.5). 'Domain Name' can be max. 16 char. 'MEG id' (Short MA Name) can be max. 16 char.<br>**ITU CC ICC**: This is defined by ITU (Y1731 Fig. A5). 'Domain Name' is not used. 'MEG id' must be max. 15 char. |
| Domain Name | This is the IEEE Maintenance Domain Name and is only used in case of 'IEEE String' |

|  | format. This string can be empty giving Maintenance Domain Name Format 1 - Not present. This can be max 16 char. |
|---|---|
| **MEG Id** | This is either ITU MEG ID or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this must be 13 char. In case of ITU CC ICC format this must be 15 char. In case of IEEE String format this can be max 16 char. |
| **MEP Id** | This value will become the transmitted two byte CCM MEP ID. |
| **Tagged VID** | This value will be the VID of a TAG added to the OAM PDU. |
| **VOE** | This will attempt to utilize VOE HW for MEP implementation. Not all platforms support VOE. |
| **cLevel** | Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP. |
| **cMEG** | Fault Cause indicating that a CCM is received with a MEG ID different from configured for this MEP. |
| **cMEP** | Fault Cause indicating that a CCM is received with a MEP ID different from all 'Peer MEP ID' configured for this MEP. |
| **cAIS** | Fault Cause indicating that AIS PDU is received. |
| **cLCK** | Fault Cause indicating that LCK PDU is received. |
| **cDEG** | Fault Cause indicating that server layer is indicating Signal Degraded. |
| **cSSF** | Fault Cause indicating that server layer is indicating Signal Fail. |
| **aBLK** | The consequent action of blocking service frames in this flow is active. |
| **aTSD** | The consequent action of indicating Trail Signal Degrade is calculated. |
| **aTSF** | The consequent action of indicating Trail Signal Fail to-wards protection is active. |

### Peer MEP Configuration

| Object | Description |
|---|---|
| **Delete** | This box is used to mark a Peer MEP for deletion in next Save operation. |
| **Peer MEP ID** | This value will become an expected MEP ID in a received CCM - see 'cMEP'. |
| **Unicast Peer MAC** | This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP. |
| **cLOC** | Fault Cause indicating that no CCM has been received (in 3,5 periods) - from this peer MEP. |
| **cRDI** | Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP. |
| **cPeriod** | Fault Cause indicating that a CCM is received with a period different what is configured for this MEP - from this peer MEP. |
| **cPriority** | Fault Cause indicating that a CCM is received with a priority different what is configured for this MEP - from this peer MEP. |

### Functional Configuration

### Continuity Check

| Object | Description |
|---|---|
| **Enable** | Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1. |
| **Priority** | The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be |

| | the same. |
|---|---|
| **Frame rate** | Selecting the frame rate of CCM PDU. This is the inverse of transmission period as described in Y.1731. This value has the following uses:<br>* The transmission rate of the CCM PDU.<br>* Fault Cause cLOC is declared if no CCM PDU has been received within 3.5 periods - see 'cLOC'.<br>* Fault Cause cPeriod is declared if a CCM PDU has been received with different period - see 'cPeriod'.<br>Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same. |
| **TLV** | Enable/disable of TLV insertion in the CCM PDU. |

### APS Protocol

| Object | Description |
|---|---|
| **Enable** | Automatic Protection Switching protocol information transportation based on transmitting/receiving R-APS/L-APS PDU can be enabled/disabled. Must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured. |
| **Priority** | The priority to be inserted as PCP bits in TAG (if any). |
| **Cast** | Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. Unicast is only valid for L-APS - see 'Type'. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032. |
| **Type** | R-APS: APS PDU is transmitted as R-APS - this is for ERPS.<br>L-APS: APS PDU is transmitted as L-APS - this is for ELPS. |
| **Last Octet** | This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031 (03/2010) a RAPS multi-cast MAC is defined as 01-19-A7-00-00-XX. In current standard the value for this last octet is '01' and the usage of other values is for further study. |

### TLV Configuration

Configuration of the OAM PDU TLV. Currently only TLV in the CCM is supported.

| Object | Description |
|---|---|
| **Organization Specific<br>- OUI First** | The transmitted first value in the OS TLV OUI field. |
| **- OUI Second** | The transmitted second value in the OS TLV OUI field. |
| **- OUI Third** | The transmitted third value in the OS TLV OUI field. |
| **- Sub-Type** | The transmitted value in the OS TLV Sub-Type field. |
| **- Value** | The transmitted value in the OS TLV Value field. |

### TLV Status

Display of the last received TLV. Currently only TLV in the CCM is supported.

| Object | Description |
|---|---|
| **CC Organization Specific<br>- OUI First** | The last received first value in the OS TLV OUI field. |

| - OUI Second | The last received second value in the OS TLV OUI field. |
|---|---|
| - OUI Third | The last received third value in the OS TLV OUI field. |
| - Sub-Type | The last received value in the OS TLV Sub-Type field. |
| - Value | The last received value in the OS TLV Value field. |
| - Last RX | OS TLV was received in the last received CCM PDU. |
| **CC Port Status**<br>- Value | The last received value in the PS TLV Value field. |
| - Last RX | PS TLV was received in the last received CCM PDU. |
| **CC Interface Status**<br>- Value | The last received value in the IS TLV Value field. |
| - Last RX | IS TLV was received in the last received CCM PDU. |

### Link State Tracking

| Object | Description |
|---|---|
| **Enable** | When LST is enabled in an instance, Local SF or received 'isDown' in CCM Interface Status TLV, will bring down the residence port. Only valid in Up-MEP. The CCM rate must be 1 f/s or faster. |

**Buttons**

 : Click to add a new peer MEP.





 : Click to go to Fault Management page.

 : Click to go to Performance Monitor page.

 : Click to refresh the page immediately.

 : Click to apply changes.

 : Click to apply and save changes.

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

## Fault Management - Instance 1 - MEP id 1

This page allows the user to inspect and configure the Fault Management of the current MEP Instance.

### Fault Management - Instance 1 - MEP id 1

#### Loop Back

| Enable | DEI | Priority | Cast | Peer MEP | Unicast MAC | To Send | Size | Interval |
|--------|-----|----------|------|----------|-------------|---------|------|----------|
| ☐ | ☐ | 0 | Multi ▾ | 1 | 00-00-00-00-00-00 | 10 | 64 | 100 |

#### Loop Back State

| Transaction ID | Transmitted | Reply MAC | Received | Out Of Order |
|----------------|-------------|-----------|----------|--------------|
| 1 | 0 | 00-00-00-00-00-00 | 0 | 0 |

#### Link Trace

| Enable | Priority | Peer MEP | Unicast MAC | Time To Live |
|--------|----------|----------|-------------|--------------|
| ☐ | 0 | 1 | 00-00-00-00-00-00 | 1 |

#### Link Trace State

| Transaction ID | Time To Live | Mode | Direction | Forwarded | Relay | Last MAC | Next MAC |
|----------------|--------------|------|-----------|-----------|-------|----------|----------|
| No Transactions | | | | | | | |

#### Test Signal

| Tx | Rx | DEI | Priority | Peer MEP | Rate | Size | Pattern | Sequence Number |
|----|----|----|----------|----------|------|------|---------|-----------------|
| ☐ | ☐ | ☐ | 0 | 1 | 1 | 64 | All Zero ▾ | ☐ |

#### Test Signal State

| TX frame count | RX frame count | RX rate | Test time | Clear |
|----------------|----------------|---------|-----------|-------|
| 0 | 0 | 0 | 0 | ☐ |

#### Client Configuration

| | Flow | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Domain | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ |
| Instance | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Level | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| AIS prio | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ |
| LCK prio | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ |

#### AIS

| Enable | Frame Rate | Protection |
|--------|------------|------------|
| ☐ | 1 f/sec ▾ | ☐ |

#### LOCK

| Enable | Frame Rate |
|--------|------------|
| ☐ | 1 f/sec ▾ |

Back

### Loop Back

| Object | Description |
|--------|-------------|
| **Enable** | Loop Back based on transmitting/receiving LBM/LBR PDU can be enabled/disabled. Loop Back is automatically disabled when all 'To Send' LBM PDU has been transmitted - waiting 5 sec. for all LBR from the end. |
| **DEI** | The DEI to be inserted as PCP bits in TAG (if any). |
| **Priority** | The priority to be inserted as PCP bits in TAG (if any). |

SOLTECH
INFONET INC.

| Cast | Selection of LBM PDU transmitted unicast or multi-cast. The unicast MAC will be configured through 'Peer MEP' or 'Unicast Peer MAC'. To-wards MIP only unicast Loop Back is possible. |
|---|---|
| Peer MEP | This is only used if the 'Unicast MAC' is configured to all zero. The LBM unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer. |
| Unicast MAC | This is only used if NOT configured to all zero. This will be used as the LBM PDU unicast MAC. This is the only way to configure Loop Back to-wards a MIP. |
| To Send | The number of LBM PDU to send in one loop test. The value 0 indicate infinite transmission (test behavior). This is HW based LBM/LBR and Requires VOE. |
| Size | The LBM frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing LBM OAM PDU - including CRC (four bytes). <br> Example when 'Size' = 64=> Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + LBM PDU LENGTH(46) + CRC(4) = 64 bytes <br> The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC. <br> There are two frame MAX sizes to consider. <br> Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 10240 Bytes <br> CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 1526 Bytes <br> Consider that the Peer MEP must be able to handle the selected frame size. Consider that In case of SW based MEP, the received LBR PDU must be copied to CPU <br> Warning will be given if selected frame size exceeds the CPU RX frame MAX size <br> Frame MIN Size is 64 Bytes. |
| Interval | The interval between transmitting LBM PDU. In 10ms. in case 'To Send' != 0 (max 100 - '0' is as fast as possible) In 1us. in case 'To Send' == 0 (max 10.000)". |

### Loop Back State

| Object | Description |
|---|---|
| Transaction ID | The transaction id of the first LBM transmitted. For each LBM transmitted the transaction id in the PDU is incremented. |
| Transmitted | The total number of LBM PDU transmitted. |
| Reply MAC | The MAC of the replying MEP/MIP. In case of multi-cast LBM, replies can be received from all peer MEP in the group. This MAC is not shown in case of 'To Send' == 0. |
| Received | The total number of LBR PDU received from this 'Reply MAC'. |
| Out Of Order | The number of LBR PDU received from this 'Reply MAC' with incorrect 'Transaction ID'. |

### Link Trace

| Object | Description |
|---|---|
| Enable | Link Trace based on transmitting/receiving LTM/LTR PDU can be enabled/disabled. Link Trace is automatically disabled when all 5 transactions are done with 5 sec. interval - waiting 5 sec. for all LTR in the end. The LTM PDU is always transmitted as Multi-cast Class 2. |
| Priority | The priority to be inserted as PCP bits in TAG (if any). |
| Peer MEP | This is only used if the 'Unicast MAC' is configured to all zero. The Link Trace Target MAC will be taken from the 'Unicast Peer MAC' configuration of this peer. |

| Unicast MAC | This is only used if NOT configured to all zero. This will be used as the Link Trace Target MAC. This is the only way to configure a MIP as Target MAC. |
| Time To Live | This is the LTM PDU TTL value as described in Y.1731. This value is decremented each time forwarded by a MIP. Will not be forwarded reaching zero. |

### Link Trace State

| Object | Description |
| --- | --- |
| Transaction ID | The transaction id is incremented for each LTM send. This value is inserted the transmitted LTM PDU and is expected to be received in the LTR PDU. Received LTR with wrong transaction id is ignored. There are five transactions in one Link Trace activated. |
| Time To Live | This is the TTL value taken from the LTM received by the MIP/MEP sending this LTR - decremented as if forwarded. |
| Mode | Indicating if is was a MEP/MIP sending this LTR. |
| Direction | Indicating if MEP/MIP sending this LTR is ingress/egress. |
| Forwarded | Indicating if MEP/MIP sending this LTR has forwarded the LTM. |
| Relay | The Relay action can be one of the following<br>MAC: The was a hit on the LT Target MAC<br>FDB: LTM is forwarded based on hit in the Filtering DB<br>MFDB: LTM is forwarded based on hit in the MIP CCM DB |
| Last MAC | The MAC identifying the last sender of the LBM causing this LTR - initiating MEP or previous MIP forwarding. |
| Next MAC | The MAC identifying the next sender of the LBM causing this LTR - MIP forwarding or terminating MEP. |

### Test Signal

| Object | Description |
| --- | --- |
| Enable | Test Signal based on transmitting TEST PDU can be enabled/disabled. |
| DEI | The DEI to be inserted as PCP bits in TAG (if any). |
| Priority | The priority to be inserted as PCP bits in TAG (if any). |
| Peer MEP | The TEST frame destination MAC will be taken from the 'Unicast Peer MAC' configuration of this peer. |
| Rate | The transmission rate of the test frame. |
| Size | The TEST frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing TEST OAM PDU - including CRC (four bytes).<br>Example when 'Size' = 64=> Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TEST PDU LENGTH(46) + CRC(4) = 64 bytes<br>The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.<br>There are two frame MAX sizes to consider.<br>Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 10240 Bytes<br>CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 1526 Bytes<br>Consider that the Peer MEP must be able to handle the selected frame size. Consider that in order to calculate the 'RX rate' a received TEST PDU must be copied to CPU |

| | |
|---|---|
| | Warning will be given if selected frame size exceeds the CPU RX frame MAX size Frame MIN Size is 64 Bytes. |
| **Pattern** | The 'empty' TEST PDU has the size of 12 bytes. In order to achieve the configured frame size a data TLV will be added with a pattern.<br>Example when 'Size' = 64=> Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TEST PDU LENGTH(46) + CRC(4) = 64 bytes<br>The TEST PDU needs to be 46 bytes so a pattern of 46-12=34 bytes will be added.<br>All Zero: Pattern will be '00000000'<br>All One: Pattern will be '11111111'<br>10101010: Pattern will be '10101010' |

### Test Signal State

| Object | Description |
|---|---|
| **TX frame count** | The number of transmitted TEST frames since last 'Clear'. |
| **RX frame count** | The number of received TEST frames since last 'Clear'. |
| **RX rate** | The current received TEST frame bit rate in Kbps. This is calculated on a 1 s. basis, starting when first TEST frame is received after 'Clear'. The frame size used for this calculation is the first received after 'Clear' |
| **Test time** | The number of seconds passed since first TEST frame received after last 'Clear'. |
| **Clear** | This will clear all Test Signal State. Transmission of TEST frame will be restarted. Calculation of 'Rx frame count', 'RX rate' and 'Test time' will be started when receiving first TEST frame. |

### Client Configuration

Only a Port MEP is able to be a server MEP with flow configuration. The Priority in the client flow is always the highest priority configured in the EVC.

| Object | Description |
|---|---|
| **Domain** | The domain of the client layer flow. |
| **Instance** | Client layer flow instance numbers. |
| **Level** | Client layer level - AIS and LCK PDU transmitted in this client layer flow will be on this level. |
| **AIS Prio** | The priority to be used when transmitting AIS in each client flow. Priority resulting in highest possible PCP can be selected. |
| **LCK Prio** | The priority to be used when transmitting LCK in each client flow. Priority resulting in highest possible PCP can be selected. |

### AIS

| Object | Description |
|---|---|
| **Enable** | Insertion of AIS signal (AIS PDU transmission) in client layer flows, can be enable/disabled. |
| **Frame Rate** | Selecting the frame rate of AIS PDU. This is the inverse of transmission period as described in Y.1731. |
| **Protection** | Selecting this means that the first 3 AIS PDU is transmitted as fast as possible - in case of using this for protection in the end point. |

**LOCK**

| Object | Description |
|--------|-------------|
| **Enable** | Insertion of LOCK signal (LCK PDU transmission) in client layer flows, can be enable/disabled. |
| **Frame Rate** | Selecting the frame rate of LCK PDU. This is the inverse of transmission period as described in Y.1731.: |

**Buttons**

Back : Click to go back to this MEP instance main page.

Refresh : Click to refresh the page immediately.

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

## Performance Monitor - Instance 1 - MEP id 1

You can use this page to inspect and configure the performance monitor of the current MEP instance.

**Performance Monitor - Instance 1 - MEP id 1**                                                          Refresh

**Performance Monitoring Data Set**

| Enable |
|---|
| ☐ |

**Loss Measurement**

| Tx | Rx | Priority | Cast | Peer MEP | Rate | Size | Synthetic | Ended | FLR Interval | Meas. Interval | Loss Threshold | SLM Test ID |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | ☐ | 0 | Multi ▾ | 1 | 1 f/sec ▾ | 64 | ☐ | Single ▾ | 5 | 1000 | 0 | 0 |

**Loss Measurement State**

| Peer MEP ID | Tx | Rx | Near End Loss Count | Far End Loss Count | Interval Elapsed | Interval Near End Loss Ratio | Interval Far End Loss Ratio | Total Near End Loss Ratio | Total Far End Loss Ratio | Clear |
|---|---|---|---|---|---|---|---|---|---|---|
| No Peer MEP Added | | | | | | | | | | |

**Loss Measurement Availability**

| Enable | Interval | FLR Threshold | Maintenance |
|---|---|---|---|
| ☐ | 10 | 10 | ☐ |

**Loss Measurement Availability State**

| Peer MEP ID | Near Availability Count | Far Availability Count | Near Unavailability Count | Far Unavailability Count | Near State | Far State |
|---|---|---|---|---|---|---|
| No Peer MEP Added | | | | | | |

**Loss Measurement High Loss Interval**

| Enable | FLR Threshold | Consecutive Interval |
|---|---|---|
| ☐ | 100 | 100 |

**Loss Measurement High Loss Interval State**

| Peer MEP ID | Near Count | Far Count | Near Consecutive Count | Far Consecutive Count |
|---|---|---|---|---|
| No Peer MEP Added | | | | |

**Loss Measurement Signal Degrade**

| Enable | TX Minimum | FLR Threshold | Bad Threshold | Good Threshold |
|---|---|---|---|---|
| ☐ | 0 | 10 | 10 | 10 |

**Delay Measurement**

| Enable | Priority | Cast | Peer MEP | Ended | Tx Mode | Calc | Gap | Count | Unit | Synchronized | Counter Overflow Action |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 0 | Multi ▾ | 1 | Single ▾ | Standardize ▾ | Flow ▾ | 10 | 10 | us ▾ | ☐ | Keep ▾ |

**Delay Measurement State**

| | Tx | Rx | Rx Timeout | Rx Error | Av Delay Tot | Av Delay last N | Delay Min. | Delay Max. | Av Delay-Var Tot | Av Delay-Var last N | Delay-Var Min. | Delay-Var Max. | Overflow | Clear |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| One-way | | | | | | | | | | | | | | |
| F-to-N | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| N-to-F | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Two-way | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☐ |

**Delay Measurement Bins**

| Measurement Bins for FD | Measurement Bins for IFDV | Measurement Threshold |
|---|---|---|
| 3 | 3 | 5000 |

**Delay Measurement Bins for FD**

| | bin0 | bin1 | bin2 |
|---|---|---|---|
| One-way | | | |
| F-to-N | 0 | 0 | 0 |
| N-to-F | 0 | 0 | 0 |
| Two-way | 0 | 0 | 0 |

**Delay Measurement Bins for IFDV**

| | bin0 | bin1 | bin2 |
|---|---|---|---|
| One-way | | | |
| F-to-N | 0 | 0 | 0 |
| N-to-F | 0 | 0 | 0 |
| Two-way | 0 | 0 | 0 |

F-to-N :Far-end-to-near-end

N-to-F :Near-end-to-far-end

Back

SOLTECH
INFONET INC.

### Performance Monitoring Data Set

| Object | Description |
|---|---|
| **Enable** | When enabled this MEP instance will contribute to the 'PM Data Set' gathered by the PM Session. |

### Loss Measurement

| Object | Description |
|---|---|
| **Tx** | Loss Measurement initiator is enabled/disabled. Initiator is transmitting/receiving CCM or LMM/LMR or SLM/SLR/1SL PDUs - see 'Synthetic' and 'Ended'.<br>Service frame LM (not 'Synthetic') is only allowed with one Peer MEP configured.<br>Synthetic frame LM is allowed with multiple Peer MEPs configured. |
| **Rx** | Enable loss calculation when receiving LM PDUs (LMM/SLM/1SL). This is ignored when LM initiator is enabled. |
| **Priority** | The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same. |
| **Cast** | Selection of LM PDU transmitted unicast or multicast. The unicast MAC will be taken from the 'Unicast Peer MAC' database. In case of enable of Continuity Check and dual ended Loss Measurement both implemented on SW based CCM, 'Cast' has to be the same. |
| **Peer MEP** | Peer MEP-ID for unicast LM. The MAC is taken from the 'Unicast Peer MAC' database. Only used in case of multiple peers ('Synthetic' LM). |
| **Rate** | Selecting the frame rate of LM PDU. This is the inverse of transmission period as described in Y.1731.<br>Selecting 100f/sec is only valid in case of 'Synthetic' LM.<br>Selecting 6f/min is not valid in case of dual ended 'Service frame' LM (CCM PDU based).<br>In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same. |
| **Size** | The 'Synthetic' SLM/1SL frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing LM OAM PDU - including CRC (four bytes).<br>Example when 'Size' = 64=> Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + LBM PDU LENGTH(46) + CRC(4) = 64 bytes<br>The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.<br>There are two frame MAX sizes to consider.<br>Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of Bytes<br>CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of Bytes<br>Consider that the Peer MEP must be able to handle the selected frame size. Consider that the received SLR PDU must be copied to CPU<br>Warning will be given if selected frame size exceeds the CPU RX frame MAX size<br>Frame MIN Size is 64 Bytes. |
| **Synthetic** | Synthetic frame LM is enabled. This is SLM/SLR/1SL PDU based LM. |
| **Ended** | Single: Single ended Loss Measurement implemented on LMM/LMR or SLM/SLR.<br>Dual: Dual ended Loss Measurement implemented on SW based CCM or 1SL. |

| FLR Interval | This is the interval in number of measurement intervals where the interval Frame Loss Ratio is calculated. |
|---|---|
| Meas Interval | This is the 'synthetic' LM measurement interval in milliseconds. This must be a whole number of the LM PDU transmission interval (inverse 'Rate'). This is the interval in time where the loss and FLR is calculated based on the counted number of SL OAM PDUs. It is in this interval that the calculated FLR is checked against availability, high loss and degraded FLR threshold. example: 'Rate' = 100f/sec => 'Meas Interval' = N*10 milliseconds. example: 'Rate' = 10f/sec => 'Meas Interval' = N*100 milliseconds. In case of service frame based LM this attribute is not used and the measurement interval is always the LM PDU transmission interval. |
| Loss Threshold | Far end loss threshold count is incremented if a loss measurement is above this threshold. |
| SLM Test ID | The Test ID value to use in SLM PDUs (see G.8013, section 9.22.1). The default value is 0. |

### Loss Measurement State

| Object | Description |
|---|---|
| Peer MEP | The Peer MEP ID that the following state relates to. |
| Tx | The accumulated transmitted LM PDUs - since last 'clear'. |
| Rx | The accumulated received LM PDUs - since last 'clear'. |
| Near End Loss Count | The accumulated near end frame loss count - since last 'clear'. |
| Far End Loss Count | The accumulated far end frame loss count - since last 'clear'. |
| Interval Elapsed | The accumulated number of 'FLR Interval' elapsed - since last 'clear'. |
| Interval Near End Loss Ratio | The near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted - in the latest 'FLR Interval'. This is shown in (Loss/Tx)*10000. Same as 1/100 Percent. |
| Interval Far End Loss Ratio | The far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted - in the latest 'FLR Interval'. This is shown in (Loss/Tx)*10000. Same as 1/100 Percent. |
| Total Near End Loss Ratio | The near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted - since last 'clear'. This is shown in (Loss/Tx)*10000. Same as 1/100 Percent. |
| Interval Far End Loss Ratio | The far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted - since last 'clear'. This is shown in (Loss/Tx)*10000. Same as 1/100 Percent. |
| Clear | Set of this check and save will clear the accumulated counters and restart ratio calculation. |

### Loss Measurement Availability

| Object | Description |
|---|---|
| Enable | Enable/disable of loss measurement availability. |
| Interval | Availability interval - number of measurements with same availability in order to change availability state. The valid range is 1 to 1000. |
| FLR Threshold | Availability frame loss ratio threshold in per mile. |

| Maintenance | Enable/disable of loss measurement availability maintenance. |
|---|---|

### Loss Measurement Availability Status

| Object | Description |
|---|---|
| Near Avail Count | The number of measurements performed while the near end has been in the "Avail" state. |
| Far Avail Count | The number of measurements performed while the far end has been in the "Avail" state. |
| Near Unavail Count | The number of measurements performed while the near end has been in the "Unavail" state. |
| Far Unavail Count | The number of measurements performed while the far end has been in the "Unavail" state. |
| Near Window Curr | The current near-end availability window size. When Near State is "Avail" this value indicate the current number of consecutive measurements that are above the defined frame loss ratio threshold. When Near State is "Unavail" this value indicate the current number of consecutive measurements that are equal to or below the defined frame loss ratio threshold. Once this value reaches the defined "Interval" value (aka. the "window size") the availability state will change. |
| Far Window Curr | The current far-end availability window size. See the description for Near Window Curr for more details. |
| Near State | The current near end availability state. |
| Far State | The current far end availability state. |

### Loss Measurement High Loss Interval

| Object | Description |
|---|---|
| Enable | Enable/disable of loss measurement high loss interval. |
| FLR Threshold | High Loss Interval frame loss ratio threshold in per mile. |
| Consecutive Interval | High Loss Interval consecutive interval (number of measurements). |

### Loss Measurement High Loss Interval Status

| Object | Description |
|---|---|
| Near Count | Near end high loss interval count (number of measurements where availability state is available and FLR is above high loss interval FLR threshold. |
| Far Count | Far end high loss interval count (number of measurements where availability state is available and FLR is above high loss interval FLR threshold. |
| Near Consecutive Count | Near end high loss interval consecutive count. |
| Far Consecutive Count | Far end high loss interval consecutive count. |

### Loss Measurement Signal Degrade

| Object | Description |
|---|---|
| Enable | Enable/disable of loss measurement signal degrade. |
| TX Minimum | Minimum number of frames that must be transmitted in a measurement before frame loss ratio is tested against loss ratio threshold. |

| FLR Threshold | Signal Degraded frame loss ratio threshold in per mille. |
|---|---|
| Bad Threshold | Number of consecutive bad interval measurements required to set degrade state. |
| Good Threshold | Number of consecutive good interval measurements required to clear degrade state. |

### Delay Measurement

| Object | Description |
|---|---|
| Enable | Delay Measurement based on transmitting 1DM/DMM PDU can be enabled/disabled. Delay Measurement based on receiving and handling 1DM/DMR PDU is always enabled. |
| Priority | The priority to be inserted as PCP bits in TAG (if any). |
| Cast | Selection of 1DM/DMM PDU transmitted unicast or multicast. The unicast MAC will be configured through 'Peer MEP'. |
| Peer MEP | This is only used if the 'Cast' is configured to Uni. The 1DM/DMR unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer. |
| Ended | Single: Single ended Delay Measurement implemented on DMM/DMR. Dual: Dual ended Delay Measurement implemented on 1DM. |
| Tx Mode | Standardize: Y.1731 standardize way to transmit 1DM/DMR. Proprietary: Vitesse proprietary way with follow-up packets to transmit 1DM/DMR. |
| Calc | This is only used if the 'Ended' is configured to single ended. Round trip: The frame delay calculated by the transmitting and receiving timestamps of initiators. Frame Delay = RxTimeb-TxTimeStampf Flow: The frame delay calculated by the transmitting and receiving timestamps of initiators and remotes. Frame Delay = (RxTimeb-TxTimeStampf)-(TxTimeStampb-RxTimeStampf) |
| Gap | The gap between transmitting 1DM/DMM PDU in 10ms. The range is 10 to 65535. |
| Count | The number of last records to calculate. The range is 10 to 2000. |
| Unit | The time resolution. |
| Synchronized | Enable to use DMM/DMR packet to calculate dual ended DM. If the option is enabled, the following action will be taken. When DMR is received, two-way delay (roundtrip or flow) and both near-end-to-far-end and far-end-to-near-end one-way delay are calculated. When DMM or 1DM is received, only far-end-to-near-end one-way delay is calculated. |
| Counter Overflow Action | The action to counter when overflow happens. |

### Delay Measurement State

| Object | Description |
|---|---|
| Tx | The accumulated transmit count - since last 'clear'. |
| Rx | The accumulated receive count - since last 'clear'. |
| Rx Timeout | The accumulated receive timeout count for two-way only - since last 'clear'. |
| Rx Error | The accumulated receive error count - since last 'clear'. This is counting if the frame delay is larger than 1 second or if far end residence time is larger than the round trip time. |
| Av Delay Tot | The average total delay - since last 'clear'. |

| Av Delay last N | The average delay of the last n packets - since last 'clear'. |
|---|---|
| Delay Min. | The minimum delay - since last 'clear'. |
| Delay Max. | The maximum delay - since last 'clear'. |
| Av Delay-Var Tot | The average total delay variation - since last 'clear'. |
| Av Delay-Var last N | The average delay variation of the last n packets - since last 'clear'. |
| Delay-Var Min. | The minimum delay variation - since last 'clear'. |
| Delay-Var Max. | The maximum delay variation - since last 'clear'. |
| Overflow | The number of counter overflow - since last 'clear'. |
| Clear | Set of this check and save will clear the accumulated counters. |
| Far-end-to-near-end one-way delay | The one-way delay is from remote devices to the local devices. Here are the conditions to calculate this delay. 1. 1DM received. 2. DMM received with Synchronized enabled. 3. DMR received with Synchronized enabled. |
| Near-end-to-far-end one-way delay | The one-way delay is from the local devices to remote devices. The only case to calculate this delay is below. DMR received with Synchronized enabled. |

## Delay Measurement Bins

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

| Object | Description |
|---|---|
| Measurement Bins for FD | Configurable number of Frame Delay Measurement Bins per Measurement Interval. The minimum number of FD Measurement Bins per Measurement Interval supported is 2. The maximum number of FD Measurement Bins per Measurement Interval supported is 10. The default number of FD Measurement Bins per Measurement Interval supported is 3. |
| Measurement Bins for IFDV | Configurable number of Inter-Frame Delay Variation Measurement Bins per Measurement Interval. The minimum number of FD Measurement Bins per Measurement Interval supported is 2. The maximum number of FD Measurement Bins per Measurement Interval supported is 10. The default number of FD Measurement Bins per Measurement Interval supported is 2. |
| Measurement Threshold | Configurable the Measurement Threshold for each Measurement Bin. The unit for a measurement threshold is in microseconds (us). The default configured measurement threshold for a Measurement Bin is an increment of 5000 us. |

## Delay Measurement Bins for FD

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.
If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

```
Bin          Threshold               Range
bin0         0 us                    0 us <= measurement < 5,000 us
bin1         5,000 us                5,000 us <= measurement < 10,000 us
bin2         10,000 us               10,000 us <= measurement < 15,000 us
bin3         15,000 us               15,000 us <= measurement < infinite us
```

SOLTECH
INFONET INC.

### Delay Measurement Bins for IFDV

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.
If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

| Bin | Threshold | Range |
|-----|-----------|-------|
| bin0 | 0 us | 0 us <= measurement < 5,000 us |
| bin1 | 5,000 us | 5,000 us <= measurement < 10,000 us |
| bin2 | 10,000 us | 10,000 us <= measurement < 15,000 us |
| bin3 | 15,000 us | 15,000 us <= measurement < infinite us |

### Buttons

Back : Click to go back to this MEP instance main page.

Refresh : Click to refresh the page immediately.

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>MEP

✓ **Maintenance Entity Point**

➢ *Add New MEP*

• *Instance(1~100)*

• *Domain(Port | VLAN)*

• *Mode(Mep | Mip)*

• *Direction(Down | Up)*

• *Residence Port(Port Number | VLAN ID)*

• *Level(0~7)*

• *Flow Instance*

• *Tagged VID*

| Delete | Instance | Domain | Mode | Direction | Residence Port | Level | Flow Instance | Tagged VID | This MAC | Alarm |
|--------|----------|--------|------|-----------|----------------|-------|---------------|------------|----------|-------|
| Delete | 1 | Port ˅ | Mep ˅ | Down ˅ | 1 | 7 | 1 | 1000 | | |
| | | Port | Mep | Down | | | | | | |
| | | VLAN | Mip | Up | | | | | | |

**Maintenance Entity Point**

| Delete | Instance | Domain | Mode | Direction | Residence Port | Level | Flow Instance | Tagged VID | This MAC | Alarm |
|--------|----------|--------|------|-----------|----------------|-------|---------------|------------|----------|-------|
| ☐ | 1 | Port | Mep | Down | 1 | 7 | | 1000 | 02-21-6D-44-44-44 | 🔴 |
| ☐ | 2 | Port | Mep | Down | 2 | 7 | | 1000 | 06-21-6D-44-44-44 | 🔴 |

*Click Instance number*

✓ **MEP Configuration**

✓ **Instance Data**

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|----------|--------|------|-----------|----------------|---------------|------------|--------------|----------|
| 1 | Port | Mep | Down | 1 | | 1000 | 0 | 02-21-6D-44-44-44 |

✓ **Instance Configuration**

| Level | Format | Domain Name | MEG id | MEP id | Tagged VID | Syslog |
|-------|--------|-------------|--------|--------|------------|--------|
| 7 ▼ | ITU ICC ▼ | | ICC000MEG0000 | 1 | 1000 | ☐ |

➢ *Level(0~7)*

➢ *Format(ITU ICC | IEEE String | ITU CC ICC)*

➢ *Domain Name(Use only IEEE String)*

  • *This string can be empty or max 16 characters.*

➢ *MEG ID*

  • *Format ITU ICC can max 13 characters*

  • *Format ITU CC ICC can max 15 characters*

  • *Format IEEE String can max 16 characters*

➢ *MEP ID*

  • *0~8191*

➢ *Tagged VID*

  • *0~4095*

➢ *Syslog(Enable | Disable)*

✓ **Peer MEP Configuration**

| Delete | Peer MEP ID | Unicast Peer MAC |
|--------|-------------|------------------|
| | No Peer MEP Added | |

*Click* ☐ Add New Peer MEP

| Delete | Peer MEP ID | Unicast Peer MAC |
|--------|-------------|------------------|
| | No Peer MEP Added | |
| Delete | 0 | 00-00-00-00-00-00 |

➢ *Peer MEP ID (Input Peer MEP ID)*

➢ *Unicast Peer MAC (Auto | Manual)*

  • *Entering the MEP ID, the MAC is automatically retrieved*

- *Entering the Unicast Peer MAC, manually*

✓ **Functional Configuration**

➢ *Continuity Check*

- *Enable*

- *Priority(0~7)*

- *Frame rate(300f/sec | 100f/sec | 10f/sec | 1f/sec | 6f/min | 1f/min | 6f/hour)*

- *TLV*

| Continuity Check | | | |
|---|---|---|---|
| Enable | Priority | Frame rate | TLV |
| ☐ | 0 | 1 f/sec ▾ | ☐ |

```
300 f/sec
100 f/sec
10 f/sec
1 f/sec
6 f/min
1 f/min
6 f/hour
```

➢ *APS Protocol*

- *Enable*

- *Priority(0~7)*

- *Cast(Uni | Multi)*

- *Type(L-APS | R-APS)*

- *Last Octet(0~255)*

| APS Protocol | | | | |
|---|---|---|---|---|
| Enable | Priority | Cast | Type | Last Octet |
| ☐ | 0 | Multi ▾ | R-APS ▾ | 1 |

```
Uni      L-APS
Multi    R-APS
```

✓ **TLV Configuration**

➢ *Organization Specific TLV(Global)*

- *OUI First(0~255)*

- *OUI Second(0~255)*

- *OUI Third(0~255)*

- *Sub-Type(0~255)*

- *Value(0~255)*

| Organization Specific TLV (Global) | | | | |
|---|---|---|---|---|
| OUI First | OUI Second | OUI Third | Sub-Type | Value |
| 0 | 0 | 12 | 1 | 2 |

✓ **Link State Tracking**

➢ *Enable*

| Enable |
|:------:|
| ☐ |

✓ **MEP Status Alarm**

➢ *Instance Configuration*

• *cLevel, cMEG, cMEP, cAIS, cLCK, cLoop, cConfig, cSSF, aBLK, aTSD, aTSF*

| cLevel | cMEG | cMEP | cAIS | cLCK | cLoop | cConfig | cSSF | aBLK | aTSD | aTSF |
|:------:|:----:|:----:|:----:|:----:|:-----:|:-------:|:----:|:----:|:----:|:----:|
| 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🔴 | 🟢 | 🟢 | 🔴 |

➢ *Peer MEP Configuration*

• *cLOC, cRDI, cPeriod, cPriority, cDEG*

| cLOC | cRDI | cPeriod | cPriority | cDEG |
|:----:|:----:|:-------:|:---------:|:----:|
| 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |

✓ **TLV Status**

➢ *Peer MEP ID*

➢ *CC Organization Specific*

• *OUI First, OUI Second, OUI Third, Sub-Type, Value, Last RX*

➢ *CC Port Status*

• *Value, Last RX*

➢ *CC Interface Status*

• *Value, Last RX*

| Peer MEP ID | CC Organization Specific | | | | | | CC Port Status | | CC Interface Status | |
|:-----------:|:---------:|:----------:|:---------:|:--------:|:-----:|:-------:|:-----:|:-------:|:-----:|:-------:|
| | OUI First | OUI Second | OUI Third | Sub-Type | Value | Last RX | Value | Last RX | Value | Last RX |
| 2 | 0 | 0 | 0 | 0 | 0 | 🔴 | 0 | 🔴 | 0 | 🔴 |

---

## EXAMPLE CLI CONFIGURATION

---

✓ **Ethernet Protection Switching**

➢ *Add New EPS*

• *Instance(1~100)*

• *Domain(Port | VLAN)*

• *Mode(Mep | Mip)*

• *Direction(Down | Up)*

• *Residence Port(Port Number | VLAN ID)*

SOLTECH
INFONET INC.

- **Level(0~7)**

- **Flow Instance**

- **Tagged VID**

```
(config)# mep <inst> [ mip ] { up | down } domain { port | evc | vlan | tp-link | tunnel-tp | pw | lsp }
[ vid <vid> ] [ flow <flow> ] level <level> [ interface <port_type> <port> ]
(config)# mep 1 down domain port vid 1000 level 7 interface GigabitEthernet 1/1
(config)# mep 2 down domain port vid 1000 level 7 interface GigabitEthernet 1/2
```

✓ **MEP Configuration**

✓ **Instance Data**

✓ **Instance Configuration**

➢ **Level(0~7)**

```
(config)# mep <inst> level <level>
(config)# mep 1 level 1
```

➢ **Format(ITU ICC | IEEE String | ITU CC ICC)**

➢ **Domain Name(Use only IEEE String)**

- **This string can be empty or max 16 characters.**

➢ **MEG ID**

- **Format ITU ICC can max 13 characters**

- **Format ITU CC ICC can max 15 characters**

- **Format IEEE String can max 16 characters**

```
(config)# mep <inst> meg-id <megid> { itu | itu-cc | { ieee [ name <name> ] } }
(config)# mep 1 meg-id example itu
(config)# mep 1 meg-id example itu-cc
(config)# mep 1 meg-id example ieee name example1
```

➢ **MEP ID**

- **0~8191**

```
(config)# mep <inst> mep-id <mepid>
(config)# mep 1 meg-id example itu
(config)# mep 1 meg-id example itu-cc
(config)# mep 1 meg-id example ieee name example1
```

➢ **Tagged VID**

- **0~4095**

```
(config)# mep <inst> vid <vid>
(config)# mep 1 vid 1000
```

➢ **Syslog(Enable | Disable)**

```
(config)# mep <inst> syslog
(config)# mep 1 syslog
```

✓ **Peer MEP Configuration**

➢ *Peer MEP ID (Input Peer MEP ID)*

➢ *Unicast Peer MAC (Auto | Manual)*

• *Entering the MEP ID, the MAC is automatically retrieved*

• *Entering the Unicast Peer MAC, manually*

```
(config)# mep <inst> peer-mep-id <mepid> [ mac <mac> ]
(config)# mep 1 peer-mep-id 2
(config)# mep 1 peer-mep-id 2 mac 00-21-6d-00-00-00
```

✓ **Functional Configuration**

➢ *Continuity Check*

• *Enable*

• *Priority(0~7)*

• *Frame rate(300f/sec | 100f/sec | 10f/sec | 1f/sec | 6f/min | 1f/min | 6f/hour)*

```
(config)# mep <inst> cc <prio> [ fr300s | fr100s | fr10s | fr1s | fr6m | fr1m | fr6h ]
(config)# mep 1 cc 7 fr1s
(config)# mep 1 cc 0
```

• *TLV*

```
(config)# mep <inst> ccm-tlv
(config)# mep 1 ccm-tlv
```

➢ *APS Protocol*

• *Enable*

• *Priority(0~7)*

• *Cast(Uni | Multi)*

• *Type(L-APS | R-APS)*

• *Last Octet(0~255)*

```
(config)# mep <inst> aps <prio> [ multi | uni ] { laps | { raps [ octet <octet> ] } }
(config)# mep 1 aps 0 raps octet 1
(config)# mep 2 aps 7 raps octet 255
(config)# mep 1 aps 7 laps
```

✓ **TLV Configuration**

➢ *Organization Specific TLV(Global)*

• *OUI First, OUI Second, OUI Third(0-0xffffff)*

- **Sub-Type(0-0xff)**

- **Value(0-0xff)**

```
(config)# mep os-tlv oui <oui> sub-type <subtype> value <value>
(config)# mep os-tlv oui 0xffffff sub-type 0xff value 0xff
(config)# mep os-tlv oui 0xC sub-type 0x1 value 0x2
```

✓ **Link State Tracking**

➢ **Enable**

```
(config)# mep 1 link-state-tracking
```

✓ **MEP Status Alarm**

➢ **Instance Configuration**

- **cLevel, cMEG, cMEP, cAIS, cLCK, cLoop, cConfig, cSSF, aBLK, aTSD, aTSF**

➢ **Peer MEP Configuration**

- **cLOC, cRDI, cPeriod, cPriority, cDEG**

```
# show mep

MEP state is:
 Inst  cLevel  cMeg  cMep  cAis  cLck  cLoop  cConf  cSsf  aBlk  aTsd  aTsf  Peer MEP  cLoc  cRdi
    1  False  False  False  False False  False  False  True False  False  True       2  False False

cPeriod cPrio  cDeg
False   False  False
```

✓ **TLV Status**

➢ **Peer MEP ID**

➢ **CC Organization Specific**

- **OUI First, OUI Second, OUI Third, Sub-Type, Value, Last RX**

➢ **CC Port Status**

- **Value, Last RX**

➢ **CC Interface Status**

- **Value, Last RX**

```
# show mep tlv

MEP CCM TLV Status is:
    Inst  Peer MEP    OS OUI   OS Sub   OS Value  PS Value  IS Value  OS RX   PS RX   IS RX
       1      2      00-00-00     0        0         0         0      False   False   False
```

## 6.15. ERPS

## 6.15.1. ERPS Configuration

WEB MENU Configuration>ERPS

The ERPS instances are configured here.

**Ethernet Ring Protection Switching**                                    [Refresh]

| Delete | ERPS ID | Port 0 | Port 1 | Port 0 APS MEP | Port 1 APS MEP | Port 0 SF MEP | Port 1 SF MEP | Ring Type | Interconnected Node | Virtual Channel | Major Ring ID | Alarm |
|--------|---------|--------|--------|----------------|----------------|---------------|---------------|-----------|---------------------|-----------------|---------------|-------|

[Add New Protection Group]

### Ethernet Ring Protection Switching

| Object | Description |
|--------|-------------|
| **Delete** | This box is used to mark an ERPS for deletion in next Save operation. |
| **ERPS ID** | The ID of the created Protection group, It must be an integer value between 1 and 64. The maximum number of ERPS Protection Groups that can be created are 64. Click on the ID of an Protection group to enter the configuration page. |
| **Port 0** | This will create a Port 0 of the switch in the ring. |
| **Port 1** | This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance |
| **Port 0 SF MEP** | The Port 0 Signal Fail reporting MEP. |
| **Port 1 SF MEP** | The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance. |
| **Port 0 APS MEP** | The Port 0 APS PDU handling MEP. |
| **Port 1 APS MEP** | The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance. |
| **Ring Type** | Type of Protecting ring. It can be either major ring or sub-ring. |
| **Interconnected Node** | Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected. |
| **Virtual Channel** | Sub-rings can either have virtual channel or not on the interconnected node. This is configured using "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring doesn't have virtual channel. |
| **Major Ring ID** | Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring. |
| **Alarm** | There is an active alarm on the ERPS. |

**Buttons**

Add New Protection Group : Click to add a new Protection group entry.

Refresh : Click to refresh the page immediately.

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

## ERPS Configuration 1

This page allows the user to inspect and configure the current ERPS Instance.

**ERPS Configuration 1**

Auto-refresh ☐ Refresh

**Instance Data**

| ERPS ID | Port 0 | Port 1 | Port 0 SF MEP | Port 1 SF MEP | Port 0 APS MEP | Port 1 APS MEP | Ring Type |
|---|---|---|---|---|---|---|---|
| 1 | 7 | 8 | 7 | 8 | 7 | 8 | Major Ring |

**Instance Configuration**

| Configured | Guard Time | WTR Time | Hold Off Time | Version | Revertive | VLAN config |
|---|---|---|---|---|---|---|
| 🟢 | 500 | 1min ▾ | 0 | v2 ▾ | ☑ | VLAN Config |

**RPL Configuration**

| RPL Role | RPL Port | Clear |
|---|---|---|
| None ▾ | None ▾ | ☐ |

**Instance Command**

| Command | Port |
|---|---|
| None ▾ | None ▾ |

**Instance State**

| Protection State | Port 0 | Port 1 | Transmit APS | Port 0 Receive APS | Port 1 Receive APS | WTR Remaining | RPL Un-blocked | No APS Received | Port 0 Block Status | Port 1 Block Status | FOP Alarm |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Pending | OK | OK | NR BPR0 | | | 0 | 🟢 | 🟢 | Blocked | Unblocked | 🟢 |

### ERPS Configuration 1

#### Instance Data

| Object | Description |
|---|---|
| **ERPS ID** | The ID of the Protection group |
| **Port 0** | See help on ERPS create WEB. |
| **Port 1** | See help on ERPS create WEB. |
| **Port 0 SF MEP** | See help on ERPS create WEB. |
| **Port 1 SF MEP** | See help on ERPS create WEB. |
| **Port 0 APS MEP** | See help on ERPS create WEB. |
| **Port 1 APS MEP** | See help on ERPS create WEB. |
| **Ring Type** | Type of Protecting ring. It can be either major ring or sub-ring. |

#### Instance Configuration

| Object | Description |
|---|---|
| **Configured** | Red: This ERPS is only created and has not yet been configured - is not active. <br> Green: This ERPS is configured - is active. |

| Guard Time | Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages. The period of the guard timer can be configured in 10 ms steps between 10 ms and 2 seconds, with a default value of 500 ms |
|---|---|
| WTR Time | The Wait To Restore timing value to be used in revertive switching. The period of the WTR time can be configured by the operator in 1 minute steps between 5 and 12 minutes with a default value of 5 minutes. |
| Hold Off Time | The timing value to be used to make persistent check on Signal Fail before switching. The range of the hold off timer is 0 to 10 seconds in steps of 100 ms |
| Version | ERPS Protocol Version - v1 or v2 |
| Revertive | In Revertive mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL. In Non-Revertive mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared. |
| VLAN config | VLAN configuration of the Protection Group. Click on the "VLAN Config" link to configure VLANs for this protection group. |

### RPL Configuration

| Object | Description |
|---|---|
| RPL Role | It can be either RPL owner or RPL Neighbor. |
| RPL Port | This allows to select the east port or west port as the RPL block. |
| Clear | If the owner has to be changed, then the clear check box allows to clear the RPL owner for that ERPS ring. |

### Sub-Ring Configuration

| Object | Description |
|---|---|
| Topology Change | Clicking this checkbox indicates that the topology changes in the sub-ring are propagated in the major ring. |

### Instance Command

| Object | Description |
|---|---|
| Command | Administrative command. A port can be administratively configured to be in either manual switch or forced switch state. |
| Forced Switch | Forced Switch command forces a block on the ring port where the command is issued. |
| Manual Switch | In the absence of a failure or FS, Manual Switch command forces a block on the ring port where the command is issued. |
| Clear | The Clear command is used for clearing an active local administrative command (e.g., Forced Switch or Manual Switch). |
| Port | Port selection - Port0 or Port1 of the protection Group on which the command is applied. |

### Instance State

| Object | Description |
|---|---|
| Protection State | ERPS state according to State Transition Tables in G.8032. |
| Port 0 | OK: State of East port is ok SF: State of East port is Signal Fail |

| Port 1 | OK: State of West port is ok <br> SF: State of West port is Signal Fail |
|---|---|
| Transmit APS | The transmitted APS according to State Transition Tables in G.8032. |
| Port 0 Receive APS | The received APS on Port 0 according to State Transition Tables in G.8032. |
| Port 1 Receive APS | The received APS on Port 1 according to State Transition Tables in G.8032. |
| WTR Remaining | Remaining WTR timeout in milliseconds. |
| RPL Un-blocked | APS is received on the working flow. |
| No APS Received | RAPS PDU is not received from the other end. |
| Port 0 Block Status | Block status for Port 0 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel. |
| Port 1 Block Status | Block status for Port 1 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel. |
| FOP Alarm | Failure of Protocol Defect(FOP) status. If FOP is detected, red LED glows; else green LED glows. |

**Buttons**

Refresh : Click to refresh the page immediately.

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

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

### ERPS VLAN Configuration n

**ERPS VLAN Configuration 1**

| Delete | VLAN ID |

Add New Entry   Back

#### ERPS VLAN Configuration n

| Object | Description |
|---|---|
| Delete | To delete a VLAN entry, check this box. The entry will be deleted during the next Save. |
| VLAN ID | Indicates the ID of this particular VLAN. |
| Adding a New VLAN | Click Add New Entry to add a new VLAN ID. Legal values for a VLAN ID are 1 through 4095. <br> The VLAN is enabled when you click on "Save". <br> A VLAN without any port members will be deleted when you click "Save". <br> The Delete button can be used to undo the addition of new VLANs. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

Back : Click to go back to this MEP instance main page.

Refresh : Refreshes the displayed table starting from the "VLAN ID" input fields.

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>ERPS

✓ **Ethernet Ring Protection Switching**

   ➤ *Add New Protection Group*

     • *ERPS ID(1~64)*

     • *Port 0(Enter Port Number)*

     • *Port 1(Enter Port Number)*

     • *Port 0 APS MEP(Enter MEP Instance Number)*

     • *Port 1 APS MEP(Enter MEP Instance Number)*

     • *Port 0 SF MEP(Enter MEP Instance Number)*

     • *Port 1 SF MEP(Enter MEP Instance Number)*

     • *Ring Type(Major | Sub)*

     • *Interconnected Node(Enable | Disable)*

     • *Virtual Channel(can be set on the sub ring)*

     • *Major Ring ID(can be set when it is both an Interconnected Node and a sub ring)*

**Ethernet Ring Protection Switching**

| Delete | ERPS ID | Port 0 | Port 1 | Port 0 APS MEP | Port 1 APS MEP | Port 0 SF MEP | Port 1 SF MEP | Ring Type | Interconnected Node | Virtual Channel | Major Ring ID | Alarm |
|--------|---------|--------|--------|----------------|----------------|---------------|---------------|-----------|---------------------|-----------------|---------------|-------|
| Delete | 1 | 1 | 2 | 1 | 2 | 1 | 2 | Major ▾ | ☐ | ☐ | 0 | 🔴 |

| Delete | ERPS ID | Port 0 | Port 1 | Port 0 APS MEP | Port 1 APS MEP | Port 0 SF MEP | Port 1 SF MEP | Ring Type | Interconnected Node | Virtual Channel | Major Ring ID | Alarm |
|--------|---------|--------|--------|----------------|----------------|---------------|---------------|-----------|---------------------|-----------------|---------------|-------|
| ☐ | 1 | 1 | 2 | 1 | 2 | 1 | 2 | Major | No | No | 1 | 🔴 |

*Click ERPS ID*

✓ **ERPS Configuration n**

✓ **Instance Data**

   ➤ *ERPS ID*

   ➤ *Port 0*

   ➤ *Port 1*

   ➤ *Port 0 SF MEP*

   ➤ *Port 1 SF MEP*

   ➤ *Port 0 APS MEP*

   ➤ *Port 1 APS MEP*

   ➤ *Ring Type*

| ERPS ID | Port 0 | Port 1 | Port 0 SF MEP | Port 1 SF MEP | Port 0 APS MEP | Port 1 APS MEP | Ring Type |
|---------|--------|--------|---------------|---------------|----------------|----------------|-----------|
| 1 | 1 | 2 | 1 | 2 | 1 | 2 | Major Ring |

✓ **Instance Configuration**

&#10095; *Configured*

&#10095; *Guard Time*

- *10~2000(msec)*

&#10095; *WTR Time*

- *1min | 2min | 3min | 4min | 5min | 6min | 7min | 8min | 9min | 10min | 11min | 12min*

&#10095; *Hold Off Time*

- *0~10000(msec)*

&#10095; *Version*

- *v1 | v2*

&#10095; *Revertive*

- *Enable | Disable*

&#10095; *VLAN config*

- *VLAN Config (Click to move to the ERPS VLAN Configuration page)*

| Configured | Guard Time | WTR Time | Hold Off Time | Version | Revertive | VLAN config |
|---|---|---|---|---|---|---|
| 🟢 | 500 | 1min ▾ | 0 | v2 ▾ | ☑ | VLAN Config |

1min
2min
3min
4min
5min
6min
7min
8min
9min
10min
11min
12min

v1
v2

✓ **RPL Configuration**

&#10095; *RPL Role*

- *None | RPL_Owner | RPL_Neighbour*

&#10095; *RPL Port*

- *None | Port0 | Port1*

&#10095; *Clear*

- *Check Box*
  *(If you want to reset the RPL settings, check and apply.)*

| RPL Role | RPL Port | Clear |
|---|---|---|
| RPL_Owner ▾ | Port0 ▾ | ☐ |

None
RPL_Owner
RPL_Neighbour

None
Port0
Port1

✓ **Instance Command**

  ➢ *Command*

    • *None | Manual Switch | Forced Switch | Clear*

  ➢ *Port*

    • *None | Port0 | Port1*

| Command | Port |
|---------|------|
| None ▾  | None ▾ |
| **None** | **None** |
| Manual Switch | Port0 |
| Forced Switch | Port1 |
| Clear | |

✓ **Instance State**

  ➢ *Protection State | Port 0 | Port 1 | Transmit APS | Port 0 Receive APS | Port 1 Receive APS | WTR Remaining | RPL Un-blocked | No APS Received | Port 0 Block Status | Port 1 Block Status | FOP Alarm*

| Protection State | Port 0 | Port 1 | Transmit APS | Port 0 Receive APS | Port 1 Receive APS | WTR Remaining | RPL Un-blocked | No APS Received | Port 0 Block Status | Port 1 Block Status | FOP Alarm |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Protected | SF | SF | SF BPR0 | | | 0 | ● | ● | Blocked | Blocked | ● |

**Click VLAN Config**

✓ **ERPS VLAN Configuration n**

  ➢ *Add New Entry*

    • *VLAN ID(1~4095)*

**ERPS VLAN Configuration 1**

| Delete | VLAN ID |
|--------|---------|
| Delete | 0 |

Add New Entry   Back

---

# EXAMPLE CLI CONFIGURATION

---

✓ **Ethernet Ring Protection Switching**

  ➢ *Add New Protection Group*

    • *ERPS ID(1~64)*

    • *Port 0(Enter Port Number)*

    • *Port 1(Enter Port Number)*

    • *Interconnected Node(Enable | Disable)*

    • *Ring Type(Major | Sub)*

    • *Virtual Channel(can be set on the sub ring)*

SOLTECH
INFONET INC.

- • ***Major Ring ID(can be set when it is both an Interconnected Node and a sub ring)***

```
(config)# erps <group> major port0 interface <port_type> <port0> port1 interface <port_type>
<port1> [ interconnect ]
(config)# erps 1 major port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet 1/2
(config)# erps 1 major port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet 1/2
interconnect
```

```
(config)# erps <group> sub port0 interface <port_type> <port0> { { port1 interface <port_type>
<port1> } | { interconnect <major_ring_id> } } [ virtual-channel ]
(config)# erps 1 sub port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet 1/2 virtual-
channel
(config)# erps 1 sub port0 interface GigabitEthernet 1/1 interconnect 1 virtual-channel
```

- • ***Port 0 APS MEP(Enter MEP Instance Number)***

- • ***Port 1 APS MEP(Enter MEP Instance Number)***

- • ***Port 0 SF MEP(Enter MEP Instance Number)***

- • ***Port 1 SF MEP(Enter MEP Instance Number)***

```
(config)# erps <group> mep port0 sf <p0_sf> aps <p0_aps> port1 sf <p1_sf> aps <p1_aps>
(config)# erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
(config)# erps 1 mep port0 sf 1 aps 1
```

✓ **Instance Configuration**

- ➢ ***Guard Time***

  - • ***10~2000(msec)***

```
(config)# erps <group> guard <guard_time_ms>
(config)# erps 1 guard 500
```

- ➢ ***WTR Time***

  - • ***1min | 2min | 3min | 4min | 5min | 6min | 7min | 8min | 9min | 10min | 11min | 12min***

- ➢ ***Revertive***

  - • ***Enable | Disable***

```
(config)# erps <group> revertive <wtr_time_minutes>
(config)# erps 1 revertive 12
(config)# no erps 1 revertive
```

- ➢ ***Hold Off Time***

  - • ***0~10000(msec)***

```
(config)# erps <group> holdoff <holdoff_time_ms>
(config)# erps 1 holdoff 10000
(config)# erps 1 holdoff 0
```

- ➢ ***Version***

  - • ***v1 | v2***

```
(config)# erps <group> version { 1 | 2 }
(config)# erps 1 version 1
(config)# erps 1 version 2
```

✓ **RPL Configuration**

➢ *RPL Role*

• *None | RPL_Owner | RPL_Neighbour*

➢ *RPL Port*

• *None | Port0 | Port1*

```
(config)# erps <group> rpl { owner | neighbor } { port0 | port1 }
(config)# erps 1 rpl owner port0
(config)# erps 1 rpl neighbor port0
```

➢ *Clear*

```
(config)# no erps <group> rpl
```

✓ **Instance Command**

➢ *Command*

• *None | Manual Switch | Forced Switch | ClearPort*

• *None | Port0 | Port1*

```
# erps <group> command { force | manual | clear } { port0 | port1 }
# erps 1 command manual port0
# erps 1 command force port1
# erps 1 command clear port1
```

✓ **Instance State**

• *Protection State | Port 0 | Port 1 | Transmit APS | Port 0 Receive APS | Port 1 Receive APS | WTR Remaining | RPL Un-blocked | No APS Received | Port 0 Block Status | Port 1 Block Status | FOP Alarm*

```
# show erps 1 detail
Grp#  Port 0       Port 1       RPL:Role   Port    Blocking
  1   Gi 1/1       Gi 1/2       Owner      Port 0  Blocked

    Protected VLANS:      None

    Protection Group State       :Active
    Port 0 SF MEP                :1
    Port 1 SF MEP                :2
    Port 0 APS MEP               :1
    Port 1 APS MEP               :2
    WTR Timeout                  :1
    WTB Timeout                  :5500
    Hold-Off Timeout             :0
    Guard Timeout                :500
    Node Type                    :Major
    Reversion                    :Revertive
```

```
Version                        :2
ERPSv2 Administrative Command      :None


FSM State                      :IDLE
Port 0 Link Status             :Link Down
Port 1 Link Status             :Link Down
Port 0 Block Status            :BLOCKED
Port 1 Block Status            :UNBLOCKED
R-APS Transmission              :NR RB DNF BPR 0
R-APS Port 0 Reception          :NONE
R-APS Port 1 Reception          :NONE
FOP Alarm                       :OFF
```

✓ **ERPS VLAN Configuration n**

  ➢ *Add New Entry*

   • *VLAN ID(1~4095)*

```
(config)# erps <group> vlan { none | [ add | remove ] <vlans> }
(config)# erps 1 vlan 1
(config)# erps 1 vlan add 1
(config)# erps 1 vlan remove 1
```

# 6.16. Q-ERPS

## 6.16.1.Q-ERPS Configuration

WEB MENU Configuration>Q-ERPS

This page is configured to make it quick and easy to configure a single major ERPS. The values set on this page are automatically applied to MEP and ERPS. It is configured to allow basic configuration (operation of a single major ring of the ERPS protocol), and detailed settings can be changed in the MEP and ERPS settings.

**Quick ERPS Configuration**

| Delete | ERPS ID | Port 0 | Port 1 | RPL Role | Control VLAN | Protected VLAN | Alarm |

### Quick ERPS Configuration

| Object | Description |
|--------|-------------|
| **Delete** | This box is used to mark an ERPS and MEP for deletion in next Apply operation. |
| **ERPS ID** | The ID of the created Protection group, It must be an integer value between 1 and 64. The maximum number of ERPS Protection Groups that can be created are 64. Click on the ID of a Protection group to enter the configuration page. |
| **Port 0** | This will create a Port 0 of the switch in the Ring.(MEP is created concurrently) |
| **Port 1** | This will create a Port 1 of the switch in the Ring.(MEP is created concurrently) |
| **RPL Role** | Set the RPL Owner Node. The RPL of the owner node is set to port 0. |
| **Control VLAN** | Set the Control VLAN for ERPS. |
| **Protected VLAN** | Set the Protected VLAN (Data VLAN) to be protected by ERPS. |
| **Alarm** | Shows the current state of ERPS. |

**Buttons**

Add New Protection Group : Click to add a new protection group entry.

Refresh : Click to refresh the page immediately.

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

### EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>Q-ERPS

✓ **Quick ERPS Configuration**

➢ *Add New Protection Group*

• *ERPS ID(1~64)*

• *Port 0(Enter Port Number)*

• *Port 1(Enter Port Number)*

SOLTECH
INFONET INC.

- *RPL Role(None | RPL_Owner)*

- *Control VLAN(1~4095)*

- *Protected VLAN(1~4095)*

| Delete | ERPS ID | Port 0 | Port 1 | RPL Role | Control VLAN | Protected VLAN | Alarm |
|--------|---------|--------|--------|----------|--------------|----------------|-------|
| Delete | 1 | 1 | 2 | RPL_Owner ▾ | 100 | 1-10,12,15 | |

None
RPL_Owner

| Delete | ERPS ID | Port 0 | Port 1 | RPL Role | Control VLAN | Protected VLAN | Alarm |
|--------|---------|--------|--------|----------|--------------|----------------|-------|
| ☐ | 1 | 1 | 2 | RPL_Owner | 100 | VLAN Config | 🔴 |

**Click ERPS ID(Check on the ERPS Configuration page.)**

**Click VLAN Config(Check on the ERPS Configuration page.)**

---

## EXAMPLE CLI CONFIGURATION

---

✓ **Quick ERPS Configuration**

  ➢ *Add New Protection Group*

- *ERPS ID(1~64)*

- *Port 0(Enter Port Number)*

- *Port 1(Enter Port Number)*

- *RPL Role(None | RPL_Owner)*

- *Control VLAN(1~4095)*

- *Protected VLAN(1~4095)*

```
(config)# quick-erps <group> port0 <port_type> <port0> port1 <port_type> <port1> role { owner |
ordinary } control <control_vlan> protected <protected_vlans>
(config)# quick-erps 1 port0 GigabitEthernet 1/1 port1 GigabitEthernet 1/2 role owner control 100
protected 1-10,12,15
```

SOLTECH
INFONET INC.

## 6.17. S-Ring

### 6.17.1. S-Ring Configuration

WEB MENU Configuration>S-Ring

S-Ring is a protocol within the Ring Protocol that manages the Ring by determining whether packets transmitted from the 2nd Port of the Master node are received by the 1st Port.
If packets are received during the configured time, it keeps the 1st Port in a Blocking state.

This page is used to configure the S-Ring group and is available when there are three or more devices that support S-Ring.

**Sring Configuration & Status**

| | | | | Sring Configuration | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ID | Mode | Status | Alarm | 1st Port | 2nd Port | Robustness | Master ID | Order | Reordering |
| 1 | Disable ∨ | - | ⬤ | 10 ∨ | 9 ∨ | 2 ∨ | - | - | Refresh |
| 2 | Disable ∨ | - | ⬤ | 8 ∨ | 7 ∨ | 2 ∨ | - | - | Refresh |

### S-Ring Configuration & Status

| Object | Description |
|---|---|
| **Ring ID** | Ring ID. Each device can configure up to two rings |
| **Mode** | Use or nonuse of s-ring, Show S-ring mode. Disabled: Nonuse of S-ring. Slave: Set Slave mode of S-ring. Master: Set Master mode of S-ring. |
| **Status** | Displays the status of the S-ring. (-): The S-Ring is not configured. Failover: A state in which packet sent from the 2nd port are not received by the 1st port. Ring: A state in which the packet sent from the 2nd port is received by the 1st port. |
| **Alarm** | Show the status of S-ring using pictures. ⬤ : Disable  🔴 : Failover state  🟢 : Ring state |
| **1st Port** | Set a port to configure S-ring. (S-Ring #1 port) |
| **2nd Port** | Set a port to configure S-ring. (S-Ring #2 port) |
| **Robustness** | Robustness indicates a time of 10ms per setting value of 1, and if the packet is not received during the set time, the [Ring] status changes to [Failover]. Mainly increase the value when communication is unstable. If this value is high, the node hang time increases when changing from [Ring] to [Failover]. |
| **Master ID** | This value indicates the master ID number of the ring. This value on the master is the same as the Ring ID. |
| **Order** | This value indicates how far the node is from the master. The master starts with this value, so it is always '1', and it starts at the 2nd_Port of the master. |
| **Reordering** | Send orderring packet. Sending ordering packets is only possible for the 'master'. |

SOLTECH
INFONET INC.

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

Refresh : Click to refresh the page.

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>S-Ring

✓   **S-Ring Configuration & Status**

➢   *Mode*

•   *Disable | Slave | Master*

| ID | Mode | Status | Alarm | 1st Port | 2nd Port | Robustness | Master ID | Order | Reordering |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Disable ⌄ | - | ⬤ | 10 ⌄ | 9 ⌄ | 2 ⌄ | - | - | Refresh |
| 2 | Disable | - | ⬤ | 8 ⌄ | 7 ⌄ | 2 ⌄ | - | - | Refresh |
|   | Slave |  |  |  |  |  |  |  |  |
|   | Master |  |  |  |  |  |  |  |  |

*Sring Configuration*

•   *1st Port | 2nd Port*

| ID | Mode | Status | Alarm | 1st Port | 2nd Port | Robustness | Master ID | Order | Reordering |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Master ⌄ | - | ⬤ | 10 ⌄ | 9 ⌄ | 2 ⌄ | - | - | Refresh |
| 2 | Disable ⌄ | - | ⬤ | 1 | 7 ⌄ | 2 ⌄ | - | - | Refresh |
|   |  |  |  | 2 |  |  |  |  |  |
|   |  |  |  | 3 |  |  |  |  |  |
|   |  |  |  | 4 |  |  |  |  |  |
|   |  |  |  | 5 |  |  |  |  |  |
|   |  |  |  | 6 |  |  |  |  |  |
|   |  |  |  | 7 |  |  |  |  |  |
|   |  |  |  | 8 |  |  |  |  |  |
|   |  |  |  | 9 |  |  |  |  |  |
|   |  |  |  | 10 |  |  |  |  |  |

*Sring Configuration*

➢   *Robustness*

•   *1~10*

| ID | Mode | Status | Alarm | 1st Port | 2nd Port | Robustness | Master ID | Order | Reordering |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Master ⌄ | - | ⬤ | 10 ⌄ | 9 ⌄ | 2 ⌄ | - | - | Refresh |
| 2 | Disable ⌄ | - | ⬤ | 8 ⌄ | 7 ⌄ | 1 | - | - | Refresh |
|   |  |  |  |  |  | 2 |  |  |  |
|   |  |  |  |  |  | 3 |  |  |  |
|   |  |  |  |  |  | 4 |  |  |  |
|   |  |  |  |  |  | 5 |  |  |  |
|   |  |  |  |  |  | 6 |  |  |  |
|   |  |  |  |  |  | 7 |  |  |  |
|   |  |  |  |  |  | 8 |  |  |  |
|   |  |  |  |  |  | 9 |  |  |  |
|   |  |  |  |  |  | 10 |  |  |  |

*Sring Configuration*

> ➢ **Reordering**

>> • **Refresh**

| **Sring Configuration** |||||||||||
| ID | Mode | Status | Alarm | 1st Port | 2nd Port | Robustness | Master ID | Order | Reordering |
|----|------|--------|-------|----------|----------|------------|-----------|-------|------------|
| 1 | Master ˅ | Failover | 🔴 | 10 ˅ | 9 ˅ | 2 ˅ | 1 | 1 | Refresh |
| 2 | Disable ˅ | - | ⚪ | 8 ˅ | 7 ˅ | 2 ˅ | - | - | Refresh |

---

## EXAMPLE CLI CONFIGURATION

---

✓ **S-Ring Configuration & Status**

> ➢ **Mode**

>> • **Disable | Slave | Master**

> ➢ **1st Port | 2nd Port**

> ➢ **Robustness**

>> • **1~10**

```
(config)# sring id <v_id> [ mode { disable | { master | slave } 1st-port <v_ingressPort>
2nd-port <v_egressPort> } ] [ robustness <v_robustnessValue> ]
(config)# sring id 1 mode disable
(config)# sring id 1 mode master 1st-port 12 2nd-port 11 robustness 2
(config)# sring id 2 mode slave 1st-port 10 2nd-port 9 robustness 2
(config)# sring id 2 robustness 2
(config)# no sring
(config)# no sring id 1
```

# 6.18. MAC Table

## 6.18.1. MAC Table Configuration

WEB MENU Configuration>MAC Table

The MAC Address Table is configured on this page.
Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

**MAC Address Table Configuration**

**Aging Configuration**

| Disable Automatic Aging | ☐ | |
|---|---|---|
| Aging Time | 300 | seconds |

**MAC Table Learning**

| | Port Members | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Auto | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ |
| Disable | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Secure | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

**Static MAC Table Configuration**

| | | | Port Members | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Delete | VLAN ID | MAC Address | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

Add New Static Entry

### Aging Configuration

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds; for example, **Age time** [_____] seconds.

The allowed range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by checking ☐ **Disable automatic aging.**

### MAC Table Learning

If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.
Each port can do learning based upon the following settings.

| Object | Description |
|---|---|
| **Auto** | Learning is done automatically as soon as a frame with unknown SMAC is received. |
| **Disable** | No learning is done. |
| **Secure** | Only static MAC entries are learned, all other frames are dropped.<br>**Note:** Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface. |

### Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

SOLTECH
INFONET INC.

The MAC table is sorted first by VLAN ID and then by MAC address.

| Object | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **VLAN ID** | The VLAN ID of the entry. |
| **MAC Address** | The MAC address of the entry. |
| **Port Members** | Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

Add New Static Entry : Click  to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>MAC Table

✓ **Aging Configuration**

➢ *Disable Automatic Aging*



➢ *Aging Time(Enable Automatic Aging | Aging Time 300)*



✓ **Mac Table Learning**

➢ *Auto | Disable | Secure*



✓ **Static MAC Table Configuration**

➢ *Add New Static Entry*

**Static MAC Table Configuration**

| Delete | VLAN ID | MAC Address | Port Members 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|--------|---------|-------------|---|---|---|---|---|---|---|---|
| Delete | 1 | 00-21-6d-00-00-01 | ☐ | ☐ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ |

**Static MAC Table Configuration**

| Delete | VLAN ID | MAC Address | Port Members 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|--------|---------|-------------|---|---|---|---|---|---|---|---|
| ☐ | 1 | 00-21-6D-00-00-01 | ☐ | ☐ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ |

---

# EXAMPLE CLI CONFIGURATION

---

✓ **Aging Configuration**

➢ *Disable Automatic Aging*

```
(config)# mac address-table aging-time <v_0_10_to_1000000>
(config)# mac address-table aging-time 0
```

➢ *Aging Time(Enable Automatic Aging | Aging Time 300)*

```
(config)# mac address-table aging-time <v_0_10_to_1000000>
(config)# mac address-table aging-time 300
```

✓ **Mac Table Learning**

➢ *Auto*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1
(config-if)# mac address-table learning
```

➢ *Disable*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/2
(config-if)# no mac address-table learning
```

➢ *Secure*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/3
(config-if)# mac address-table learning secure
```

✓ **Static MAC Table Configuration**

➢ *Add New Static Entry*

```
(config)# mac address-table static <v_mac_addr> vlan <v_vlan_id> [ interface
( <port_type> [ <v_port_type_list> ] ) ]
(config)# mac address-table static 00-21-6d-00-00-01 vlan 1 interface GigabitEthernet 1/3
```

SOLTECH
INFONET INC.

## 6.18.2. MAC Table Monitor

WEB MENU Monitor>MAC Table

Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

**MAC Address Table**

Start from VLAN `1` and MAC address `00-00-00-00-00-00` with `20` entries per page.

| Type | VLAN | MAC Address | Port Members | | | | | | | | |
|------|------|-------------|---|---|---|---|---|---|---|---|---|
| | | | CPU | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

### MAC Table Columns

| Object | Description |
|--------|-------------|
| **Type** | Indicates whether the entry is a static or a dynamic entry. |
| **MAC address** | The MAC address of the entry. |
| **VLAN** | The VLAN ID of the entry. |
| **Port Members** | The ports that are members of the entry. |

**Buttons**

Auto-refresh ☐ : Automatic refresh occurs every 3 seconds.

`Refresh` : Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

`Cancel` : Flushes all dynamic entries..

`|<<` : Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.

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

## EXAMPLE WEB CONFIGURATION

WEB MENU Monitor>MAC Table

✓ **MAC Address Table**

**MAC Address Table**

Start from VLAN `1` and MAC address `00-00-00-00-00-00` with `20` entries per page.

| Type | VLAN | MAC Address | Port Members |  |  |  |  |  |  |  |  |
|------|------|-------------|:---:|:---:|:---:|:---:|:---:|:---:|:---:|:---:|:---:|
|      |      |             | CPU | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Static | 1 | 00-21-6D-00-00-01 |  |  | ✓ |  |  |  |  |  |  |
| Static | 1 | 33-33-00-00-00-01 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Static | 1 | 33-33-00-00-00-02 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Static | 1 | 33-33-FF-AE-DA-82 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Dynamic | 1 | C0-18-50-7E-50-56 |  | ✓ |  |  |  |  |  |  |  |
| Static | 1 | FF-FF-FF-FF-FF-FF | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

## EXAMPLE CLI CONFIGURATION

✓ **MAC Address Table**

```
# show mac address-table

Type      VID   MAC Address         Ports
Static    1     00:21:6d:00:00:01   GigabitEthernet 1/3
Static    1     33:33:00:00:00:01   GigabitEthernet 1/1-4 10GigabitEthernet 1/1-4 CPU
Static    1     33:33:00:00:00:02   GigabitEthernet 1/1-4 10GigabitEthernet 1/1-4 CPU
Static    1     33:33:ff:ae:da:82   GigabitEthernet 1/1-4 10GigabitEthernet 1/1-4 CPU
Dynamic   1     c0:18:50:7e:50:56   GigabitEthernet 1/1
Static    1     ff:ff:ff:ff:ff:ff   GigabitEthernet 1/1-4 10GigabitEthernet 1/1-4 CPU
```

SOLTECH
INFONET INC.

## 6.19. VLANs

## 6.19.1. VLAN Configuration

WEB MENU Configuration>VLANs

This page allows for controlling VLAN configuration on the switch.

The page is divided into a global section and a per-port configuration section.

**Global VLAN Configuration**

| Allowed Access VLANs | 1 |
| Ethertype for Custom S-ports | 88A8 |

**Port VLAN Configuration**

| Port | Mode | Port VLAN | Port Type | Ingress Filtering | Ingress Acceptance | Egress Tagging | Allowed VLANs | Forbidden VLANs |
|---|---|---|---|---|---|---|---|---|
| * | <> | 1 | <> | ☑ | <> | <> | 1 | |
| 1 | Access | 1 | C-Port | ☑ | Tagged and Untagged | Untag All | 1 | |
| 2 | Access | 1 | C-Port | ☑ | Tagged and Untagged | Untag All | 1 | |
| 3 | Access | 1 | C-Port | ☑ | Tagged and Untagged | Untag All | 1 | |
| 4 | Access | 1 | C-Port | ☑ | Tagged and Untagged | Untag All | 1 | |
| 5 | Access | 1 | C-Port | ☑ | Tagged and Untagged | Untag All | 1 | |
| 6 | Access | 1 | C-Port | ☑ | Tagged and Untagged | Untag All | 1 | |
| 7 | Access | 1 | C-Port | ☑ | Tagged and Untagged | Untag All | 1 | |
| 8 | Access | 1 | C-Port | ☑ | Tagged and Untagged | Untag All | 1 | |

### Global VLAN Configuration

| Object | Description |
|---|---|
| **Allowed Access VLANs** | This field shows the allowed Access VLANs, i.e. it only affects ports configured as Access ports. Ports in other modes are members of the VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash(-) separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters. |
| **Ethertype for Custom S-ports** | This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port. |

### Port VLAN Configuration

| Object | Description |
|---|---|
| **Port** | This is the logical port number of this row. |
| **Mode** | The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below. Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port will get when the mode is applied. **Access** Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics: 1. Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1 2. Accepts untagged and C-tagged frames |

| | | 3. Discards all frames not classified to the Access VLAN |
| | | 4. On egress all frames are transmitted untagged |
| | Trunk | Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:<br>1. By default, a trunk port is member of all VLANs (1-4095).<br>2. The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs.<br>3. Frames classified to a VLAN that the port is not a member of are discarded<br>4. By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress<br>5. Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress |
| | Hybrid | Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:<br>1. Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware<br>2. Ingress filtering can be controlled<br>3. Ingress acceptance of frames and configuration of egress tagging can be configured independently |
| **Port VLAN** | | Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1.<br>On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).<br>On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.<br>The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode. |
| **Port Type** | | Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.<br>Unaware:<br>On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.<br>C-Port:<br>On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag.<br>If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN.<br>If frames must be tagged on egress, they will be tagged with a C-tag.<br>S-Port:<br>On egress, if frames must be tagged, they will be tagged with an S-tag.<br>On ingress, frames with a VLAN tag with TPID = 0x88A8 get classified to the VLAN ID embedded in the tag.<br>Priority-tagged frames are classified to the Port VLAN. |

| | If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped. |
| --- | --- |
| | S-Custom-Port: |
| | On egress, if frames must be tagged, they will be tagged with the custom S-tag. |
| | On ingress, frames with a VLAN tag with a TPID equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. |
| | Priority-tagged frames are classified to the Port VLAN. |
| | If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped. |
| **Ingress Filtering** | Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled. |
| | If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. |
| | If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of. |

| **Ingress Acceptance** | Hybrid ports allow for changing the type of frames that are accepted on ingress. | |
| --- | --- | --- |
| | Tagged and Untagged | Both tagged and untagged frames are accepted. See Port Type for a description of when a frame is considered tagged. |
| | Tagged Only | Only frames tagged with the corresponding Port Type tag are accepted on ingress. |
| | Untagged Only | Only untagged frames are accepted on ingress. See Port Type for a description of when a frame is considered untagged. |

| **Egress Tagging** | Ports in Trunk and Hybrid mode may control the tagging of frames on egress. | |
| --- | --- | --- |
| | Untag Port VLAN | Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag. |
| | Tag All | All frames, whether classified to the Port VLAN or not, are transmitted with a tag. |
| | Untag All | All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode. |

| **Allowed VLANs** | Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. |
| --- | --- |
| | The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to 1-4095. The field may be left empty, which means that the port will not become member of any VLANs. |

| **Forbidden VLANs** | A port may be configured to never become member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. |
| --- | --- |
| | The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field. |
| | By default, the field is left blank, which means that the port may become a member of all possible VLANs. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

SOLTECH
INFONET INC.

## 6.19.2. VLAN Monitor

## 6.19.2.1. Membership

WEB MENU Monitor>VLANs>Membership

This page provides an overview of membership status of VLAN users.

**VLAN Membership Status for Combined users**

Start from VLAN `1` with `20` entries per page. `|<<` `>>`

| VLAN ID | Port Members |
|---------|:---:|
| | 1 2 3 4 5 6 7 8 |
| 1 | ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ |

**VLAN Membership Status for Combined users**

| Object | Description |
|--------|-------------|
| **VLAN User** | Various internal software modules may use VLAN services to configure VLAN memberships on the fly.<br>The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.<br>The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware. |
| **VLAN ID** | VLAN ID for which the Port members are displayed. |
| **Port Members** | A row of check boxes for each port is displayed for each VLAN ID.<br>If a port is included in a VLAN, the following image will be displayed: ✓.<br>If a port is in the forbidden port list, the following image will be displayed: ✗.<br>If a port is in the forbidden port list and at the same time attempted included in the VLAN, the following image will be displayed: ✗c. The port will not be a member of the VLAN in this case. |

**Buttons**

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

Refresh : Click to refresh the page immediately.

|<< : Use the button to start over.

>> : The button will use the last entry of the currently displayed VLAN entry as a basis for the next lookup.
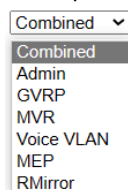
Combined ⌄
Combined
Admin
GVRP
MVR
Voice VLAN
MEP
RMirror      : Select VLAN Users from this drop down list.

## 6.19.2.2. Ports

WEB MENU Monitor>VLANs>Ports

This page provides VLAN Port Status.

**VLAN Port Status for Combined users**

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

### VLAN Port Status for Combined users

| Object | Description |
|--------|-------------|
| **VLAN User** | Various internal software modules may use VLAN services to configure VLAN port configuration on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware. If a given software modules hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table. |
| **Port** | The logical port for the settings contained in the same row. |
| **Port Type** | Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port.) that a given user wants to configure on the port. The field is empty if not overridden by the selected user. |
| **Ingress Filtering** | Shows whether a given user wants ingress filtering enabled or not. The field is empty if not overridden by the selected user. |
| **Frame Type** | Shows the acceptable frame types (All, Taged, Untagged) that a given user wants to configure on the port. The field is empty if not overridden by the selected user. |
| **Port VLAN ID** | Shows the Port VLAN ID (PVID) that a given user wants the port to have. The field is empty if not overridden by the selected user. |
| **Tx Tag** | Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port. The field is empty if not overridden by the selected user. |
| **Untagged VLAN ID** | If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field will show the VLAN ID the user wants to tag or untag on egress. The field is empty if not overridden by the selected user. |
| **Conflicts** | Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress. Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized |

| | way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list: The higher in the list, the higher priority. If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module. |
| --- | --- |
| | The "Combined" user reflects what is actually configured in hardware. |

**Buttons**

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

Refresh : Click to refresh the page immediately.

Combined ▼
Combined
Admin
GVRP
MVR
Voice VLAN
MSTP
ERPS
MEP
VCL
RMirror　 : Select VLAN Users from this drop down list.

## 6.20. QoS

## 6.20.1. QoS Configuration

## 6.20.1.1. Port Classification

WEB MENU Configuration>QoS>Port Classification

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

**QoS Ingress Port Classification**

| Port | CoS | DPL | PCP | DEI | Tag Class. | DSCP Based | WRED Group |
|------|-----|-----|-----|-----|------------|------------|------------|
| *    | <>  | <>  | <>  | <>  |            | ☐          | <>         |
| 1    | 0   | 0   | 0   | 0   | Disabled   | ☐          | 1          |
| 2    | 0   | 0   | 0   | 0   | Disabled   | ☐          | 1          |
| 3    | 0   | 0   | 0   | 0   | Disabled   | ☐          | 1          |
| 4    | 0   | 0   | 0   | 0   | Disabled   | ☐          | 1          |
| 5    | 0   | 0   | 0   | 0   | Disabled   | ☐          | 1          |
| 6    | 0   | 0   | 0   | 0   | Disabled   | ☐          | 1          |
| 7    | 0   | 0   | 0   | 0   | Disabled   | ☐          | 1          |
| 8    | 0   | 0   | 0   | 0   | Disabled   | ☐          | 1          |

### QoS Ingress Port Classification

| Object | Description |
|--------|-------------|
| **Port** | The port number for which the configuration below applies. |
| **CoS** | Controls the default class of service. All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS. The classified CoS can be overruled by a QCL entry. Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS. |
| **DPL** | Controls the default drop precedence level. All frames are classified to a drop precedence level. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL. The classified DPL can be overruled by a QCL entry. |
| **PCP** | Controls the default PCP value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value. |
| **DEI** | Controls the default DEI value. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value. |
| **Tag Class** | Shows the classification mode for tagged frames on this port. |

| | Disabled: Use default CoS and DPL for tagged frames. |
| | Enabled: Use mapped versions of PCP and DEI for tagged frames. |
| | Click on the mode in order to configure the mode and/or mapping. |
| | Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL. |
| **DSCP Based** | Click to Enable DSCP Based QoS Ingress Port Classification. |
| **WRED Group** | Controls the WRED group membership. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

### QoS Ingress Port Tag Classification Port n

When you click on 'Tag Class' the settings page will open.

The classification mode for tagged frames are configured on this page.



**Tagged Frames Settings**

| Object | Description |
|---|---|
| **Tag Classification** | Controls the classification mode for tagged frames on this port. |
| | **Disabled** — Use default QoS class and Drop Precedence Level for tagged frames. |
| | **Enabled** — Use mapped versions of PCP and DEI for tagged frames. |

**(PCP, DEI) to (QoS class, DP level) Mapping**

| Object | Description |
|---|---|
| **Tag Classification** | Controls the mapping of the classified (PCP, DEI) to (QoS class, DP level) values when Tag Classification is set to Enabled. |

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>QoS>Port Classification

✓  **QoS Ingress Port Classification**

➢  ***CoS***

•  0~7 (0 – The Lowest Priority)

**QoS Ingress Port Classification**

| Port | CoS | DPL | PCP | DEI | Tag Class. | DSCP Based | WRED Group |
|------|-----|-----|-----|-----|------------|------------|------------|
| * | <> ∨ | <> ∨ | <> ∨ | <> ∨ | | ☑ | <> ∨ |
| 1 | 0 ∨ | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 2 | 0 | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 3 | 1 | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 4 | 2 3 | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 5 | 4 | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 6 | 5 | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 7 | 6 | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 8 | 7 | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 9 | 0 ∨ | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 10 | 0 ∨ | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 11 | 0 ∨ | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 12 | 0 ∨ | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |

➢  ***DPL***

•  0~3 (0 – Low drop probability)

**QoS Ingress Port Classification**

| Port | CoS | DPL | PCP | DEI | Tag Class. | DSCP Based | WRED Group |
|------|-----|-----|-----|-----|------------|------------|------------|
| * | <> ∨ | <> ∨ | <> ∨ | <> ∨ | | ☑ | <> ∨ |
| 1 | 0 ∨ | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 2 | 0 ∨ | 0 | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 3 | 0 ∨ | 1 | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 4 | 0 ∨ | 2 3 | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 5 | 0 ∨ | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 6 | 0 ∨ | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 7 | 0 ∨ | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 8 | 0 ∨ | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 9 | 0 ∨ | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 10 | 0 ∨ | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 11 | 0 ∨ | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |
| 12 | 0 ∨ | 0 ∨ | 0 ∨ | 0 ∨ | Disabled | ☑ | 1 ∨ |

SOLTECH
INFONET INC.

➢ **PCP**

• 0~7 (0 - The Lowest Priority)

**QoS Ingress Port Classification**

| Port | CoS | DPL | PCP | DEI | Tag Class. | DSCP Based | WRED Group |
|------|-----|-----|-----|-----|-----------|-----------|-----------|
| * | <> ✓ | <> ✓ | <> ✓ | <> ✓ | | ☑ | <> ✓ |
| 1 | 0 ✓ | 0 ✓ | 0 ✓ | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 2 | 0 ✓ | 0 ✓ | 0 | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 3 | 0 ✓ | 0 ✓ | 1 | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 4 | 0 ✓ | 0 ✓ | 2 3 | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 5 | 0 ✓ | 0 ✓ | 4 | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 6 | 0 ✓ | 0 ✓ | 5 | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 7 | 0 ✓ | 0 ✓ | 6 | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 8 | 0 ✓ | 0 ✓ | 7 | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 9 | 0 ✓ | 0 ✓ | 0 ✓ | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 10 | 0 ✓ | 0 ✓ | 0 ✓ | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 11 | 0 ✓ | 0 ✓ | 0 ✓ | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 12 | 0 ✓ | 0 ✓ | 0 ✓ | 0 ✓ | Disabled | ☑ | 1 ✓ |

➢ **DEI**

• 0~1 (0 – Low drop probability)

**QoS Ingress Port Classification**

| Port | CoS | DPL | PCP | DEI | Tag Class. | DSCP Based | WRED Group |
|------|-----|-----|-----|-----|-----------|-----------|-----------|
| * | <> ✓ | <> ✓ | <> ✓ | <> ✓ | | ☑ | <> ✓ |
| 1 | 0 ✓ | 0 ✓ | 0 ✓ | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 2 | 0 ✓ | 0 ✓ | 0 ✓ | 0 | Disabled | ☑ | 1 ✓ |
| 3 | 0 ✓ | 0 ✓ | 0 ✓ | 1 | Disabled | ☑ | 1 ✓ |
| 4 | 0 ✓ | 0 ✓ | 0 ✓ | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 5 | 0 ✓ | 0 ✓ | 0 ✓ | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 6 | 0 ✓ | 0 ✓ | 0 ✓ | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 7 | 0 ✓ | 0 ✓ | 0 ✓ | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 8 | 0 ✓ | 0 ✓ | 0 ✓ | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 9 | 0 ✓ | 0 ✓ | 0 ✓ | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 10 | 0 ✓ | 0 ✓ | 0 ✓ | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 11 | 0 ✓ | 0 ✓ | 0 ✓ | 0 ✓ | Disabled | ☑ | 1 ✓ |
| 12 | 0 ✓ | 0 ✓ | 0 ✓ | 0 ✓ | Disabled | ☑ | 1 ✓ |

➢ **Tag Class**

• Disabled

**QoS Ingress Port Tag Classification Port n**

**Tagged Frames Settings**

• **Tag Classification**

✓ Disabled | Enabled

**Tagged Frames Settings**

| Tag Classification | Disabled ✓ |
|---|---|

(PCP, DEI) to (QoS  Disabled
Enabled

SOLTECH
INFONET INC.

### (PCP, DEI) to (QoS class, DP level) Mapping

- **QoS class**
  - ✓ 0~7 (0 - The Lowest Priority)



- **DP level**
  - ✓ 0~3 (0 – Low drop probability)

➢ **DSCP Based**

- Enabled | Disabled

**QoS Ingress Port Classification**

| Port | CoS | DPL | PCP | DEI | Tag Class. | DSCP Based | WRED Group |
|------|-----|-----|-----|-----|-----------|-----------|-----------|
| * | <> | <> | <> | <> | | ☐ | <> |
| 1 | 0 | 0 | 0 | 0 | Disabled | ☐ | 1 |
| 2 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 3 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 4 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 5 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 6 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 7 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 8 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 9 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 10 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 11 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 12 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |

➢ **WRED Group**

- 1~3 (WRED group)

**QoS Ingress Port Classification**

| Port | CoS | DPL | PCP | DEI | Tag Class. | DSCP Based | WRED Group |
|------|-----|-----|-----|-----|-----------|-----------|-----------|
| * | <> | <> | <> | <> | | ☑ | <> |
| 1 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 2 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 3 | 0 | 0 | 0 | 0 | Disabled | ☑ | 2 |
| 4 | 0 | 0 | 0 | 0 | Disabled | ☑ | 3 |
| 5 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 6 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 7 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 8 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 9 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 10 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 11 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |
| 12 | 0 | 0 | 0 | 0 | Disabled | ☑ | 1 |

## EXAMPLE CLI CONFIGURATION

✓ **QoS Ingress Port Classification**

➢ *CoS*

• 0~7 (0 – The Lowest Priority)

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos cos <cos>
(config-if)# qos cos 0
```

➢ *DPL*

• 0~3 (0 – Low drop probability)

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos dpl <dpl>
(config-if)# qos dpl 0
```

➢ *PCP*

• 0~7 (0 – The Lowest Priority)

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos pcp <pcp>
(config-if)# qos pcp 0
```

➢ *DEI*

• 0~1 (0 – Low drop probability)

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos dei <dei>
(config-if)# qos dei 0
```

> ➢ *Tag Class*

  • Disabled

  ### QoS Ingress Port Tag Classification Port n

  ### Tagged Frames Settings

  • *Tag Classification*

    ✓ Disabled | Enabled

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos trust tag
```

  ### (PCP, DEI) to (QoS class, DP level) Mapping

  • *QoS class*

    ✓ 0~7 (0 - The Lowest Priority)

  • *DP level*

    ✓ 0~3 (0 – Low drop probability)

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos map tag-cos pcp <pcp> dei <dei> cos <cos> dpl <dpl>
(config-if)# qos map tag-cos pcp 0 dei 0 cos 1 dpl 0
```

> ➢ *DSCP Based*

  • Enabled | Disabled

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos trust dscp
(config-if)# no qos trust dscp
```

> ➢ *WRED Group*

  • 1~3 (WRED group)

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos wred-group <wred_group>
(config-if)# qos wred-group 1
```

## 6.20.1.2. Port Policing

WEB MENU Configuration>QoS>Port Policing

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

**QoS Ingress Port Policers**

| Port | Enable | Rate | Unit | Flow Control |
|------|--------|------|------|--------------|
| * | ☐ | 500 | <> ▾ | ☐ |
| 1 | ☐ | 500 | kbps ▾ | ☐ |
| 2 | ☐ | 500 | kbps ▾ | ☐ |
| 3 | ☐ | 500 | kbps ▾ | ☐ |
| 4 | ☐ | 500 | kbps ▾ | ☐ |
| 5 | ☐ | 500 | kbps ▾ | ☐ |
| 6 | ☐ | 500 | kbps ▾ | ☐ |
| 7 | ☐ | 500 | kbps ▾ | ☐ |
| 8 | ☐ | 500 | kbps ▾ | ☐ |

### QoS Ingress Port Policers

| Object | Description |
|--------|-------------|
| **Port** | The port number for which the configuration below applies. |
| **Enable** | Enable or disable the port policer for this switch port. |
| **Rate** | Controls the rate for the port policer. This value is restricted to 10-13128147 when "Unit" is kbps or fps, and 1-13128 when "Unit" is Mbps or kfps. The rate is internally rounded up to the nearest value supported by the port policer. |
| **Unit** | Controls the unit of measure for the port policer rate as kbps, Mbps, fps or kfps. |
| **Flow Control** | If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

### EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>QoS>Port Policing

- ✓ **QoS Ingress Port Policers**

  - ➢ *Enable*

    - • Enabled | Disabled

SOLTECH
INFONET INC.

**QoS Ingress Port Policers**

> ## Rate

- 10-13128147(kbps, fps) or 1-13128(Mbps, kfps)



**QoS Ingress Port Policers**

> ## Unit

- kbps, Mbps, fps, kfps



**QoS Ingress Port Policers**

> ## Flow Control

- Enabled | Disabled

**QoS Ingress Port Policers**

| Port | Enable | Rate | Unit | Flow Control |
|------|--------|------|------|--------------|
| * | ☑ | 1 | <> ▼ | ☐ |
| 1 | ☑ | 1 | Mbps ▼ | ☑ |
| 2 | ☐ | 1 | Mbps ▼ | ☐ |
| 3 | ☐ | 1 | Mbps ▼ | ☐ |
| 4 | ☐ | 1 | Mbps ▼ | ☐ |
| 5 | ☐ | 1 | Mbps ▼ | ☐ |
| 6 | ☐ | 1 | Mbps ▼ | ☐ |
| 7 | ☐ | 1 | Mbps ▼ | ☐ |
| 8 | ☐ | 1 | Mbps ▼ | ☐ |
| 9 | ☐ | 1 | Mbps ▼ | ☐ |
| 10 | ☐ | 1 | Mbps ▼ | ☐ |
| 11 | ☐ | 1 | Mbps ▼ | ☐ |
| 12 | ☐ | 1 | Mbps ▼ | ☐ |

## EXAMPLE CLI CONFIGURATION

✓ **QoS Ingress Port Policers**

➢ *Enable*

- Enabled | Disabled

➢ *Rate*

- 10-13128147(kbps, fps) or 1-13128(Mbps, kfps)

➢ *Unit*

- kbps, Mbps, fps, kfps

➢ *Flow Control*

- Enabled | Disabled

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos policer <rate> [ kbps | mbps | fps | kfps ] [ flowcontrol ]
(config-if)# qos policer 1 mbps flowcontrol
(config-if)# qos policer 1 mbps
(config-if)# qos policer 10 kbps
(config-if)# no qos policer
```

SOLTECH
INFONET INC.

## 6.20.1.3. Queue Policing

WEB MENU Configuration>QoS>Queue Policing

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

**QoS Ingress Queue Policers**

| Port | Queue 0 Enable | Queue 1 Enable | Queue 2 Enable | Queue 3 Enable | Queue 4 Enable | Queue 5 Enable | Queue 6 Enable | Queue 7 Enable |
|------|------|------|------|------|------|------|------|------|
| * | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 2 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 3 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 4 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 5 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 6 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 7 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 8 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

### QoS Ingress Queue Policers

| Object | Description |
|--------|-------------|
| **Port** | The port number for which the configuration below applies. |
| **Enable (E)** | Enable or disable the queue policer for this switch port. |
| **Rate** | Controls the rate for the queue policer. This value is restricted to 25-13128147 when "Unit" is kbps, and 1-13128 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer. This field is only shown if at least one of the queue policers are enabled. |
| **Unit** | Controls the unit of measure for the queue policer rate as kbps or Mbps. This field is only shown if at least one of the queue policers are enabled. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

### EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>QoS>Queue Policing

✓ **QoS Ingress Queue Policers**

➢ *Queue n (n, 0~7)*

➢ *Enable (E)*

• Enabled | Disabled

SOLTECH
INFONET INC.

**QoS Ingress Queue Policers**

| Port | | Queue 0 | | Queue 1 | Queue 2 | Queue 3 | Queue 4 | Queue 5 | Queue 6 | Queue 7 |
| | E | Rate | Unit | Enable | Enable | Enable | Enable | Enable | Enable | Enable |
|---|---|---|---|---|---|---|---|---|---|---|
| * | ☐ | 1 | <> | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | ☑ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 2 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 3 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 4 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 5 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 6 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 7 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 8 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 9 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 10 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 11 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 12 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

➢ **Rate**

- 25-13128147(kbps) or 1-13128(Mbps)

**QoS Ingress Queue Policers**

| Port | | Queue 0 | | Queue 1 | Queue 2 | Queue 3 | Queue 4 | Queue 5 | Queue 6 | Queue 7 |
| | E | Rate | Unit | Enable | Enable | Enable | Enable | Enable | Enable | Enable |
|---|---|---|---|---|---|---|---|---|---|---|
| * | ☑ | 25 | <> | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | ☑ | 25 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 2 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 3 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 4 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 5 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 6 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 7 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 8 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 9 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 10 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 11 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 12 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

➢ **Unit**

- kbps, Mbps

**QoS Ingress Queue Policers**

| Port | | Queue 0 | | Queue 1 | Queue 2 | Queue 3 | Queue 4 | Queue 5 | Queue 6 | Queue 7 |
| | E | Rate | Unit | Enable | Enable | Enable | Enable | Enable | Enable | Enable |
|---|---|---|---|---|---|---|---|---|---|---|
| * | ☑ | 1 | <> | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | ☑ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 2 | ☐ | 1 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 3 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 4 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 5 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 6 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 7 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 8 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 9 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 10 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 11 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 12 | ☐ | 1 | Mbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

SOLTECH
INFONET INC.

## EXAMPLE CLI CONFIGURATION

✓ **QoS Ingress Queue Policers**

➢ *Queue n (n, 0~7)*

➢ *Enable (E)*

• Enabled | Disabled

➢ *Rate*

• 25-13128147(kbps) or 1-13128(Mbps)

➢ *Unit*

• kbps, Mbps

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos queue-policer queue <queue> <rate> [ kbps | mbps ]
(config-if)# qos queue-policer queue 0 1 mbps
(config-if)# qos queue-policer queue 0 25 kbps
(config-if)# no qos queue-policer queue 0
```

## 6.20.1.4. Port Scheduler

WEB MENU Configuration>QoS>Port Scheduler

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

**QoS Egress Port Schedulers**

| Port | Mode | Weight | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Q0 | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 |
| 1 | Strict Priority | - | - | - | - | - | - | - | - |
| 2 | Strict Priority | - | - | - | - | - | - | - | - |
| 3 | Strict Priority | - | - | - | - | - | - | - | - |
| 4 | Strict Priority | - | - | - | - | - | - | - | - |
| 5 | Strict Priority | - | - | - | - | - | - | - | - |
| 6 | Strict Priority | - | - | - | - | - | - | - | - |
| 7 | Strict Priority | - | - | - | - | - | - | - | - |
| 8 | Strict Priority | - | - | - | - | - | - | - | - |

### QoS Egress Port Schedulers

| Object | Description |
|---|---|
| **Port** | The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers. |
| **Mode** | Shows the scheduling mode for this port. |
| **Qn** | Shows the weight for this queue and port. |

### QoS Egress Port Scheduler and Shapers Port n

Click a port No. to configure Scheduler.

This page allows you to configure the Scheduler and Shapers for a specific port.

### QoS Egress Port Schedulers and Shapers Port n

| Object | Description |
|---|---|
| **Scheduler Mode** | Controls how many of the queues are scheduled as strict and how many are scheduled as weighted on this switch port. |
| **Queue Shaper Enable** | Controls whether the queue shaper is enabled for this queue on this switch port. |
| **Queue Shaper Rate** | Controls the rate for the queue shaper. This value is restricted to 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue shaper. |
| **Queue Shaper Unit** | Controls the unit of measure for the queue shaper rate as kbps or Mbps. |
| **Queue Scheduler Weight** | Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted". |
| **Queue Scheduler Percent** | Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted". |
| **Port Shaper Enable** | Controls whether the port shaper is enabled for this switch port. |
| **Port Shaper Rate** | Controls the rate for the port shaper. This value is restricted to 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the port shaper. |
| **Port Shaper Unit** | Controls the unit of measure for the port shaper rate as kbps or Mbps. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

Back : Click to undo any changes made locally and return to the previous page.

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>QoS>Port Scheduler

✓ **QoS Egress Port Schedulers**

**QoS Egress Port Schedulers**

| Port | Mode | Weight | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Q0 | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 |
| 1 | Strict Priority | - | - | - | - | - | - | - | - |
| 2 | Strict Priority | - | - | - | - | - | - | - | - |
| 3 | Strict Priority | - | - | - | - | - | - | - | - |
| 4 | Strict Priority | - | - | - | - | - | - | - | - |
| 5 | Strict Priority | - | - | - | - | - | - | - | - |
| 6 | Strict Priority | - | - | - | - | - | - | - | - |
| 7 | Strict Priority | - | - | - | - | - | - | - | - |
| 8 | Strict Priority | - | - | - | - | - | - | - | - |
| 9 | Strict Priority | - | - | - | - | - | - | - | - |
| 10 | Strict Priority | - | - | - | - | - | - | - | - |
| 11 | Strict Priority | - | - | - | - | - | - | - | - |
| 12 | Strict Priority | - | - | - | - | - | - | - | - |

➢ *Port*

Click on the port number in order to configure the schedulers.

✓ **QoS Egress Port Schedulers and Shapers Port n**

➢ *Scheduler Mode*

- Strict Priority | Queues Weighted

➤ **Queue Shaper Enable**

• Enabled | Disabled



➤ **Queue Shaper Rate**

• 100-13107100(kbps) or 1-13107(Mbps)



➤ **Queue Shaper Unit**

• kbps or Mbps

**QoS Egress Port Scheduler and Shapers Port 1**

➢ *Queue Scheduler Weight*

• 1~100(Scheduler Mode should be set to 'Weighted')



**QoS Egress Port Scheduler and Shapers Port 1**
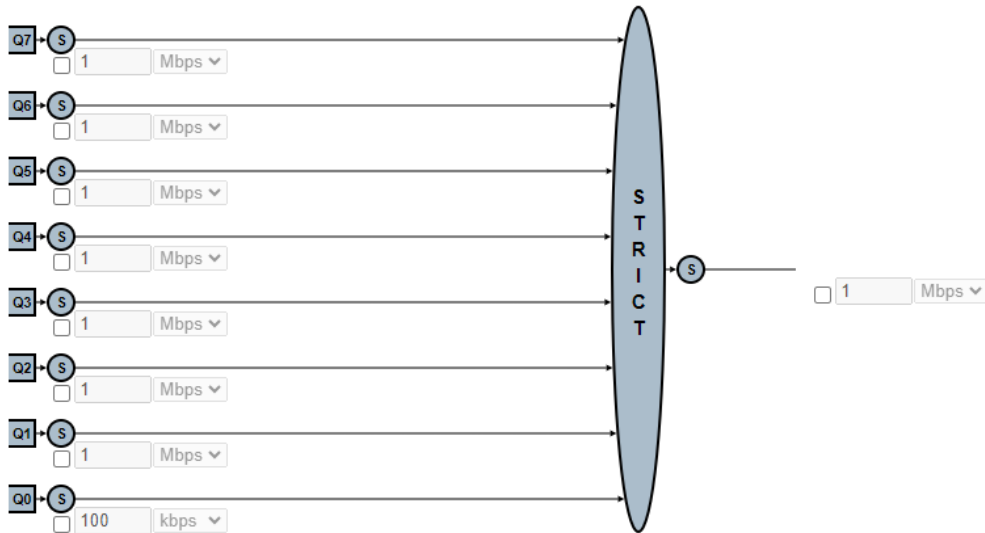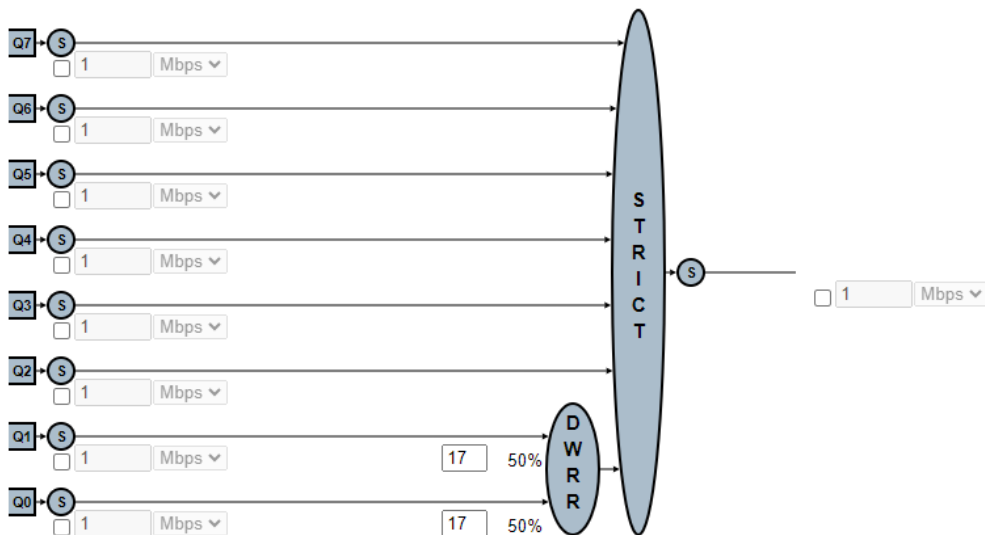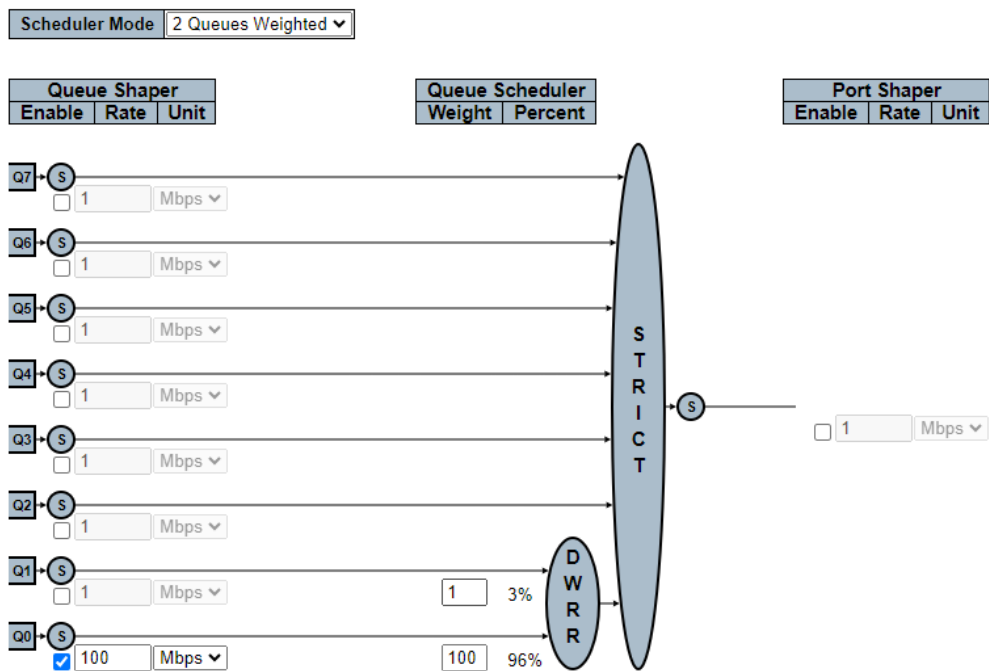
➢ *Port Shaper Enable*

• Enabled | Disabled

QoS Egress Port Scheduler and Shapers Port 1
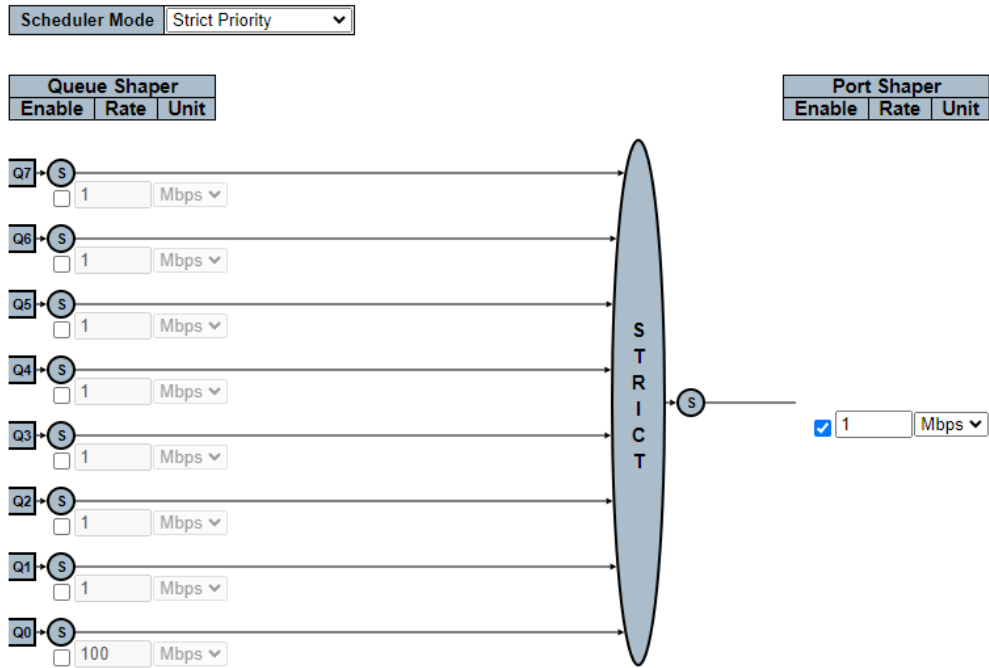
> *Port Shaper Rate*

   • 100-13107100(kbps) or 1-13107(Mbps)



QoS Egress Port Scheduler and Shapers Port 1

> *Port Shaper Unit*

   • kbps or Mbps

QoS Egress Port Scheduler and Shapers Port 1

---

## EXAMPLE CLI CONFIGURATION

✓ **QoS Egress Port Schedulers**

➢ *Port*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1
```

✓ **QoS Egress Port Schedulers and Shapers Port n**

➢ *Scheduler Mode*

• Strict Priority | Queues Weighted

```
(config-if)# no qos wrr

(config-if)# qos wrr <w0> <w1> [ <w2> [ <w3> [ <w4> [ <w5> [ <w6> [ <w7> ] ] ] ] ] ]
(config-if)# qos wrr 17 17
```

➢ *Queue Shaper Enable*

• Enabled | Disabled

➢ *Queue Shaper Rate*

• 100-13107100(kbps) or 1-13107(Mbps)

➢ *Queue Shaper Unit*

• kbps or Mbps

```
(config-if)# qos queue-shaper queue <queue> <rate> [ kbps | mbps ] [ excess ] [ rate-type { line |
data } ]
(config-if)# no qos queue-shaper queue 0
(config-if)# qos queue-shaper queue 0 1 mbps
(config-if)# qos queue-shaper queue 0 100 kbps
```

> ### Queue Scheduler Weight

  • 1~100(Scheduler Mode should be set to 'Weighted')

```
(config-if)# qos wrr <w0> <w1> [ <w2> [ <w3> [ <w4> [ <w5> [ <w6> [ <w7> ] ] ] ] ] ]
(config-if)# qos wrr 100 1
```

> ### Port Shaper Enable

  • Enabled | Disabled

> ### Port Shaper Rate

  • 100-13107100(kbps) or 1-13107(Mbps)

> ### Port Shaper Unit

  • kbps or Mbps

```
(config-if)# qos shaper <rate> [ kbps | mbps ] [ rate-type { line | data } ]
(config-if)# no qos shaper
(config-if)# qos shaper 1 mbps
(config-if)# qos shaper 100 kbps
```

## 6.20.1.5. Port Shaping

WEB MENU Configuration>QoS>Port Shaping

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

**QoS Egress Port Shapers**

| Port | Shapers | | | | | | | | |
|------|---|---|---|---|---|---|---|---|------|
|      | Q0 | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 | Port |
| 1 | - | - | - | - | - | - | - | - | - |
| 2 | - | - | - | - | - | - | - | - | - |
| 3 | - | - | - | - | - | - | - | - | - |
| 4 | - | - | - | - | - | - | - | - | - |
| 5 | - | - | - | - | - | - | - | - | - |
| 6 | - | - | - | - | - | - | - | - | - |
| 7 | - | - | - | - | - | - | - | - | - |
| 8 | - | - | - | - | - | - | - | - | - |

### QoS Egress Port Shapers

| Object | Description |
|--------|-------------|
| **Port** | The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers. |
| **Qn** | Shows "-" for disabled or actual queue shaper rate - e.g. "800 Mbps". |
| **Port** | Shows "-" for disabled or actual port shaper rate - e.g. "800 Mbps". |

## 6.20.1.6. Port Tag Remarking

WEB MENU Configuration>QoS>Port Tag Remarking

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

**QoS Egress Port Tag Remarking**

| Port | Mode |
|------|------|
| 1 | Classified |
| 2 | Classified |
| 3 | Classified |
| 4 | Classified |
| 5 | Classified |
| 6 | Classified |
| 7 | Classified |
| 8 | Classified |

### QoS Egress Port Tag Remarking

| Object | Description |
|--------|-------------|
| **Port** | The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking. |
| **Mode** | Shows the tag remarking mode for this port. Classified: Use classified PCP/DEI values. Default: Use default PCP/DEI values. Mapped: Use mapped versions of QoS class and DP level. |

## QoS Egress Port Tag Remarking Port

The QoS Egress Port Tag Remarking for a specific port are configured on this page.

**QoS Egress Port Tag Remarking  Port 1**

| Tag Remarking Mode | Classified ⌄ |

### QoS Egress Port Tag Remarking Port n

| Object | Description |
|--------|-------------|
| **Mode** | Controls the tag remarking mode for this port. Classified: Use classified PCP/DEI values. Default: Use default PCP/DEI values. Mapped: Use mapped versions of QoS class and DP level. |
| **PCP/DEI Configuration** | Controls the default PCP and DEI values used when the mode is set to Default. |
| **(QoS class, DP level) to (PCP, DEI) Mapping** | Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to Mapped. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

Cancel : Click to undo any changes made locally and return to the previous page.

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>QoS>Port Tag Remarking

✓ **QoS Egress Port Tag Remarking**

➢ *Port(*Click on the port number in order to configure tag remarking.*)*

**QoS Egress Port Tag Remarking**

| Port | Mode |
|------|------|
| 1 | Classified |
| 2 | Classified |
| 3 | Classified |
| 4 | Classified |
| 5 | Classified |
| 6 | Classified |
| 7 | Classified |
| 8 | Classified |
| 9 | Classified |
| 10 | Classified |
| 11 | Classified |
| 12 | Classified |

✓ **QoS Egress Port Tag Remarking Port n**

➢ *Tag Remarking Mode*

• Classified

**QoS Egress Port Tag Remarking  Port 1**

| Tag Remarking Mode | Classified ⌄ |
|---|---|

• Default

**QoS Egress Port Tag Remarking  Port 1**

| Tag Remarking Mode | Default ⌄ |
|---|---|

**PCP/DEI Configuration**

| Default PCP | 0 ⌄ |
|---|---|
| Default DEI | 0 ⌄ |

• Mapped

**QoS Egress Port Tag Remarking  Port 1**

| Tag Remarking Mode | Mapped ⌄ |
|---|---|

**(QoS class, DP level) to (PCP, DEI) Mapping**

| QoS class | DP level | PCP | DEI |
|-----------|----------|-----|-----|
| * | * | <> ⌄ | <> ⌄ |
| 0 | 0 | 1 ⌄ | 0 ⌄ |
| 0 | 1 | 1 ⌄ | 1 ⌄ |
| 1 | 0 | 0 ⌄ | 0 ⌄ |
| 1 | 1 | 0 ⌄ | 1 ⌄ |
| 2 | 0 | 2 ⌄ | 0 ⌄ |
| 2 | 1 | 2 ⌄ | 1 ⌄ |
| 3 | 0 | 3 ⌄ | 0 ⌄ |
| 3 | 1 | 3 ⌄ | 1 ⌄ |
| 4 | 0 | 4 ⌄ | 0 ⌄ |
| 4 | 1 | 4 ⌄ | 1 ⌄ |
| 5 | 0 | 5 ⌄ | 0 ⌄ |
| 5 | 1 | 5 ⌄ | 1 ⌄ |
| 6 | 0 | 6 ⌄ | 0 ⌄ |
| 6 | 1 | 6 ⌄ | 1 ⌄ |
| 7 | 0 | 7 ⌄ | 0 ⌄ |
| 7 | 1 | 7 ⌄ | 1 ⌄ |

✓ **PCP/DEI Configuration**

The following items are displayed when the mode is set to "Default".

➢ *Default PCP*

- 0~7



➢ *Default DEI*

- 0~1



✓ **(QoS class, DP level) to (PCP, DEI) Mapping**

When the Mode is set to 'Mapped' you will see the following entries

➢ *PCP*

- 0~7

➢ **DEI**

• 0~1

**QoS Egress Port Tag Remarking  Port 1**

Tag Remarking Mode  | Mapped ▾ |

**(QoS class, DP level) to (PCP, DEI) Mapping**

| QoS class | DP level | PCP | DEI |
|---|---|---|---|
| * | * | <> ▾ | <> ▾ |
| 0 | 0 | 1 ▾ | 0 ▾ |
| 0 | 1 | 1 ▾ | 0 |
| 1 | 0 | 0 ▾ | 1 |
| 1 | 1 | 0 ▾ | 0 ▾ |
| 2 | 0 | 2 ▾ | 0 ▾ |
| 2 | 1 | 2 ▾ | 1 ▾ |
| 3 | 0 | 3 ▾ | 0 ▾ |
| 3 | 1 | 3 ▾ | 1 ▾ |
| 4 | 0 | 4 ▾ | 0 ▾ |
| 4 | 1 | 4 ▾ | 1 ▾ |
| 5 | 0 | 5 ▾ | 0 ▾ |
| 5 | 1 | 5 ▾ | 1 ▾ |
| 6 | 0 | 6 ▾ | 0 ▾ |
| 6 | 1 | 6 ▾ | 1 ▾ |
| 7 | 0 | 7 ▾ | 0 ▾ |
| 7 | 1 | 7 ▾ | 1 ▾ |

## EXAMPLE CLI CONFIGURATION

✓ **QoS Egress Port Tag Remarking**

➢ **Port**

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1
```

✓ **QoS Egress Port Tag Remarking Port n**

➢ **Tag Remarking Mode**

• Classified

```
(config-if)# no qos tag-remark
```

• Default

```
(config-if)# qos tag-remark { pcp <pcp> dei <dei> | mapped }
(config-if)# qos tag-remark pcp <pcp> dei <dei>
```

• Mapped

```
(config-if)# qos tag-remark { pcp <pcp> dei <dei> | mapped }
(config-if)# qos tag-remark mapped
```

✓ **PCP/DEI Configuration**

➢ **Default PCP**

• 0~7

➢ ***Default DEI***

- 0~1

```
(config-if)# qos tag-remark pcp <pcp> dei <dei>
(config-if)# qos tag-remark pcp 0 dei 0
```

✓ **(QoS class, DP level) to (PCP, DEI) Mapping**

➢ ***PCP***

- 0~7

➢ ***DEI***

- 0~1

```
(config-if)# qos map cos-tag cos <cos> dpl <dpl> pcp <pcp> dei <dei>
(config-if)# qos map cos-tag cos 0 dpl 0 pcp 1 dei 0
```

## 6.20.1.7. Port DSCP

WEB MENU Configuration>QoS>Port DSCP

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

**QoS Port DSCP Configuration**

| Port | Ingress | | Egress |
|---|---|---|---|
| | Translate | Classify | Rewrite |
| * | ☑ | DSCP=0 ▾ | <> ▾ |
| 1 | ☑ | DSCP=0 ▾ | Disable ▾ |
| 2 | ☑ | DSCP=0 ▾ | Disable ▾ |
| 3 | ☑ | DSCP=0 ▾ | Disable ▾ |
| 4 | ☑ | DSCP=0 ▾ | Disable ▾ |
| 5 | ☑ | DSCP=0 ▾ | Disable ▾ |
| 6 | ☑ | DSCP=0 ▾ | Disable ▾ |
| 7 | ☑ | DSCP=0 ▾ | Disable ▾ |
| 8 | ☑ | DSCP=0 ▾ | Disable ▾ |

### QoS Port DSCP Configuration

| Object | Description |
|---|---|
| **Port** | The Port column shows the list of ports for which you can configure DSCP ingress and egress settings. |
| **Ingress** | In Ingress settings you can change ingress translation and classification settings for individual ports.<br>There are two configuration parameters available in Ingress:<br>1. Translate<br>2. Classify |
| **1. Translate** | To Enable the Ingress Translation click the checkbox. |
| **2. Classify** | Classification for a port have 4 different values.<br>1. Disable: No Ingress DSCP Classification.<br>2. DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0.<br>3. Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.<br>4. All: Classify all DSCP. |
| **Egress** | Port Egress Rewriting can be one of -<br>1. Disable: No Egress rewrite.<br>2. Enable: Rewrite enabled without remapping.<br>3. Remap: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

SOLTECH
INFONET INC.

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>QoS>Port DSCP

✓ **QoS Port DSCP Configuration**

➢ *Ingress Translate*

• Enable | Disable

➢ *Ingress Classify*

• Disable | DSCP=0 | Slected | All

➢ *Egress Rewrite*

• Disable | Enable | Remap DP Unaware | Remap DP Aware

• Disable | Enable | Remap

| Port | Ingress | | Egress |
|------|---------|---------|--------|
| | Translate | Classify | Rewrite |
| * | ☐ | <> | <> |
| 1 | ☑ | Disable | Disable |
| 2 | ☐ | Disable | Disable |
| 3 | ☐ | DSCP=0 | Enable |
| 4 | ☐ | Selected | Remap DP Unaware |
| 5 | ☐ | All / Disable | Remap DP Aware / Disable |
| 6 | ☐ | Disable | Disable |
| 7 | ☐ | Disable | Disable |
| 8 | ☐ | Disable | Disable |
| 9 | ☐ | Disable | Disable |
| 10 | ☐ | Disable | Disable |

## EXAMPLE CLI CONFIGURATION

✓ **QoS Port DSCP Configuration**

➢ *Ingress Translate*

• Enable | Disable

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1
```
```
(config-if)# qos dscp-translate
(config-if)# no qos dscp-translate
```

➢ *Ingress Classify*

• Disable | DSCP=0 | Slected | All

```
(config-if)# qos dscp-classify { zero | selected | any }
(config-if)# no qos dscp-classify
(config-if)# qos dscp-classify zero
(config-if)# qos dscp-classify selected
(config-if)# qos dscp-classify any
```

SOLTECH
INFONET INC.

➢ **Egress Rewrite**

- Disable | Enable | Remap DP Unaware | Remap DP Aware

- Disable | Enable | Remap

```
(config-if)# qos dscp-remark { rewrite | remap | remap-dp }
(config-if)# no qos dscp-remark
(config-if)# qos dscp-remark rewrite
(config-if)# qos dscp-remark remap
(config-if)# qos dscp-remark remap-dp
```

```
(config-if)# qos dscp-remark { rewrite | remap }
(config-if)# no qos dscp-remark
(config-if)# qos dscp-remark rewrite
(config-if)# qos dscp-remark remap
```

## 6.20.1.8. DSCP-Based QoS

WEB MENU Configuration>QoS>DSCP-Based QoS

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

**DSCP-Based QoS Ingress Classification**

| DSCP | Trust | QoS Class | DPL |
|------|-------|-----------|-----|
| * | ☐ | <> ▾ | <> ▾ |
| 0 (BE) | ☐ | 0 ▾ | 0 ▾ |
| 1 | ☐ | 0 ▾ | 0 ▾ |
| 2 | ☐ | 0 ▾ | 0 ▾ |
| 3 | ☐ | 0 ▾ | 0 ▾ |
| 4 | ☐ | 0 ▾ | 0 ▾ |
| | | 0 ▾ | 0 ▾ |
| 58 | ☐ | 0 ▾ | 0 ▾ |
| 59 | ☐ | 0 ▾ | 0 ▾ |
| 60 | ☐ | 0 ▾ | 0 ▾ |
| 61 | ☐ | 0 ▾ | 0 ▾ |
| 62 | ☐ | 0 ▾ | 0 ▾ |
| 63 | ☐ | 0 ▾ | 0 ▾ |

**DSCP-Based QoS Ingress Classification**

| Object | Description |
|--------|-------------|
| **DSCP** | Maximum number of supported DSCP values are 64. |
| **Trust** | Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame. |
| **QoS Class** | QoS class value can be any of (0-7) |
| **DPL** | Drop Precedence Level (0-3) |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

### EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>QoS>DSCP-Based QoS

✓ **DSCP-Based QoS Ingress Classification**

SOLTECH
INFONET INC.

➢   ***DSCP***

➢   ***Trust***

•   Trusted | Untrusted

➢   ***QoS Class***

•   0~7

➢   ***DPL***

•   0~1

| DSCP | Trust | QoS Class | DPL |
|------|-------|-----------|-----|
| * | ☑ | <> ∨ | <> ∨ |
| 0 (BE) | ☑ | 0 ∨ | 0 ∨ |
| 1 | ☑ | 0 | 0 |
| 2 | ☑ | 1 2 | 1 0 ∨ |
| 3 | ☑ | 3 | 0 ∨ |
| 4 | ☑ | 4 5 | 0 ∨ |
| 5 | ☑ | 6 | 0 ∨ |
| 6 | ☑ | 7 | 0 ∨ |

---

## EXAMPLE CLI CONFIGURATION

---

✓   **DSCP-Based QoS Ingress Classification**

➢   ***DSCP***

➢   ***Trust***

•   Trusted | Untrusted

➢   ***QoS Class***

•   0~7

➢   ***DPL***

•   0~1

```
(config-if)# qos map dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33
| af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } cos <cos> dpl <dpl>
(config)# no qos map dscp-cos 0
(config)# qos map dscp-cos 0 cos 0 dpl 0
(config)# qos map dscp-cos 63 cos 7 dpl 1
(config)# qos map dscp-cos cs1 cos 7 dpl 1
```

## 6.20.1.9. DSCP Translation

WEB MENU Configuration>QoS>DSCP Translation

This page allows you to configure the basic QoS DSCP Translation settings for all switches.

DSCP translation can be done in Ingress or Egress.

**DSCP Translation**

| DSCP | Ingress | | Egress |
|---|---|---|---|
| | Translate | Classify | Remap |
| * | <> | ☐ | <> |
| 0 (BE) | 0 (BE) | ☐ | 0 (BE) |
| 1 | 1 | ☐ | 1 |
| 2 | 2 | ☐ | 2 |
| 3 | 3 | ☐ | 3 |
| 4 | 4 | ☐ | 4 |
| 58 | 58 | ☐ | 58 |
| 59 | 59 | ☐ | 59 |
| 60 | 60 | ☐ | 60 |
| 61 | 61 | ☐ | 61 |
| 62 | 62 | ☐ | 62 |
| 63 | 63 | ☐ | 63 |

**DSCP Translation**

| Object | Description |
|---|---|
| **DSCP** | Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63. |
| **Ingress** | Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.<br>There are two configuration parameters for DSCP Translation<br>1. Translate<br>2. Classify |
| **1. Translate** | DSCP at Ingress side can be translated to any of (0-63) DSCP values. |
| **2. Classify** | Click to enable Classification at Ingress side. |
| **Egress** | There is the following configurable parameter for Egress side<br>Remap |
| **Remap** | Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>QoS>DSCP Translation

  ✓ **DSCP Translation**

➢ **DSCP**

➢ **Ingress Translate**

• 0~63

➢ **Ingress Classify**

• Enable | Disable

➢ **Egress Remap**

• 0~63

| DSCP | Ingress | | Egress |
|------|---------|----------|--------|
| | Translate | Classify | Remap |
| * | <> | ☐ | <> |
| 0 (BE) | 1 | ☑ | 0 (BE) |
| 1 | 0 (BE) | ☐ | 0 (BE) |
| 2 | 1<br>2 | ☐ | 1<br>2 |
| 3 | 3 | ☐ | 3 |
| 4 | 4 | ☐ | 4 |
| 5 | 5 | ☐ | 5 |
| 6 | 6<br>7 | ☐ | 6<br>7 |
| 7 | 8 (CS1) | ☐ | 8 (CS1) |
| 8 (CS1) | 9 | ☐ | 9 |
| 9 | 10 (AF11) | ☐ | 10 (AF11) |
| 10 (AF11) | 11<br>12 (AF12) | ☐ | 11<br>12 (AF12) |
| 11 | 13 | ☐ | 13 |
| 12 (AF12) | 14 (AF13) | ☐ | 14 (AF13) |
| 13 | 15 | ☐ | 15 |
| 14 (AF13) | 16 (CS2)<br>17 | ☐ | 16 (CS2)<br>17 |
| 15 | 18 (AF21) | ☐ | 18 (AF21) |
| 16 (CS2) | 19 | ☐ | 19 |

# EXAMPLE CLI CONFIGURATION

✓ **DSCP Translation**

➢ **DSCP**

➢ **Ingress Translate**

• 0~63

```
(config)# qos map dscp-ingress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31
| af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } to { <dscp_num_tr> | { be |
af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 |
cs7 | ef | va } }
(config)# qos map dscp-ingress-translation 0 to 1
(config)# qos map dscp-ingress-translation 60 to 63
(config)# qos map dscp-ingress-translation be to 1
```

➢ **Ingress Classify**

• Enable | Disable

```
(config)# qos map dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 |
af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }
(config)# qos map dscp-classify 0
(config)# qos map dscp-classify 63
(config)# qos map dscp-classify be
(config)# no qos map dscp-classify 0
```

➢ **Egress Remap**

- 0~63

```
(config)# qos map dscp-egress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 |
af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } <dpl> to { <dscp_num_tr> |
{ be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 |
cs6 | cs7 | ef | va } }
(config)# qos map dscp-egress-translation 0 to 1
(config)# qos map dscp-egress-translation 60 to 63
(config)# qos map dscp-egress-translation be to 1
```

## 6.20.1.10. DSCP Classification

WEB MENU Configuration>QoS>DSCP Classification

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

**DSCP Classification**

| QoS Class | DSCP DP0 | DSCP DP1 | DSCP DP2 | DSCP DP3 |
|---|---|---|---|---|
| * | <> | <> | <> | <> |
| 0 | 0 (BE) | 0 (BE) | 0 (BE) | 0 (BE) |
| 1 | 0 (BE) | 0 (BE) | 0 (BE) | 0 (BE) |
| 2 | 0 (BE) | 0 (BE) | 0 (BE) | 0 (BE) |
| 3 | 0 (BE) | 0 (BE) | 0 (BE) | 0 (BE) |
| 4 | 0 (BE) | 0 (BE) | 0 (BE) | 0 (BE) |
| 5 | 0 (BE) | 0 (BE) | 0 (BE) | 0 (BE) |
| 6 | 0 (BE) | 0 (BE) | 0 (BE) | 0 (BE) |
| 7 | 0 (BE) | 0 (BE) | 0 (BE) | 0 (BE) |

### DSCP Classification

| Object | Description |
|---|---|
| **QoS Class** | Actual QoS class. |
| **DSCP DP0** | Select the classified DSCP value (0-63) for Drop Precedence Level 0. |
| **DSCP DP1** | Select the classified DSCP value (0-63) for Drop Precedence Level 1. |
| **DSCP DP2** | Select the classified DSCP value (0-63) for Drop Precedence Level 2. |
| **DSCP DP3** | Select the classified DSCP value (0-63) for Drop Precedence Level 3. |

**Buttons**

`Apply` : Click to apply changes.

`Apply&Save` : Click to apply and save changes.

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

### EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>QoS>DSCP Classification

✓ **DSCP Classification**

➢ *QoS Class*
- 0~7

➢ *DP*
- 0~1, 0~3

➢ *DSCP*
- 0~63

---

## EXAMPLE CLI CONFIGURATION

---

✓ **DSCP Classification**

➢ *QoS Class*

- 0~7

➢ *DP*

- 0~1, 0~3

➢ *DSCP*

- 0~63

```
(config)# qos map cos-dscp <cos> dpl <dpl> dscp { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 |
af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }
(config)# qos map cos-dscp 0 dpl 0 dscp 0
(config)# qos map cos-dscp 7 dpl 1 dscp 63
(config)# qos map cos-dscp 7 dpl 1 dscp be
```

## 6.20.1.11. QoS Control List

WEB MENU Configuration>QoS>QoS Control List

This page shows the QoS Control List(QCL), which is made up of the QCEs.

Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch.

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

**QoS Control List Configuration**

| QCE | Port | DMAC | SMAC | Tag Type | VID | PCP | DEI | Frame Type | Action | | | | | |
|-----|------|------|------|----------|-----|-----|-----|------------|--------|--|--|--|--|--|
| | | | | | | | | | CoS | DPL | DSCP | PCP | DEI | Policy |

### QoS Control List Configuration

| Object | Description |
|--------|-------------|
| **QCE** | Indicates the QCE id. |
| **Port** | Indicates the list of ports configured with the QCE or 'Any'. |
| **DMAC** | Indicates the destination MAC address. Possible values are: <br> Any: Match any DMAC. <br> Unicast: Match unicast DMAC. <br> Multicast: Match multicast DMAC. <br> Broadcast: Match broadcast DMAC. <br> <MAC>: Match specific DMAC. <br> The default value is 'Any'. |
| **SMAC** | Match specific source MAC address or 'Any'. |
| **Tag Type** | Indicates tag type. Possible values are: <br> Any: Match tagged and untagged frames. <br> Untagged: Match untagged frames. <br> Tagged: Match tagged frames. <br> C-Tagged: Match C-tagged frames. <br> S-Tagged: Match S-tagged frames. <br> The default value is 'Any'. |
| **VID** | Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any' |
| **PCP** | Priority Code Point: Valid values of PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'. |
| **DEI** | Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'. |
| **Frame Type** | Indicates the type of frame. Possible values are: <br> Any: Match any frame type. <br> Ethernet: Match EtherType frames. <br> LLC: Match (LLC) frames. <br> SNAP: Match (SNAP) frames. <br> IPv4: Match IPv4 frames. <br> IPv6: Match IPv6 frames. |
| **Action** | Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. <br> Possible actions are: |

| | |
|---|---|
| | CoS: Classify Class of Service.<br>DPL: Classify Drop Precedence Level.<br>DSCP: Classify DSCP value.<br>PCP: Classify PCP value.<br>DEI: Classify DEI value.<br>Policy: Classify ACL Policy number. |
| **Modification Buttons** | You can modify each QCE (QoS Control Entry) in the table using the following buttons:<br>⊕: Inserts a new QCE before the current row.<br>ⓔ: Edits the QCE.<br>⊕: Moves the QCE up the list.<br>⊕: Moves the QCE down the list.<br>⊗: Deletes the QCE.<br>⊕: The lowest plus sign adds a new entry at the bottom of the QCE listings. |

## QCE Configuration

This page allows to edit | insert a single QoS Control Entry at a time. A QCE consists of several parameters. These parameters vary according to the frame type that you select.

**QCE Configuration**

Port Members
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |

**Key Parameters**

| DMAC | Any |
| SMAC | Any |
| Tag | Any |
| VID | Any |
| PCP | Any |
| DEI | Any |
| Inner Tag | Any |
| Inner VID | Any |
| Inner PCP | Any |
| Inner DEI | Any |
| Frame Type | Any |

**Action Parameters**

| CoS | 0 |
| DPL | Default |
| DSCP | Default |
| PCP | Default |
| DEI | Default |
| Policy | |

### QCE Configuration

| Object | Description |
|---|---|
| **Port Members** | Check the checkbox button to include the port in the QCL entry.<br>By default all ports are included. |
| **Key Parameters** | Key configuration is described as below:<br><br>DMAC: Destination MAC address: Possible values are 'Unicast', 'Multicast', 'Broadcast', 'Specific' (xx-xx-xx-xx-xx-xx) or 'Any'.<br><br>SMAC: Source MAC address: xx-xx-xx-xx-xx-xx or 'Any'.<br><br>Tag: Value of Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.<br><br>VID: Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.<br><br>PCP: Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.<br><br>DEI: Valid value of DEI can be '0', '1' or 'Any'. |

| | | |
|---|---|---|
| | Inner Tag | Value of Inner Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'. |
| | Inner VID | Valid value of Inner VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs. |
| | Inner PCP | Valid value of Inner PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'. |
| | Inner DEI | Valid value of Inner DEI can be '0', '1' or 'Any'. |
| | Frame Type | Frame Type can have any of the following values: 1.Any, 2,EtherType, 3.LLC, 4.SNAP, 5.IPv4, 6.IPv6 |
| **1. Any** | Allow all types of frames. | |
| **2. EtherType** | Ether Type | Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'. |
| **3. LLC** | DSAP Address | Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'. |
| | SSAP Address | Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'. |
| | Control | Valid Control field can vary from 0x00 to 0xFF or 'Any'. |
| **4. SNAP** | PID | Valid PID(a.k.a Ether Type) can be 0x0000-0xFFFF or 'Any'. |
| **5. IPv4** | Protocol | IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'. |
| | Source IP | Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero. |
| | Destination IP | Specific Destination IP address in value/mask format or 'Any'. |
| | IP Fragment | IPv4 frame fragmented option: 'Yes', 'No' or 'Any'. |
| | DSCP | Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43. |
| | Sport | Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP. |
| | Dport | Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP. |
| **6. IPv6** | Protocol | IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'. |
| | Source IP | 32 LS bits of IPv6 source address in value/mask format or 'Any'. |
| | Destination IP | Specific Destination IP address in value/mask format or 'Any'. |
| | DSCP | Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43. |
| | Sport | Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP. |
| | Dport | Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP. |
| **Action Parameters** | CoS | Class of Service: (0-7) or 'Default'. |
| | DP | Drop Precedence Level: (0-3) or 'Default' |

| | | |
|---|---|---|
| | DSCP | DSCP (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'. |
| | PCP | PCP: (0-7) or 'Default'. Note: PCP and DEI cannot be set individually. |
| | DEI | DEI: (0-1) or 'Default'. |
| | Policy | ACL Policy number: (0-255) or 'Default' (empty field). |
| | 'Default' means that the default classified value is not modified by this QCE. | |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

Cancel : Return to the previous page without saving the configuration change.

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>QoS>QoS Control List

✓ **QoS Control List Configuration**

    ➢ *QCE*

    ➢ *Port*

    ➢ *DMAC*

    ➢ *SMAC*

    ➢ *Tag Type*

    ➢ *VID*

    ➢ *PCP*

    ➢ *DEI*

    ➢ *Frame Type*

    ➢ *Action*

        • CoS

        • DPL

        • DSCP

        • PCP

        • DEI

        • Policy

**QoS Control List Configuration**

| QCE | Port | DMAC | SMAC | Tag Type | VID | PCP | DEI | Frame Type | Action | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | CoS | DPL | DSCP | PCP | DEI | Policy |
| | | | | | | | | | | | | | | ⊕ |

*Click ⊕ Button*

✓ **QCE Configuration**

➢ *Port Members*

• Select Port



✓ **Key Parameters**

➢ *DMAC*

• Any | Unicast | Multicast | Broadcast



➢ *SMAC*

• Any | Specific(Selecting this option will generate additional configuration options.)



➢ *Tag*

• Any | Untagged | Tagged | C-Tagged | S-Tagged



➢ *VID*

• Any | Specific(additional configuration options.) | Range(additional configuration options.)



➢ *PCP*

• Any | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0-1 | 2-3 | 4-5 | 6-7 | 0-3 | 4-7

> ➢ **DEI**

  • Any | 0 | 1



> ➢ **Frame Type**(additional configuration options.)

  • Any | EtherType | LLC | SNAP | IPv4 | IPv6



✓ **EtherType Parameters**

> ➢ **Ether Type**

  • Any | Specific(0x600-0x7ff,0x801-0x86dc,0x86de-0xffff)



✓ **LLC Parameters**

> ➢ **DSAP Address**

  • Any | Specific(additional configuration options.)

> ➢ **SSAP Address**

  • Any | Specific(additional configuration options.)

> ➢ **Control**

  • Any | Specific(additional configuration options.)

| DSAP Address | Specific ˅ | Value: 0x | FF |
| SSAP Address | Any | Value: 0x | FF |
| Control | Specific | Value: 0x | FF |

✓ **SNAP Parameters**

➢ *PID*

- Any | Specific(<0-0xffff>)

| PID | Specific ˅ | Value: 0x | FFFF |
| | Any | | |
| | Specific | | |

✓ **IPv4 Parameters**

➢ *Protocol*(additional configuration options.)

- Any | UDP | TCP | Other

| Protocol | Other ˅ | Value: | 0 |
| SIP | Any ˅ | | |
| IP Fragment | UDP | | |
| DSCP | TCP ˅ | | |
| | Other | | |

➢ *SIP*

- Any | Specific(additional configuration options.)

| Protocol | Any ˅ | | | | |
| SIP | Specific ˅ | Value: | 0.0.0.0 | Mask: | 0.0.0.0 |
| IP Fragment | Any | | | | |
| DSCP | Specific | | | | |

➢ *IP Fragment*

- Any | Yes | No

| Protocol | Any ˅ |
| SIP | Any ˅ |
| IP Fragment | Any ˅ |
| DSCP | Any ˅ |
| | Yes |
| | No |

➢ *DSCP*

- Any | Specific(additional configuration options.) | Range(additional configuration options.)

| Protocol | Any ˅ | | | | |
| SIP | Any ˅ | | | | |
| IP Fragment | Any ˅ | | | | |
| DSCP | Range ˅ | 0 (BE) ˅ | - | 63 ˅ | |
| | Any | | | | |
| | Specific | | | | |
| | Range | | | | |

✓ **IPv6 Parameters**

➢ *Protocol*(additional configuration options.)

- Any | UDP | TCP | Other

| Protocol | Other ˅ | Value: | 0 |
| SIP (32 LSB) | Any ˅ | | |
| DSCP | UDP ˅ | | |
| | TCP | | |
| | Other | | |

➢ *SIP (32LSB)*

- Any | Specific(additional configuration options.)

| Protocol | Any ˅ | | | | |
| SIP (32 LSB) | Specific ˅ | Value: | 0.0.0.0 | Mask: | 0.0.0.0 |
| DSCP | Any | | | | |
| | Specific | | | | |

➢ *DSCP*

- Any | Specific(additional configuration options.) | Range(additional configuration options.)

- ✓ **UDP Parameters**

  - ➢ *Sport*

    - • Any | Specific(additional configuration options.) | Range(additional configuration options.)

    

  - ➢ *Dport*

    - • Any | Specific(additional configuration options.) | Range(additional configuration options.)

    

- ✓ **TCP Parameters**

  - ➢ *Sport*

    - • Any | Specific(additional configuration options.) | Range(additional configuration options.)

    

  - ➢ *Dport*

    - • Any | Specific(additional configuration options.) | Range(additional configuration options.)

    

- ✓ **Action Parameters**

  - ➢ *CoS*

    - • Default | 0~7

    

  - ➢ *DPL*

    - • Default | 0~1

    

  - ➢ *DSCP*

- Default | 0~63

| CoS | Default ∨ |
| DPL | Default ∨ |
| DSCP | Default ∨ |
| PCP | **Default** |
| DEI | 0 (BE) |
| Policy | 1 |
| | 2 |
| | 3 |
| | 4 |
| | 5 |
| | 6 |
| | 7 |

➢ **PCP**

- Default | 0~7

| CoS | Default ∨ |
| DPL | Default ∨ |
| DSCP | Default ∨ |
| PCP | Default ∨ |
| DEI | **Default** |
| Policy | 0 |
| | 1 |
| | 2 |
| | 3 |
| | 4 |
| | 5 |
| | 6 |
| | 7 |

➢ **DEI**

- Default | 0~1

| CoS | Default ∨ |
| DPL | Default ∨ |
| DSCP | Default ∨ |
| PCP | Default ∨ |
| DEI | Default ∨ |
| Policy | **Default** |
| | 0 |
| | 1 |

➢ **Policy**

- Default(empty field) | 0~255

| CoS | 0 ∨ |
| DPL | Default ∨ |
| DSCP | Default ∨ |
| PCP | Default ∨ |
| DEI | Default ∨ |
| Policy | 255 |

## EXAMPLE CLI CONFIGURATION

✓ **QCE Configuration**

```
(config)# qos qce { [ update ] } <qce_id> [ { next <qce_id_next> } | last ] [ interface (<port_type>
[ <port_list> ] ) ) ] [ smac { <smac> | <smac_24> | any } ] [ dmac { <dmac> | unicast | multicast | broadcast |
any } ] [ tag { [ type { untagged | tagged | c-tagged | s-tagged | any } ] [ vid { <ot_vid> | any } ] [ pcp
{ <ot_pcp> | any } ] [ dei { <ot_dei> | any } ] }*1 ] [ inner-tag { [ type { untagged | tagged | c-tagged | s-
tagged | any } ] [ vid { <it_vid> | any } ] [ pcp { <it_pcp> | any } ] [ dei { <it_dei> | any } ] }*1 ] [ frame-type
{ any | { etype [ { <etype_type> | any } ] } | { llc [ dsap { <llc_dsap> | any } ] [ ssap { <llc_ssap> | any } ]
[ control { <llc_control> | any } ] } | { snap [ { <snap_data> | any } ] } | { ipv4 [ proto { <pr4> | tcp | udp |
any } ] [ sip { <sip4> | any } ] [ dip { <dip4> | any } ] [ dscp { <dscp4> | { be | af11 | af12 | af13 | af21 | af22
```

```
| af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any } ]
 fragment { yes | no | any } ] [ sport { <sp4> | any } ] [ dport { <dp4> | any } ] } | { ipv6 [ proto { <pr6> | tcp
| udp | any } ] [ sip { <sip6> | any } ] [ dip { <dip6> | any } ] [ dscp { <dscp6> | { be| af11 | af12 | af13 | af21
| af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any } ]
[ sport { <sp6> | any } ] [ dport { <dp6> | any } ] } } ] [ action { [ cos { <action_cos> | default } ] [ dpl
{ <action_dpl> | default } ] [ pcp-dei { <action_pcp> <action_dei> | default } ] [ dscp { <action_dscp_dscp> |
{ be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 |
cs6 | cs7 | ef | va } | default } ] [ policy { <action_policy> | default } ] }*1 ]
```

➢ **Port Members**

- Select Port

```
(config)# qos qce 1 interface *
(config)# qos qce 1 GigabitEthernet 1/1
(config)# qos qce 1 interface 2.5GigabitEthernet 1/1
```

✓ **Key Parameters**

➢ **DMAC**

- Any | Unicast | Multicast | Broadcast

```
(config)# qos qce 1 dmac any
(config)# qos qce 1 dmac unicast
(config)# qos qce 1 dmac multicast
(config)# qos qce 1 dmac broadcast
```

➢ **SMAC**

- Any | Specific

```
(config)# qos qce 1 smac any
(config)# qos qce 1 smac 00-21-6d-00-00-00
```

➢ **Tag**

- Any | Untagged | Tagged | C-Tagged | S-Tagged

```
(config)# qos qce 1 tag type any
(config)# qos qce 1 tag type untagged
(config)# qos qce 1 tag type tagged
(config)# qos qce 1 tag type c-tagged
(config)# qos qce 1 tag type s-tagged
```

➢ **VID**

- Any | Specific | Range

```
(config)# qos qce 1 tag vid any
(config)# qos qce 1 tag vid 1
(config)# qos qce 1 tag vid 1-2
```

➢ **PCP**

- Any | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0-1 | 2-3 | 4-5 | 6-7 | 0-3 | 4-7

```
(config)# qos qce 1 tag pcp any
(config)# qos qce 1 tag pcp 0
(config)# qos qce 1 tag pcp 0-1
(config)# qos qce 1 tag pcp 0-3
```

➢ **DEI**

- Any | 0 | 1

```
(config)# qos qce 1 tag dei any
(config)# qos qce 1 tag dei 0
(config)# qos qce 1 tag dei 1
```

> ### Frame Type
>    • Any | EtherType | LLC | SNAP | IPv4 | IPv6

```
(config)# qos qce 1 frame-type any
(config)# qos qce 1 frame-type etype
(config)# qos qce 1 frame-type ipv4
(config)# qos qce 1 frame-type ipv6
(config)# qos qce 1 frame-type llc
(config)# qos qce 1 frame-type snap
```

✓ **EtherType Parameters**

> ### Ether Type
>    • Any | Specific(<0x600-0x7ff,0x801-0x86dc,0x86de-0xffff>)

```
(config)# qos qce 1 frame-type etype any
(config)# qos qce 1 frame-type etype 0x600
```

✓ **LLC Parameters**

> ### DSAP Address
>    • Any | Specific(<0-0xff>)

```
(config)# qos qce 1 frame-type llc dsap any
(config)# qos qce 1 frame-type llc dsap 0xff
```

> ### SSAP Address
>    • Any | Specific(<0-0xff>)

```
(config)# qos qce 1 frame-type llc ssap any
(config)# qos qce 1 frame-type llc ssap 0xff
```

> ### Control
>    • Any | Specific(<0-0xff>)

```
(config)# qos qce 1 frame-type llc control any
(config)# qos qce 1 frame-type llc control 0xff
```

✓ **SNAP Parameters**

> ### PID
>    • Any | Specific(<0-0xffff>)

```
(config)# qos qce 1 frame-type snap any
(config)# qos qce 1 frame-type snap 0xffff
```

✓ **IPv4 Parameters**

> ### Protocol
>    • Any | UDP | TCP | Other(<0-255>)

```
(config)# qos qce 1 frame-type ipv4 proto any
(config)# qos qce 1 frame-type ipv4 proto udp
(config)# qos qce 1 frame-type ipv4 proto tcp
(config)# qos qce 1 frame-type ipv4 proto 255
```

> ### SIP
>    • Any | Specific(<ipv4_subnet>)

```
(config)# qos qce 1 frame-type ipv4 sip any
(config)# qos qce 1 frame-type ipv4 sip 192.168.10.100/255.255.255.0
```

> ### IP Fragment

- Any | Yes | No

```
(config)# qos qce 1 frame-type ipv4 fragment any
(config)# qos qce 1 frame-type ipv4 fragment yes
(config)# qos qce 1 frame-type ipv4 fragment no
```

➢ *DSCP*

- Any | Specific(0-63, BE, CS1-CS7, EF or AF11-AF43) | Range(0-63)

```
(config)# qos qce 1 frame-type ipv4 dscp any
(config)# qos qce 1 frame-type ipv4 dscp 0
(config)# qos qce 1 frame-type ipv4 dscp be
(config)# qos qce 1 frame-type ipv4 dscp 62-63
```

✓ **IPv6 Parameters**

➢ *Protocol*(additional configuration options.)

- Any | UDP | TCP | Other(<0-255>)

```
(config)# qos qce 1 frame-type ipv6 proto any
(config)# qos qce 1 frame-type ipv6 proto udp
(config)# qos qce 1 frame-type ipv6 proto tcp
(config)# qos qce 1 frame-type ipv6 proto 255
```

➢ *SIP (32LSB)*

- Any | Specific(<ipv4_subnet>)

```
(config)# qos qce 1 frame-type ipv6 sip any
(config)# qos qce 1 frame-type ipv6 sip 192.168.10.100/255.255.255.0
```

➢ *DSCP*

- Any | Specific(0-63, BE, CS1-CS7, EF or AF11-AF43) | Range(0-63)

```
(config)# qos qce 1 frame-type ipv6 dscp any
(config)# qos qce 1 frame-type ipv6 dscp 0
(config)# qos qce 1 frame-type ipv6 dscp be
(config)# qos qce 1 frame-type ipv6 dscp 62-63
```

✓ **UDP Parameters**

➢ *Sport*

- Any | Specific(0~65535) | Range(0-65535)

```
(config)# qos qce 1 frame-type ipv4 proto udp sport any
(config)# qos qce 1 frame-type ipv4 proto udp sport 100
(config)# qos qce 1 frame-type ipv4 proto udp sport 0-65535
(config)# qos qce 1 frame-type ipv6 proto udp sport any
(config)# qos qce 1 frame-type ipv6 proto udp sport 100
(config)# qos qce 1 frame-type ipv6 proto udp sport 0-65535
```

➢ *Dport*

- Any | Specific(0~65535) | Range(0-65535)

```
(config)# qos qce 1 frame-type ipv4 proto udp dport any
(config)# qos qce 1 frame-type ipv4 proto udp dport 100
(config)# qos qce 1 frame-type ipv4 proto udp dport 0-65535
(config)# qos qce 1 frame-type ipv6 proto udp dport any
(config)# qos qce 1 frame-type ipv6 proto udp dport 100
(config)# qos qce 1 frame-type ipv6 proto udp dport 0-65535
```

✓ **TCP Parameters**

➢ *Sport*

- Any | Specific | Range

SOLTECH
INFONET INC.

```
(config)# qos qce 1 frame-type ipv4 proto tcp sport any
(config)# qos qce 1 frame-type ipv4 proto tcp sport 100
(config)# qos qce 1 frame-type ipv4 proto tcp sport 0-65535
(config)# qos qce 1 frame-type ipv6 proto tcp sport any
(config)# qos qce 1 frame-type ipv6 proto tcp sport 100
(config)# qos qce 1 frame-type ipv6 proto tcp sport 0-65535
```

➢ **Dport**

 • Any | Specific | Range

```
(config)# qos qce 1 frame-type ipv4 proto tcp dport any
(config)# qos qce 1 frame-type ipv4 proto tcp dport 100
(config)# qos qce 1 frame-type ipv4 proto tcp dport 0-65535
(config)# qos qce 1 frame-type ipv6 proto tcp dport any
(config)# qos qce 1 frame-type ipv6 proto tcp dport 100
(config)# qos qce 1 frame-type ipv6 proto tcp dport 0-65535
```

✓ **Action Parameters**

➢ **CoS**

 • Default | 0~7

```
(config)# qos qce 1 action cos default
(config)# qos qce 1 action cos 7
```

➢ **DPL**

 • Default | 0~1

```
(config)# qos qce 1 action dpl default
(config)# qos qce 1 action dpl 0
```

➢ **DSCP**

 • Default | 0~63

```
(config)# qos qce 1 action dscp default
(config)# qos qce 1 action dscp 0
(config)# qos qce 1 action dscp be
(config)# qos qce 1 action dscp 63
```

➢ **PCP**

 • Default | 0~7

➢ **DEI**

 • Default | 0~1

```
(config)# qos qce 1 action pcp-dei default
(config)# qos qce 1 action pcp-dei 7 1
(config)# qos qce 1 action pcp-dei 0 0
```

➢ **Policy**

 • Default | 0~255

```
(config)# qos qce 1 action policy default
(config)# qos qce 1 action policy 255
(config)# qos qce 1 action policy 0
```

## 6.20.1.12. Storm Policing

WEB MENU Configuration>QoS>Storm Policing

Global storm policers for the switch are configured on this page.

**Global Storm Policer Configuration**

| Frame Type | Enable | Rate | Unit |
|---|---|---|---|
| Unknown Unicast | ☑ | 1 | kfps |
| Multicast | ☑ | 1 | kfps |
| Broadcast | ☑ | 1 | kfps |

**Port Storm Policer Configuration**

| Port | Unicast Frames | | | Broadcast Frames | | | Unknown Frames | | |
|---|---|---|---|---|---|---|---|---|---|
| | Enable | Rate | Unit | Enable | Rate | Unit | Enable | Rate | Unit |
| * | ☐ | 1 | <> | ☑ | 1 | <> | ☐ | 1 | <> |
| 1 | ☐ | 1 | kfps | ☑ | 1 | kfps | ☐ | 1 | kfps |
| 2 | ☐ | 1 | kfps | ☑ | 1 | kfps | ☐ | 1 | kfps |
| 3 | ☐ | 1 | kfps | ☑ | 1 | kfps | ☐ | 1 | kfps |
| 4 | ☐ | 1 | kfps | ☑ | 1 | kfps | ☐ | 1 | kfps |
| 5 | ☐ | 1 | kfps | ☑ | 1 | kfps | ☐ | 1 | kfps |
| 6 | ☐ | 1 | kfps | ☑ | 1 | kfps | ☐ | 1 | kfps |
| 7 | ☐ | 1 | kfps | ☑ | 1 | kfps | ☐ | 1 | kfps |
| 8 | ☐ | 1 | kfps | ☑ | 1 | kfps | ☐ | 1 | kfps |
| 9 | ☐ | 1 | kfps | ☑ | 1 | kfps | ☐ | 1 | kfps |
| 10 | ☐ | 1 | kfps | ☑ | 1 | kfps | ☐ | 1 | kfps |
| 11 | ☐ | 1 | kfps | ☑ | 1 | kfps | ☐ | 1 | kfps |
| 12 | ☐ | 1 | kfps | ☑ | 1 | kfps | ☐ | 1 | kfps |

### Global Storm Policer Configuration

There is a unicast storm policer, multicast storm policer, and a broadcast storm policer.

These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table. The displayed settings are:

| Object | Description |
|---|---|
| **Frame Type** | The frame type for which the configuration below applies. |
| **Enable** | Enable or disable the global storm policer for the given frame type. |
| **Rate** | Controls the rate for the global storm policer. This value is restricted to 10-13128147 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the global storm policer. |
| **Unit** | Controls the unit of measure for the global storm policer rate as fps, kfps, kbps or Mbps. |

### Port Storm Policer Configuration

Port storm policers for all switch ports are configured on this page.

There is a storm policer for unicast frames, broadcast frames and unknown (flooded) frames.

The displayed settings are

| Object | Description |
|---|---|
| **Port** | The port number for which the configuration below applies. |
| **Enable** | Enable or disable the storm policer for this switch port. |

SOLTECH
INFONET INC.

| | |
|---|---|
| **Rate** | Controls the rate for the port storm policer. This value is restricted to 10-13128147 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the port storm policer. |
| **Unit** | Controls the unit of measure for the port storm policer rate as fps, kfps, kbps or Mbps. |

**Buttons**

`Apply` : Click to apply changes.

`Apply&Save` : Click to apply and save changes.

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

## EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>QoS>Storm Policing

✓ **Global Storm Policer Configuration**

  ➢ *Frame Type*

    • Unknown Unicast | Multicast | Broadcast

  ➢ *Enable*

    • Enable | Disable

  ➢ *Rate*

    • 10-13128147(fps|kbps)

    • 1-13128(kfps|Mbps)

  ➢ *Unit*

    • fps | kfps | kbps | Mbps

| Frame Type | Enable | Rate | Unit |
|---|---|---|---|
| Unknown Unicast | ☑ | 13128147 | kbps ▾ |
| Multicast | ☑ | 13128 | Mbps ▾ |
| Broadcast | ☑ | 10 | fps ▾ |

✓ **Port Storm Policer Configuration**

  ➢ *Port*

  ➢ *Enable*

    • Enable | Disable

  ➢ *Rate*

    • 10-13128147(fps|kbps)

    • 1-13128(kfps|Mbps)

> ➢ *Unit*

  - • fps | kfps | kbps | Mbps

| Port | Unicast Frames | | | Broadcast Frames | | | Unknown Frames | | |
|------|------|------|------|------|------|------|------|------|------|
| | Enable | Rate | Unit | Enable | Rate | Unit | Enable | Rate | Unit |
| * | ☑ | 10 | <> ⌄ | ☑ | 1 | <> ⌄ | ☐ | 1 | <> ⌄ |
| 1 | ☑ | 10 | fps ⌄ | ☑ | 1 | kfps ⌄ | ☐ | 1 | kfps ⌄ |
| 2 | ☑ | 13128147 | kbps ⌄ | ☑ | 1 | kfps ⌄ | ☐ | 1 | kfps ⌄ |
| 3 | ☑ | 1 | kfps ⌄ | ☑ | 1 | kfps ⌄ | ☐ | 1 | kfps ⌄ |
| 4 | ☑ | 13128 | Mbps ⌄ | ☑ | 1 | kfps ⌄ | ☐ | 1 | kfps ⌄ |
| 5 | ☐ | 1 | kfps ⌄ | ☑ | 1 | kfps ⌄ | ☐ | 1 | kfps ⌄ |
| 6 | ☐ | 1 | kfps ⌄ | ☑ | 1 | kfps ⌄ | ☐ | 1 | kfps ⌄ |
| 7 | ☐ | 1 | kfps ⌄ | ☑ | 1 | kfps ⌄ | ☐ | 1 | kfps ⌄ |
| 8 | ☐ | 1 | kfps ⌄ | ☑ | 1 | kfps ⌄ | ☐ | 1 | kfps ⌄ |
| 9 | ☐ | 1 | kfps ⌄ | ☑ | 1 | kfps ⌄ | ☐ | 1 | kfps ⌄ |
| 10 | ☐ | 1 | kfps ⌄ | ☑ | 1 | kfps ⌄ | ☐ | 1 | kfps ⌄ |
| 11 | ☐ | 1 | kfps ⌄ | ☑ | 1 | kfps ⌄ | ☐ | 1 | kfps ⌄ |
| 12 | ☐ | 1 | kfps ⌄ | ☑ | 1 | kfps ⌄ | ☐ | 1 | kfps ⌄ |

## EXAMPLE CLI CONFIGURATION

✓ **Global Storm Policer Configuration**

> ➢ *Frame Type*

  - • Unknown Unicast | Multicast | Broadcast

> ➢ *Enable*

  - • Enable | Disable

> ➢ *Rate*

  - • 10-13128147(fps|kbps)

  - • 1-13128(kfps|Mbps)

> ➢ *Unit*

  - • fps | kfps | kbps | Mbps

```
(config)# qos storm { unicast | multicast | broadcast } <rate> [ fps | kfps | kbps | mbps ]
(config)# qos storm unicast 13128 kfps
(config)# qos storm multicast 13128147 fps
(config)# qos storm broadcast 1 mbps
```

✓ **Port Storm Policer Configuration**

> ➢ *Port*

> ➢ *Enable*

  - • Enable | Disable

> ➢ *Rate*

- • 10-13128147(fps|kbps)

- • 1-13128(kfps|Mbps)

➢ **Unit**

- • fps | kfps | kbps | Mbps

```
(config)# interface interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1
```
```
(config-if)# qos storm { unicast | multicast | broadcast } <rate> [ fps | kfps | kbps | mbps ]
(config-if)# qos storm unicast 13128 kfps
(config-if)# qos storm multicast 13128147 fps
(config-if)# qos storm broadcast 1 mbps
(config-if)# qos storm multicast 10 kbps
```

## 6.20.1.13. WRED

WEB MENU Configuration>QoS>WRED

This page allows you to configure the Random Early Detection (RED) settings.

**Weighted Random Early Detection Configuration**

| Group | Queue | DPL | Enable | Min | Max | Max Unit |
|---|---|---|---|---|---|---|
| 1 | 0 | 1 | ☐ | 0 | 50 | Drop Probability ▾ |
| 1 | 0 | 2 | ☐ | 0 | 50 | Drop Probability ▾ |
| 1 | 0 | 3 | ☐ | 0 | 50 | Drop Probability ▾ |
| 1 | 1 | 1 | ☐ | 0 | 50 | Drop Probability ▾ |
| 1 | 1 | 2 | ☐ | 0 | 50 | Drop Probability ▾ |
| 1 | 1 | 3 | ☐ | 0 | 50 | Drop Probability ▾ |
| 1 | 2 | 1 | ☐ | 0 | 50 | Drop Probability ▾ |
| 1 | 2 | 2 | ☐ | 0 | 50 | Drop Probability ▾ |
| 1 | 2 | 3 | ☐ | 0 | 50 | Drop Probability ▾ |
| 1 | 3 | 1 | ☐ | 0 | 50 | Drop Probability ▾ |
| 3 | 5 | 1 | ☐ | 0 | 50 | Drop Probability ▾ |
| 3 | 5 | 2 | ☐ | 0 | 50 | Drop Probability ▾ |
| 3 | 5 | 3 | ☐ | 0 | 50 | Drop Probability ▾ |
| 3 | 6 | 1 | ☐ | 0 | 50 | Drop Probability ▾ |
| 3 | 6 | 2 | ☐ | 0 | 50 | Drop Probability ▾ |
| 3 | 6 | 3 | ☐ | 0 | 50 | Drop Probability ▾ |
| 3 | 7 | 1 | ☐ | 0 | 50 | Drop Probability ▾ |
| 3 | 7 | 2 | ☐ | 0 | 50 | Drop Probability ▾ |
| 3 | 7 | 3 | ☐ | 0 | 50 | Drop Probability ▾ |

**Weighted Random Early Detection Configuration**

Through different RED configuration for the queues (QoS classes) it is possible to obtain Weighted Random Early Detection (WRED) operation between queues.

The settings are global for all ports in the switch.

| Object | Description |
|---|---|
| **Group** | The WRED group number for which the configuration below applies. |
| **Queue** | The queue number (QoS class) for which the configuration below applies. |
| **DPL** | The Drop Precedence Level for which the configuration below applies |
| **Enable** | Controls whether RED is enabled for this entry. |
| **Min** | Controls the lower RED fill level threshold. If the queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100%. |
| **Max** | Controls the upper RED drop probability or fill level threshold for frames marked with Drop Precedence Level > 0 (yellow frames). This value is restricted to 1-100%. |
| **Max Unit** | Selects the unit for Max.<br><br>Drop Probability  Max controls the drop probability just below 100% fill level.<br><br>Fill Level         Max controls the fill level where drop probability reaches 100%. |

SOLTECH
INFONET INC.

### RED Drop Probability Function

The following illustration shows the drop probability versus fill level function with associated parameters.
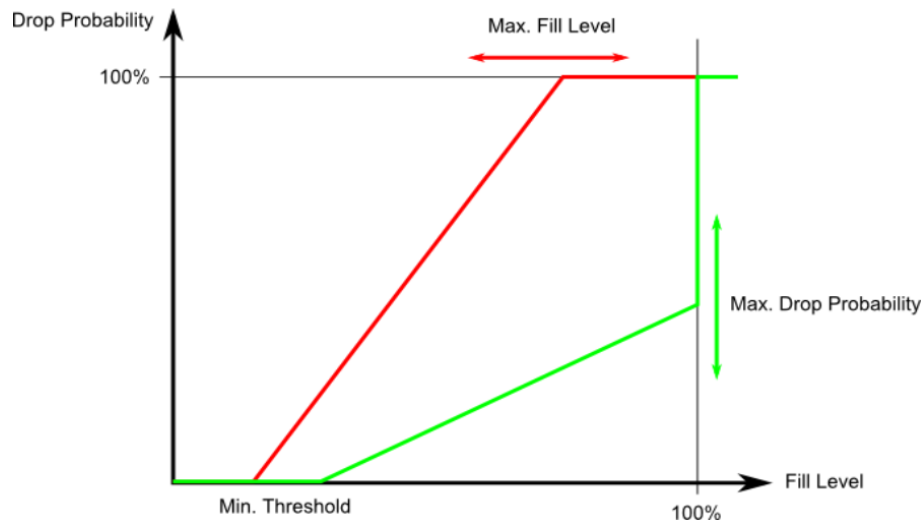


Min is the fill level where the queue randomly start dropping frames marked with Drop Precedence Level > 0 (yellow frames).

If Max Unit is 'Drop Probability' (the green line), Max controls the drop probability when the fill level is just below 100%.

If Max Unit is 'Fill Level' (the red line), Max controls the fill level where drop probability reaches 100%. This configuration makes it possible to reserve a portion of the queue exclusively for frames marked with Drop Precedence Level 0 (green frames). The reserved portion is calculated as (100 - Max) %.

Frames marked with Drop Precedence Level 0 (green frames) are never dropped.

The drop probability for frames increases linearly from zero (at Min average queue filling level) to Max Drop Probability or Fill Level.

### Buttons

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

# 6.21. Mirroring

## 6.21.1. Mirroring Configuration

WEB MENU Configuration>Mirroring

Mirroring is a feature for switched port analyzer. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

Remote Mirroring is an extend function of Mirroring. It can extend the destination port in other switch. So the administrator can analyze the network traffic on the other switches.

If you want to get the tagged mirrored traffic, you have to set VLAN egress tagging as "Tag All" on the reflector port.
On the other hand, if you want to get untagged mirrored traffic, you have to set VLAN egress tagging as "Untag ALL" on the reflector port.

**Mirroring & Remote Mirroring Configuration**

| Mode | Disabled |
|------|----------|
| Type | Mirror |
| VLAN ID | 200 |
| Reflector Port | Port 1 |

**Source VLAN(s) Configuration**

| Source VLANs | |
|--------------|--|

**Port Configuration**

| Port | Source | Intermediate | Destination |
|------|--------|--------------|-------------|
| 1 | Disabled | ☐ | ☐ |
| 2 | Disabled | ☐ | ☐ |
| 3 | Disabled | ☐ | ☐ |
| 4 | Disabled | ☐ | ☐ |
| 5 | Disabled | ☐ | ☐ |
| 6 | Disabled | ☐ | ☐ |
| 7 | Disabled | ☐ | ☐ |
| 8 | Disabled | ☐ | ☐ |
| CPU | Disabled | ☐ | ☐ |

### Mirroring & Remote Mirroring Configuration

| Object | Description |
|--------|-------------|
| **Mode** | To Enabled/Disabled the mirror or Remote Mirroring function. |
| **Type** | Select switch type. |
| | Mirror — The switch is running on mirror mode. The source port(s) and destination port are located on this switch. |
| | Source — The switch is a source node for monitor flow. The source port(s), reflector port and intermediate port(s) are located |

| | | |
|---|---|---|
| | | on this switch. |
| | Intermediate | The switch is a forwarding node for monitor flow and the switch is an option node. The object is to forward traffic from source switch to destination switch. The intermediate ports are located on this switch. |
| | Destination | The switch is an end node for monitor flow. The destination port(s) and intermediate port(s) are located on this switch. |
| **VLAN ID** | The VLAN ID points out where the monitor packet will copy to. The default VLAN ID is 200. | |
| **Reflector Port** | The reflector port is a method to redirect the traffic to Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until the Remote Mirroring is disabled. In the stacking mode, you need to select switch ID to select the correct device. If you shut down a port, it cannot be a candidate for reflector port. If you shut down the port which is a reflector port, the remote mirror function cannot work. Note1: The reflector port needs to select only on Source switch type. Note2: The reflector port needs to disable MAC Table learning and STP. Note3: The reflector port only supports on pure copper ports. | |

### Source VLAN(s) Configuration

The switch can supports VLAN-based Mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs on this field.

Note1: The Mirroring session shall have either ports or VLANs as sources, but not both.

### Port Configuration

The following table is used for port role selecting.

| Object | Description |
|---|---|
| **Port** | The logical port for the settings contained in the same row. |
| **Source** | Select mirror mode. <br> Disabled — Neither frames transmitted nor frames received are mirrored. <br> Both — Frames received and frames transmitted are mirrored on the Intermediate/Destination port. <br> Rx only — Frames received on this port are mirrored on the Intermediate/Destination port. Frames transmitted are not mirrored. <br> Tx only — Frames transmitted on this port are mirrored on the Intermediate/Destination port. Frames received are not mirrored. |
| **Intermediate** | Select intermediate port. This checkbox is designed for Remote Mirroring. The intermediate port is a switched port to connect to other switch. Note: The intermediate port needs to disable MAC Table learning. |
| **Destination** | Select destination port. This checkbox is designed for mirror or Remote Mirroring. The destination port is a switched port that you receive a copy of traffic from the source port. Note1: On mirror mode, the device only supports one destination port. Note2: The destination port needs to disable MAC Table learning. |

**Configuration Guideline for All Features**

When the switch is running on Remote Mirroring mode, the administrator also needs to check whether or not other features are enabled or disabled.

For example, the administrator is not disabled the MSTP on reflector port. All monitor traffic will be blocked on reflector port.

Refer to the help page for all recommended settings.

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

---

## EXAMPLE WEB CONFIGURATION

---

WEB MENU Configuration>Mirroring

✓ **Mirroring & Remote Mirroring Configuration**

➢ *Mode*

• Disabled | Enabled

**Mirroring & Remote Mirroring Configuration**

| Mode | Enabled |
|---|---|
| Type | Disabled |
| VLAN ID | Enabled |
| Reflector Port | Port 1 |

➢ *Type*

• Mirror | Source | Intermediate | Destination

**Mirroring & Remote Mirroring Configuration**

| Mode | Enabled |
|---|---|
| Type | Mirror |
| VLAN ID | Mirror |
| Reflector Port | Source(RMirror) |
| | Intermediate(RMirror) |
| | Destination(RMirror) |

**Source VLAN(s) Configuration**

➢ *VLAN ID*

Only "Source | Intermediate | Destination(RMirror) type can configuration

• 1~4095

**Mirroring & Remote Mirroring Configuration**

| Mode | Enabled |
|---|---|
| Type | Source(RMirror) |
| VLAN ID | 4095 |
| Reflector Port | Port 1 |

➢ **Reflector Port**

Only "Source(RMirror)" type can configuration

**Mirroring & Remote Mirroring Configuration**

| Mode | Enabled |
|---|---|
| Type | Source(RMirror) |
| VLAN ID | 4095 |
| Reflector Port | Port 1 |

Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
Port 7
Port 8

Source VLAN(s)

Source VLANs

Port Configurat

Port    Sourc

✓ **Source VLAN(s) Configuration**

➢ **Source VLANs**

Only "Mirror, Source(RMirror)" type can configuration

• 1~4095(This can affect the Source in Port Configuration.)

**Source VLAN(s) Configuration**

| Source VLANs | 1-10,100 |
|---|---|

✓ **Port Configuration**

➢ **Source**

• Disabled | Both | Rx Only | Tx Only

**Port Configuration**

| Port | Source | Intermediate | Destination |
|---|---|---|---|
| 1 | Both | ☐ | ☐ |
| 2 | Disabled | ☐ | ☐ |
| 3 | Both | ☐ | ☐ |
| 4 | Rx only / Tx only | ☐ | ☐ |
| 5 | Disabled | ☐ | ☐ |
| 6 | Disabled | ☐ | ☐ |
| 7 | Disabled | ☐ | ☐ |
| 8 | Disabled | ☐ | ☐ |
| 9 | Disabled | ☐ | ☐ |
| 10 | Disabled | ☐ | ☐ |
| 11 | Disabled | ☐ | ☐ |
| 12 | Disabled | ☐ | ☐ |
| CPU | Disabled | ☐ | ☐ |

➢ **Intermediate**

**SOLTECH**
INFONET INC.

Only "Source | Intermediate | Destination(RMirror) type can configuration

**Port Configuration**

| Port | Source | Intermediate | Destination |
|---|---|---|---|
| 1 | Disabled ∨ | ☐ | ☐ |
| 2 | Disabled ∨ | ☐ | ☐ |
| 3 | Disabled ∨ | ☑ | ☐ |
| 4 | Disabled ∨ | ☑ | ☐ |
| 5 | Disabled ∨ | ☐ | ☐ |
| 6 | Disabled ∨ | ☐ | ☐ |
| 7 | Disabled ∨ | ☐ | ☐ |
| 8 | Disabled ∨ | ☐ | ☐ |
| 9 | Disabled ∨ | ☐ | ☐ |
| 10 | Disabled ∨ | ☐ | ☐ |
| 11 | Disabled ∨ | ☐ | ☐ |
| 12 | Disabled ∨ | ☐ | ☐ |
| CPU | Disabled ∨ | ☐ | ☐ |

➢ ***Destination***

Only "Mirror, Destination(RMirror) type can configuration

**Port Configuration**

| Port | Source | Intermediate | Destination |
|---|---|---|---|
| 1 | Disabled ∨ | ☐ | ☐ |
| 2 | Disabled ∨ | ☐ | ☑ |
| 3 | Disabled ∨ | ☐ | ☐ |
| 4 | Disabled ∨ | ☐ | ☐ |
| 5 | Disabled ∨ | ☐ | ☐ |
| 6 | Disabled ∨ | ☐ | ☐ |
| 7 | Disabled ∨ | ☐ | ☐ |
| 8 | Disabled ∨ | ☐ | ☐ |
| 9 | Disabled ∨ | ☐ | ☐ |
| 10 | Disabled ∨ | ☐ | ☐ |
| 11 | Disabled ∨ | ☐ | ☐ |
| 12 | Disabled ∨ | ☐ | ☐ |
| CPU | Disabled ∨ | ☐ | ☐ |

## EXAMPLE CLI CONFIGURATION

✓ **Mirroring & Remote Mirroring Configuration**

➢ ***Mode***

• Disabled | Enabled

```
(config)# no monitor session 1

(config)# monitor session 1
```

➢ ***Type***

• Mirror(Default) | Source | Intermediate | Destination

> ***VLAN ID***

Only "Source | Intermediate | Destination(RMirror) type can configuration

- 1~4095

> ***Reflector Port***

Only "Source(RMirror)" type can configuration

```
(config)# monitor session <session_number> [ destination { interface ( <port_type>
[ <di_list> ] ) | remote vlan <drvid> reflector-port <port_type> <rportid> } | source
{ interface ( <port_type> [ <si_list> ] ) [ both | rx | tx ] | remote vlan <srvid> | vlan
<source_vlan_list> | cpu [ both | rx | tx ] } | intermediate { interface ( <port_type>
[ <ii_list> ] ) | remote vlan <irvid> } ]

(config)# monitor session 1 destination remote vlan 4095 reflector-port
GigabitEthernet 1/1
(config)# monitor session 1 intermediate remote vlan 4095
(config)# monitor session 1 source remote vlan 4095
```

✓ **Source VLAN(s) Configuration**

> ***Source VLANs***

Only "Mirror, Source(RMirror)" type can configuration

- 1~4095(This can affect the Source in Port Configuration.)

```
(config)# monitor session <session_number> [ destination { interface ( <port_type>
[ <di_list> ] ) | remote vlan <drvid> reflector-port <port_type> <rportid> } | source
{ interface ( <port_type> [ <si_list> ] ) [ both | rx | tx ] | remote vlan <srvid> | vlan
<source_vlan_list> | cpu [ both | rx | tx ] } | intermediate { interface ( <port_type>
[ <ii_list> ] ) | remote vlan <irvid> } ]

(config)# monitor session 1 source vlan 1-10
(config)# monitor session 1 source vlan 100
```

✓ **Port Configuration**

> ***Source***

- Disabled | Both | Rx Only | Tx Only

```
(config)# monitor session <session_number> [ destination { interface ( <port_type>
[ <di_list> ] ) | remote vlan <drvid> reflector-port <port_type> <rportid> } | source
{ interface ( <port_type> [ <si_list> ] ) [ both | rx | tx ] | remote vlan <srvid> | vlan
<source_vlan_list> | cpu [ both | rx | tx ] } | intermediate { interface ( <port_type>
[ <ii_list> ] ) | remote vlan <irvid> } ]

(config)# monitor session 1 source interface GigabitEthernet 1/1 both
(config)# monitor session 1 source interface GigabitEthernet 1/1 rx
(config)# monitor session 1 source interface GigabitEthernet 1/1 tx
(config)# monitor session 1 source cpu both
```

> ***Intermediate***

Only "Source | Intermediate | Destination(RMirror) type can configuration

```
(config)# monitor session <session_number> [ destination { interface ( <port_type>
[ <di_list> ] ) | remote vlan <drvid> reflector-port <port_type> <rportid> } | source
{ interface ( <port_type> [ <si_list> ] ) [ both | rx | tx ] | remote vlan <srvid> | vlan
<source_vlan_list> | cpu [ both | rx | tx ] } | intermediate { interface ( <port_type>
[ <ii_list> ] ) | remote vlan <irvid> } ]

(config)# monitor session 1 intermediate interface GigabitEthernet 1/3-4
```

➢ **Destination**

Only "Mirror, Destination(RMirror) type can configuration

```
(config)# monitor session <session_number> [ destination { interface ( <port_type>
[ <di_list> ] ) | remote vlan <drvid> reflector-port <port_type> <rportid> } | source
{ interface ( <port_type> [ <si_list> ] ) [ both | rx | tx ] | remote vlan <srvid> | vlan
<source_vlan_list> | cpu [ both | rx | tx ] } | intermediate { interface ( <port_type>
[ <ii_list> ] ) | remote vlan <irvid> } ]

(config)# monitor session 1 destination interface GigabitEthernet 1/2
```

# EXAMPLE

✓ **Example**

➢ **Mirror**

Source - CPU, Mirror Port - Gigabit Ethernet 1/1

**Mirroring & Remote Mirroring Configuration**

| Mode | Enabled |
|---|---|
| Type | Mirror |
| VLAN ID | 200 |
| Reflector Port | Port 1 |

**Source VLAN(s) Configuration**

| Source VLANs | |
|---|---|

**Port Configuration**

| Port | Source | Intermediate | Destination |
|---|---|---|---|
| 1 | Disabled | ☐ | ☑ |
| 2 | Disabled | ☐ | ☐ |
| 3 | Disabled | ☐ | ☐ |
| 4 | Disabled | ☐ | ☐ |
| 5 | Disabled | ☐ | ☐ |
| 6 | Disabled | ☐ | ☐ |
| 7 | Disabled | ☐ | ☐ |
| 8 | Disabled | ☐ | ☐ |
| 9 | Disabled | ☐ | ☐ |
| 10 | Disabled | ☐ | ☐ |
| 11 | Disabled | ☐ | ☐ |
| 12 | Disabled | ☐ | ☐ |
| CPU | Both | ☐ | ☐ |

```
(config)# monitor session 1
(config)# monitor session 1 source cpu both
(config)# monitor session 1 destination interface GigabitEthernet 1/1
```

## 6.22. GVRP

## 6.22.1. Global config

WEB MENU Configuration>GVRP>Global config

This page allows you to configure the global GVRP configuration settings that are commonly applied to all GVRP enabled ports.

**GVRP Configuration**

☐ Enable GVRP

| Parameter | Value |
|---|---|
| Join-time: | 20 |
| Leave-time: | 60 |
| LeaveAll-time: | 1000 |
| Max VLANs: | 20 |

### GVRP Configuration

| Object | Description | |
|---|---|---|
| **Enable GVRP globally** | The GVRP feature is globally enabled by setting the check mark in the checkbox named Enable GVRP and pressing the Save button. | |
| **GVRP protocol timers** | Join-time | Join-time is a value in the range of 1-20cs, i.e. in units of one hundredth of a second. The default value is 20cs. |
| | Leave-time | Leave-time is a value in the range of 60-300cs, i.e. in units of one hundredth of a second. The default is 60cs. |
| | LeaveAll-time | LeaveAll-time is a value in the range of 1000-5000cs, i.e. in units of one hundredth of a second. The default is 1000cs. |
| **Max number of VLANs** | When GVRP is enabled, a maximum number of VLANs supported by GVRP is specified. By default this number is 20. This number can only be changed when GVRP is turned off. | |

**Buttons**

`Apply` : Click to apply changes.

`Apply&Save` : Click to apply and save changes.

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

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

---

### EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>GVRP>Global config

✓ **GVRP Configuration**

➢ **Enable GVRP**
- Enable | Disable

➢ **GVRP protocol timers**
- Join-time(1~20csec)

- Leave-time(60~300csec)

SOLTECH
INFONET INC.

- *Leave All-time(1000~5000csec)*

➢ ***Max number of VLANs***

- 1~4095(The change requires GVRP to be disabled.)

☑ Enable GVRP

| Parameter | Value |
|---|---|
| Join-time: | 20 |
| Leave-time: | 60 |
| LeaveAll-time: | 1000 |
| Max VLANs: | 20 |

---

## EXAMPLE CLI CONFIGURATION

---

✓ **GVRP Configuration**

➢ ***Enable GVRP***

- Enable | Disable

```
(config)# gvrp
(config)# no gvrp
```

➢ ***GVRP protocol timers***

- Join-time(1~20csec)

- Leave-time(60~300csec)

- *Leave All-time(1000~5000csec)*

```
(config)# gvrp time { [ join-time <jointime> ] [ leave-time <leavetime> ] [ leave-all-time
<leavealltime> ] }
(config)# gvrp time join-time 20 leave-time 60 leave-all-time 1000
```

➢ ***Max number of VLANs***

- 1~4095(The change requires GVRP to be disabled.)

```
(config)# gvrp max-vlans <maxvlans>
(config)# gvrp max-vlans 20
```

SOLTECH
INFONET INC.

## 6.22.2. Port config

WEB MENU Configuration>GVRP>Port config

This page allows you to configure the global GVRP configuration settings that are commonly applied to all GVRP enabled ports.

**GVRP Port Configuration**

| Port | Mode |
|------|------|
| * | <> |
| 1 | Disabled |
| 2 | Disabled |
| 3 | Disabled |
| 4 | Disabled |
| 5 | Disabled |
| 6 | Disabled |
| 7 | Disabled |
| 8 | Disabled |
| 9 | Disabled |
| 10 | Disabled |
| 11 | Disabled |
| 12 | Disabled |

### GVRP Port Configuration

| Object | Description |
|--------|-------------|
| **Port** | The logical port that is to be configured. |
| **Mode** | Mode can be either 'Disabled' or 'GVRP enabled'. These values turn the GVRP feature off or on respectively for the port in question. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

### EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>GVRP>Port config

✓ **GVRP Port Configuration**

➢ *Mode*

• Disabled | GVRP Enabled

## EXAMPLE CLI CONFIGURATION

✓ **GVRP Port Configuration**

➢ *Mode*

• Disabled | GVRP Enabled

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# gvrp
```

## 6.23. DDMI

## 6.23.1. DDMI Configuration

WEB MENU Configuration>DDMI

Configure DDMI on this page.

**DDMI Configuration**

| Mode | Enabled ∨ |
| Update Interval Time(s) | 1 ∨ |
| Check Polling Count | OFF ∨ |

### DDMI Configuration

| Object | Description |
|---|---|
| **Mode** | Indicates the DDMI mode operation. Possible modes are:<br>Enabled   Enable DDMI mode operation.<br>Disabled   Disable DDMI mode operation. |
| **Update Interval Time(s)** | The update time interval of DDMI.<br>The unit is seconds, and can be set from a minimum of 1 to a maximum of 12. |
| **Check Polling Count** | Polling Count for DDMI Interval.<br>This is the count that automatically updates DDMI information.<br>Polling Count I OFF and has a minimum of 1 and a maximum of 10.<br>The default value is OFF |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

### EXAMPLE WEB CONFIGURATION

WEB MENU Configuration>DDMI

✓ **DDMI Configuration**

➢ *Mode*

• Enabled | Disabled

| Mode | Enabled ∨ |
| Update Interval Time(s) | Disabled |
| Check Polling Count | Enabled |

➢ *Update Interval Time(s)*

• 1~12

SOLTECH
INFONET INC.

| Mode | Enabled ▾ |
|---|---|
| Update Interval Time(s) | 1 ▾ |
| Check Polling Count | 1 |
| | 2 |
| | 3 |
| | 4 |
| | 5 |
| | 6 |
| | 7 |
| | 8 |
| | 9 |
| | 10 |
| | 11 |
| | 12 |

➢ **Check Polling Count**

• OFF | 1~10

| Mode | Enabled ▾ |
|---|---|
| Update Interval Time(s) | 1 ▾ |
| Check Polling Count | OFF ▾ |
| | OFF |
| | 1 |
| | 2 |
| | 3 |
| | 4 |
| | 5 |
| | 6 |
| | 7 |
| | 8 |
| | 9 |
| | 10 |

## EXAMPLE CLI CONFIGURATION

✓ **DDMI Configuration**

➢ **Mode**

• Enabled | Disabled

```
(config)# ddmi
(config)# no ddmi
```

➢ **Update Interval Time(s)**

• 1~12

```
(config)# ddmi update-interval <interval_time>
(config)# ddmi update-interval 1
```

➢ **Check Polling Count**

• 0~10 (0:OFF)

```
(config)# ddmi check-polling-count <polling_cnt>
(config)# ddmi check-polling-count 0
(config)# ddmi check-polling-count 10
```

## 6.23.2. DDMI Monitor

## 6.23.2.1. Overview

WEB MENU Configuration>DDMI>Overview

Display DDMI overview information on this page.

**DDMI Overview**

| Port | Vendor | Part Number | Serial Number | Revision | Data Code | Transceiver |
|------|--------|-------------|---------------|----------|-----------|-------------|
| 5 | - | - | - | - | - | - |
| 6 | - | - | - | - | - | - |
| 7 | - | - | - | - | - | - |
| 8 | - | - | - | - | - | - |

### DDMI Configuration

| Object | Description |
|--------|-------------|
| **Port** | DDMI port. (Navigating to the Detail page by clicking on the port number.) |
| **Vendor** | Indicates Vendor name SFP vendor name. |
| **Part Number** | Indicates Vendor PN Part number provided by SFP vendor. |
| **Serial Number** | Indicates Vendor SN Serial number provided by vendor. |
| **Revision** | Indicates Vendor rev Revision level for part number provided by vendor. |
| **Data Code** | Indicates Date code Vendor's manufacturing date code. |
| **Transeiver** | Indicates Transceiver compatibility. |

### EXAMPLE WEB MONITOR

WEB MENU Configuration>DDMI>Overview

✓ **DDMI Overview**

**DDMI Overview**

| Port | Vendor | Part Number | Serial Number | Revision | Data Code | Transceiver |
|------|--------|-------------|---------------|----------|-----------|-------------|
| 5 | Soltech | GP-3148-L2CD | S2005136619 | 1.0 \| ♣ | 2020-05-19 | 2G5 |
| 6 | OEM | SFP-LX | S1231240320176 | A0 \| ♣ | 2014-03-09 | 1000BASE_LX |
| 7 | soltech | SFP-10G-LR | S1804239531 | A \| ♣ | 2018-05-07 | 10G |
| 8 | OEM | SFP-SM | S0131241120202 | A0 \| ♣ | 2014-11-12 | 100BASE_LX |

### EXAMPLE CLI MONITOR

✓ **DDMI Overview**

```
# show interface ( <port_type> [ <plist> ] ) transceiver
# show interface 10GigabitEthernet 1/1-4 transceiver

10GigabitEthernet 1/1
```

```
------------------------------
Transceiver Information
==========================================================
Vendor          : Soltech
Part Number       : GP-3148-L2CD
Serial Number     : S2005136619
Revision        : 1.0
Data Code        : 2020-05-19
Transceiver      : 2G5

DDMI Information

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.
==========================================================
          current   High Alarm   High Warn   Low Warn    Low Alarm
                    Threshold    Threshold   Threshold   Threshold
--------------  --------  ----------  ----------  ----------  --------

Temperature(C)
Voltage(V)
Tx Bias(mA)
Tx Power(mW)
Rx Power(mW)



10GigabitEthernet 1/2
------------------------------
Tranceiver Information
==========================================================
Vendor          : OEM
Part Number       : SFP-LX
Serial Number      : S1231240320176
Revision        : A0
Data Code        : 2014-03-09
Transceiver       : 1000BASE_LX

DDMI Information

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.
==========================================================
% SFP module doesn't support DDMI



10GigabitEthernet 1/3
------------------------------
Tranceiver Information
==========================================================
Vendor          : soltech
Part Number       : SFP-10G-LR
Serial Number      : S1804239531
Revision        : A
Data Code        : 2018-05-07
Transceiver       : 10G

DDMI Information

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
```

```
Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.
============================================================

            current   High Alarm   High Warn   Low Warn     Low Alarm
                      Threshold    Threshold   Threshold    Threshold
-------------  --------  ----------   ----------  ----------   --------
Temperature(C)
Voltage(V)
Tx Bias(mA)
Tx Power(mW)
Rx Power(mW)


10GigabitEthernet 1/4
------------------------------
Tranceiver Information
============================================================
Vendor           : OEM
Part Number       : SFP-SM
Serial Number      : S0131241120202
Revision         : A0
Data Code        : 2014-11-12
Transceiver       : 100BASE_LX

DDMI Information

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.

Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.

============================================================

% SFP module doesn't support DDMI
```

## 6.23.2.2. Detailed

WEB MENU Configuration>DDMI>Detailed

**Transceiver Information**

| Vendor | - |
|---|---|
| Part Number | - |
| Serial Number | - |
| Revision | - |
| Data Code | - |
| Transeiver | - |

**DDMI Information**

| Type | Current | High Alarm Threshold | High Warn Threshold | Low Warn Threshold | Low Alarm Threshold |
|---|---|---|---|---|---|
| Temperature(C) | - | - | - | - | - |
| Voltage(V) | - | - | - | - | - |
| Tx Bias(mA) | - | - | - | - | - |
| Tx Power(mV) | - | - | - | - | - |
| Rx Power(mV) | - | - | - | - | - |

### Transceiver Information

Display DDMI detailed information on this page.

| Object | Description |
|---|---|
| **Vendor** | Indicates Vendor name SFP vendor name. |
| **Part Number** | Indicates Vendor PN Part number provided by SFP vendor. |
| **Serial Number** | Indicates Vendor SN Serial number provided by vendor. |
| **Revision** | Indicates Vendor rev Revision level for part number provided by vendor. |
| **Data Code** | Indicates Date code Vendor's manufacturing date code. |
| **Transeiver** | Indicates Transceiver compatibility. |

### DDMI Information

Display DDMI infomration on this page.

| Object | Description |
|---|---|
| **Current** | The current value of temperature, voltage, TX bias, TX power, and RX power. |
| **High Alarm Threshold** | The high alarm threshold value of temperature, voltage, TX bias, TX power, and RX power. |
| **High Warn Threshold** | The high warn threshold value of temperature, voltage, TX bias, TX power, and RX power. |
| **Low Warn Threshold** | The low warn threshold value of temperature, voltage, TX bias, TX power, and RX power. |
| **Low Alarm Threshold** | The low alarm threshold value of temperature, voltage, TX bias, TX power, and RX power. |

### Buttons

Port 5 ▾
Port 5
Port 6
Port 7
Port 8
: Select port number. The detailed information page for the selected port will be displayed.

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

Refresh :Click to refresh the page immediately.

## EXAMPLE WEB MONITOR

WEB MENU Configuration>DDMI>Detailed

✓ **Transceiver Information**

✓ **DDMI Information**

**Transceiver Information**

| Vendor | Soltech |
|---|---|
| Part Number | GP-3148-L2CD |
| Serial Number | S2005136619 |
| Revision | 1.0 | 🔺 |
| Data Code | 2020-05-19 |
| Transeiver | 2G5 |

**DDMI Information**

| Type | Current | High Alarm Threshold | High Warn Threshold | Low Warn Threshold | Low Alarm Threshold |
|---|---|---|---|---|---|
| Temperature(C) | | | | | |
| Voltage(V) | | | | | |
| Tx Bias(mA) | | | | | |
| Tx Power(mV) | | | | | |
| Rx Power(mV) | | | | | |

## EXAMPLE CLI MONITOR

✓ **Transceiver Information**

✓ **DDMI Information**

```
# show interface ( <port_type> [ <plist> ] ) transceiver
# show interface 10GigabitEthernet 1/1-4 transceiver

10GigabitEthernet 1/1
------------------------------
Tranceiver Information
============================================================
Vendor          : Soltech
Part Number        : GP-3148-L2CD
Serial Number      : S2005136619
Revision        : 1.0
Data Code          : 2020-05-19
Transceiver        : 2G5

DDMI Information

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.
============================================================
          current   High Alarm   High Warn   Low Warn    Low Alarm
                    Threshold    Threshold   Threshold   Threshold
-------------- --------  ---------- ---------- ---------- --------

Temperature(C)
Voltage(V)
Tx Bias(mA)
Tx Power(mW)
```

SOLTECH
INFONET INC.

```
Rx Power(mW)


10GigabitEthernet 1/2
-----------------------------
Tranceiver Information
===============================================================
Vendor          : OEM
Part Number       : SFP-LX
Serial Number     : S1231240320176
Revision       : A0
Data Code        : 2014-03-09
Transceiver       : 1000BASE_LX

DDMI Information

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.
===============================================================

% SFP module doesn't support DDMI


10GigabitEthernet 1/3
-----------------------------
Tranceiver Information
===============================================================
Vendor          : soltech
Part Number       : SFP-10G-LR
Serial Number     : S1804239531
Revision        : A
Data Code        : 2018-05-07
Transceiver       : 10G

DDMI Information

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.
===============================================================

           current   High Alarm   High Warn    Low Warn     Low Alarm
                      Threshold    Threshold    Threshold     Threshold
-------------- -------- ---------- ----------  ----------   --------
Temperature(C)
Voltage(V)
Tx Bias(mA)
Tx Power(mW)
Rx Power(mW)


10GigabitEthernet 1/4
-----------------------------
Tranceiver Information
===============================================================
Vendor          : OEM
Part Number       : SFP-SM
Serial Number      : S0131241120202
Revision        : A0
Data Code         : 2014-11-12
```

```
Transceiver        : 100BASE_LX

DDMI Information

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.

Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.

==============================================================

% SFP module doesn't support DDMI
```

## 6.24. Digital I/O

### 6.24.1. Digital I/O Configuration

WEB MENU Configuration>Digital I/O

This page is used to configure the Digital Input/Output group

**Digital Input/Output Control Configuration**

**Digital Output Configuration**

| Digital Output | Status | Mode | Polarity |
|---|---|---|---|
| Digital Output1 | ⚫ | Disable ⌄ | Active High ⌄ |

**System Power Configuration**

| Power | Status | Mode | Output | | |
|---|---|---|---|---|---|
| | | | Syslog | SNMP Trap | Digital Output1 |
| Power1 | ⚫ | Disable ⌄ | ☐ | ☐ | ☐ |
| Power2 | 🟢 | Disable ⌄ | ☐ | ☐ | ☐ |

**Digital Input Configuration**

| Digital Input | Status | Mode | Polarity | Output | | |
|---|---|---|---|---|---|---|
| | | | | Syslog | SNMP Trap | Digital Output1 |
| Digital Input1 | ⚫ | Disable ⌄ | Active Low ⌄ | ☐ | ☐ | ☐ |

**System Temperature Configuration**

| Temperature | Status | | Limit ['C] | | Mode | Output | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Syslog | SNMP Trap | Digital Output1 |
| Temperature1 | Temperature | 0.000['C] | High | 85 ⌄ | Disable ⌄ | ☐ | ☐ | ☐ |
| | Status | ⚫ | Low | 30 ⌄ | | | | |

**System Port Configuration**

| Port | Status | Mode | Output |
|---|---|---|---|
| | | | Digital Output1 |
| Port1 | ⚫ | Disable ⌄ | ☐ |
| Port2 | 🟢 | Disable ⌄ | ☐ |
| Port3 | ⚫ | Disable ⌄ | ☐ |
| Port4 | ⚫ | Disable ⌄ | ☐ |
| Port5 | ⚫ | Disable ⌄ | ☐ |
| Port6 | ⚫ | Disable ⌄ | ☐ |
| Port7 | ⚫ | Disable ⌄ | ☐ |
| Port8 | ⚫ | Disable ⌄ | ☐ |
| Port9 | ⚫ | Disable ⌄ | ☐ |
| Port10 | ⚫ | Disable ⌄ | ☐ |
| Port11 | ⚫ | Disable ⌄ | ☐ |
| Port12 | ⚫ | Disable ⌄ | ☐ |

**Digital Input/Output Control Configuration**

**Digital Output Configuration**

| Object | Description |
|---|---|
| **Digital Output** | It is the name of Digital Output.(Digital Output is OUT1 and Digital Output is OUT 2) |
| **Mode** | Set the mode of the Digital Output. |
| **Polarity** | Set the polarity of the Digital Output. |

SOLTECH
INFONET INC.

| Status | It shows the status of the Digital Output. |
|---|---|

## System Power Configuration

| Object | Description |
|---|---|
| Power | It is the name of the power. |
| Status | It shows the status of the Power. (Normal : green, Fail: dark gray) |
| Mode | Set the mode of the Power. |
| Output | Set whether to send out the status of the Power to Output.<br>Please make sure syslog and SNMP are set before you set up 'Output'. |

## Digital Input Configuration

| Object | Description |
|---|---|
| Digital Input | It is the name of Digital Input. |
| Mode | Set the mode of Digital Input. |
| Polarity | Set the polarity of the Digital Input. |
| Status | It shows the status of the Digital Input. |
| Output | Set whether to send out the status of the Digital input to Output.<br>Please make sure syslog and SNMP are set before you set up 'Output'. |

## System Temperature Configuration

| Object | Description |
|---|---|
| Temperature | It is the name of the Temperature. |
| Mode | Set the mode of the Temperature. |
| Status | It shows the status of the Temperature.<br>Temperature: It shows the present temperature of the equipment.<br>Status: (Normal: green, Fail: dark gray) |
| Temperature Limit | High: Set the high temperature limit among the High-setup temperature range.<br>Low: Set the low temperature limit among the Low-setup temperature range. |
| Output | Set whether to send out the status of the Temperature to Output.<br>Please make sure syslog and SNMP are set before you set up 'Output'. |

## System Port Configuration

| Object | Description |
|---|---|
| Port | It is the name of the Port. |
| Status | It shows the status of the Port. (Normal: green, Fail: dark gray) |
| Mode | Set the mode of the Port. |
| Output | Set whether to send out the status of the Port to Output. |

**Buttons**

Apply : Click to apply changes.

Apply&Save : Click to apply and save changes.

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

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

Refresh : Click to refresh the page immediately.

Syslog : Click to move to the Syslog configuration page.

SNMP Trap : Click to move to the SNMP Trap configuration page.

SOLTECH
INFONET INC.

# 7. Switch Diagnostics Guide

## 7.1. Diagnostics

## 7.1.1. Ping

WEB MENU Diagnostics>Ping

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

**ICMP Ping**

| IP Address | 0.0.0.0 |
| Ping Length | 56 |
| Ping Count | 5 |
| Ping Interval | 1 |

Start

### ICMP Ping

After you press Start, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested data space(the ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

## 7.1.2. Link OAM

## 7.1.2.1. MIB Retrieval

WEB MENU Diagnostics>Link OAM>MIB Retrieval

This page allows you to retrieve the local or remote OAM MIB variable data on a particular port.

**Link OAM MIB Retrieval**

Local ⦿
Peer ○
Port [                    ]

[ Start ]

### Link OAM MIB Retrieval

Select the appropriate radio button and enter the port number of the switch to retrieve the content of interest. Click on 'Start' to retrieve the content. Click on 'New Retrieval' to retrieve another content of interest.

# 7.1.3. Ping6

WEB MENU Diagnostics>Ping6

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

**ICMPv6 Ping**

| | |
|---|---|
| IP Address | 0:0:0:0:0:0:0:0 |
| Ping Length | 56 |
| Ping Count | 5 |
| Ping Interval | 1 |
| Egress Interface | |

Start

## ICMPv6 Ping

After you press 'Start', ICMPv6 packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

| Object | Description |
|---|---|
| IP Address | The destination IP Address. |
| Ping Length | The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes. |
| Ping Count | The count of the ICMP packet. Values range from 1 time to 60 times. |
| Ping Interval | The interval of the ICMP packet. Values range from 0 second to 30 seconds. |
| Egress Interface (Only for IPv6) | The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. When the egress interface is not given, PING6 finds the best match interface for destination. Do not specify egress interface for loopback address. Do specify egress interface for link-local or multicast address. |

**Buttons**

Start : Click to start transmitting ICMP packets.

New Ping : Click to re-start diagnostics with PING.

## 7.1.4. VeriPHY

WEB MENU Diagnostics>VeriPHY

This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.

**VeriPHY Cable Diagnostics**

Port [ All ∨ ]

[ Start ]

| Cable Status | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Port | Pair A | Length A | Pair B | Length B | Pair C | Length C | Pair D | Length D |
| 1 | -- | -- | -- | -- | -- | -- | -- | -- |
| 2 | -- | -- | -- | -- | -- | -- | -- | -- |
| 3 | -- | -- | -- | -- | -- | -- | -- | -- |
| 4 | -- | -- | -- | -- | -- | -- | -- | -- |

### VeriPHY Cable Diagnostics

Press 'Start' to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

| Object | Description | |
|---|---|---|
| **Port** | The port where you are requesting VeriPHY Cable Diagnostics. | |
| **Cable Status** | **Port** | Port number. |
| | **Pair** | The status of the cable pair. |
| | | OK - Correctly terminated pair |
| | | Open - Open pair |
| | | Short - Shorted pair |
| | | Short A - Cross-pair short to pair A |
| | | Short B - Cross-pair short to pair B |
| | | Short C - Cross-pair short to pair C |
| | | Short D - Cross-pair short to pair D |
| | | Cross A - Abnormal cross-pair coupling with pair A |
| | | Cross B - Abnormal cross-pair coupling with pair B |
| | | Cross C - Abnormal cross-pair coupling with pair C |
| | | Cross D - Abnormal cross-pair coupling with pair D |
| | **Length** | The length (in meters) of the cable pair. The resolution is 3 meters |

SOLTECH
INFONET INC.

# 8. Switch Maintenance Guide

## 8.1. Maintenance

## 8.1.1. Restart Device

WEB MENU Maintenance>Restart Device

You can restart the switch on this page. After restart, the switch will boot normally.

When restarting, the startup-config will be loaded. (If not saved, the configuration will be lost upon restart.)

**Restart Device**

| Are you sure you want to perform a Restart (Delayed)? |
|---|

Delayed Restart(0~300(S)) [ 0 ]

| Object | Description |
|---|---|
| **Delayed Restart** | Restart will begin after the specified waiting time. (You can set a delay from 0 to 300 seconds. 0: Restart immediately) |

**Buttons**

[ Restart ] : Click to restart device.

[ No ] : Click to return to the Port State page without restarting.

[ Save Configuration ] : This copies running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot.

---

### EXAMPLE WEB

---

WEB MENU Maintenance>Restart Device

1. Restart immediately

**Restart Device**

| Are you sure you want to perform a Restart (Delayed)? |
|---|

Delayed Restart(0~300(S)) [ 0 ]

[ Restart ]  [ No ]  [ Save Configuration ]

Click the "Restart" button(The Delayed Restart value is 0)

SOLTECH
INFONET INC.

2.  Restart with delay

**Restart Device**

<div style="color:white; background:red; text-align:center; font-weight:bold; padding:2em;">
Are you sure you want to perform a Restart (Delayed)?
</div>

| Delayed Restart(0~300(S) | 30 |

| Restart | No | Save Configuration |

Click the "Restart" button(The Delayed Restart value is 1~300)

**System restart in progress**

<div style="color:white; background:red; text-align:center; font-weight:bold; padding:2em;">
The system is now restarting.
</div>

|IIIIIIIIIIIIIII|

*Waiting, please stand by...*

After waiting for a few minutes, the Login page will be displayed, and the restart will be completed.

# EXAMPLE CLI

✓  **Restart Device(Load Startup-Config and Restart)**

```
# reload { { { cold [ <delay_sec> | now ]
# reload cold
# reload cold now
# reload cold 300

% Cold reload in progress, please stand by.
#
###############################################
###: Start SOLTECH_boot_v1_1            ###
###############################################
###: CPU   Test..........................PASS!
###: TCAM  Test..........................PASS!
###: DRAM  Test..........................PASS!
###: Flash Test..........................PASS!
###: Loading flash: IMG.bin ..................
###: Verifying firmware image integrity.......
###: IMG-KEY:7F80C36F18AA01DA22999FE8EDE2B57B
          AAD7096D8EC4D49840B026A19C9766E4
###: CAL-KEY:7F80C36F18AA01DA22999FE8EDE2B57B
          AAD7096D8EC4D49840B026A19C9766E4
###: SHA256 hash verified: SUCCESS !!!
###: Start Decompress Image ..................
###: Please wait system up ...................


###: Dev MAC addr: [00:21:6D:00:00:00]
###: Dev-Name: Product Name

###: Board Serial: Serial Number
###: Board Name: Model Name
###: Port Info: Port:12[UTP:8(PoE:8),SFP:4]


###: Press ENTER to get started
```

SOLTECH
INFONET INC.

## 8.1.2. Factory Defaults

WEB MENU Maintenance>Factory Defaults

You can reset the configuration of the switch on this page. Only the IP configuration is retained.

The new configuration is available immediately, which means that no restart is necessary.

**Factory Defaults (Keeping IP-address)**

> Are you sure you want to reset the configuration(including All Users Info.) to
> Factory Defaults?
> % Keeping IP-address!

**Buttons**

FactoryDefaults & Save : Click to reset the configuration to Factory Defaults. (IP configuration is retained)

FactoryDefaults : Click to reset the configuration to Factory Defaults. (Not Save config to Flash!!)

☐ Keeping IP-address : Checking the box resets to factory settings while keeping the IP address.

### EXAMPLE WEB

WEB MENU Maintenance>Factory Defaults

**Factory Defaults (Keeping IP-address)**

> Are you sure you want to reset the configuration(including All Users Info.) to
> Factory Defaults?
> % Keeping IP-address!

✓ **Factory Defaults**

➢ *Factory Defaults & Save*

When you run Factory Defaults on the web, all settings except the IP configuration will be reset. When you click the button, the currently saved startup-config will also be reset (IP remains as the current IP).

➢ *Factory Defaults*

When you run Factory Defaults on the web, all settings except the IP configuration will be reset. When you click the button, the currently saved startup-config will be retained (Startup-config will be loaded upon restart).

➢ *Keeping IP-address*

When executing Factory Defaults on the web, you can configure whether to include the IP settings. If you uncheck the option and proceed with the reset, a complete factory reset will occur, and the IP will be reset to the default of 192.168.10.100.

SOLTECH
INFONET INC.

## EXAMPLE CLI

✓ **Factory Defaults**

➢ **Defaults**
Executing "Defaults" in the CLI will reset the device, including IP configurations, to their default settings. (Startup-config initialization)

```
# reload defaults

% Reloading defaults (Update startup-config). Please stand by.
Config Factory-Default applied! (Update startup-confg, By CLI)

###: Press ENTER to get started
```

➢ **Defaults keep-ip**
Executing "Defaults" in the CLI will reset the device to its default settings, excluding the IP configurations. (The IP settings in the Startup-config will be overwritten.)

```
# reload defaults keep-ip

% Reloading defaults, attempting to keep VLAN 1 IP address (Update startup-config).
Please stand by.
Config Factory-Default applied! (Update startup-confg, Keeping IP-addr, By CLI)

###: Press ENTER to get started
```

➢ **Defaults no-save**
Executing "Defaults" in the CLI will reset the device to its default settings, including the IP configurations.
(The Startup-config will remain unchanged.
Do not enter the security model initial setup password into flash.)
Upon restart after the configuration, the previously saved Startup-config will be loaded as it was.

```
# reload defaults-no-save

% Reloading defaults . Please stand by.
Config Factory-Default applied! (By CLI)
###: Press ENTER to get started

#: Please input a new admin password:**********
#: Please input the new password AGAIN:**********
#: Save admin password to flash now ? (yes/no):no

#
```

➢ **Defaults no-save keep-ip**

Executing "Defaults" in the CLI will reset the device to its default settings, excluding the IP configurations.
(The Startup-config will remain unchanged.
Do not enter the security model initial setup password into flash.)
Upon restart after the configuration, the previously saved Startup-config will be loaded as it was.

```
# reload defaults-no-save keep-ip

% Reloading defaults, attempting to keep VLAN 1 IP address . Please stand by.
```

```
Config Factory-Default applied! (By CLI)
###: Press ENTER to get started


#: Please input a new admin password:**********
#: Please input the new password AGAIN:**********
#: Save admin password to flash now ? (yes/no):no

#
```

## 8.1.3. Software

## 8.1.3.1. Upload

WEB MENU Maintenance>Software>Upload

This page facilitates an update of the firmware controlling the switch.

**Software Upload**

Choose File | No file chosen    Upload    ☐ Disable Automatic Restart After Updates

**Buttons**

Choose File : Click this button, you can find the software image to upload.

Upload : Click this button, upload the selected software image.

☐ Disable Automatic Restart After Updates : If this button is checked, the system will not automatically restart after updates.(Only the upload is performed, and a device reboot is required for the firmware to take effect.)

After the software image is uploaded, a page announces that the firmware update is initiated. After some minutes, the firmware is updated and the switch restarts.

> **Warning : Do not restart or power off the device at this time or the switch may fail to function afterwards.**

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

### EXAMPLE WEB

✓ **Software Upload**

**Software Upload**

Choose File | SONOS.dat    Upload

After clicking on " Choose File " choose the folder containing the image. Once selected, the file name will be displayed as shown above. The required file for the update is a (.dat) file extension.
Click the "Upload" button to proceed with the update.(default)

To prevent the device from automatically restarting, select "Disable Automatic Restart After Updates."
(Only the upload is performed, and a device reboot is required for the firmware to take effect.)

**SOLTECH**
INFONET INC.

# EXAMPLE CLI

The method for software upgrade using console (utilizing TFTP)
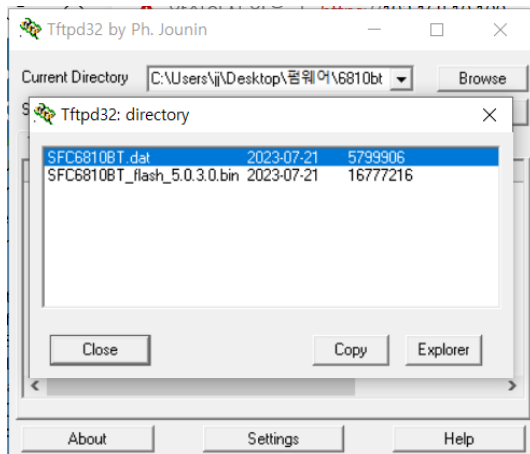
✓ **Software Upload**

1. Run the Tftpd32 program.
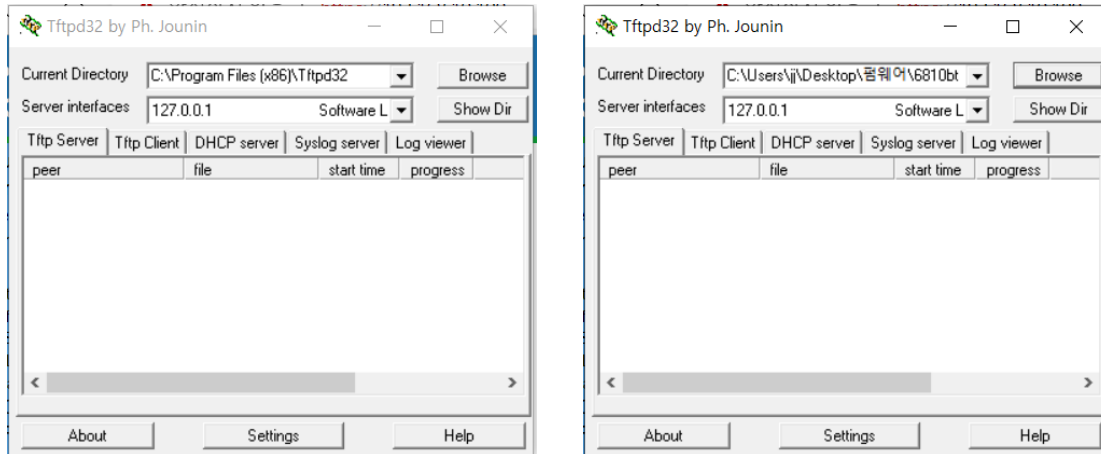


2. Click on "Browse" to locate the file you want to update.

3. Click on "Show Dir" to select the file, then click "Copy." and click "Close" to close the window.



4. Return to the console window and enter the following commands.

```
# firmware upgrade <url_file> [ forced ] [ not-reboot ]
# firmware upgrade tftp://192.168.10.130/SONOS.dat
# firmware upgrade tftp://192.168.10.130/SONOS.dat not-reboot

Downloaded "SONOS.dat", 5799906 bytes
TFTP Host:192.168.10.130 Upgrade Start (Download:5799906 Bytes)
###: Verifying firmware image integrity .....
IMG-KEY:3D5801C74658E0DA4C0AEDC28ABCF896D0C46331A1843DC7A930787659122861
CAL-KEY:3D5801C74658E0DA4C0AEDC28ABCF896D0C46331A1843DC7A930787659122861
SHA256 hash verified: SUCCESS
```

## 8.1.3.2. Image Select

WEB MENU Maintenance>Software>Image Select

This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

The web page displays two tables with information about the active and alternate firmware images.

**Software Image Selection**

| Active Image | |
|---|---|
| Image | managed |
| Version | SFC6810G 5.0.1.0 |
| Date | 2023-06-15T09:16:47+09:00 |

| Alternate Image | |
|---|---|
| Image | managed.bk |
| Version | OneImg_JAGUAR2 (standalone) build 5.0.1.0 by Soltech Corp. |
| Date | 2023-06-15T09:16:47+09:00 |

Note:

1. In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.
2. If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

### Software Image Selection

| Object | Description |
|---|---|
| **Image** | The file name of the firmware image, from when the image was last updated. |
| **Version** | The version of the firmware image. |
| **Date** | The date where the firmware was produced. |

**Buttons**

Activate Alternate Image : Click to use the alternate image. This button may be disabled depending on

system state.

Cancel : Cancel activating the backup image. Navigates away from this page.

SOLTECH
INFONET INC.

## EXAMPLE WEB

WEB MENU Maintenance>Software>Image Select

**Software Image Selection**

| Active Image | |
|---|---|
| Image | SFC6810BT.dat |
| Version | SFC6810BT 5.0.3.0 |
| Date | 2023-07-21T14:21:27+09:00 |

| Alternate Image | |
|---|---|
| Image | managed.bk |
| Version | OneImg_JAGUAR2 (standalone) build 5.0.1.0 by Soltech Corp. |
| Date | 2023-07-17T15:20:33+09:00 |

[ Activate Alternate Image ]  [ Cancel ]

Clicking on [ Activate Alternate Image ] will activate the alternative image. Use it if there are issues with the existing image.

**System restart in progress**

The system is now restarting.

Waiting, please stand by...

## EXAMPLE CLI

✓ **Software Image Selection**

```
# firmware swap

... Erase from 0x40fd0000-0x40fdffff: .
... Program from 0x8ffdfffc-0x8ffefffc to 0x40fd0000: .
... Program from 0x8ffe0006-0x8ffe0008 to 0x40fd000a: .
Alternate image activated, now rebooting.
#
```

SOLTECH
INFONET INC.

## 8.1.4. Configuration

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch.

1. running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.

2. startup-config: The startup configuration for the switch, read at boot time. If this file doesn't exist at boot time, the switch will start up in default configuration.

3. default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

   Up to 31 other files, typically used for configuration backups or alternative configurations.

## 8.1.4.1. CLI dir

This page provides instructions on how to view the currently stored config file on the Flash using the CLI.

In the case of the web interface, this functionality is already implemented on the required page.

### EXAMPLE CLI

✓ **Dir Command in CLI**

```
# dir
Directory of flash:
    r- 1970-01-01 00:00:00      316 default-config
    rw 1970-01-01 07:43:36     1083 startup-config
2 files, 1399 bytes total.
```

A total of 32 files can be stored on Flash. You can create them using the "Upload" option.

## 8.1.4.2. Save startup-config

WEB MENU Maintenance>Configuration>Save startup-config

**Save Running Configuration to startup-config**

Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

Save Configuration

This copies running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot.

**Buttons**

Save Configuration : Click "Save configuration" to copy the running-config to the startup-config.

### EXAMPLE WEB

WEB MENU Maintenance>Configuration>Save startup-config

**Save Running Configuration to startup-config**
**Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.**

Save Configuration

Click on Save Configuration to store the current configuration state. Even after restarting, the current configuration state will be retained.

### EXAMPLE CLI

✓ **Copy running-config to start-config**

```
# copy running-config startup-config

Building configuration...
% Saving 1083 bytes to flash:startup-config
#
```

## 8.1.4.3. Download

WEB MENU Maintenance>Configuration>Download

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

**Download Configuration**

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

| File Name |
| --- |
| ○ running-config |
| ○ default-config |
| ○ startup-config |

Download Configuration

Select the file and Click 'Download Configuration'.

Download of running-config may take a little while to complete, as the file must be prepared for download.

---

## EXAMPLE WEB

---

WEB Menu Maintenance>Configuration>Download

**Download Configuration**

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

| File Name |
| --- |
| ◉ running-config |
| ○ default-config |
| ○ startup-config |

Download Configuration

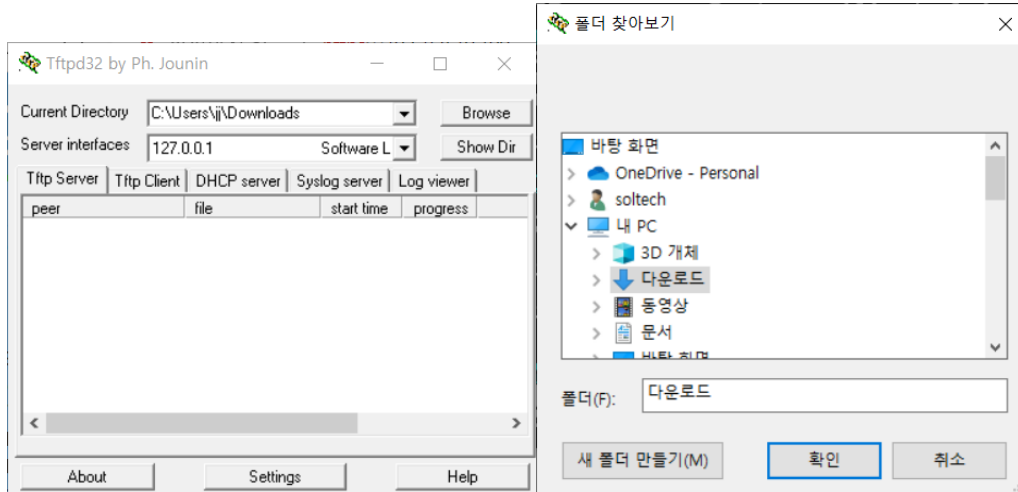Please select the file and click on 'Download Configuration'.

Downloads

running-config
Open file

The downloaded file will be displayed.

SOLTECH
INFONET INC.

## EXAMPLE CLI

✓ **Download Configuration**

Run Tftpd32 and choose the destination to save the file.



Click on "Browse" to set the location where the file will be saved.

Subsequently, enter the CLI command.

```
# copy flash-filename tftp://PC IPv4 Address/save-filename
# copy running-config tftp://192.168.10.130/running-config
Building configuration...
% Saving 1083 bytes to TFTP server 192.168.10.130: running-config
```

Please check if the file has been saved in the respective folder.

## 8.1.4.4. Upload

WEB MENU Maintenance>Configuration>Upload

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

**Upload Configuration**

**File To Upload**

Choose File | No file chosen

**Destination File**

| File Name | Parameters |
|---|---|
| ○ running-config | ● Replace    ○ Merge |
| ○ startup-config | |
| ○ Create new file | |

Upload Configuration

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

**File To Upload**

**Buttons**

Choose File  : Select the file to upload

**Destination File**

Select the destination file on the target

| Object | Description |
|---|---|
| **Running-config** | The file will be applied to the switch configuration. This can be done in two ways: |
| | **Replace mode**    The current configuration is fully replaced with the configuration in the uploaded file. |
| | **Merge mode**    The uploaded file is merged into running-config. |
| **Startup-config** | The file will be stored in the startup-config. It will be applied after the device is restarted. |
| **Create new file** | If the flash file system is full (i.e. contains default-config and 32 other files, usually including startup-config), it is not possible to create new files. Instead an existing file must be overwritten or another file must be deleted. |

**Buttons**

Upload Configuration  : To upload the configuration file to the destination file, click "Upload Configuration".

## EXAMPLE WEB

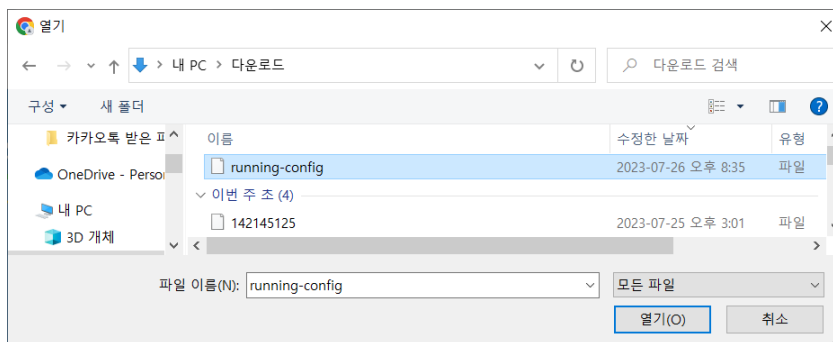WEB Menu Maintenance>Configuration>Upload

### Upload Configuration

#### File To Upload

| Choose File | No file chosen |

#### Destination File

| File Name | Parameters | |
|---|---|---|
| ○ running-config | ● Replace | ○ Merge |
| ○ startup-config | | |
| ○ Create new file | | |

| Upload Configuration |

1. Click on  Choose File  to load the saved configuration.

2. After selecting the desired file, click the "Open" button.

### Upload Configuration

#### File To Upload

| Choose File | running-config |

#### Destination File

| File Name | Parameters | |
|---|---|---|
| ● running-config | ● Replace | ○ Merge |
| ○ startup-config | | |
| ○ Create new file | | |

| Upload Configuration |

3. Select the desired Destination File and click on "Upload Configuration".

(For the Running-config, you can choose to Replace or Merge.)

**Activating New Configuration**

Please note: If the configuration changes IP settings, management connectivity may be lost.

**Status**

Activation completed successfully.

**Output**

```
10GigabitEthernet 1/1 does not have PoE support
10GigabitEthernet 1/2 does not have PoE support
10GigabitEthernet 1/3 does not have PoE support
10GigabitEthernet 1/4 does not have PoE support
```
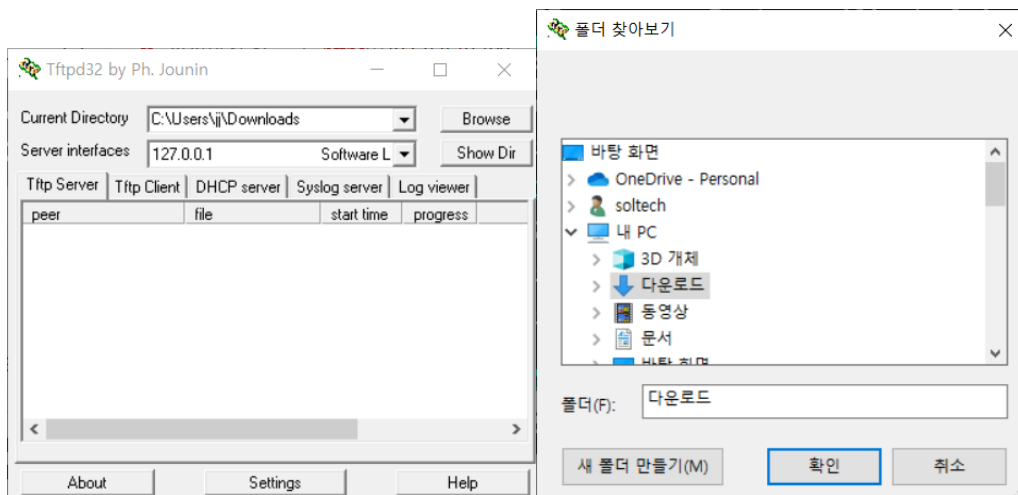
The screen will appear, and the configuration will be uploaded.
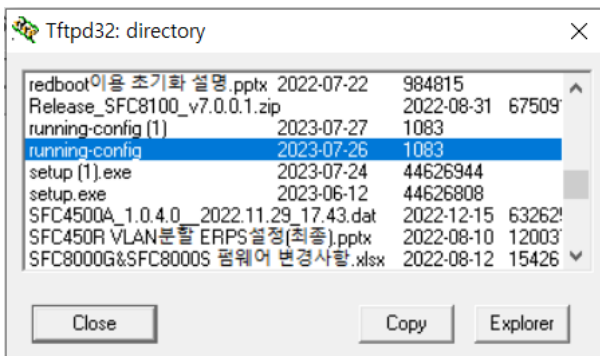
## EXAMPLE CLI

✓ **Upload Configuration**

Since direct uploading to the Running-Config is currently unavailable, let me introduce an alternative method.

1. Click on "Browse" in tftp32 to set the path.

2. Click on "show Dir" to select the file, then click on "Copy", and finally click "Close" to close the window.



3. Return to the console window and enter the following.

```
# copy tftp://<PC IPv4 Address>/<upload_filename> startup-config
# copy tftp://192.168.10.130/running-config startup-config
% Loading 123 from TFTP server 192.168.10.130
% Saving 1083 bytes to flash:startup-config

# reload cold
```

## 8.1.4.5. Activate

WEB MENU Maintenance>Configuration>Activate

**Activate Configuration**

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will <u>not</u> be saved to startup-config automatically.

| File Name |
|---|
| ○ default-config |
| ○ startup-config |

[ Activate Configuration ]

### Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will not be saved to startup-config automatically.

| Object | Description |
|---|---|
| **Default-config** | Except for Running-config, the Default-config will be activated. |
| **Startup-config** | Except for Running-config, the Startup-config will be activated. |

**Buttons**

[ Activate Configuration ] : Clicking on will replace the Running-config with the selected file.

---

## EXAMPLE WEB

---

WEB Menu Maintenance>Configuration>Activate

**Activate Configuration**

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will <u>not</u> be saved to startup-config automatically.

| File Name |
|---|
| ⦿ default-config |
| ○ startup-config |

[ Activate Configuration ]

Select the desired configuration file and click on "Activate Configuration".

The following screen will be displayed, and the running-config of the device will be replaced.

SOL TECH
INFONET INC.

**Activating New Configuration**

Please note: If the configuration changes IP settings, management connectivity may be lost.

**Status**

Activation completed successfully.

**Output**

```
(No output was generated.)
```

# EXAMPLE CLI

✓ **Activate Configuration**

```
# copy <flash file> running-config
# copy flash:default-config running-config
```

## 8.1.4.6. Delete

WEB MENU Maintenance>Configuration>Delete

It is possible to delete any of the writable files stored in flash, including startup-config. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration.

**Delete Configuration File**

Select configuration file to delete.

| File Name |
|-----------|
| ○ startup-config |

[ Delete Configuration File ]

**Buttons**

[ Delete Configuration File ] : Clicking on it will delete the selected file.

---

### EXAMPLE WEB

---

WEB MENU Maintenance>Configuration>Delete

✓    **Delete Configuration File**

**Delete Configuration File**

Select configuration file to delete.

| File Name |
|-----------|
| ◉ startup-config |

[ Delete Configuration File ]

Select the file you want to delete and click on "Delete Configuration File".

**192.168.10.100 says**

Are you sure you want to delete
startup-config?

[ OK ]    [ Cancel ]

**Delete Configuration File**

SOLTECH
INFONET INC.

startup-config successfully deleted.

(Delete is complete. The device will go to default settings upon restart.)

---

## EXAMPLE CLI

---

✓ **Delete Configuration File**

```
# delete <url_file>
# delete flash:startup-config
```

# 9. **Fault Recovery Method**

## **9.1. Emergency Recovery**

### **9.1.1. 3seconds Reset**

If the device is not functioning or the settings are incorrect, there is a hardware button for quick equipment reset.

It is labeled "Reset" on the front panel. To perform the reset, use a thin and long clip or pen to press and hold it for about 3 seconds until the Port LEDs blink.

This will reset the device to its Factory Defaults, while the IP address will remain unchanged.

Please be cautious and make sure to reconfigure or upload the previously saved configuration to continue using the device.

### **9.1.2. 10seconds Reset**

If the device is not functioning or the settings are incorrect, there is a hardware button for quick equipment reset.

It is labeled "Reset" on the front panel. To initiate the reset, use a thin and long clip or pen to press and hold it for about 10 seconds until the Port LEDs blink.

(Please note that the LED blinking pattern will be different from the 3-second reset.)

During this reset, all settings of the device, including the IP address, will be reverted to Factory Defaults.

(The default initial IP of the device is 192.168.10.100 Please reconfigure the device or upload the previously saved configuration to continue using it.)
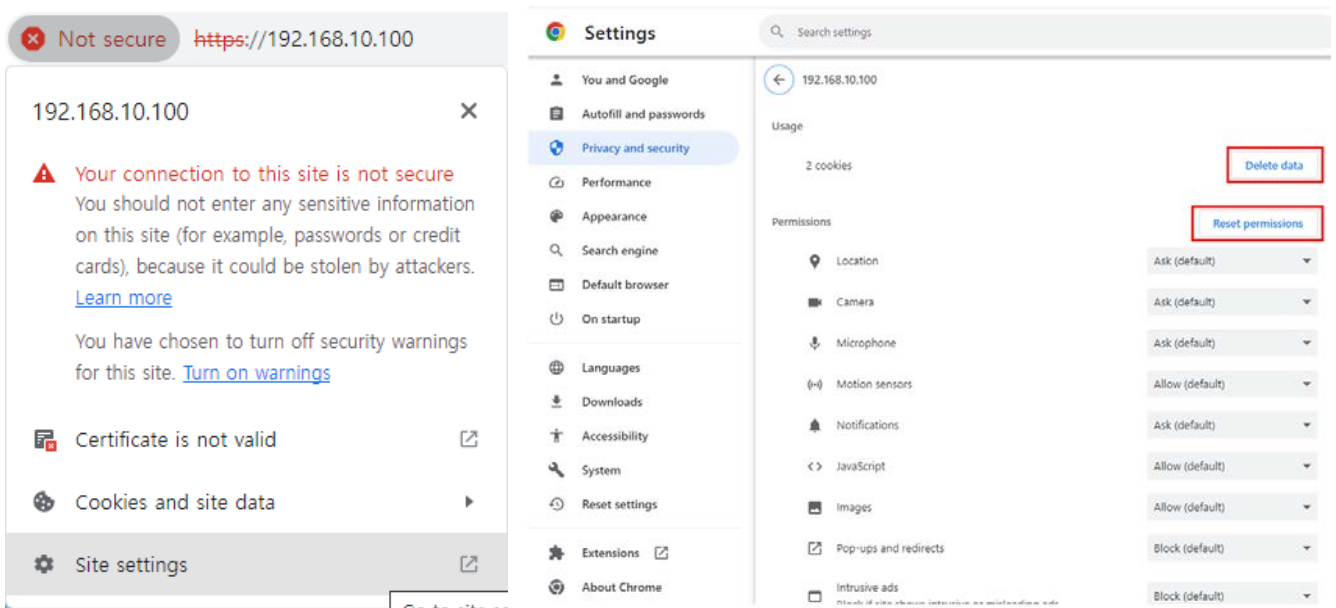
## 9.2. WEB Interface Connectivity Problem

If you are experiencing intermittent login failures or difficulty maintaining the login during WEB access, please follow the steps below.

Typically, closing and reopening all web browsers resolves the issue.
However, if the problem persists, please proceed with the following steps.

## 9.2.1. Google Chrome Browser



1.  Click on the 'Not secure' next to the equipment's URL.

2.  Click on the 'Site settings'

3.  Verify the equipment's IP, then 'Delete Data' / 'Reset Permissions.'

4.  After the setting changes, please restart the web browser.

## 9.2.2. Microsoft Edge Browser



1.  Click on the 'Not secure' next to the equipment's URL.

2.  Click on 'Cookies,' remove the cookies, then restart the web browser.



3.  Click on the permissions for this site.

4.  After verifying the equipment's IP, 'Reset Permissions.'