



ES2402-24P-2C-V2 /
ES2402-16P-2C-V2 /
ES2402-8P-2C-V2

Important information

Limitation of liability

To the maximum extent permitted by applicable law, in no event will UTCFS be liable for any lost profits or business opportunities, loss of use, business interruption, loss of data, or any other indirect, special, incidental, or consequential damages under any theory of liability, whether based in contract, tort, negligence, product liability, or otherwise. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages the preceding limitation may not apply to you. In any event the total liability of UTCFS shall not exceed the purchase price of the product. The foregoing limitation will apply to the maximum extent permitted by applicable law, regardless of whether UTCFS has been advised of the possibility of such damages and regardless of whether any remedy fails of its essential purpose.

Installation in accordance with this manual, applicable codes, and the instructions of the authority having jurisdiction is mandatory.

While every precaution has been taken during the preparation of this manual to ensure the accuracy of its contents, UTCFS assumes no responsibility for errors or omissions.

Advisory messages

Advisory messages alert you to conditions or practices that can cause unwanted results. The advisory messages used in this document are shown and described below.

WARNING: Warning messages advise you of hazards that could result in injury or loss of life. They tell you which actions to take or to avoid in order to prevent the injury or loss of life.

Caution: Caution messages advise you of possible equipment damage. They tell you which actions to take or to avoid in order to prevent damage.

Note: Note messages advise you of the possible loss of time or effort. They describe how to avoid the loss. Notes are also used to point out important information that you should read.

Chapter 1

Introduction

Thank you for purchasing an IFS ES2402-V2 series switch, featuring 10/100Mbps 802.3at PoE + 2-port Gigabit TP/SFP Combo Managed PoE+ multi-port Fast Ethernet switch and SFP fiber optical connectivity and robust Layer 2 features. The description of this series is shown below:

Unless specified, the term “managed switch” mentioned in this user manual refers to the ES2402-V2 series.

ES2402-8P-2C-V2	8-Port 10/100TX 802.3at PoE + 2-Port Gigabit TP/SFP Combo Managed Ethernet Switch (120 W)
ES2402-16P-2C-V2	16-Port 10/100TX 802.3at PoE + 2-Port Gigabit TP/SFP Combo Managed Ethernet Switch (190 W)
ES2402-24P-2C-V2	24-Port 10/100TX 802.3at PoE + 2-Port Gigabit TP/SFP Combo Managed Ethernet Switch (400 W)

Package contents

Open the box of the managed switch and carefully unpack it. The box should contain the following items:

- The managed switch × 1
- Quick installation guide × 1
- Rubber feet × 4
- Rack-mounting accessory kit × 1
- Power cord × 1
- SFP dust-proof cap × 2

If any of these are missing or damaged, contact your dealer immediately. If possible, retain the carton including the original packing materials for repacking the product in case there is a need to return it to us for repair.

Note: User manuals and install guides are available for download from www.interlogix.com.

- Circuit protection prevents power interference between ports.
- Remote power feeding up to 100 meters.
- PoE power usage LED indicators.
- PoE management:
 - Per port PoE function enable/disable
 - PoE port power feeding priority
 - Per PoE port power limitation
 - PD classification detection
 - PoE power sequential

Intelligent PoE features

- Real-time display of PoE chipset temperature
- PD alive check
- PoE port sequence
- PoE schedule

Layer 2 features

- Prevents packet loss with back pressure (half-duplex) and IEEE 802.3x pause frame flow control (full-duplex).
- High performance Store and Forward architecture, runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth.

Supports VLAN

- Port-based VLAN, up to 26 VLAN groups
- IEEE 802.1Q tagged VLAN
- Protocol VLAN
- Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad)
- GVRP
- Voice VLAN

Supports STP

- STP, IEEE 802.1D Spanning Tree Protocol
- RSTP, IEEE 802.1w Rapid Spanning Tree Protocol
- MSTP (IEEE 802.1s Multiple Spanning Tree Protocol)
- STP BPDU filtering, BPDU Guard

Supports link aggregation

- IEEE 802.3ad Link Aggregation Control Protocol (LACP)

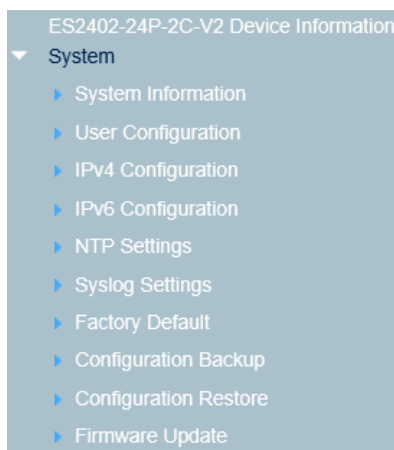
	Many-to-1 monitor
VLAN	Port-based VLAN, up to 26 VLAN groups IEEE 802.1Q tagged VLAN (Up to 256 VLAN groups, out of 4094 VLAN IDs) Protocol VLAN Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad) GVRP Voice VLAN
Link Aggregation	IEEE 802.3ad LACP supports one 2-port trunk group; static trunk supports one 2-port trunk group
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) STP BPDU filtering, BPDU Guard
Access Control List	IPv4/IPv6 IP-based ACL MAC-based ACL
QoS	Ingress/Egress Rate Limit per port bandwidth control Storm Control support – Broadcast/ Multicast /DLF (Destination Lookup Failure)/ARP/ICMP Traffic classification – IEEE 802.1p Qos/CoS – TCP/UDP/DSCP/IP precedence of IPv4/IPv6 packets Strict priority and Weighted Round Robin (WRR) CoS policies
IGMP Snooping	IPv4 IGMP snooping v1/ v2 and v3
MLD Snooping	IPv6 MLD snooping v1, v2
Security Control	Access Control List – IPv4/IPv6 IP-based ACL – MAC-based ACL Port-MAC-IP Address Binding – Port-MAC-IP Port Setting – Port-MAC-IP Entry Setting MAC Address Binding – Static MAC – MAC Filtering DHCP snooping to filter distrusted DHCP messages ARP Inspection discards ARP packets with invalid MAC address to IP address binding
Management	
Basic Management Interfaces	IPv4 and IPv6 dual stack management Switch management interface - Web switch management - Telnet command line interface - SNMP v1, v2c and v3 BOOTP and DHCP for IP address assignment

	– Static MAC – MAC Filtering DHCP snooping to filter distrusted DHCP messages ARP Inspection discards ARP packets with invalid MAC address to IP address binding
Management	
Basic Management Interfaces	IPv4 and IPv6 dual stack management Switch management interface - Web switch management - Telnet command line interface - SNMP v1, v2c and v3 BOOTP and DHCP for IP address assignment System maintenance - Firmware upgrade via HTTP - Configuration upload/download through web interface - Hardware-based reset button for system reset to factory default SNTP Network Time Protocol Link Layer Discovery Protocol (LLDP) Event message logging to remote Syslog server Smart discovery utility
Secure Management Interfaces	SNMP v3, SSH, SSL
Standards Conformance	
Regulation Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x flow control and back pressure IEEE 802.3ad port trunk with LACP IEEE 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1p Class of Service IEEE 802.1Q VLAN tagging IEEE 802.1ab LLDP IEEE 802.3af Power over Ethernet IEEE 802.3at Power over Ethernet Plus RFC 2068 HTTP RFC 1112 IGMP version 1 RFC 2236 IGMP version 2 RFC 3376 IGMP version 3 RFC 2710 MLD version 1 RFC 3810 MLD version 2
Environment	

Operating	Temperature: 0 to 50°C Relative Humidity: 5 to 95% (non-condensing)
Storage	Temperature: -10 to 70°C Relative Humidity: 5 to 95% (non-condensing)



Note: Never pull out the module without making use of the lever or the push bolts on the module. Removing the module with force could damage the module and the SFP/SFP+ module slot of the managed switch.



System Information	The switch system information is provided here.
User Configuration	Configure the username and password information on this page.
IPv4 Configuration	Configure the managed IPv4 information on this page.
IPv6 Configuration	Configure the managed IPv6 information on this page.
NTP Settings	Configure the NTP function on this page.
Syslog Settings	Configure the System log function on this page.
Factory Default	Reset the managed switch to default mode excluding the IP address, user name, and password.
Configuration Backup	Configure the configuration file backup.
Configuration Rackup	Configure the configuration file restore.
Firmware Update	This page facilitates update of the firmware controlling the managed switch.

System information

The System Information page provides information on the current device such as the hardware MAC address, firmware version, and system uptime. It also permits configuration the device name, comment, location, and contact information.

System Information

MAC Address

Firmware Version v2.2120190812

System Up Time 03:21:39

Device Name

Comment

Location

Contact

Apply

Network Time Protocol (NTP) settings

NTP synchronizes the clocks of computer systems and uses UDP (data grams) as a transport layer. Specify NTP Servers and set GMT time zone on this page.

The page includes the following fields:

Item	Function
System Time	Displays current system time.
State	Indicates the NTP mode operation. Selections include: Enable: Enable NTP mode operation. The agent forwards and transfers NTP messages between the clients and the server when they are not on the same subnet domain. Disable: Disable NTP mode operation.
Time Zone	Permits selecting the time zone according to the current location of the managed switch.
Primary Server IP	Type the NTP server IPv4 IP address in this box.
Secondary Server IP	Type the NTP server IPv4 IP address in this box.

Buttons

- Click **Apply** to apply changes.

Syslog settings

The Syslog settings include global, facility, and remote server settings.

VLAN Tag-based Entry Config										
Add										
Name	State	VID	Don't care	Add Tag	Remove Tag	Forbidden	Priority	GVRP Forward	Action	
Default	Static	1	1-26	0	0	0	0	Deny	Edit	Delete
Protocol_VLAN1	Static	4081	1-26	0	0	0	0	Deny	Edit	Delete
Protocol_VLAN2	Static	4082	1-26	0	0	0	0	Deny	Edit	Delete
Protocol_VLAN3	Static	4083	1-26	0	0	0	0	Deny	Edit	Delete
Protocol_VLAN4	Static	4084	1-26	0	0	0	0	Deny	Edit	Delete
Voice-VLAN	Static	4080	0	0	0	0	0	Deny	Edit	Delete

The page includes the following fields:

Object	Description
Name	The name of the specific VLAN group.
Static	The state of the specific VLAN group.
VID	The VLAN ID of the specific VLAN group.
Don't care	The per port don't care information for a specific VLAN group.
Add	The per port Add Tag state of a specific VLAN group.
Remove	The per port Remove Tag state of a specific VLAN group.
Forbidden	The per port Forbidden state of a specific VLAN group.
Priority	The Priority state of a specific VLAN group.
GVRP Forward	The GVRP Forward state of a specific VLAN group.
Action	Click Edit to edit a specific VLAN group. Click Delete to delete a specific VLAN group.

Buttons

- Click **Add** to create a new specific VLAN group.
- Click **Delete** to delete a specific VLAN group.
- Click **Edit** to edit a specific VLAN group. When clicking **Edit** to edit a member port state, the following page appears:

VLAN Tag-based Entry Config

VLAN Name:
VID:
Priority:
GVRP forward:

VLAN Member													
Port	1	2	3	4	5	6	7	8	9	10	11	12	13
Don't care	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Add	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Remove	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Forbidden	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Not member	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Port	14	15	16	17	18	19	20	21	22	23	24	25	26
Don't care	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Add	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Remove	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Forbidden	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Not member	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Apply

The page includes the following fields:

Object	Description
VLAN Name	Type the VLAN group name information in this box if necessary. The maximum description length is 20 characters.
VID	The VLAN ID of the specific VLAN group.
Priority	The priority value of the specific VLAN group.
GVRP Forward	The GVRP Forward mode. When GVRP is enabled, configure this value if the Tag VLAN will be transmitted through GVRP.
Port	Per port list of the managed switch.
Don't care	A VLAN member of a specific VLAN group without any assigned action.
Add	Add the Tag action to the packet sent out by this port.
Remove	Remove the Tag action to the packet sent out by this port.
Forbidden	Configure this port to not register this Tag VLAN dynamically through GVRP.
Not Member	Not a VLAN member.

Buttons

- Click **Apply** to apply changes.

Note: GVRP (GARP VLAN Registration Protocol) maintains VLAN dynamic registration information for GVRP devices based on the working mechanism of GARP to maintain VLAN dynamic registration information that supports GVRP devices and propagate this information to other devices to achieve agreement on VLAN information for all devices supporting GVRP in the same LAN. The VLAN registration information propagated by GVRP includes both local manual static registration information and dynamic registration information from other switches.

VLAN port configuration

This page is used for configuring the managed switch port VLAN. It contains fields for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is also configured on this page. All untagged packets arriving to the device are tagged by the port's PVID.

Managed switch nomenclature:

IEEE 802.1Q tagged and untagged

Every port on an 802.1Q compliant switch can be configured as tagged or untagged.

Tagged: Ports with tagging enabled put the VID number, priority, and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.

Untagged: Ports with untagging enabled strip the 802.1Q tag from all packets that flow into those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port have no 802.1Q VLAN information (remember that the PVID is only used internally within the managed switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Frame Income Frame Leave	Income Frame is tagged	Income Frame is untagged
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remains untagged

VLAN Port Config

Port Selection

1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

PVID Tag Force Uplink Exclusive Egress Ingress-check GVRP Ingress-frame

Apply

Port	PVID	Tagging	Force VLAN Group	Uplink	Exclusive	Egress	Ingress Check	GVRP	Ingress Frame
1	1	None					v		All
2	1	None					v		All
3	1	None					v		All
4	1	None					v		All
5	1	None					v		All
6	1	None					v		All
7	1	None					v		All
8	1	None					v		All

The page includes the following fields:

Object	Description
Port Selection	Select a specific port for VLAN settings.
PVID	The PVID will be inserted into all untagged frames entering the ingress port. The PVID must be the same as the VLAN ID that the port belongs to in the VLAN group, or the untagged traffic will be dropped.
Tag	Determine if a VLAN Tag is added or removed from the packet sent out by selected port. Selections include: Add RMV None
Force	Sets priority according to the group VLAN setting for the action.
Uplink	Set up the Uplink port, which automatically sends the packet out of the uplink port when the destination port is not the same as the VLAN.
Exclusive	Enable or disable the exclusive function on a specific port, the exclusive port unable to transfer packets.
Egress	Enable or disable the egress function on a specific port. When the destination port of the packet is not in the same VLAN, it can still be transmitted to the destination port via the egress rule.
Ingress-Check	Enable or disable the ingress check function. Check if the port is a member of this VLAN through VID.
GVRP	Enable or disable the port GVRP function.
Ingress-Frame	Setting allows the specified frame to do the forwarding action. Selections include: Tag-Frame All
Port	Per port list.
PVID	Per port PVID information.
Tagging	Per port Tagging information.
Force VLAN Group	Per port Force VLAN Group information.
Uplink	Per port Uplink information.
Exclusive	Per port Exclusive information.
Egress	Per port Egress information.
Ingress Check	Per port Ingress Check information.
GVRP	Per port GVRP information.
Ingress-Frame	Per port Ingress Frame information.

Note: The port must be a member of the same VLAN as the Port ID VLAN.

Buttons

- Click **Apply** to apply changes.

Protocol VLAN config

Use this page to configure Protocol VLAN.

Protocol VLAN Config

☒ Protocol VLAN Enable

Enable	No.	VID	Protocol Type	Protocol Select
☐	1	4081	0x0	Ether_type ▼
☐	2	4082	0x0	Ether_type ▼
☐	3	4083	0x0	Ether_type ▼
☐	4	4084	0x0	Ether_type ▼

Apply

The page includes the following fields:

Object	Description
Protocol VLAN Enable	Click to activate the Protocol VLAN settings.
Enable	Select the number of groups to enable.
No.	The group number.
VID	Set the VID value. When the packet conforms to the set protocol on this page, the VLAN member is queried with VID.
Protocol Type	Set the protocol type.
Protocol Select	Select the protocol. Selections include: Ether Type: The set value of the protocol type must be greater than 0x0600 when selecting Ether Type. Its format is DA+SA+Protocol type. LLC: Its format is DA+SA+Protocol Type. RFC1042: Its format is DA+SA+length+AAAA03+000000+Protocol Type.

Buttons

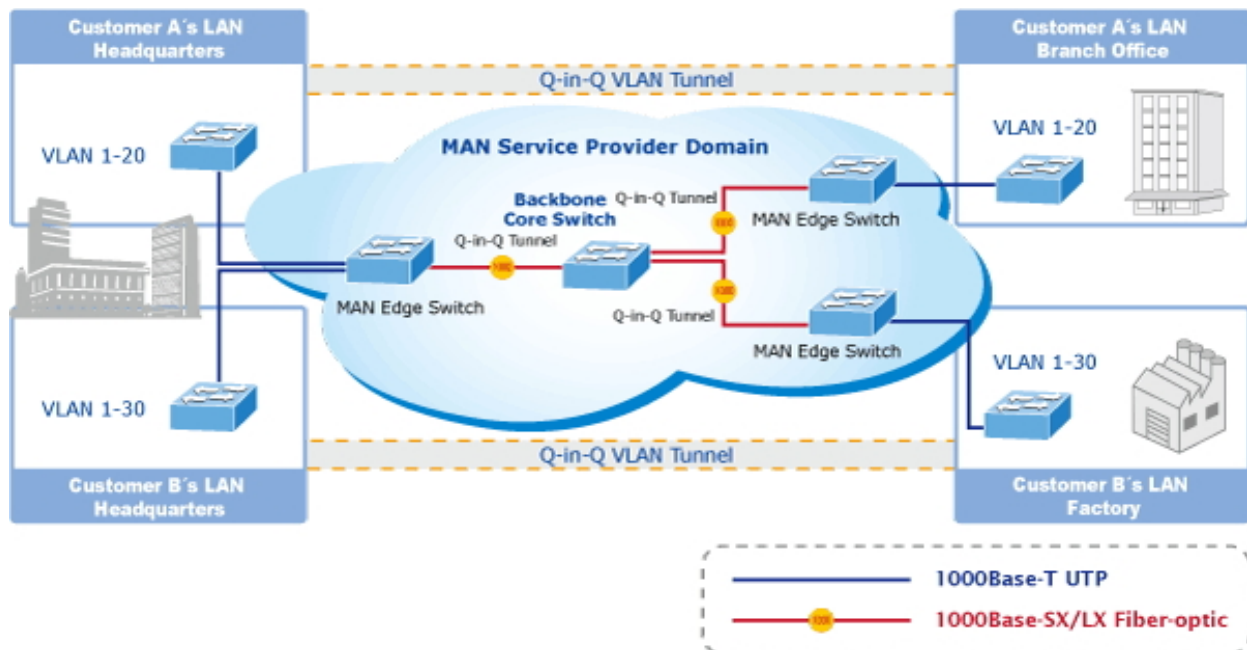
- Click **Apply** to apply changes.

Q-in-Q configuration

IEEE 802.1Q tunneling (Q-in-Q) is designed for service providers carrying traffic for multiple customers across their networks. Q-in-Q tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in

the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.



The managed switch supports multiple VLAN tags and can therefore be used in MAN (Metro Access Network) applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the MAN space. One of the purposes of the provider bridge is to recognize and use VLAN tags so that the VLANs in the MAN space can be used independent of the customers' VLANs. This is accomplished by adding a VLAN tag with a MAN-related VID for frames entering the MAN. When leaving the MAN, the tag is stripped and the original VLAN tag with the customer-related VID is again available.

This provides a tunneling mechanism to connect remote customer VLANs through a common MAN space without interfering with the VLAN tags. All tags use EtherType 0x8100 or 0x88A8, where 0x8100 is used for customer tags and 0x88A8 is used for service provider tags.

In cases where a given service VLAN only has two member ports on the switch, the learning can be disabled for the particular VLAN and can therefore rely on flooding as the forwarding mechanism between the two ports. This way, the MAC table requirements are reduced.

Q-in-Q port configuration

QinQ Port Config

Port Selection												
1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Index
Tagging
Rx Detect
Keep PCP/DEI

Apply

Port	Index	Tagging	Rx Detect	Keep PCP/DEI
1	1	None		
2	1	None		
3	1	None		
4	1	None		
5	1	None		
6	1	None		
7	1	None		
8	1	None		

The page includes the following fields:

Object	Description
Port Selection/Port	Select a specific port for Q-in-Q Port configuration. Per port numbers are listed.
Index	Choose to use the set of indexes in which the service tag value is placed in the Q-in-Q Index config page setting. Also displays the current Index information.
Tagging	Set a VLAN tag to be added or removed from the packet sent out by the selected port. Selections include: Add: Perform the new service tag action on the incoming and outgoing packet from this port. If the incoming packet itself has a service tag, modify or directly replace the service tag action depending on if the RX detect is open. RMV: RX detect enable state to remove the service tag. Also displays current tagging information. None
RX Detect	Enable or disable the packet that enters the port to perform the service tag check. Also displays the current RX Detect information.
Keep PCP/DEI	Retain the original PCP and DEI values when modifying the service tag entered into the packet. Also displays the current Keep PCP/DEI information.

Buttons

- Click **Apply** to apply changes.

Q-in-Q index configuration

QinQ Index Config

Type: 88A8

Index

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Apply

The page includes the following fields:

Object	Description
Type	Set the type value of the service tag.
Index	Set the service tag value for each index.

Buttons

- Click **Apply** to apply changes.

Spanning Tree Protocol (STP)

Theory

STP can be used to detect and disable network loops, and to provide backup links between switches, bridges, or routers. This allows the switch to interact with other bridging devices in the network to ensure that only one route exists between any two stations on the network, and provides backup links that automatically take over when a primary link goes down. The spanning tree algorithms supported by this switch include these versions:

- STP** – Spanning Tree Protocol (IEEE 802.1D)
- RSTP** – Rapid Spanning Tree Protocol (IEEE 802.1w)
- MSTP** – Multi Spanning Tree Protocol (IEEE 802.1s)

The IEEE 802.1D Spanning Tree Protocol and IEEE 802.1w Rapid Spanning Tree Protocol allow for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. After the STP is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the spanning tree algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation of the performance of the network if the spanning tree is incorrectly configured. Please read the following before making any changes from the default values.

The switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees from any combination of ports contained within a single switch, in user specified groups.
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

Bridge protocol data units

For STP to arrive at a stable network topology, the following information is used:

- The unique switch identifier.
- The path cost to the root associated with each switch port.
- The port identifier

STP communicates between switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch.
- The path cost to the root from the transmitting port.
- The port identifier of the transmitting port.

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU and, if the topology changes, initiates a BPDU transmission.

The communication between switches via BPDUs results in the following:

- One switch is elected as the root switch.
- The shortest distance to the root switch is calculated for each switch.
- A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

Creating a stable STP topology

The goal is to make the root port the fastest link. If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network becomes the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.

When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For example, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

STP port states

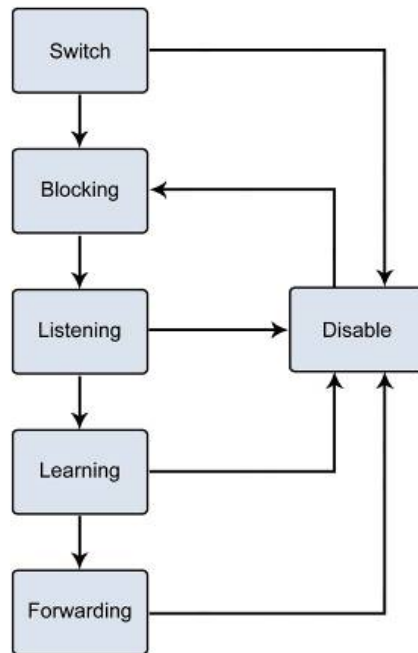
The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a blocking state to a forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition through to further ensure that a stable network topology is created after a topology change.

Each port on a switch using STP exists in one of the following five states:

- **Blocking** – The port is blocked from forwarding or receiving packets.
- **Listening** – The port is waiting to receive BPDU packets that may tell the port to go back to the blocking state.
- **Learning** – The port is adding addresses to its forwarding database, but not yet forwarding packets.
- **Forwarding** – The port is forwarding packets.
- **Disabled** – The port only responds to network management messages and must return to the blocking state first.

A port transitions from one state to another as follows:

- From initialization (switch boot) to blocking.
- From blocking to listening or to disabled.
- From listening to learning or to disabled.
- From learning to forwarding or to disabled.
- From forwarding to disabled.
- From disabled to blocking.



You can modify each port state by using management software. When STP is enabled, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state. No packets (except BPDUs) are forwarded from, or received by, STP-enabled ports until the forwarding state is enabled for that port.

STP parameters

STP operation levels

The managed switch allows for two levels of operation: the switch level and the port level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.

Note: On the switch level, STP calculates the bridge identifier for each switch and then sets the root bridge and the designated bridges. On the port level, STP sets the root port and the designated ports.

The following are the user-configurable STP parameters for the switch level:

Parameter	Description	Default Value
Bridge Identifier (Not user configurable except by setting priority below)	A combination of the user-set priority and the switch's MAC address. The Bridge Identifier consists of two parts: A 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC.	32768 + MAC
Priority	A relative priority for each switch – lower numbers give a higher priority and a greater chance of a given switch being elected as the root bridge	32768
Hello Time	The length of time between broadcasts of the hello message by the switch	2 seconds
Maximum Age Timer	Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	20 seconds
Forward Delay Timer	The amount of time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

The following are the user-configurable STP parameters for the port or port group level:

Variable	Description	Default Value
Port Priority	A relative priority for each port – lower numbers give a higher priority and a greater chance of a given port being elected as the root port	128
Port Cost	A value used by STP to evaluate paths – STP calculates path costs and selects the path with the minimum cost as the active path	200,000-100Mbps Fast Ethernet ports 20,000-1000Mbps Gigabit Ethernet ports 0 - Auto

Default spanning-tree configuration

Feature	Default Value
Enable state	STP disabled for all ports
Port priority	128
Port cost	0
Bridge Priority	32,768

User-changeable STA parameters

The factory default settings for the switch should cover the majority of installations. It is advisable to keep the default settings as set at the factory unless it is absolutely necessary. The user changeable parameters in the switch are as follows:

- **Priority** – A priority for the switch can be set from 0 to 65535. 0 is equal to the highest priority.

- **Hello Time** – The hello time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the root bridge to tell all other switches that it is indeed the root bridge. If you set a hello time for the switch and it is not the root bridge, the set hello time will be used if and when the switch becomes the root bridge.

Note: The hello time cannot be longer than the max. age or a configuration error will occur.

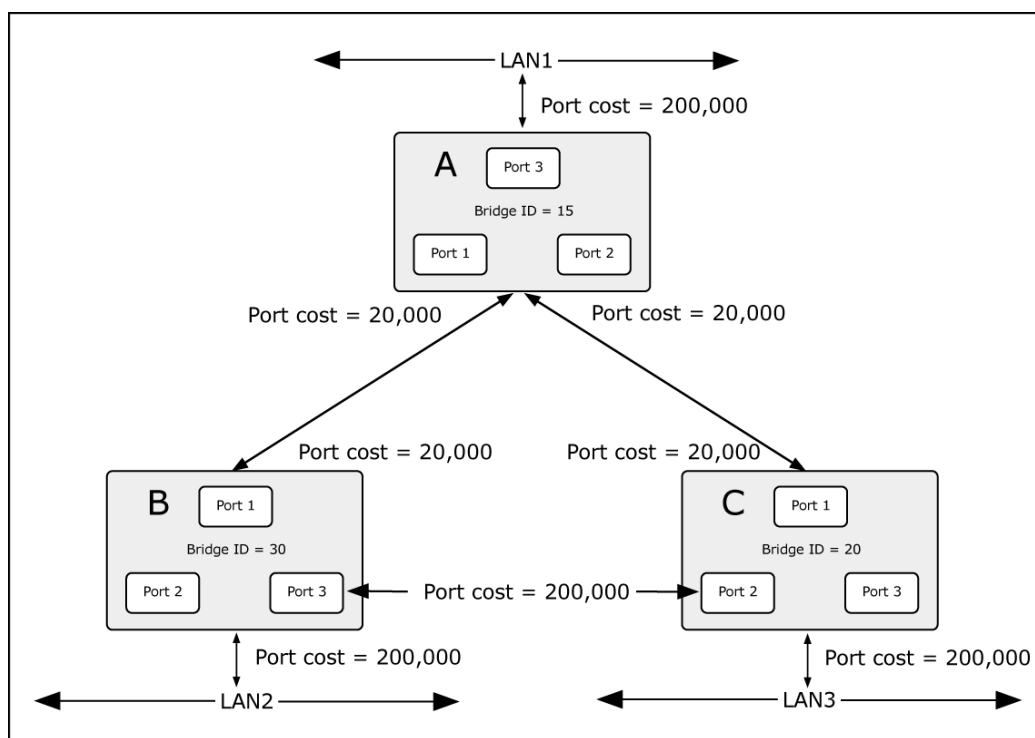
- **Max. Age** – The max. age can be from 6 to 40 seconds. At the end of the max age, if a BPDU has still not been received from the root bridge, the switch starts sending its own BPDU to all other switches for permission to become the root bridge. If the switch has the lowest bridge identifier, it will become the root bridge.
- **Forward Delay Timer** – The forward delay can be from 4 to 30 seconds. This is the time any port on the switch spends in the listening state while moving from the blocking state to the forwarding state.

Note: Observe the following formulas when setting the above parameters: **Max. Age** $\geq 2 \times (\text{Forward Delay} - 1 \text{ second})$, **Max. Age** $\geq 2 \times (\text{Hello Time} + 1 \text{ second})$.

- **Port Priority** – A port priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the root port.
- **Port Cost** – A port cost can be set from 0 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets.

Illustration of STP

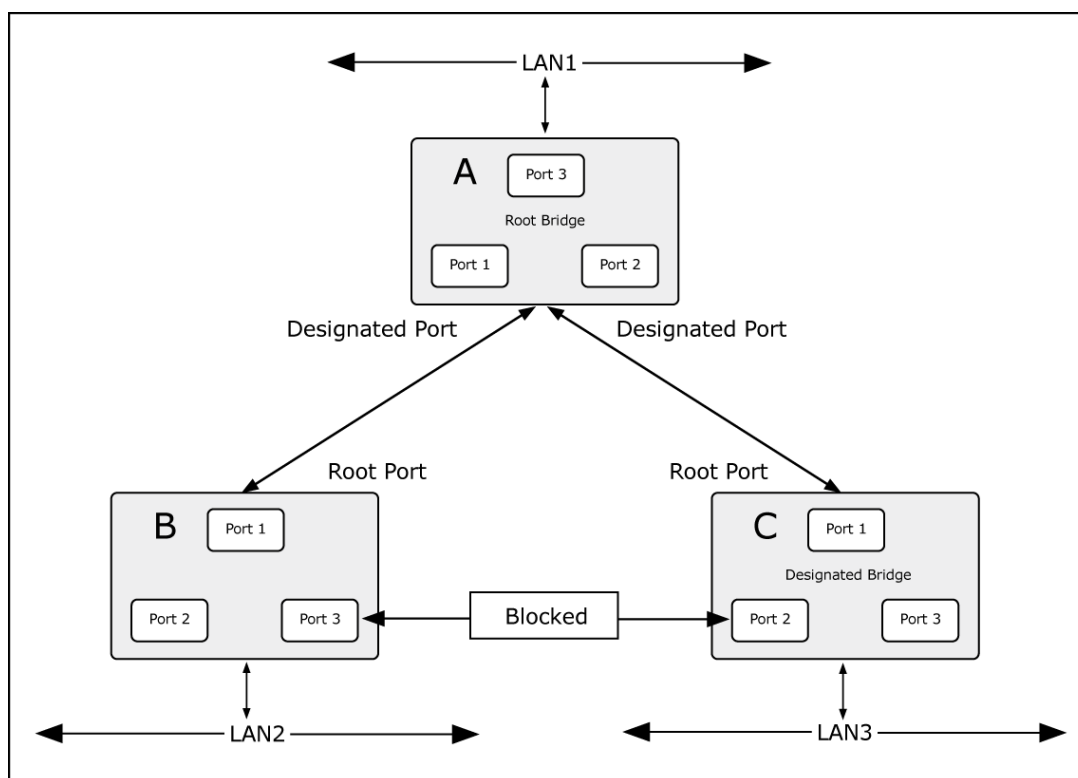
A simple illustration of three switches connected in a loop is depicted in the following diagram. In this example, you can anticipate some major network problems if the STP assistance is not applied.



If switch A broadcasts a packet to switch B, switch B broadcasts to switch C, and switch C broadcasts back to switch A and so on. The broadcast packet will be passed indefinitely in a loop, potentially causing a network failure. In this example, STP breaks the loop by blocking the connection between switch B and C. The decision to block a particular connection is based on the STP calculation of the most current bridge and port settings.

Now, if switch A broadcasts a packet to switch C, then switch C drops the packet at port 2 and the broadcast ends there. Setting up STP using values other than the defaults, can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using the priority setting, or influencing STP to choose a particular port to block using the port priority and port cost settings is, however, relatively straightforward.

In this example, only the default STP values are used:



The switch with the lowest bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 20,000) on switch A are connected to one (optional) Gigabit port on both switch B and C. The redundant link between switch B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 200,000). Gigabit ports could be used, but the port cost should be increased from the default to ensure that the link between switch B and switch C is the blocked link.

The STP section contains the following main topics:

STP Global Settings	Configure and display STP Global settings on this page.
STP Port Settings	Configure and display STP Port settings on this page.

MST Configuration Identification	Configure and display MST Configuration Identification settings on this page.
STP Instance Settings	Configure and display STP Instance settings on this page.
MSTP Port Information	Configure and display MSTP Port Information on this page.
STP Loop Detect Settings	Configure and display STP Loop Detect settings on this page.

STP global settings

Configure STP global settings on this page.

STP Global Settings

STP State	Disable
STP Version	MSTP
Bridge Max Age (6-40)	20 sec
Bridge Hello Time (1-10)	2 sec
Bridge Forward Delay (4-30)	15 sec
Max Hops (6-40)	20 sec
TC Counts (5-30)	5
STP BPDU Filter	Disable

Note:

2 x (Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 x (Bridge_Hello_Time + 1.0 seconds)

The page includes the following fields:

Object	Description
STP State	Enable or disable the spanning tree function.
STP Version	Select the spanning tree operation version. Selections include: MSTP (default), STP , and RSTP .
Bridge Max Age (6-40)	Set the value for Bridge Max Age. The default value is 20 seconds and the available range is 6 to 40 seconds.
Bridge Hello Time (1-10)	Set the value for Bridge Hello Time. The default value is 2 seconds and the available range is 1 to 10 seconds.
Bridge Forward Delay (4-30)	Set the value for Bridge Forward Delay. The default value is 15 seconds and the available range is 4 to 30 seconds.
Max Hops (6-40)	Set the value for Max Hops. The default value is 20 seconds and the available range is 6 to 40 seconds.
TC Counters (5-30)	Set the value for TC Counters. The default value is 5 and the available range is 5 to 30.
STP BPDU Filter	Enable or disable the spanning BPDU Filter function.

Buttons

- Click **Apply** to apply changes.

STP port settings

Configure STP port settings on this page:

STP Port Settings

Port Selection

1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

State

Edge Port

BPDU Protect

Root Protect

Loop Protect

Apply

Port	State	Edge Port	BPDU Protect	Root Protect	Loop Protect
01	Disabled	Disabled	Disabled	Disabled	Disabled
02	Disabled	Disabled	Disabled	Disabled	Disabled
03	Disabled	Disabled	Disabled	Disabled	Disabled
04	Disabled	Disabled	Disabled	Disabled	Disabled
05	Disabled	Disabled	Disabled	Disabled	Disabled
06	Disabled	Disabled	Disabled	Disabled	Disabled
07	Disabled	Disabled	Disabled	Disabled	Disabled
08	Disabled	Disabled	Disabled	Disabled	Disabled
09	Disabled	Disabled	Disabled	Disabled	Disabled
10	Disabled	Disabled	Disabled	Disabled	Disabled

Refresh

The page includes the following fields:

Object	Description
Port Selection	Select a specific port for further configuration.
State	Enable or disable the spanning tree function on a specific port. The default mode is Disable . The current status of the port appears.
Edge Port	Enable or disable the Edge Port function on specific port. The default mode is Disable . The current status of the port appears.
BPDU Protect	Enable or disable the BPDU Protect function on specific port. The default mode is Disable . The current status of the port appears.
Root Protect	Enable or disable the Root Protect function on specific port. The default mode is Disable . The current status of the port appears.
Loop Protect	Enable or disable the Loop Protect function on specific port. The default mode is Disable . The current status of the port appears.
Port	Displays the per port list.

Buttons

- Click **Apply** to apply changes.
- Click **Refresh** to update the window.

MST configuration identification

Configure MST configuration identification settings on this page:

MST Configuration Identification

MST Configuration Identification Settings

Configuration Name

FGSW-2624HPS4

Revision Level(0-65535)

0

Apply

Instance ID Settings

MSTI ID (1-4094)

Action

Add VID ▾

VID List (1-4094)

Apply

MSTI ID	VID List	Action
CIST	1-4094	Edit Delete

The page includes the following fields:

Object	Description
MST Configuration Identification Settings	
Configuration Name	Type the configuration name in this box, 32 characters maximum.
Revision Level	Type the Revision Level setting in this box. The available range is 0 to 65535.
Instance ID Settings	
MSTI ID (1-4094)	Type the MSTI ID setting in this box. The available range is 1 to 4094.
Action	Select the action of MSTI; Add VID (default) or Remove VID .
VID List (1-4094)	Configure the VID List settings for MSTI; the available VID range is 1 to 4094.
MSTI ID	Displays the MSTI ID information.
VID List	Displays the VID List information.
Action	Click Edit to edit specific Instance ID Settings. Click Delete to delete specific Instance ID Settings.

Buttons

- Click **Apply** to apply changes.

STP instance settings

Configure STP instance settings on this page:

STP Instance Settings

MSTI ID
Priority (0-61440)

Instance Type	Instance Priority	Action	
CIST	32768	Edit	View

STP Instance Operational Status

MSTP ID	--	Designated Root Bridge	--
External Root Cost	--	Regional Root Bridge	--
Internal Root Cost	--	Designated Bridge	--
Root Port	--	Max. Age	--
Forward Delay	--	Max. Hops	--

The page includes the following fields:

Object	Description
MSTI ID	Type the MSTI ID setting in this box.
Priority	Type the Priority setting in this box. The available range is 0 to 61440.
Instance Type	Displays the instance type information.
Instance Priority	Displays the instance priority information.
Action	Click Edit to edit specific Instance ID Settings. Click View to view STP Instance operational status.
STP Instance Operational Status	
MSTP ID	Displays MSTP ID information.
External Root Cost	Displays External Root Cost information.
Internal Root Cost	Displays Internal Root Cost information.
Root Port	Displays Root Port information.
Forward Delay	Displays Forward Delay information.
Designated Root Bridge	Displays Designated Root Bridge information.
Regional Root Bridge	Displays Regional Root Bridge information.
Designated Bridge	Displays Designated Bridge information.
Max. Age	Displays Max. Age information.
Max. Hops	Displays Max. Hops information.

Buttons

- Click **Apply** to apply changes.

MSTP port information

Configure MSTP port information settings on this page:

Port

MSTP Port Settings

Instance ID Internal Path Cost (0-200000000,0=Auto) Priority (0-240)

Port 1 Settings

MSTI	Designated Bridge	Internal Path Cost	Priority	Status	Role	Action
0	32768/66-09-07-03-04-09	200000(Auto)	128	Disabled	Disabled Port	Edit

The page includes the following fields:

Object	Description
Port	Select a specific port for further configuration.
MSTP Port Settings	
Instance ID	Type the Instance ID setting in this box.
Internal Path Cost (0-200000000,0=Auto)	Type the Internal Path Cost setting into this box. The available range is 0 to 200000000, 0=Auto.
Priority (0-240)	Type the Priority setting into this box. The available VID range is 0 to 240.
MSTI	MSTI information.
Designated Bridge	Designated Bridge information.
Internal Path Cost	Internal Path Cost information.
Priority	Priority information.
Status	Status information.
Role	Role information.
Action	Click Edit to edit specific MSTP port settings.

Buttons

- Click **Apply** to apply changes.
- Click **Find** to find MSTP port information.

STP loop detect settings

The loopback detection function avoids user network loops. Configure loopback detection on the STP Loop Detect Settings page.

STP Loop Detect Settings

STP Loop Detect Setting

STP Loop Detection State

Enable

Block Release Time

9

sec

Apply

Loop Detect Port State

Port	State
1	---
2	---
3	---
4	---
5	---
6	---
7	---
8	---

Refresh

The page includes the following fields:

Object	Description
STP Loop Detect Setting	
SFP Loop Detection State	Enable or disable the SFP Loop Detection State function on a specific port. The default mode is Enable .
Block Release Time	Type the Block Release Time setting into this box. The available range is 1 to 255.
Loop Detect Port State	
Port	Per port list.
State	Per port state information.

Buttons

- Click **Apply** to apply changes.
- Click **Refresh** to refresh the window.

Multicast

IGMP snooping

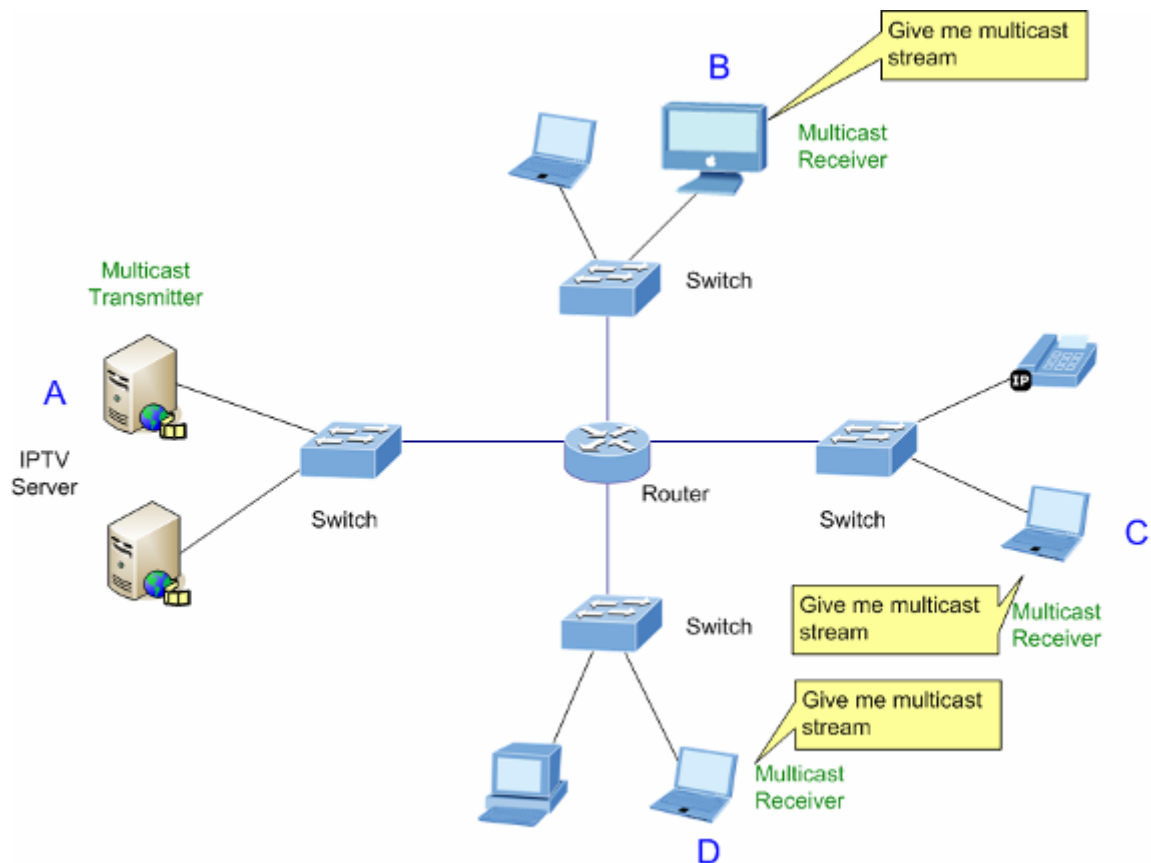
The Internet Group Management Protocol (IGMP) allows hosts and routers share information about multicast groups memberships. IGMP snooping is a switch feature that monitors the exchange of IGMP messages and copies them to the CPU for feature

processing. The overall purpose of IGMP snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.

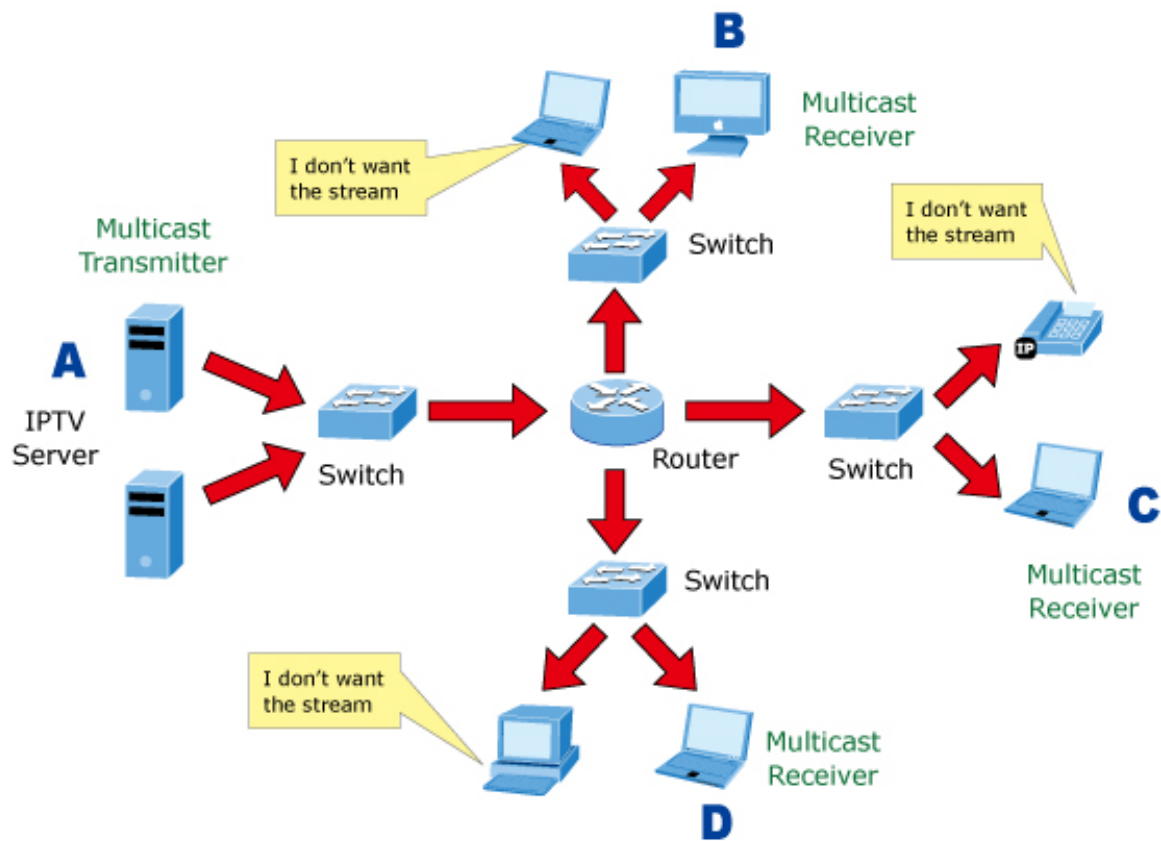
About IGMP snooping

Computers and network devices that need to receive multicast transmissions must inform nearby routers that they will become members of a multicast group. IGMP is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active. In the case where there is more than one multicast router on a sub network, one router is elected as 'querier.' This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine whether or not multicast packets should be forwarded to a given sub network. Using IGMP, the router can check to see if there is at least one member of a multicast group on a given sub network. If there are no members on a sub network, packets will not be forwarded to that sub network.

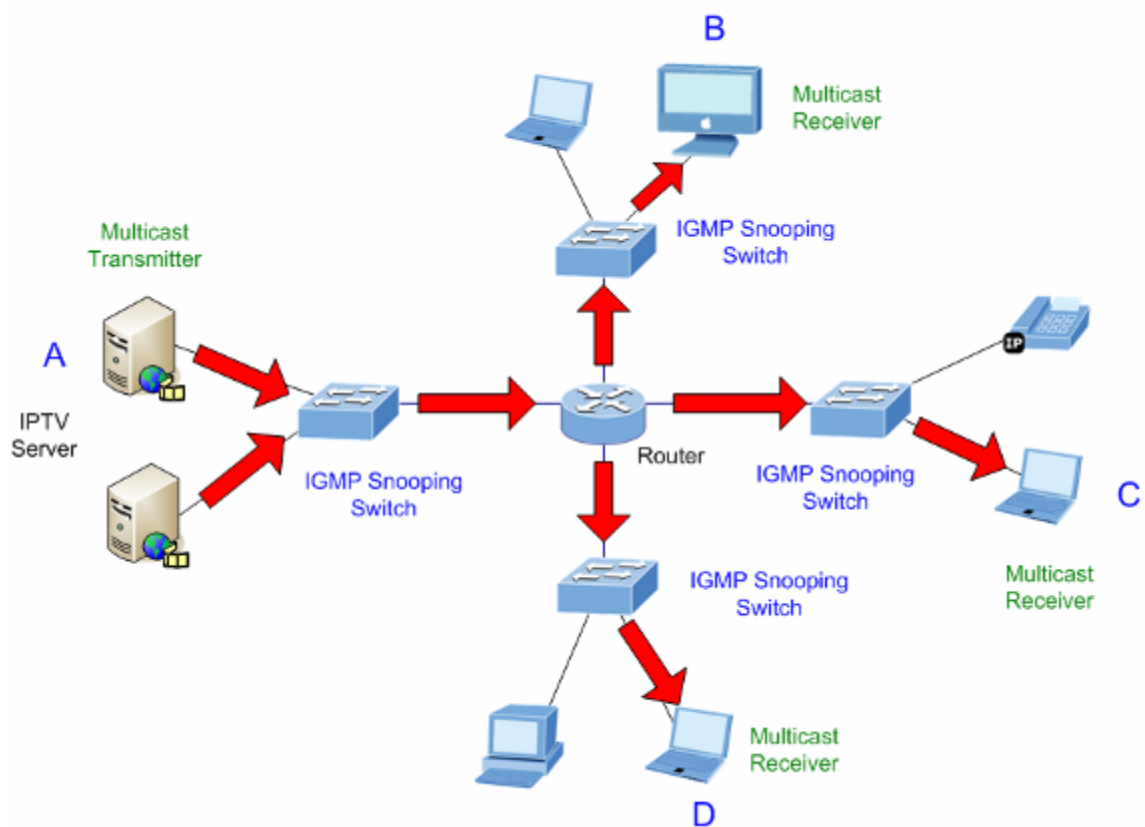
Multicast service



Multicast flooding



IGMP snooping multicast stream control

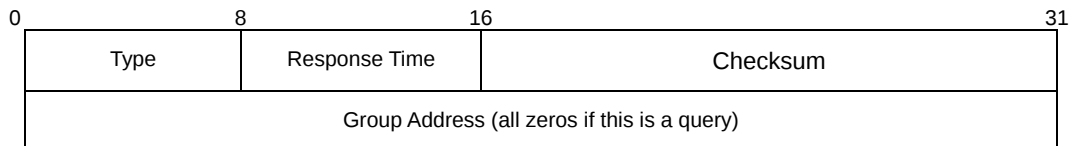


IGMP versions 1 and 2

Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group. IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data. The format of an IGMP packet is shown below:

IGMP message format

Octets:



The IGMP type codes are shown below:

Type	Meaning
0x11	Membership Query (if Group Address is 0.0.0.0)
0x11	Specific Group Membership Query (if Group Address is Present)
0x16	Membership Report (version 2)
0x17	Leave a Group (version 2)
0x12	Membership Report (version 1)

IGMP packets allow multicast routers to keep track of the membership of multicast groups on their respective sub networks. The following outlines what is communicated between a multicast router and a multicast group member using IGMP.

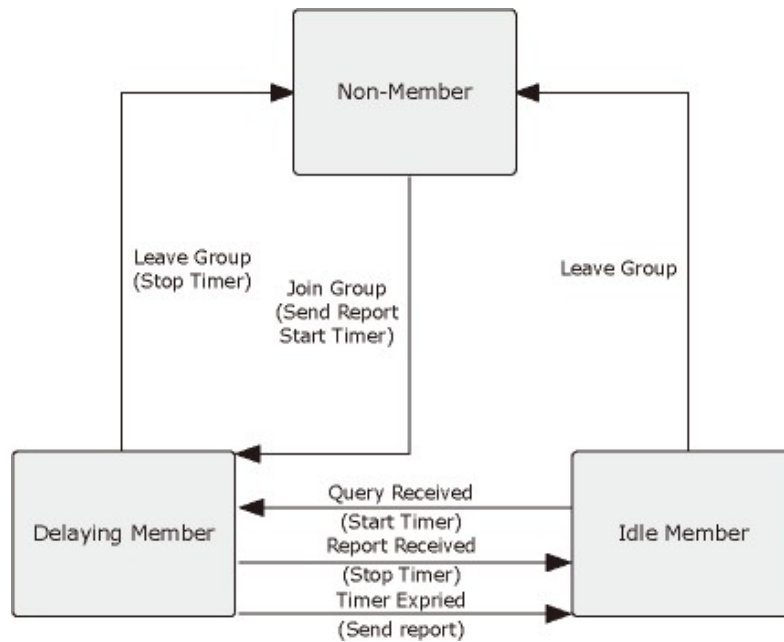
- A host sends an IGMP “report” to join a group
- A host will never send a report when it wants to leave a group (for version 1).
- A host will send a “leave” report when it wants to leave a group (for version 2).

Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their sub networks. If there is no response from a particular group, the router assumes that there are no group members on the network.

The Time-to-Live (TTL) field of query messages is set to 1 so that the queries will not be forwarded to other sub networks.

IGMP version 2 introduces some enhancements such as a method to elect a multicast queried for each LAN, an explicit leave message, and query messages that are specific to a given group.

The states a computer will go through to join or to leave a multicast group are as follows:



IGMP querier

A router or multicast-enabled switch can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected “querier” and assumes the role of querying the LAN for group members. It then propagates the service requests to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Note: Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

IGMP snooping settings

The IGMP Snooping Settings page provides IGMP snooping-related configuration information.

IGMP Snooping Settings	
IGMP Snooping State	Disable ▾
Version	IGMPv3 ▾
IGMP Group Aged Out	Enable ▾
GMI (10-65535)	100 sec
Router Aging Time (10-65535)	100 sec
IGMP Immediate Leave	Disable ▾
Apply	

The page includes the following fields:

Object	Description
--------	-------------

Object	Description
IGMP Snooping State	Enable or disable the IGMP Snooping function.
Version	Select the IGMP Snooping operation version; IGMPv1 , IGMPv2 , or IGMPv3 (default).
IGMP Group Aged Out	Enable or disable the IGMP Group Aged Out function.
GMI (10-65535)	Type the value for Group Member Interval Time in this box. The default value is 100 seconds and the available range is 10 to 65535 seconds. After the dynamic group is established, the time is used to query member status.
Router Aging Time (10-65535)	Type the value for Router Aging Time in this box. The default value is 100 seconds and the available range is 10 to 65535 seconds. Based on the time the dynamic router port exists, and if the query packet is not continuously received, the dynamic router port clears.
IGMP Immediate Leave	Enable or disable the IGMP Immediate Leave function.

Buttons

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

IGMP snooping router ports settings

Configure the IGMP snooping router ports settings.

IGMP Snooping Router Ports Settings

IGMP Snooping Static Router Ports												
1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Apply

IGMP Snooping Dynamic Router Ports												
1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

The page includes the following fields:

Object	Description
IGMP Snooping Static Router Ports	Select the IGMP snooping static router ports.
IGMP Snooping Dynamic Router Ports	Select the IGMP snooping dynamic router ports.

Buttons

- Click **Apply** to apply changes.

IGMP snooping groups

Configure IGMP snooping group settings.

IGMP Snooping Groups

IGMP Snooping Static Group Configuration

Group Address

Priority

0

Member Port

1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Apply

IGMP Snooping Group Information

Group	State	Member Port	Priority	Action
-------	-------	-------------	----------	--------

The page includes the following fields:

Object	Description
IGMP Snooping Static Group Configuration	
Group Address	Type the Group Address into this box.
Priority	Select Priority. Selections range from 0 (default) to 7.
Member Port	Select specific ports for IGMP Snooping Groups settings.
IGMP Snooping Group Information	
Group	Group list.
State	Group status.
Member Port	Group member port status.
Priority	Group priority status.
Action	Click Edit to edit specific IGMP Snooping Groups Settings. Click Delete to delete specific IGMP Snooping Groups Settings.

Buttons

- Click **Apply** to apply changes.

IGMP snooping ports

Configure the IGMP snooping ports on this page.

IGMP Snooping Ports					
IGMP Snooping Port Information					
Port 1 ▼					
Group	State	Mode	Uptime	Expires	Source List

The page includes the following fields:

Object	Description
IGMP Snooping Port Information	
Port	Select a specific port for IGMP Snooping Ports settings.
Group	Group list.
State	Port status.
Mode	Port status.
Uptime	Port uptime status.
Expires	Port expire status.
Source List	Port source list status.

IGMP snooping example

The ES2402-V2 series switches do not support IGMP Querier. Thus, when configuring the IGMP snooping application, another IFS switch such the NS3552-16P-2T-2S-V2 model with IGMP Querier function should be used as in the example below:

1. Enable IGMP snooping.

IGMP Snooping Settings	
IGMP Snooping State	Enable ▼
Version	IGMPv3 ▼
IGMP Group Aged Out	Enable ▼
GMI (10-65535)	100 sec
Router Aging Time (10-65535)	100 sec
IGMP Immediate Leave	Disable ▼

2. Enable IGMP snooping static router ports.

IGMP Snooping Router Ports Settings												
IGMP Snooping Static Router Ports												
☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

3. Connect the ES2402-V2 series switch to an IFS series switch such as the NS3552-16P-2T-2S-V2 and check the status.

IGMP Snooping Group Information					
Group	State	Member Port	Priority	Action	
224.0.0.252	dynamic	2	0	Edit	Delete
239.255.255.250	dynamic	2	0	Edit	Delete
224.0.0.251	dynamic	2	0	Edit	Delete

IGMP Snooping Ports					
IGMP Snooping Port Information					
Port 2					
Group	State	Mode	Uptime	Expires	Source List
224.0.0.252	dynamic	Exclude	95.000000	6	
239.255.255.250	dynamic	Exclude	97.000000	5	
224.0.0.251	dynamic	Exclude	95.000000	6	

MLD snooping settings

Configure the MLD snooping settings on this page.

MLD Snooping Settings	
MLD Snooping State	Disable
Version	MLDv2
MLD Group Aged Out	Enable
GMI (10-65535)	100 sec
Router Aging Time (10-65535)	100 sec
MLD Immediate Leave	Disable
Apply	

The page includes the following fields:

Object	Description
MLD Snooping State	Enable or disable the MLD Snooping function.
Version	Select the MLD Snooping operation version; MLDv1 or MLDv2 (default).
MLD Group Aged Out	Enable or disable the MLD Group Aged Out function.
GMI (10-65535)	Type the value for Group Member Interval Time in this box. The default value is 100 seconds and the available range is 10 to 65535 seconds. After the dynamic group is established, the time is used to query member status.
Router Aging Time (10-65535)	Type the value for Router Aging Time in this box. The default value is 100 seconds and the available range is 10 to 65535 seconds. Based on the time the dynamic router port exists, and if the query packet is not continuously received, the dynamic router port clears.
MLD Immediate Leave	Enable or disable the MLD Immediate Leave function.

Buttons

- Click **Apply** to apply changes.

MLD snooping router ports setting

Configure the MLD snooping router ports settings.

MLD Snooping Router Ports Settings

MLD Snooping Static Router Ports

1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

MLD Snooping Dynamic Router Ports

1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

The page includes the following fields:

Object	Description
MLD Snooping Static Router Ports	Select the MLD snooping static router ports.
MLD Snooping Dynamic Router Ports	Select the MLD snooping dynamic router ports.

Buttons

- Click **Apply** to apply changes.

MLD snooping groups

Configure MLD snooping group settings.

IGMP Snooping Groups

IGMP Snooping Static Group Configuration

Group Address		Priority	0									
Member Port												
1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

IGMP Snooping Group Information

Group	State	Member Port	Priority	Action
-------	-------	-------------	----------	--------

The page includes the following fields:

Object	Description
MLD Snooping Static Group Configuration	
Group Address	Type the Group Address into this box.
Priority	Select Priority. Selections range from 0 (default) to 7.
Member Port	Select specific ports for MLD Snooping Groups settings.
MLD Snooping Group Information	
Group	Group list.
State	Group status.
Member Port	Group member port status.
Priority	Group priority status.
Action	Click Edit to edit specific MLD Snooping Groups Settings. Click Delete to delete specific MLD Snooping Groups Settings.

Buttons

- Click **Apply** to apply changes.

MLD snooping ports

Configure the MLD snooping ports on this page.

MLD Snooping Ports

MLD Snooping Port Information

Port **1** ▼

Group	State	Mode	Uptime	Expires	Source List
-------	-------	------	--------	---------	-------------

The page includes the following fields:

Object	Description
MLD Snooping Port Information	
Port	Select a specific port for MLD Snooping Ports settings.
Group	Group list.
State	Port status.
Mode	Port status.
Uptime	Port uptime status.
Expires	Port expire status.
Source List	Port source list status.

Quality of Service (QoS)

Understanding QoS

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS permits the assignment of various grades of network service to different types of traffic such as multi-media, video, protocol-specific, time critical, and file-backup traffic.

QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of data and permits prioritization of certain applications across the network. You can define exactly how you want the switch to treat selected applications and types of traffic. Use QoS on the system to control a wide variety of network traffic functions by:

- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, setting higher priorities for time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Providing predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improving performance for specific types of traffic and preserving performance as the amount of traffic grows.
- Reducing the need to constantly add bandwidth to the network.
- Managing network congestion.

QoS terminology

- **Classifier** – Classifies the traffic on the network. Traffic classifications are determined by protocol, application, source, destination, and so on. You can create and modify classifications. The managed switch then groups classified traffic in order to schedule them with the appropriate service level.
- **DiffServ Code Point (DSCP)** – Traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network.
- **Service Level** – Defines the priority given to a set of classified traffic. You can create and modify service levels.
- **Policy** – Comprises a set of rules that are applied to a network so that a network meets the needs of the business. That is, traffic can be prioritized across a network according to its importance to that particular business type.
- **QoS Profile** – Consists of multiple sets of rules (classifier plus service level combinations). The QoS profile is assigned to a port(s).
- **Rules** – Comprises a service level and a classifier to define how the managed switch will treat certain types of traffic. Rules are associated with a QoS profile.

To implement QoS on a network, perform the following actions:

1. Define a service level to determine the priority that will be applied to traffic.
2. Apply a classifier to determine how the incoming traffic will be classified and thus treated by the managed switch.
3. Create a QoS profile that associates a service level and a classifier.
4. Apply a QoS profile to a port(s).

QoS configuration

QoS Group Member	Configure QoS Group Member configuration settings on this page.
QoS Mode Set	Configure QoS Mode Set configuration settings on this page.
QoS Out Queue Aging	Display and configure QoS Out Queue Aging settings on this page.
QoS Remap	Display and configure QoS Remap settings on this page.
Class of Service	Display and configure QoS Class of Service settings on this page.
802.1p-based QoS	Display and configure 802.1p-based QoS settings on this page.
DSCP-based Priority	Display and configure DSCP-based Priority settings on this page.
TCP/UDP Port-based QoS	Display and configure TCP/UDP Port-based QoS settings on this page.

QoS group member

Configure MLD snooping group settings.

QoS Group Member													
Port	1	2	3	4	5	6	7	8	9	10	11	12	13
Group A	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Group B	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Port	14	15	16	17	18	19	20	21	22	23	24	25	26
Group A	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Group B	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Group	Member Port
A	1-26
B	0

The page includes the following fields:

Object	Description
Port	Display per port list.
Group A	Allow assigning specific port to Group A.
Group B	Allow assigning specific port to Group B.
Group	Display Group A and Group B.
Member Port	Display Member Port setting on Group A and Group B.

Buttons

- Click **Apply** to apply changes.

QoS mode set

Configure the QoS mode settings on this page.

QoS Mode Set					
Group	Queue Mode	Queue Method	Queue Ratio (0-255)	Queue Max Bandwidth (0-255)	Unit (BW Throttle Period / TWRR Tickle Unit)
A	First-In-First-Out ▼	WRR ▼	Q0: 0 Q1: 0 Q2: 0 Q3: 0 Q4: 0 Q5: 0 Q6: 0 Q7: 0	Q0: 0 Q1: 0 Q2: 0 Q3: 0 Q4: 0 Q5: 0 Q6: 0 Q7: 0	64Kbps / 51.2ms ▼
B	First-In-First-Out ▼	WRR ▼	Q0: 0 Q1: 0 Q2: 0 Q3: 0 Q4: 0 Q5: 0 Q6: 0 Q7: 0	Q0: 0 Q1: 0 Q2: 0 Q3: 0 Q4: 0 Q5: 0 Q6: 0 Q7: 0	64Kbps / 51.2ms ▼

Apply

The page includes the following fields:

Object	Description
Group	Display Group A and Group B.
Queue Mode	Select the Queue Mode for QoS. Selections include: First-In-First-Out WRR/WFQ/Bwassurance/Bwlimit/TWRR SPx1 WRR/WFQ/Bwassurance/Bwlimit/TWRRx7 SPx2 WRR/WFQ/Bwassurance/Bwlimit/TWRRx6 SPx4 WRR/WFQ/Bwassurance/Bwlimit/TWRRx4 SPx8
Queue Method	Select the Queue Method for QoS. Selections include: WRR : Configure the priority ratio of each Queue, using the number of packets as measuring unit WFQ : Configure the weight ratio of each Queue. 4096 Bytes is the measuring unit Bwassurance : Dynamic Bandwidth Management. Configure the bandwidth and its maximum value of each Queue. The bandwidth specification method is Queue Ratio x BW throttle period, when Queue bandwidth reaches its bandwidth setting, excessive bandwidth continues to increase to maximum bandwidth. Bwlimit : Static Bandwidth Management. Configure the maximum bandwidth of each Queue. The bandwidth specification method is Queue Ratio x BW

Object	Description
	throttle period. TWRR : Configure the transmission cycle of each Queue. Its cycle specification method should be Queue Ratio x TWRR tickle unit
Queue Ratio (0-255)	Set priority for each mode. The available range is 0-255.
Queue Maximum Bandwidth (0-255)	Set the maximum bandwidth under Bwassurance method. The available range is 0-255.
Unit (BW Throttle Period/TWRR Tickle Unit)	Set Queue Ratio Unit for each mode. Selections include: 64Kbps/51.2ms 1Mbps/3.1ms 2Mbps/1.55ms 4Mbps/0.82ms

Buttons

- Click **Apply** to apply changes.

QoS out queue aging

Configure QoS out queue aging settings on this page.

QoS Out Queue Aging

Aging Time

Out Queue Aging Time : (1~2)*0 *100ms. (The Value Range is 0-255)

☐ Fast Aging Time Enable (Unit: 1.638ms)

Apply

QoS Out Queue Aging

Port Selection												
1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Q0

Q1

Q2

Q3

Q4

Q5

Q6

Q7

Apply

Port No.	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
01								
02								
03								
04								
05								
06								
07								
08								

The page includes the following fields:

Object	Description
Out Queue Aging Time	Set Out Queue Aging time. The available range is 0-255.
Fast Aging Time Enable	Set the conversion unit of aging time from 100 ms to 1.638 ms.
Port Selection	Select a specific port for QoS Out Queue Aging settings.
Q0 ~ Q7	Enable or disable the QoS Out Queue Aging settings.
Port No.	Per port list.
Q0-Q7	Per port QoS Out Queue Aging settings.

Buttons

- Click **Apply** to apply changes.

QoS remap

Configure QoS remap settings on this page.

QoS Remap

Port Selection												
1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Mode

Q0
Q1
Q2
Q3
Q4
Q5
Q6
Q7

Tx&Rx
--
--
--
--
--
--
--

Apply

Port No.	Tx Remap								Rx Remap							
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
01	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
02	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
03	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
04	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
05	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
06	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
07	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
08	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7

The page includes the following fields:

Object	Description
Port Selection	Select a specific port for QoS Remap settings.
Mode	Set the operation mode for a specific port. Selections include: Tx&Rx Tx

Object	Description
	Rx
Q0 ~Q7	Set each queue to the queue number of QoS Remap.
Port No.	Per port list.
TX Remap Q0-Q7	Per port queue number of Q0 to Q7 from TX Remap.
RX Remap Q0-Q7	Per port queue number of Q0 to Q7 from RX Remap.

Buttons

- Click **Apply** to apply changes.

Class of service

Configure and view class of service settings for all switch ports on this page.

Class of Service

Port Selection

1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

ACL

IGMP

IP Addr

MAC Addr

VID

TCP/UDP Port

DSCP

802.1p

Physical Port

Apply

Port No.	ACL	IGMP	IP Addr	MAC Addr	VID	TCP/UDP Port	DSCP	802.1p	Physical Port
01									Queue0
02									Queue0
03									Queue0
04									Queue0
05									Queue0
06									Queue0
07									Queue0
08									Queue0

The page includes the following fields:

Object	Description
Port Selection	Select a specific port for QoS Class of Service settings.
ACL	Enable or disable the ACL function for a specific port.
IGMP	Enable or disable the IGMP function for a specific port.
IP Addr	Enable or disable the IP Address function for a specific port.
MAC Addr	Enable or disable the MAC Address function for a specific port.
VID	Enable or disable the VID function for a specific port.

Object	Description
TCP/UDP Port	Enable or disable the TCP/UDP Port function for a specific port.
DSCP	Enable or disable the DSCP function for a specific port.
802.1p	Enable or disable the 802.1p function for a specific port.
Physical Port	Select Queue ratio for a specific port. The available range is Queue0-Queue7.
Port No.	Per port list.

Buttons

- Click **Apply** to apply changes.

802.1p-based QoS

Configure 802.1p-based QoS settings on this page.

802.1p Base QoS

☐ Earlier Edition
 ☒ 2005 Edition
 ☐ Exchange the priority of 3'b000 and 3'b001 for 2005 Edition

Priority Field	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
Earlier Edition	2	0	1	3	4	5	6	7
2005 Edition	1	0	2	3	4	5	6	7

Apply

The page includes the following fields:

Object	Description
Earlier Edition	Click to select the Earlier Edition for 802.1p-based QoS.
2005 Edition	Click to select the 2005 Edition for 802.1p-based QoS.
Exchange the priority of 3'b001 for 2005 Edition	Click to Exchange the priority of 3'b001 for 2005 Edition for 802.1p-based QoS.
Priority Field	Display the priority field of Q0 to Q7.
Earlier Edition	Display the earlier edition for 802.1p-based QoS.
2005 Edition	Display the 2005 edition for 802.1p-based QoS.

Buttons

- Click **Apply** to apply changes.

DSCP-based priority

Configure DSCP-based priority settings on this page.

DSCP Base Priority

Priority For DSCP Not Match

☒ Regard as low priority (priority 0)
☐ Ignore IP priority (priority will according to tag/port)

Apply

IP ToS/DSCP CoS Base Priority

DSCP List: DSCP1 ▼
Value(0-63):
Priority: Q0 ▼

Apply

List	Value	Priority
DSCP1	0	Queue7
DSCP2	0	Queue7
DSCP3	0	Queue7
DSCP4	0	Queue7
DSCP5	0	Queue7
DSCP6	0	Queue7
DSCP7	0	Queue7
DSCP8	0	Queue7

The page includes the following fields:

Object	Description
Priority For DSCP Not Match	Selections include: Regard as low priority (priority 0) Ignore IP priority (priority will according to tag/port)
IP ToS/DSCP CoS Base Priority	Selections include: DSCP List: provide DSCP1 to DSCP8 options to choose. Value(0-63): allow input the value range from 0 to 63. Priority: provide Q0 to Q7 options to choose.
List	Displays DSCP1 to DSCP8.
Value	Displays the value setting of per DSCP1 to DSCP8.
Priority	Displays the priority setting of per DSCP1 to DSCP8.

Buttons

- Click **Apply** to apply changes.

TCP/UDP port-based QoS

Configure TCP/UDP port-based QoS settings on this page.

TCP/UDP Port Base QoS							
TCP/UDP Port Base Priority							
NOTE: (1)Q0~Q7 options are effective for the selected physical port only. (2)"Drop" option is the global setting for all physical ports. (3)"BOOTP/DHCP" is not effective when DHCP relay agent enabled.							
Protocol	Priority	Protocol	Priority	Protocol	Priority	Protocol	Priority
FTP	Q0 ▼	SSH	Q0 ▼	TELNET	Q0 ▼	SMTP	Q0 ▼
DNS	Q0 ▼	BOOTP/DHCP	Q0 ▼	TFTP	Q0 ▼	HTTP_0,1	Q0 ▼
POP3	Q0 ▼	NEWS	Q0 ▼	SNTP	Q0 ▼	NETBIOS_0,1,2	Q0 ▼
IMAP_0,1	Q0 ▼	SNMP_0,1	Q0 ▼	HTTPS	Q0 ▼	User Defined A	Q0 ▼
User Defined B	Q0 ▼	User Defined C	Q0 ▼	User Defined D	Q0 ▼		
User Define TCP/UDP Port Number							
NOTE: These User-Defined TCP/UDP port are the same as that used in TCP/UDP filter.							
User Defined A	User Defined B	User Defined C	User Defined D				
Port: 1	Port: 1	From Port: 1 To Port: 1	From Port: 1 To Port: 1				
Apply							

The page includes the following fields:

Object	Description
TCP/UDP Port-based Priority	Provides Q0 to Q7 and Drop options for the following protocols: FTP/SSH/TELNET/SMTP/DNS/BOOTP/DHCP/TFTP/HTTP_0.1/POP3/NEWS/SNTP/NETBIOS_0.1.2/IMAP_0.1/SNMP_0.1/HTTPS/User Defined A/ User Defined B/User Defined C/User Defined D.
User Defined TCP/UDP Port Number	Type port numbers in the following boxes: User Defined A (Port #) User Defined B (Port #) User Defined C (From Port# To Port#) User Defined D (From Port# To Port#)

Buttons

- Click **Apply** to apply changes.

Access Control Lists (ACL)

ACL is an acronym for Access Control List. It is the list table of ACEs containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine if there are specific traffic object access rights.

ACL implementations can be quite complex (as when the ACEs are prioritized for various situations). In networking, the ACL refers to a list of service ports or network

services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACLs can generally be configured to control inbound traffic and, in this context, they are similar to firewalls.

ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual applications.

ACL configuration

ACL Profile List	Configure and display ACL Profile List configuration settings on this page.
ACL Ctag Settings	Configure and display ACL Ctag Settings configuration settings on this page.
ACL Stag Settings	Configure and display ACL Stag Settings configuration settings on this page.
ACL VLAN Settings	Configure and display ACL VLAN Settings configuration settings on this page.
ACL Bandwidth Settings	Configure and display ACL Bandwidth Settings configuration settings on this page.
ACL DSCP Settings	Configure and display ACL DSCP Settings configuration settings on this page.

ACL profile list

Configure the ACL profile list on this page.

ACL Profile List

Used Entries : 0 / 128

Profile Name

Type

MAC ▼

Add

Profile Name	Type	Action	
MAC	mac	Edit	Delete
IP	ip	Edit	Delete
IPExt	ip_ext	Edit	Delete
IPv6	ipv6	Edit	Delete
Advanced	advanced	Edit	Delete

The page includes the following fields:

Object	Description
User Entries	The amount of entry occupied by rules set up successfully, with a maximum of 128. It is not a rule that takes up an entry; the number of entry occupied as a rule is automatically calculated according to the setting.
Profile Name	Display and configure the name of a specific ACL Profile; the maximum length is 20 characters.
Type	Indicates the frame type of the ACL Profile. Selections include: MAC : The ACL will match the MAC address. IP : The ACL will match all IPv4 frames. IP_Ext : The ACL will match all IPv4 frames with VID/CoS/TCP Flag/ DSCP/IP protocol. IPv6 : The ACL will match all IPv6 standard frames. Advanced : The ACL will match all MAC address and IPv4 frames with VID/CoS/TCP Flag/ DSCP/IP protocol.
Conflict	Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations. Click Edit to edit the specific ACL Profile. Click Delete to delete the specific ACL Profile.

Buttons

- Click **Add** to complete the add ACL profile procedure.
- Click **Edit** to edit the specific ACL profile.
- Click **Delete** to delete the specific ACL profile.

MAC

The ACL configuration includes a MAC address-based function.

Name		MAC
☐	Source MAC Address	(22:55:66:AA:BB:cc)
	Source MAC Mask	FF:FF:FF:FF:FF:FF ▼
☐	Destination MAC Address	(22:55:66:AA:BB:cc)
	Destination MAC Mask	FF:FF:FF:FF:FF:FF ▼
☐	VID	(1 ~ 4094)
☐	CoS	(0 ~ 7, VID should enabled)
☐	Ethernet Type	0x (0000 ~ FFFF, hexadecimal value)
☐	Ingress Port	Port1 ▼
Action Drop ▼		

The page includes the following fields:

Object	Description
Name	Display the ACL profile name.
Source MAC Address	Configure the Source MAC Address.
Source MAC Mask	Configure the Source MAC Mask. Selections include: FF:FF:FF:FF:FF:FF FF:FF:FF:00:00:00 FF:FF:00:00:00:00
Destination MAC Address	Configure the Destination MAC Address.
Destination MAC Mask	Configure the Destination MAC Mask. Selections include: FF:FF:FF:FF:FF:FF FF:FF:FF:00:00:00 FF:FF:00:00:00:00
VID	Configure the VID and the available range is 1-4094.
CoS	Configure the CoS and the available range is 0-7.
Ethernet Type	Configure the Ethernet Type.
Ingress Port	Select a specific port as the Ingress port.
Action	Select the action. Selections include: Drop Type 1 Type 2

Buttons

- Click **Apply** to apply changes.

Action Drop

Action	Drop ▼
--------	--------

Action Type 1

Action	Type1 ▼	☐	Redirect	Port 1 ▼
		☐	Priority	(0 ~ 7)
		☐	DSCP	(1 ~ 8, index select)
		☐ Copy to CPU		
		☐ Mirror Enable		

Action Type 2

Action	Type2 ▼	☐	Redirect	Port 1 ▼
		☐	Priority	(0 ~ 7)
		☐	Bandwidth	(1 ~ 15, index select)
		☐ Copy to CPU		
		☐ PTP Enable		
		☐ Sflow Enable		

Object	Description
Redirect	Configure redirect to a Port
Priority	Configure Priority. The available range is 0-7.
DSCP	Configure the DSCP Index and edit the sent DSCP according to ACL DSCP settings.
Bandwidth	Configure Bandwidth Index according to the value configured by ACL Bandwidth Settings to restrict the packets traffic
Copy to CPU	Made a copy and send to CPU.
PTP Enable	Configure the time when packets records is enabled.
Sflow Enable	Configure to enable the Sflow function.

IP

The ACL configuration includes an IP address-based function.

ACL Profile Configuration - IP

Name		IP	
☐	Source IP Address		(192.168.0.1)
☐	Source IP Mask	255.255.255.255 ▼	
☐	Source Port Range	Low:	(0 ~ 65535) High:
☐	Destination Port Range	Low:	(0 ~ 65535) High:
☐	Ingress Port	Port1 ▼	
Action		Drop ▼	

Apply

The page includes the following fields:

Object	Description
Name	Display the ACL profile name.
Source IP Address	Configure the Source IP Address.
Source IP Mask	Configure the Source IP Mask. Selections include: 255:255:255:255 255:255:255:240 255:255:255:0 255:255:240:0 255.255:0:0 255.0.0.0 240.0.0.0
Source Port Range	Configure the Source Port Range of Low and High.
Destination Port Range	Configure the Destination Port Range of Low and High.
Ingress Port	Select a specific port as an Ingress port.
Action	Select the action. Selections include:

Object	Description
	Drop
	Type 1
	Type 2

Buttons

- Click **Apply** to apply changes.

IP_EXT

The ACL configuration includes an IP address extension-based function.

ACL Profile Configuration - IP Extension

	Name	IPExt
☐	Source IP Address	(192.168.0.1)
	Source IP Mask	255.255.255.255 ▼
☐	Destination IP Address	(192.168.0.1)
	Destination IP Mask	255.255.255.255 ▼
☐	Source Port	☐ (0 ~ 65535) ☐ Low: (0 ~ 65535) High: (0 ~ 65535)
☐	Destination Port	☐ (0 ~ 65535) ☐ Low: (0 ~ 65535) High: (0 ~ 65535)
☐	VID	(1 ~ 4094)
☐	CoS	(0 ~ 7, VID should enabled)
☐	TCP Flag	☐ URG ☐ ACK ☐ PSH ☐ RST ☐ SYN ☐ FIN ☐ 0 ☐ 0 ☐ 0 ☐ 0 ☐ 0 ☐ 0 ☐ 1 ☐ 1 ☐ 1 ☐ 1 ☐ 1 ☐ 1
☐	DSCP	(0 ~ 63)
☐	IP Protocol	0x (00 ~ FF)
☐	Ingress Port	Port1 ▼
	Action	Drop ▼

Apply

The page includes the following fields:

Object	Description
Name	Display the ACL profile name.
Source IP Address	Configure the Source IP Address.
Source IP Mask	Configure the Source IP Mask. Selections include: 255:255:255:255 255:255:255:240 255:255:255:0 255:255:240:0 255.255:0:0 255.0.0.0 240.0.0.0

Object	Description
Destination IP Address	Configure the Destination IP Address.
Destination IP Mask	Configure the Destination IP Mask. Selections include: 255:255:255:255 255:255:255:240 255:255:255:0 255:255:240:0 255.255:0:0 255.0.0.0 240.0.0.0
Source Port	Configure the Source Port of Low and High.
Destination Port	Configure the Destination Port of Low and High.
VID	Configure the VID and the available range is 1-4094.
CoS	Configure the CoS and the vailable range is 0-7.
TCP Flag	Configure the TCP Flag. Selections include: URG/0/1 ACK/0/1 PSH/0/1 RST/0/1 SYN/0/1 FIN/0/1
DSCP	Configure the DSCP. The available range is 0-63.
IP Protocol	Configure the IP Protocol.
Ingress Port	Select a specific port as an Ingress port.
Action	Select the action. Selections include: Drop Type 1 Type 2

Buttons

- Click **Apply** to apply changes.

IPv6

The ACL configuration includes an IPv6 address -based function.

ACL Profile Configuration - IPv6

Name		IPv6
☐	Source IPv6 Address	AAAA:::DDDD (AAAA:::DDDD)
	Source IPv6 Mask	FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF (FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF) ▼
☐	Destination IPv6 Address	AAAA:::DDDD (AAAA:::DDDD)
	Destination IPv6 Mask	FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF (FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF) ▼
☐	Ingress Port	Port1 Port1 ▼
Action Drop Drop ▼		

Apply

The page includes the following fields:

Object	Description
Name	Display the ACL profile name.
Source IPv6 Address	Configure the Source IPv6 Address.
Source IP Mask	Configure the Source IPv6 Mask. Selections include: FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:0000:0000 FFFF:FFFF:FFFF:0000:0000:0000:0000:0000 FFFF:0000:0000:0000:0000:0000:0000:0000
Destination IPv6 Address	Configure the Destination IPv6 Address.
Destination IP Mask	Configure the Destination IPv6 Mask. Selections include: FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:0000:0000 FFFF:FFFF:FFFF:0000:0000:0000:0000:0000 FFFF:0000:0000:0000:0000:0000:0000:0000
Ingress Port	Select a specific port as an Ingress port.
Action	Select the action. Selections include: Drop Type 1 Type 2

Buttons

- Click **Apply** to apply changes.

Advanced

The ACL configuration includes an IPv6 address advanced-based function.

Name		Advanced	
☐	Source MAC Address		(22:55:66:AA:BB:cc)
	Source MAC Mask		FF:FF:FF:FF:FF:FF ▼
☐	Destination MAC Address		(22:55:66:AA:BB:cc)
	Destination MAC Mask		FF:FF:FF:FF:FF:FF ▼
☐	Source IP Address		(192.168.0.1)
	Source IP Mask		255.255.255.255 ▼
☐	Destination IP Address		(192.168.0.1)
	Destination IP Mask		255.255.255.255 ▼
☐	Source Port	☐ (0 ~ 65535) ☐ Low: (0 ~ 65535) High: (0 ~ 65535)	
☐	Destination Port	☐ (0 ~ 65535) ☐ Low: (0 ~ 65535) High: (0 ~ 65535)	
☐	VID		(1 ~ 4094)
☐	CoS		(0 ~ 7, VID should enabled)
☐	Ethernet Type	0x	(0000 ~ FFFF, hexadecimal value)
☐	TCP Flag	☐ URG ☐ ACK ☐ PSH ☐ RST ☐ SYN ☐ FIN ☐ 0 ☐ 0 ☐ 0 ☐ 0 ☐ 0 ☐ 0 ☐ 1 ☐ 1 ☐ 1 ☐ 1 ☐ 1 ☐ 1	
☐	DSCP		(0 ~ 63)
☐	IP Protocol	0x	(00 ~ FF)
☐	Ingress Port	Port1 ▼	
Action		Drop ▼	

The page includes the following fields:

Object	Description
Name	Display the ACL profile name.
Source MAC Address	Configure the Source MAC Address.
Source MAC Mask	Configure the Source MAC Mask. Selections include: FF:FF:FF:FF:FF:FF FF:FF:FF:00:00:00 FF:FF:00:00:00:00
Destination MAC Address	Configure the Destination MAC Address.
Destination MAC Mask	Configure the Destination MAC Mask. Selections include: FF:FF:FF:FF:FF:FF FF:FF:FF:00:00:00 FF:FF:00:00:00:00
Source IP Address	Configure the Source IP Address.
Source IP Mask	Configure the Source IP Mask. Selections include: 255:255:255:255 255:255:255:240

Object	Description
	255:255:255:0 255:255:240:0 255.255:0:0 255.0.0.0 240.0.0.0
Destination IP Address	Configure the Destination IP Address.
Destination IP Mask	Configure the Destination IP Mask. Selections include: 255:255:255:255 255:255:255:240 255:255:255:0 255:255:240:0 255.255:0:0 255.0.0.0 240.0.0.0
Source Port	Configure the Source Port of Low and High.
Destination Port	Configure the Destination Port of Low and High.
VID	Configure the VID and the available range is 1-4094.
CoS	Configure the CoS and the vailable range is 0-7.
Ethernet Port	Configure the Ethernet Type.
TCP Flag	Configure the TCP Flag. Selections include: URG/0/1 ACK/0/1 PSH/0/1 RST/0/1 SYN/0/1 FIN/0/1
DSCP	Configure the DSCP. The available range is 0-63.
IP Protocol	Configure the IP Protocol.
Ingress Port	Select a specific port as an Ingress port.
Action	Select the action. Selections include: Drop Type 1 Type 2 Type 3 Type 4

Buttons

- Click **Apply** to apply changes.

ACL Ctag settings

Configure the ACL Ctag settings on this page.

ACL Ctag Settings

Index

(1 ~ 24)

Value

0x

(0x0000~0x7FFF)

Apply

Index	Value	Index	Value
1	0x0000	13	0x0000
2	0x0000	14	0x0000
3	0x0000	15	0x0000
4	0x0000	16	0x0000
5	0x0000	17	0x0000
6	0x0000	18	0x0000
7	0x0000	19	0x0000
8	0x0000	20	0x0000
9	0x0000	21	0x0000
10	0x0000	22	0x0000
11	0x0000	23	0x0000
12	0x0000	24	0x0000

The page includes the following fields:

Object	Description
Index	Select a specific index for ACL Ctag settings. The available range is 1 to 24.
Value	Configure and indicate per index value of the ACL Ctag settings. The value must be hexadecimal and the available range is 0x0000 to 0x7FFF.

Buttons

- Click **Apply** to apply changes.

ACL Stag settings

Configure the ACL Stag settings on this page.

ACL Stag Settings

Index

(1 ~ 24)

Value

0x

(0x0000~0xFFFF)

Apply

Index	Value	Index	Value
1	0x0000	13	0x0000
2	0x0000	14	0x0000
3	0x0000	15	0x0000
4	0x0000	16	0x0000
5	0x0000	17	0x0000
6	0x0000	18	0x0000
7	0x0000	19	0x0000
8	0x0000	20	0x0000
9	0x0000	21	0x0000
10	0x0000	22	0x0000
11	0x0000	23	0x0000
12	0x0000	24	0x0000

The page includes the following fields:

Object	Description
Index	Select a specific index for ACL Stag settings. The available range is 1 to 24 .
Value	Configure and indicate per index value of the ACL Stag settings. The value must be hexadecimal and the available range is 0x0000 to 0x7FFF.

Buttons

- Click **Apply** to apply changes.

ACL VLAN settings

Configure the ACL VLAN settings on this page.

ACL VLAN Settings

Index

1

Member Port

1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Apply

Index	Member Port	Index	Member Port
1		13	
2		14	
3		15	
4		16	
5		17	
6		18	
7		19	
8		20	
9		21	
10		22	
11		23	
12		24	

The page includes the following fields:

Object	Description
Index	Select a specific index for ACL VLAN settings. The available range is 1 to 24 .
Member Port	Configure and indicate per index member port of the ACL VLAN settings.

Buttons

- Click **Apply** to apply changes.

ACL bandwidth settings

Configure the ACL bandwidth settings on this page.

ACL Bandwidth Settings

Index (1 ~ 15)
Value (0~2540)(0.1Mbps)

Index	Value
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0

The page includes the following fields:

Object	Description
Index	Select a specific index for ACL bandwidth settings. The available range is 1 to 15 .
Value	Configure and indicate per index value of the ACL bandwidth settings. The available range is 0 to 2540.

Buttons

- Click **Apply** to apply changes.

ACL DSCP settings

Configure the ACL DSCP settings on this page.

ACL DSCP Settings

Index

(1 ~ 8)

Value

0x

(0x0~0x3F)

Apply

Index	Value
1	0x00
2	0x00
3	0x00
4	0x00
5	0x00
6	0x00
7	0x00
8	0x00

The page includes the following fields:

Object	Description
Index	Select a specific index for ACL DSCP settings. The available range is 1 to 8.
Value	Configure and indicate per index value of the ACL DSCP settings. The available range is 0x0 to 0x3F.

Buttons

- Click **Apply** to apply changes.

Security

This section describes how to control access to the managed switch and contains the following main topics:

- Access Security
- Port-MAC-IP Binding
- MAC Address Binding

Access security

Configure the ACL security settings on this page. All settings are enabled by default.

Access Security Setting			
Configuration Selection			
SSH	Telnet	HTTPS	HTTP
☒	☒	☒	☒

Apply

The page includes the following fields:

Object	Description
SSH	Enable or disable the SSH function.
Telnet	Enable or disable the Telnet function.
HTTPS	Enable or disable the HTTPS function.
HTTP	Enable or disable the HTTP function.

Buttons

- Click **Apply** to apply changes.

Port-MAC-IP binding

The Port-MAC-IP Binding configuration provides basic security protection and filtering by checking the source IP address of the packet. Each port can be configured on this page to check if the source IP address and the source port match. The matching packets are affected by the two filtering modes selected.

The Port-MAC-IP Binding configuration includes the Port-MAC-IP Port Setting, Port-MAC-IP Entry Setting, and DHCP Snooping Entry Setting.

Port-MAC-IP port setting

Configure the Port-MAC-IP port settings on this page.

Port-MAC-IP Port Setting

IMP Ports Configure

Port Selection												
1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Status Disable ▾
All Clear

Max. Learning Entry 1 ▾

Recovery Learning Entry Disable ▾
Apply

Port Status

Port	State	Max. Learning Entry	Recovery Learning Entry
01	Disabled	3	Disabled
02	Disabled	3	Disabled
03	Disabled	3	Disabled
04	Disabled	3	Disabled
05	Disabled	3	Disabled
06	Disabled	3	Disabled
07	Disabled	3	Disabled
08	Disabled	3	Disabled

The page includes the following fields:

Object	Description
Port Selection	Select a specific port for Port-MAC-IP Port settings.
Status	Enable or disable the Port-MAC-IP Port setting. The default mode is disabled.
Max. Learning Entry	Select the maximum number of dynamic binding groups for each port. The available range is 1 to 3.
Recovery Learning Entry	Enable or disable automatically overrides the earliest bound group when the number of dynamically bound groups reaches the upper limit. The default mode is Disable .
Port Status	
Port	The per port list.
State	The per port current operation mode.
Max. Learning Entry	The per port maximum number of Max. Learning Entry function.
Recovery Learning Entry	The per port current operation mode of Recovery Learning Entry function.

Buttons

- Click **Apply** to apply changes.
- Click **All** to select all ports.

- Click **Clear** to clear all ports.

Port-MAC-IP entry setting

Configure the Port-MAC-IP entry settings on this page.

The page includes the following fields:

Object	Description
Create IMP Entry	Select IPv4 or IPv6 and type the IPv4 or IPv6 IP address in the box.
IMP Entry Management	
IP	The IMP Entry IP Address.
Check Port	Enable or disable the check source port compliance.
Port	Select the port for this IP address.
Check MAC	This column provides configuring enable or disable the check source MAC compliance.
MAC	Type the corresponding source MAC for this IP address into the box.
Action	Select the corresponding action filter / priority when the condition is met.
Priority	Configure the queue for this IMP Entry when the action is selected as priority. The available range is 0 to 7.
IP Table Monitor	
IP	The IPv4 or IPv6 address.
Type	The type information.
Port	The port information.
MAC	The MAC information.
Action	The Action status.
Priority	The priority status.

Object	Description
Action	Click Edit to edit a specific Port-MAC-IP Entry setting. Click Delete to delete a Port-MAC-IP Entry setting.

Buttons

- Click **Apply** to apply changes.

DHCP snooping entry setting

Configure the DHCP snooping entry settings on this page.

DHCP Snooping Entry Setting

DHCP Snooping Configure

DHCP Snooping: Disable ▾

ARP Inspection: Disable ▾

MAC Verification: Disable ▾ Apply

Snooping Table

Port	IP	MAC	Leave Time	Action
------	----	-----	------------	--------

The page includes the following fields:

Object	Description
DHCP Snooping Configure	
DHCP Snooping	Enable or disable the DHCP snooping function. DHCP Snooping is used to block intruders on the untrusted ports of DUT when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.
ARP Inspection	Enable or disable the ARP inspection function. ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through DUT.
MAC Verification	Enable or disable the MAC verification function.
Snooping Table	
Port	The port information.
IP	The IPv4 or IPv6 address.
MAC	The MAC information.
Leave Time	The leave time information.
Action	Click Edit to edit a specific DHCP snooping entry setting. Click Delete to delete a DHCP snooping entry setting.

Buttons

- Click **Apply** to apply changes.

MAC address binding

The MAC Address Binding configuration page provides a MAC address-based security function. When this function is enabled, the port discards packets that do not conform to the MAC table, or discards a specific MAC address, mirror forwarding, and sampling to the CPU port and other activities.

Only when the port learning function is disabled can the MAC address in the non-MAC table be effectively prevented from entering the device by the port it binds. Without the broadcast port learning function, only the MAC address existing in the MAC table can be limited to enter the device by its bound port. The MAC address in the non-MAC table cannot be assigned to any port.

Configure MAC address binding on this page.

MAC Address Binding

MAC Table Binding

Port Selection												
1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Binding Enable

☐

Aging Time

300

Range:1~1,800,000. (Unit: second)

All

Clear

Re-Dynamic

Apply

Create MAC Entry

MAC Address

Port

1 ▼

Apply

MAC Entry Management

MAC

Drop

☐

Port

1 ▼

Sniffer

☐

Priority

Disable ▼

Sflow

☐

Apply

MAC Table Monitor

Entry number: 0

MAC	State	Port	Drop	Sniffer	Sflow	Priority	Action
			☐	☐	☐		Edit Delete

The page includes the following fields:

Object	Description
MAC Table Binding	
Port Selection	Select a specific port for MAC Address Binding settings.
Binding Enable	Select to enable the MAC Binding function.
Aging Time	Type the aging time for the MAC address table refresh into this box. The default aging time is 300 seconds. The available range is 1 to 1800000 seconds.
MAC Entry Creation	

Object	Description
MAC	The MAC address for a specific port.
Port	Select the port for the MAC address.
MAC Entry Management	
MAC	Display the MAC information.
Port	Select a specific port for MAC Address Binding settings.
Priority	Select a specific priority for MAC Address Binding settings. The default is Disable and selections range from 0 to 7 .
Drop	Select to enable the Drop function. When the Source MAC of packets received by the port meets the setting, drop these packets.
Sniffer	Select to enable the Sniffer function. When the Source MAC of packets received by the port meets the setting, forward these packets to the Destination Port of Port Mirror.
Sflow	Select to enable the Sflow function. Sampling transmits the matched packets to CPU ports.
MAC Table Monitor	
Entry Number	The MAC Address Binding entry number information.
MAC	The MAC information.
State	The MAC Address state information.
Port	The Port information.
Drop	The Drop status information.
Sniffer	The Sniffer status information.
Sflow	The Sflow status information.
Priority	The priority status.
Action	Click Edit to edit a specific MAC address binding setting. Click Delete to delete a MAC address binding setting.

Buttons

- Click **Apply** to apply changes.
- Click **All** to select all ports.
- Click **Re-Dynamic** to apply the re-dynamic function.
- Click **Clear** to clear all ports.

LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities,

and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

LLDP global setting

Configure the LLDP global settings on this page.

The page includes the following fields:

Object	Description
LLDP State	Enable or disable the LLDP function.
Tx Interval	The switch periodically transmits LLDP frames to its neighbors so that 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. Default: 30 seconds This attribute must comply with the following rule: $(\text{Transmission Interval} * \text{Hold Time Multiplier}) \leq 65536$, and $\text{Transmission Interval} \geq (4 * \text{Delay Interval})$
Tx Hold Multiplier	Each LLDP frame contains information about how long 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. TTL in seconds is based on the following rule: $(\text{Transmission Interval} * \text{Holdtime Multiplier}) \leq 65536$. Therefore, the default TTL is $4 * 30 = 120$ seconds.
Re-Init Delay	When a port 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 is no longer valid. Re-Init Delay controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.
Tx Delay	If a 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. This attribute must comply with the rule: $(4 * \text{Delay Interval}) \leq \text{Transmission Interval}$

Buttons

- Click **Apply** to apply changes.

LLDP port setting

Configure the LLDP port settings on this page.

LLDP Port Setting

Port Selection												
1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Admin Status
Port Description
System Name
System Description
Capability
Management Address

----- ▼

----- ▼

----- ▼

----- ▼

----- ▼

----- ▼

Apply

Port	Admin Status	Port Description	System Name	System Description	Capability	Management Address
01	Tx & Rx	Disable	Disable	Disable	Disable	Disable
02	Tx & Rx	Disable	Disable	Disable	Disable	Disable
03	Tx & Rx	Disable	Disable	Disable	Disable	Disable
04	Tx & Rx	Disable	Disable	Disable	Disable	Disable
05	Tx & Rx	Disable	Disable	Disable	Disable	Disable
06	Tx & Rx	Disable	Disable	Disable	Disable	Disable
07	Tx & Rx	Disable	Disable	Disable	Disable	Disable
08	Tx & Rx	Disable	Disable	Disable	Disable	Disable
09	Tx & Rx	Disable	Disable	Disable	Disable	Disable
10	Tx & Rx	Disable	Disable	Disable	Disable	Disable

Refresh

The page includes the following fields:

Object	Description
Port Selection	Select a specific port for LLDP port settings.
Admin Status	Select LLDP admin status. Disable The switch will not send out LLDP information, and will drop LLDP information received from neighbors. 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, and will send out LLDP information. TX & Rx The switch will send out LLDP information, and will analyze LLDP information received from neighbors.
Port Description	When enabled, the "port description" is included in LLDP information transmitted.
System Name	When enabled, the "system name" is included in LLDP information transmitted.

Object	Description
System Description	When enabled, the "system description" is included in LLDP information transmitted.
Capability	When enabled, the "system capability" is included in LLDP information transmitted.
Management Address	When enabled, the "management address" is included in LLDP information transmitted.
Port	The per port list.

Buttons

- Click **Apply** to apply changes.
- Click **Refresh** to refresh the page.

Voice VLAN settings

Voice VLAN settings enable voice traffic forwarding on the Voice VLAN, permitting the switch to classify and schedule network traffic. We recommended that there be two VLANs on a port – one for voice and one for data.

Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

This section describes the following pages:

- Voice VLAN State
- Voice VLAN Port Setting
- OUI List

Voice VLAN state

Configure the voice VLAN state settings on this page.

The page includes the following fields:

Object	Description
State	Selections include: Enabled: Enable Voice VLAN mode operation. Disabled: Disable Voice VLAN mode operation.

Object	Description
VLAN ID	Type the Voice VLAN ID in this box. The default value is 4080 .
Aging Time	Type a value for Bridge Max Age in this box. The default value is 1440 minutes and the available range is 5 to 43200 minutes.
VLAN Priority	VLAN priority information.

Buttons

- Click **Apply** to apply changes.

Voice VLAN port setting

Configure the voice VLAN port settings on this page.

Voice VLAN Port Setting

Port Selection

1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Mode

----- ▼

Apply

Port	Mode
1	Manual
2	Manual
3	Manual
4	Manual
5	Manual
6	Manual
7	Manual
8	Manual

The page includes the following fields:

Object	Description
Port Selection	Select a specific port for making Voice VLAN port settings.
Mode	Automatically or manually configure Voice VLAN port settings function.
Port	Per port list.
Mode	Per port Voice VLAN operation mode.

Buttons

- Click **Apply** to apply changes.

OUI list

Configure the Voice VLAN OUI settings on this page.

OUI MAC	OUI Mask	Description	Action
---------	----------	-------------	--------

The page includes the following fields:

Object	Description
OUI MAC	Type a value in this box to configure OUI MAC.
OUI Mask	Selections include : FF:FF:FF:FF:FF:FF FF:FF:FF:00:00:00 FF:FF:00:00:00:00
Description	Type a value in this box to configure the OUI MAC address description.
Action	Click Edit to delete a specific OUI List.

Buttons

- Click **Apply** to apply changes.

Advanced features

Advanced feature function can be configured for the managed switch. This section describes the following pages:

- Trunk & Link Aggregation
- DHCP Relay Agent
- Loop Detect
- GVRP
- Neighbor MAC ID Settings

Trunk & link aggregation

Port Aggregation optimizes port usage by linking a group of ports together to form a single Link Aggregated Group (LAG). Port aggregation multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

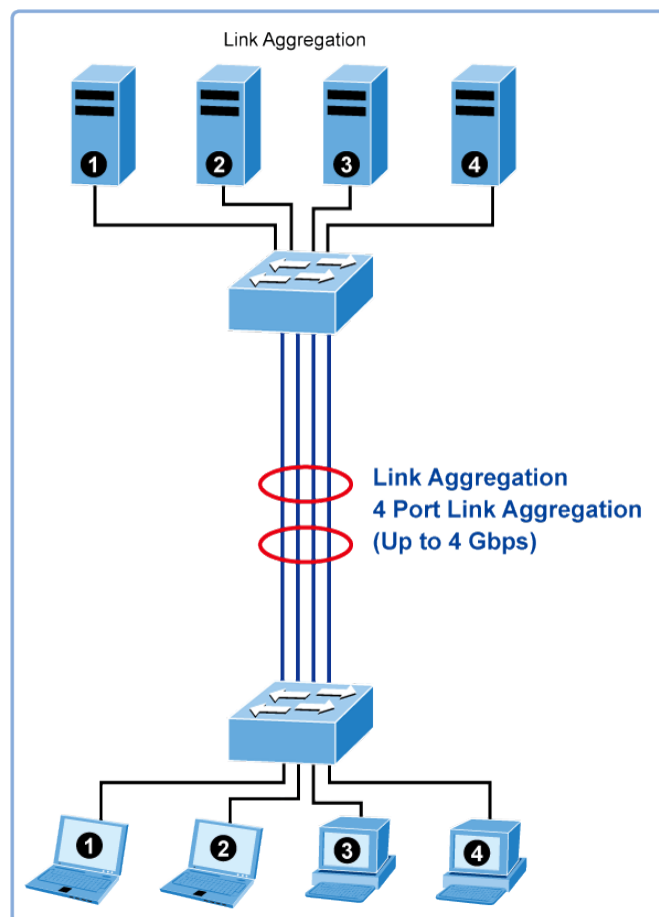
Each LAG is composed of ports of the same speed, set to full-duplex operations. Ports in a LAG can be of different media types (UTP/Fiber, or different fiber types), provided they operate at the same speed.

Aggregated links can be assigned manually (Port Trunk) or automatically by enabling Link Aggregation Control Protocol (LACP) on the relevant links.

Aggregated links are treated by the system as a single logical port. Specifically, the aggregated link has similar port attributes to a non-aggregated port, including auto-negotiation, speed, duplex setting, etc.

The managed switch supports the following aggregation links :

- **Static LAGs (Port Trunk)** – Force aggregated selected ports to be a trunk group.
- **Link Aggregation Control Protocol (LACP) LAGs** – LACP LAGs negotiate aggregated port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.



The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between partner systems that require high speed redundant links. Link aggregation permits grouping up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode (refer to the IEEE 802.3ad standard for further details).

Port link aggregations can be used to increase the bandwidth of a network connection or to ensure fault recovery. Link aggregation permits grouping up to four consecutive

ports into a single dedicated connection between any two managed switches or other Layer 2 switches. However, before making any physical connections between devices, use the link aggregation configuration menu to specify the link aggregation on the devices at both ends. When using a port link aggregation, note that:

- The ports used in a link aggregation must all be of the same media type (RJ45, 100 Mbps fiber).
- The ports that can be assigned to the same link aggregation have certain other restrictions (see below).
 - Ports can only be assigned to one link aggregation.
 - The ports at both ends of a connection must be configured as link aggregation ports.
 - None of the ports in a link aggregation can be configured as a mirror source port or a mirror target port.
 - All of the ports in a link aggregation have to be treated as a whole when moved from/to, added or deleted from a VLAN.
 - The Spanning Tree Protocol will treat all the ports in a link aggregation as a whole.
 - Enable the link aggregation prior to connecting any cable between the switches to avoid creating a data loop.
 - Disconnect all link aggregation port cables or disable the link aggregation ports before removing a port link aggregation to avoid creating a data loop.

It allows a maximum of 10 ports to be aggregated at the same time. The managed switch supports Gigabit Ethernet ports (up to five groups). If the group is defined as a LACP static link aggregation group, then any extra ports selected are placed in a standby mode for redundancy if one of the other ports fails. If the group is defined as a local static link aggregation group, then the number of ports must be the same as the group member ports.

The aggregation code ensures that frames belonging to the same frame flow (for example, a TCP connection) are always forwarded on the same link aggregation member port. Reordering of frames within a flow is therefore not possible. The aggregation code is based on the following information:

- Source MAC
- Destination MAC
- Source and destination IPv4 address.
- Source and destination TCP/UDP ports for IPv4 packets

Normally, all five contributions to the aggregation code should be enabled to obtain the best traffic distribution among the link aggregation member ports. Each link aggregation may consist of up to 10 member ports. Any quantity of link aggregations may be configured for the device (they are only limited by the quantity of ports on the device). To configure a proper traffic distribution, the ports within a link aggregation must use the same link speed.

Configure the trunk & link aggregation settings on this page.

Trunk & Link Aggregation		
Link Aggregation Algorithm	MAC Source ▼	
Group	Group1	
Port	25	26
Link Aggregation State		
State	Enable ▼	
Trunk Type	LACP ▼	
Mode	Active ▼	
Time Out	Short ▼	
Apply		

The page includes the following fields:

Object	Description
Link Aggregation Algorithm	Selections include: Port MAC Source MAC Destination MAC Source Destination IP Source IP Destination TCP/UDP Destination Port TCP/UDP Source Port
Group	Trunk & Link Aggregation group information.
Port Select	The ports selected for Trunk & Link Aggregation.
Status	Trunk & Link Aggregation member port status.
State	Enable or disable the Trunk & Link Aggregation function on a specific port. The default mode is Disable .
Trunk Type	Select the Trunk Type. Selections are Static and LACP (default).
Mode	Select the Trunk mode. Selections are Active and Passive (default).
Time Out	Select the Time Out mode. Selections are Long and Short (default).

Buttons

- Click **Apply** to apply changes.

DHCP relay agent

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server

DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically, the option works by setting two sub-options:

- **Circuit ID (option 1).** This sub-option should include information specific to which circuit the request came in on.
- **Remote ID (option 2).** This sub-option is designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is four bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes representing the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in a standalone switch it always equals 0; in the switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The remote ID is six bytes in length, and the value equals the DHCP relay agent's MAC address.

Configure the DHCP relay agent on this page:

DHCP Relay Agent

Global Setting

DHCP Relay Agent State ☐ Apply

DHCPv4 Setting

Hops Limit

DHCPv4 Server Setting		
Index	State	Address
1	☒	192.168.2.111
2	☐	
3	☐	
4	☐	
5	☐	

Apply

DHCPv6 Setting

DHCPv6 Server Setting		
Index	State	Address
1	☒	2001:1000::1
2	☐	
3	☐	
4	☐	

This page includes the following fields:

Object	Description
Global Setting	
DHCP Relay Agent State	Enable or disable the DHCP Relay Agent function.
DHCPv4 Setting	

Object	Description
Hops Limit	Limit the number of times DHCP packets can be forwarded by typing a value into the Hops Limit box. The available range is 1 to 16.
Index	Per index list (1 to 5).
State	Select to enable or disable the per index function.
Address	Type the DHCPv4 server IP address into the Address box.
DHCPv6 Setting	
Index	Per index list (1 to 5).
State	Select to enable or disable the per index function.
Address	Type the DHCPv6 server IP address into the Address box.

Buttons

- Click **Apply** to apply changes.

Loop detect

The loop detect function provides loop protection to prevent broadcast loops in the managed switch.

Configure loop protection on the Loop Detect page:

Loop Detect

Loop Detect Setting

Loop Detection State

Disable ▾

LDP Interval Time

3

, unit:500ms

Block Release Time

9

, unit:500ms

LDP MAC Destination Address

01:90:C3:00:00:00

Apply

Loop Detect Port Setting

Loop Detect Port Enabled

1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Apply

Loop Detect Port State

Port	State
1	---
2	---
3	---
4	---
5	---

This page includes the following fields:

Object	Description
Loop Detect Setting	
Loop Detection State	Enable or disable the Loop Detection State function.
LDP Interval Time	Type a value in the LDP Interval Time box. The default value is 3 and the available range is 1 to 255. Unit is 500 ms.
Block Release Time	Type a value in the Block Release Time box. The default value is 9 and the available range is 1 to 255. Unit is 500 ms.
LDP MAC Destination Address	Type a value in the LDP MAC Destination Address box if necessary.
Loop Detect Port Setting	
Loop Detect Port Enabled	Select a specific port for Loop Detect Port Enabled settings.
Loop Detect Port State	
Port	Port list.
State	Port Loop Detect Port State.

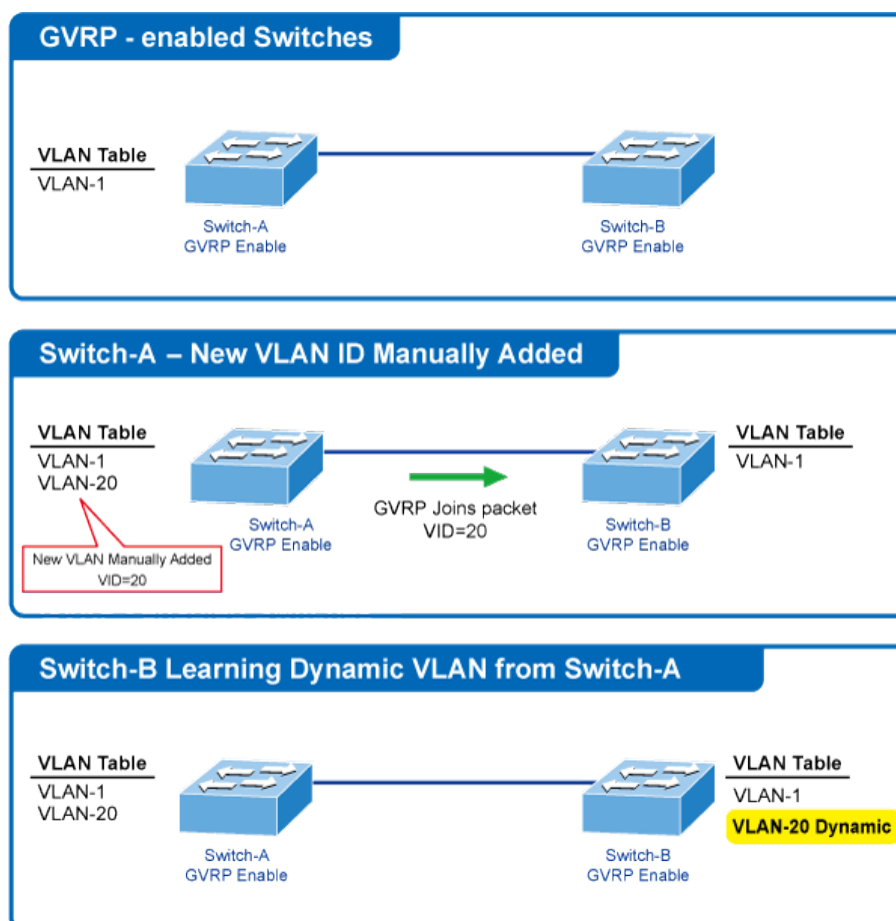
Buttons

- Click **Apply** to apply changes.

GVRP

GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network.

VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.



Configure GVRP settings on this page:

GVRP

GVRP Settings

GVRP Settings: (Dropdown menu)

Join Time: (second, >=2sec)

Leave Time: (second, >=2*Join Time)

Leave All Time: (second, >=Leave Time)

This page includes the following fields:

Object	Description
GVRP Settings	Enable or disable the GVRP function.
Join Time	Type a value for Join Time in this box. The default value is 2. The join time must not be less than 2 seconds.
Leave Time	Type a value for Leave Time in this box. The default value is 6. The leave time must not be less than 2 seconds.
Leave All Time	Type a value for Leave All Time in this box. The default value is 20. The Leave All time must not be less than Leave time.

Buttons

- Click **Apply** to apply changes.

GVRP example

This example demonstrates how switch B can learn VLAN 20 from switch A via GVRP.

1. Enable the GVRP function on switch A and switch B.

GVRP

GVRP Settings

GVRP Settings: (second, >=2sec)

Join Time: (second, >=2*Join Time)

Leave Time: (second, >=2*Join Time)

Leave All Time: (second, >=Leave Time)

2. Set the VLAN mode as Tag VLAN and the tag method as by port on switch A and switch B.

VLAN Mode

VLAN Mode	☒ Tag VLAN ☐ Group VLAN
Tag Method	☐ By Tag ☒ By Port
Egress Frame	☐ Multicast ☐ Unicast ☐ ARP

3. Set VLAN 20 and the VLAN member on switch A.

VLAN Tag-based Entry Config

VLAN Name: VID: Priority: GVRP forward:

VLAN Member													
Port	1	2	3	4	5	6	7	8	9	10	11	12	13
Don't care	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Add	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Remove	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Forbidden	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Not member	☐	☐	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

Port	14	15	16	17	18	19	20	21	22	23	24	25	26
Don't care	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Add	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Remove	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Forbidden	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Not member	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

Switch A has VLAN 20 and port 1 and port 2 are VLAN members.

VLAN Tag-based Entry Config

Name	State	VID	Don't care	Add Tag	Remove Tag	Forbidden	Priority	GVRP Forward	Action
Default	Static	1	1-26	0	0	0	0	Deny	Edit Delete
Protocol_VLAN1	Static	4081	1-26	0	0	0	0	Deny	Edit Delete
Protocol_VLAN2	Static	4082	1-26	0	0	0	0	Deny	Edit Delete
Protocol_VLAN3	Static	4083	1-26	0	0	0	0	Deny	Edit Delete
Protocol_VLAN4	Static	4084	1-26	0	0	0	0	Deny	Edit Delete
Voice-VLAN	Static	4080	0	0	0	0	0	Deny	Edit Delete
GVRP_test	static	20	0	1-2	0	0	0	Allow	Edit Delete

4. Configure the VLAN Port config to enable Port 1 and Port 2 GVRP on switch A and B.

VLAN Port Config

Port Selection

1	2	3	4	5	6	7	8	9	10
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

PVID: Tag: Force: Uplink: Exclusive: Egress: Ingress-check: GVRP: Ingress-frame:

Apply

Port	PVID	Tagging	Force VLAN Group	Uplink	Exclusive	Egress	Ingress Check	GVRP	Ingress Frame
1	1	None					v	v	All
2	1	None					v	v	All
3	1	None					v		All
4	1	None					v		All
5	1	None					v		All
6	1	None					v		All
7	1	None					v		All
8	1	None					v		All

5. Connect port 2 on switch A to port 1 on switch B and switch B will learn VLAN 20 (dynamic).

VLAN Tag-based Entry Config

Add

Name	State	VID	Don't care	Add Tag	Remove Tag	Forbidden	Priority	GVRP Forward	Action
Default	Static	1	1-10	0	0	0	0	Deny	Edit Delete
Protocol_VLAN1	Static	4081	1-10	0	0	0	0	Deny	Edit Delete
Protocol_VLAN2	Static	4082	1-10	0	0	0	0	Deny	Edit Delete
Protocol_VLAN3	Static	4083	1-10	0	0	0	0	Deny	Edit Delete
Protocol_VLAN4	Static	4084	1-10	0	0	0	0	Deny	Edit Delete
Voice-VLAN	Static	4080	0	0	0	0	0	Deny	Edit Delete
	dynamic	20	2	0	0	0	0	Allow	Edit Delete

Neighbor MAC ID settings

Use Neighbor MAC ID Settings to search for switch MAC Address IDs from each port of the managed switch, according to the send period setting for sending out the neighbor information packets. The managed switch adds or updates the MAC Address ID when receiving the neighbor information packets. The switch neighbor MAC address ID information can be obtained by using the UDP NetCMD tools.

Configure Neighbor MAC ID settings on this page:

Neighbor MAC ID Settings

Status:

Send Period:

Aging Time:

Apply

Neighbor MAC ID Information

Refresh

Port No.	MAC Addr	Aging Time
----------	----------	------------

The page includes the following fields:

Object	Description
Status	Enable or disable the Neighbor MAC ID settings function.
Send Period	Type a Send Period value in this box. The default value is 3 and the available range is 1 to 65535. Unit is second.
Aging Time	Type an Aging Time value in this box. The default value is 6 and the available range is 1 to 65535. Unit is second.
Neighbor MAC ID Information	
Port No.	The per port list.
MAC Add	The MAC address from the per port list.
Aging Time	The aging time from the per port list.

Buttons

- Click **Apply** to apply changes.
- Click **Refresh** to refresh the page.

Power over Ethernet (PoE) configuration

This section describes the following pages:

- PoE Chip Information
- PoE Port Settings
- PoE Alive Check
- PoE Port Sequential
- PoE Schedule

PoE chip information

This page displays system voltage and current PoE chipset temperature.

PoE Chip Information	
System Voltag:	53.768 (v)
List	Temperature (C)
1	44
2	49
3	48
Refresh	

The page includes the following fields:

Object	Description
System Voltage	The system voltage information.
List	The chipset numbers.
Temperature	The temperature information of each PoE chipset.

Buttons

- Click **Refresh** to refresh the page.

PoE port settings

Inspect and configure the current PoE port settings on this page.

PoE Port Settings

Total Available Power 420 Watts
Total Consumption 0.0 Watts

Port Selection											
1	2	3	4	5	6	7	8	9	10	11	12
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

State
Mode
Budget Watt (Max. 36)

Port	Settings			Status	
	State	Budget (Watt)	AT/AF	Class	Consumption (Watt)
01	Enabled	36	AT	-	-
02	Enabled	36	AT	-	-
03	Enabled	36	AT	-	-
04	Enabled	36	AT	-	-
05	Enabled	36	AT	-	-
06	Enabled	36	AT	-	-
07	Enabled	36	AT	-	-
08	Enabled	36	AT	-	-

The page includes the following fields:

Object	Description
Total Available Power	The managed switch PoE Budget.
Total Consumption	The managed switch current PoE power used in Watts (W).
Port Selection	Select a specific PoE port for further configuration.
State	Enable or disable a specific PoE port power feeding function.
Mode	Choose AT or AF PoE operation mode.
Budget (Watt)	Type in the PoE power output value. The available range is 1 to 36 W.
Port	The PoE port list.
Settings	
State	The PoE port operation status.
Budget (Watt)	The PoE port budget setting.
AT/AF	The PoE port AT/AF setting.
Status	
Class	The PoE port current PoE class value detection.
Consumption (Watt)	The PoE port current PoE power usage information in W.

Buttons

- Click **Apply** to apply changes.
- Click **Refresh** to refresh the page.

PoE alive check

The managed switch can be configured to monitor connected powered device (PD) status in real time via a ping action. After the PD stops working and responding, the managed switch resumes the PoE port power and puts the PD back to work. The managed switch greatly enhances the network reliability through the PoE port resetting the PD's power source and reducing the administrator management burden.

Configure the PD alive check function on this page .

PoE Alive Check

Global Settings

Check Every Seconds (10-600) Wake up After Seconds (1-255)

Port Settings

Port State IP of Device to Check

Port	State	IP of Device to Check
01	Disabled	-
02	Disabled	-
03	Disabled	-
04	Disabled	-
05	Disabled	-
06	Disabled	-
07	Disabled	-
08	Disabled	-

The page includes the following fields:

Object	Description
Global Settings	
Check Every xxx Seconds	Set the amount of time for issuing a ping request to the PD to detect if it is alive or dead. Check time range is from 10 to 600 seconds.
Wake up After xxx Seconds	Set the PoE device rebooting time. This function is not a defining standard, so the PoE device doesn't report reboot information to the managed switch. As a result, the user has to make sure how long the PD will take to boot, and then set the time value accordingly. The PD is checked again according to the reboot time. If you cannot precisely calculate the booting time, we suggest you to set it to a longer period of time..
Port Settings	
Port	Select a specific PoE port for further configuration and list all ports on this page.
State	Enable or disable a specific PoE port PoE Alive Check function and display the current status of each PoE port.
IP of Device to Check	Type the PoE device IP address in this box to ping to the PoE device. The PD's IP address must be set to the same network segment as the managed switch.

Buttons

- Click **Apply** to apply changes.
- Click **Refresh** to refresh the page.

PoE port sequential

This page permits the user to configure the PoE ports' start up interval time.

PoE Port Sequential

Port Selection

1	2	3	4	5	6	7	8	9	10	11	12
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

State -----

Delay Seconds (Max. 300)

Apply

Port	State	Delay Time (Seconds)
01	Disabled	0
02	Disabled	0
03	Disabled	0
04	Disabled	0
05	Disabled	0
06	Disabled	0
07	Disabled	0
08	Disabled	0

Refresh

The page includes the following fields:

Object	Description
Port Selection	Select a specific PoE port for further configuration.
State	Enable or disable a specific PoE port sequential function.
Delay xxx Seconds (Max. 300)	Type the PoE Port Start Up interval time in this box. Delay time range is from 1 to 300 seconds.
Port	The PoE port list.
State	The PoE port operation status.
Delay Time (Seconds)	The PoE port delay time (seconds) setting.

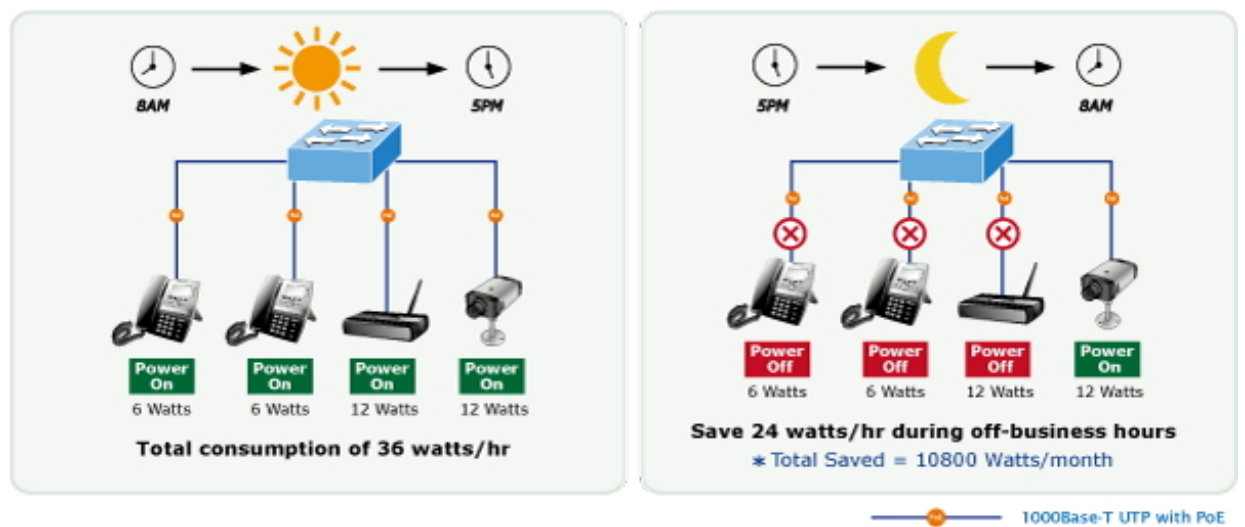
Buttons

- Click **Apply** to apply changes.
- Click **Refresh** to refresh the page.

PoE schedule

In addition to its functional use for IP surveillance, the managed switch can also be implemented in any PoE network including VoIP and Wireless LAN. Under the trend of energy saving worldwide and contributing to worldwide environmental protection, the managed switch can effectively control power supply in addition to its capability to provide high Watt power. The PoE schedule function can enable or disable PoE power

feeding for each PoE port during specified time intervals, and is a powerful function to help SMB or Enterprises save power and reduce cost.



Configure the PoE schedule on this page:

PoE Schedule

Port Selection											
1	2	3	4	5	6	7	8	9	10	11	12
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Port: 1 State: Disabled change to: -----

All	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Tue	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Wed	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Thu	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Fri	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Sat	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Sun	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

Apply

Note: PoE Schedule function needs to get NTP time

The page includes the following fields:

Object	Description
Port Selection	Select a specific PoE port for further configuration.
Port	Lists all PoE port for configuring the PoE schedule.
State: xxxxx change to	Configure the PoE Port Start Up interval time. Delay time range is from 1 to 300 seconds.
All	Select all options on this page.
Mon-Sun	Provide Mon/Tue/Wed/Thu/Fri/Sat/Sun options on this page.
00-23	Provide 24 hour options on this page.

Buttons

- Click **Apply** to apply changes.

Note: NTP time must be configured to use the PoE schedule function.

Monitoring

This section describes the following pages:

- MIB Counter
- Scan MAC ID Lookup Table
- LLDP Remote MIB
- Syslog
- CPU Resource Utilization

MIB counter

Configure the MIB counter settings on this page:

MIB Counter						
Port No.	Receive		Transmit		Action	☐
	Packets	Bytes	Packets	Bytes		
01	0	0	0	0	Detail	☐
02	0	0	0	0	Detail	☐
03	0	0	0	0	Detail	☐
04	0	0	0	0	Detail	☐
05	0	0	0	0	Detail	☐
06	0	0	0	0	Detail	☐
07	0	0	0	0	Detail	☐
08	0	0	0	0	Detail	☐
09	0	0	0	0	Detail	☐
10	0	0	0	0	Detail	☐
11	0	0	0	0	Detail	☐
12	0	0	0	0	Detail	☐
13	0	0	0	0	Detail	☐
14	0	0	0	0	Detail	☐

The page includes the following fields:

Object	Description
Port No.	The per port list.
Receive	
Packets	The per port traffic in packets received counters.
Bytes	The per port traffic in bytes received counters.
Transmit	
Packets	The per port traffic in packets transmitted counters.
Bytes	The per port traffic in bytes transmitted counters.
Action	Select all ports or specific ports for refresh or clearing current MIB counter information.
Detail	Click to open the advanced per port MIB counter web page.

Buttons

- Click **Clear** to clear current MIB counter information.
- Click **Refresh** to refresh the page.

Click Detail to open the per port MIB counter page:

MIB Counter

Port No.: 1 ▼ Apply

Type	Port 1 Counter	
	Receive	Transmit
64b	0	0
65-127b	0	0
128-255b	0	0
256-511b	0	0
512-1023b	0	0
1024-1518b	0	0
Oversize	0	0
Bcst	0	0
Mcast	0	0
Ucast	0	0
Pause	0	0
Pkts	0	0

[<<<Back](#)
Refresh Clear

The page includes the following fields:

Object	Description
Port No.	The per port list.
Type	The column displays traffic with various packet lengths and types. Table entry definitions are as follows: 64b: Packet size is under 64 bytes. 65-127b: Packet size is between 65 and 127 bytes. 128-255b: Packet size is between 128 and 255 bytes. 256-511b: Packet size is between 256 and 511 bytes 512-1023b: Packet size is between 512 and 1023 bytes. 1024-1518b: Packet size is between 1024 and 1518 bytes. Oversize: Packet size is over 1518 bytes, like jumbo frame. Bcst: Broadcast packet Mcst: Multicast packet Ucst: Unicast packet Pause: Pause packet for flow control Pkts (Packets): Total packets Bytes: Total bytes Drop: Drop packet CRC: CRC packet Alignment: Alignment error packet Runt: pkt < 64 and good frame Frag: pkt < 64 but bad CRC Jabber: pkt > 1518 but bad CRC Symbol error: symbol error packet ACL1: ACL type 1 ACL2: ACL type 2 Single Col (Single Collisions): The number of packets that encountered one collision during transmission. Multiple Col (Multiple Collisions): The number of packets that encountered between one and fifteen collisions during transmission. Late Col (Late Collisions): The number of packets that encountered a late collision. A late collision occurs when another node attempts to send a packet via the Ethernet at the same time the switch is sending a packet. Deferred tx (Deferred Transmissions): The number of transmitted packets deferred during transmission. Excessive Col (Excessive Collisions): The number of transmitted packets that encountered at least sixteen collisions during transmission.
Port X Counter (X= Port Number)	
Receive	This column displays the counters of per port traffic received with various packet lengths and types .
Transmit	This column displays the counters of per port traffic transmitted with various packet lengths and types .

Buttons

- Click **Apply** to apply changes.
- Click **Clear** to clear current MIB counter information.
- Click **Refresh** to refresh the page.

Scan MAC ID lookup table

Configure the Scan MAC ID Lookup Table settings on this page:

Scan MAC ID Lookup Table

MAC Table Clear

Port Selection												
1	2	3	4	5	6	7	8	9	10	11	12	13
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

All

Clear

Apply

MAC Table Monitor

Entry Number: 168

Refresh

MAC Address	Port
00:11:32:78:cd:4f	25
08:94:ef:4c:59:38	25
00:30:4f:b4:8b:61	25
00:30:4f:b5:cf:6a	25
50:6b:8d:96:b8:f6	25
00:30:4f:ac:9a:fc	25
00:30:4f:b6:58:71	25
00:30:4f:ac:9a:4a	25
50:6b:8d:e9:d3:bb	25

The page includes the following fields:

Object	Description
MAC Table Clear	
Port Selection	Select a specific port for the Scan MAC ID Lookup Table function.
MAC Table Monitor	
Entry Number	The entry number of the MAC address table.
MAC Address	The per port MAC address table information.
Port	This column displays the port list.

Buttons

- Click **Clear** to clear all ports.
- Click **All** to select all ports.
- Click **Apply** to apply changes.
- Click **Refresh** to refresh the page.

LLDP remote MIB

Configure the LLDP remote settings on this page:

The page includes the following fields:

Object	Description
Port	Select a specific port for the LLDP Remote MIB function.
LLDP Remote System MIB Information	
Entry	The entry number of the LLDP Remote MIB information.
Chassis ID	The chassis ID of the LLDP Remote MIB information.
Port ID	The Port ID of LLDP Remote MIB information.
Rx TTL	The Rx TTL of LLDP Remote MIB information.
Action	Click the Delete button to delete a specific LLDP Remote MIB entry.

Buttons

- Click **Find** to find the LLDP remote MIB info for a specific port.

Syslog

View syslog info on this page.

Syslog	
Refresh	
Index	Log Message
1	Jan 1 00:00:20 kernel: Loading file: ntp.config success
2	Jan 1 00:00:20 kernel: Loading file: cli_mib_counter.conf success
3	Jan 1 00:00:20 kernel: Loading file: wired.conf success
4	Jan 1 00:00:20 kernel: Loading file: lldp.config success
5	Jan 1 00:00:20 kernel: Loading file: ipv6.config success
6	Jan 1 00:00:25 misc_app[153]: Port 6 link up
7	Jan 1 00:00:25 misc_app[153]: Port 8 link up
8	Erased 65536 bytes from address 0x00000000 in flash
9	Jan 1 00:00:28 sshd[326]: Server listening on :: port 22.
10	Jan 1 00:00:28 sshd[326]: Server listening on :: port 22.
11	Jan 1 00:00:28 sshd[326]: Server listening on 0.0.0.0 port 22.
12	Jan 1 00:00:28 sshd[326]: Server listening on 0.0.0.0 port 22.
13	Jan 1 00:00:29 kernel: check_device:0
14	Jan 1 00:00:29 kernel: eth0: no IPv6 routers present
15	Jan 1 08:00:32 init: starting pid 354, tty "": "/bin/sh"

The page includes the following fields:

Object	Description
Index	The per index list.
Log Message	The log message information per index.

Buttons

- Click **Refresh** to refresh the page.

CPU resource utilization

View CPU resource utilization for the switch on this page.

CPU Resource Utilization	
Free Memory :	25752K
CPU Usage :	19%

The page includes the following fields:

Object	Description
Free Memory	This column displays the free memory status.
CPU Usage	This column displays the CPU usage status.

Chapter 5

Command line interface

Accessing the CLI

When accessing the management interface for the managed switch via a Telnet connection, it can be managed by entering command keywords and parameters at the prompt. Using the managed switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

This chapter describes how to use the Command Line Interface (CLI).

Telnet login

The managed switch supports telnet for remote management. The switch asks for a user name and password for remote login when using telnet. Use “**admin**” for the both the username and password.

```
Welcome to ES2402-24P-2C-V2 it is Thu Jan 1 08:01:54 UTC 1970
> █
```

Chapter 6

Command line mode

The CLI groups all the commands in appropriate modes according to the nature of the command. A sample of the CLI command modes are described below. Each of the command modes support specific software commands.

Command Groups:

clear	clear command, type '?' to show the list
config	config command, type '?' to show the list
create	create command, type '?' to show the list
default	default command, type '?' to show the list
delete	delete command, type '?' to show the list
disable	disable command, type '?' to show the list
enable	enable command, type '?' to show the list
exit	Exit this CLI session
reboot	reboot
restart	re-start command, type '?' to show the list
save	save setting.
show	Show command, type '?' to show the list

Clear

Command Lists:

clear	clear command, type '?' to show the list.
acl	Used to clear ACL table.
igmp_snooping	Used to clear entries of IGMP snooping.
ip	Used to clear IPv4 settings.
ipv6	Used to clear IPv6 settings.
mac_table	Used to clear dynamic entries of MAC-table function by port.
mib_counter	Used to clear MIB counters.

mld_snooping	Used to clear entries of MLD snooping.
poe	Used to clear poe informations.
syslog	Used to clear server information of syslog.
system	Used to clear system information.
vlan	Used to clear entry of protocol VLAN.

Config

Command Lists:

config	config command, type '?' to show the list
account	Used to config account information.
acl	Used to config ACL.
bandwidth_ctrl	Used to set the bandwidth parameters of ports.
cos	Used to config cos function.
dhcprelay	Used to config dhcprelay.
double-vlan	Used to config double VLAN.
gvrp	Used to config gvrp information.
igmp_snooping	Used to config IGMP snooping.
imp_table	Used to config IMP-table.
ip	Used to config IP information.
ipv6	Used to config IPv6 information.
link_aggregation	Used to config link aggregation.
lldp	Used to config LLDP.
loop-detect	Used to config loop detect information.
mac_table	Used to config MAC-table.
mirror	Used to set mirror port function and method.
mld_snooping	Used to config MLD snooping.
neighbor	Used to config neighbor MACID information.
ntp	Used to config the attributes of ntp.
poe	Used to config poe.
ports	Used to config the attributes of ports.
qosaging	Used to config Qos aging.
qosmode	Used to config Qos function.
qosremap	Used to config Qos remap function.
snmp	Used to config snmp information.
storm_ctrl	Used to config storm control.
stp	Used to config STP.

stp-loop-detect	Used to config STP loop detect information.
syslog	Used to config syslog.
system	Used to config system information.
vlan	Used to config VLAN.
voice-vlan	Used to config voice VLAN.

Create

Command Lists:

create	create command, type '?' to show the list
acl	Used to create a new profile of ACL.
igmp_snooping	Used to create a new entry of IGMP snooping.
imp_table	Used to create a new entry of IMP-table.
mac_table	Used to create a new entry of MAC-table.
mld_snooping	Used to create a new entry of MLD snooping.
snmp	Used to create snmp information.
stp	Used to create a new entry of STP.
vlan	Used to create a new entry of VLAN.

Default

Command Lists:

default	default command, type '?' to show the list
all	Load factory default .

Delete

Command Lists:

delete	delete command, type '?' to show the list
acl	Used to delete ACL profile .
igmp_snooping	Used to delete an entry of IGMP snooping .
imp_table	Used to delete an entry of IMP-table.
mac_table	Used to delete an entry of MAC-table.
mld_snooping	Used to delete an entry of MLD snooping .
snmp	Used to delete snmp informaiton.
stp	Used to delete an entry of STP .

vlan	Used to delete an entry of VLAN.
Voice-vlan	Remove OUI setting.

Disable

Command Lists:

disable	disable command, type '?' to show the list
DHCP_arp_inspection	Used to disable DHCP Dynamic ARP Inspection function.
DHCP_mac_verification	Used to disable DHCP MAC verification function.
DHCP_snooping	Used to disable DHCP Snooping function.
dhcprelay	Used to disable dhcprelay function.
gvrp	Used to disable gvrp function.
igmp_snooping	Used to disable IGMP snooping function.
imp_table	Used to disable IMP-table function.
lldp	Used to disable LLDP function.
loop-detect	Used to disable loop detect protocol.
mac_table	Used to disable MAC-table function.
mirror	Used to disable mirror in standard mode.
mld_snooping	Used to disable MLD snooping.
neighbor	Used to disable neighbor MACID function.
ntp	Used to disable network time protocol function.
poe	Used to disable poe ports.
snmp	Used to disable SNMP protocol.
storm_ctrl	Used to disable storm control function.
stp	Used to disable STP function.
stp-loop-detect	Used to disable STP loop detect protocol.
syslog	Used to disable syslog function.
vlan	Used to disable VLAN function.

Enable

Command Lists:

enable	enable command, type '?' to show the list
DHCP_arp_inspection	Used to enable DHCP Dynamic ARP Inspection function.
DHCP_mac_verification	Used to enable DHCP MAC verification function.
DHCP_snooping	Used to enable DHCP Snooping function.
dhcprelay	Used to enable dhcprelay function.

gvrp	Used to enable gvrp function.
igmp_snooping	Used to enable IGMP snooping function.
imp_table	Used to enable IMP-table function.
lldp	Used to enable LLDP function.
loop-detect	Used to enable loop detect protocol.
mac_table	Used to enable MAC-table function.
mirror	Used to enable mirror in standard mode.
mld_snooping	Used to enable MLD snooping.
neighbor	Used to enable neighbor MACID function.
ntp	Used to enable network time protocol function.
poe	Used to enable poe ports.
snmp	Used to enable SNMP protocol.
storm_ctrl	Used to enable storm control function.
stp	Used to enable STP function.
stp-loop-detect	Used to enable STP loop detect protocol.
syslog	Used to enable syslog function.
vlan	Used to enable VLAN function.

Exit

Command List:

exit	Exit this CLI session.
-------------	------------------------

Reboot

Command List:

reboot	Reboot the Managed PoE+ Switch.
---------------	---------------------------------

Restart

Command List:

restart	re-start command, type '?' to show the list
igmp_snooping	Used to restart IGMP process.
link_aggregation	Used to restart link aggregation process.
mcp	Used to restart MCP process.
mld_snooping	Used to restart MLD process.

stp	Used to restart STP process.
syslog	Used to restart syslog function.

Save

Command List:

save	save setting of Managed PoE+ Switch.
-------------	--------------------------------------

Show

Command List:

show	Show command, type '?' to show the list
account	Used to show account information.
acl	Used to show information of ACL.
bandwidth_ctrl	Used to show the information of bandwidth control.
cos	Used to show cos function information.
DHCP Snooping	Used to show information of DHCP Snooping.
dhcprelay	Used to show information of dhcprelay.
double-vlan	Used to show information of double VLAN.
gvrp	Used to show gvrp status information.
igmp_snooping	Used to show information of IGMP snooping.
imp_table	Used to show information of IMP-table.
ip	Used to show the information of IP.
ipv6	Used to show the information of IPv6.
link_aggregation	Used to show information of link aggregation.
lldp	Used to show information of LLDP.
loop-detect	Used to show loop detect status information .
mac_table	Used to show information of MAC-table.
mib_counter	Used to show information of MIB counter.
mirror	Used to show the information of mirror.
mld_snooping	Used to show information of MLD snooping.
neighbor	Used to show the neighbor MACID Information.
ntp	Used to show the attributes of ntp.
poe	Used to show the attributes of poe.
ports	Used to show the attributes of ports.
qosaging	Used to show Qos aging function information.
qosmode	Used to show Qos mode information.

qosremap	Used to show Qos remap information.
snmp	Used to show SNMP Status information.
storm_ctrl	Used to show information of storm control.
stp	Used to show information of STP.
stp-loop-detect	Used to show STP Loop Detect Status information .
syslog	Used to show information of syslog.
system	Used to show system information.
vlan	Used to show information of VLAN.
voice-vlan	Used to show voice vlan informatio.

Chapter 7

Switch operation

Address table

The switch is implemented with an address table. This address table is composed of many entries. Each entry is used to store the address information of some node in network, including MAC address, port number, etc. This information comes from the learning process of the managed switch.

Learning

When one packet comes in from any port, the switch records the source address, port number, and the other related information in the address table. This information will be used to decide either forwarding or filtering for future packets.

Forwarding and filtering

When one packet comes from a port of the switch, it checks the destination address as well as the source address learning. The switch will look up the address table for the destination address. If not found, this packet will be forwarded to all the other ports except the port that this packet comes from. These ports will transmit this packet to the network it is connected to. If found, and the destination address is located at a different port from the one this packet comes from, the switch will forward this packet to the port where this destination address is located according to the information from address table. But, if the destination address is located at the same port that this packet comes in, then this packet will be filtered, thereby increasing the network throughput and availability.

Store-and-forward

Store-and-Forward is a packet-forwarding technique. A Store-and-Forward switch stores the incoming frame in an internal buffer and completes error checking before

transmission. Therefore, no erroneous packets will occur, making it the best choice when a network needs efficiency and stability.

The switch scans the destination address from the packet header and searches the routing table provided for the incoming port and forwards the packet if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. However, the switch is most commonly used to segment existing hubs, which nearly always improves the overall performance. Ethernet switching can be easily configured in any Ethernet network environment to significantly boost bandwidth using conventional cabling and adapters.

Owing to the learning function of the switch, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is on the same segment as the source address. This confines network traffic to its respective domain and reduces the overall load on the network.

The switch performs Store-and-Forward, preventing erroneous packets and reducing the re-transmission rate. No packet loss will occur.

Auto-negotiation

The STP ports on the managed switch have built-in auto-negotiation. This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detecting the modes and speeds of both devices that are connected. Both the 10BASE-T and 100BASE-TX devices can connect with the port in either half- or full-duplex mode.

Chapter 8

PoE overview

What is PoE?

PoE is an abbreviation for Power over Ethernet. PoE technology permits a system to pass data and electrical power safely on an Ethernet UTP cable. The IEEE standard for PoE technology requires a category 5 cable or higher for high power PoE levels, but can operate with a category 3 cable for low power levels. Power is supplied in common mode over two or more of the differential pairs of wires found in Ethernet cables and comes from a power supply within a PoE-enabled networking device such as an Ethernet switch or can be injected into a cable run with a mid-span power supply.

The original IEEE 802.3af-2003 PoE standard provides up to 15.4 W of DC power (minimum 44 VDC and 350 mA) to each device. Only 12.95 W is assured to be available at the powered device as some power dissipates in the cable. The updated IEEE 802.3at-2009 PoE standard, also known as PoE+ or PoE plus, provides up to 25.5 W of power. The 2009 standard prohibits a powered device from using all four pairs for power. The 802.3af/802.3at standards define two types of source equipment:

Mid-Span – A mid-span device is placed between a legacy switch and the powered device (PD). Mid-span taps the unused wire pairs 4/5 and 7/8 to carry power. The other four pairs are for data transmission.

End-Span – An end-span device connects directly to the PD. End-span taps the 1/2 and 3/6 wire pairs.

PoE system architecture

The PoE specification typically requires two devices: the Powered Source Equipment (PSE) and the PD. The PSE is either an end-span or a mid-span, while the PD is a PoE-enabled terminal such as an IP phone, Wireless LAN, etc. Power can be delivered over data pairs or spare pairs of standard CAT-5 cabling.

Powered Source Equipment (PSE)

A PSE is a device such as a switch that provides (sources) power on the Ethernet cable. The maximum allowed continuous output power per cable in IEEE 802.3af is

15.40 W. A later specification, IEEE 802.3at, offers 25.50 W. When the device is a switch, it is commonly called an end-span, although IEEE 802.3af refers to it as endpoint. Otherwise, if it's an intermediary device between a non PoE capable switch and a PoE device, it's called a mid-span. An external PoE injector is a mid-span device.

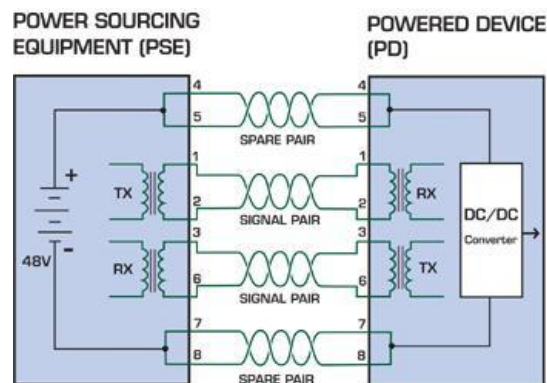
Powered Device (PD)

A PD is a device powered by a PSE and thus consumes energy. Examples include wireless access points, IP phones, and IP cameras. Many powered devices have an auxiliary power connector for an optional external power supply. Depending on the PD design, some, none, or all power can be supplied from the auxiliary port, with the auxiliary port sometimes acting as backup power in case of PoE-supplied power failure.

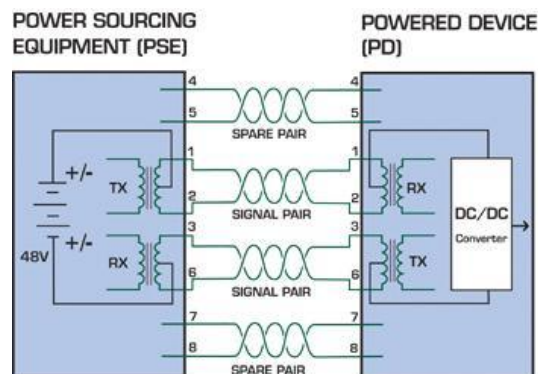
How power is transferred through the cable

A standard CAT5 Ethernet cable has four twisted pairs, but only two of these are used for 10BASE-T and 100BASE-TX. The specification allows two options for using these cables for power.

The spare pairs are used. The diagram below shows the pair on pins 4 and 5 connected together and forming the positive supply, and the pair on pins 7 and 8 connected together and forming the negative supply. (either polarity can be used).



The data pairs are used. Since Ethernet pairs are transformer-coupled at each end, it is possible to apply DC power to the center tap of the isolation transformer without interrupting the data transfer. In this mode of operation, the pair on pins 3 and 6 and the pair on pins 1 and 2 can be of either polarity.



Chapter 9

Troubleshooting

This chapter contains information to help you solve issues. If the managed switch is not functioning properly, ensure that it was set up according to the instructions in this manual.

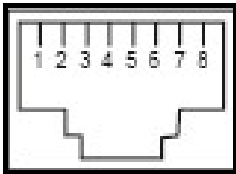
Issue	Solution
The link LED does not illuminate	Check the cable connection and remove duplex mode of the managed switch.
Some stations cannot talk to other stations located on the other port.	Check the VLAN settings, trunk settings, or port enabled/disabled status.
Poor performance	Check the full duplex status of the managed switch. If the managed switch is set to full duplex and the partner is set to half duplex, then the performance will be poor. Also check the in/out rate of the port.
The switch doesn't connect to the network	1. Check the LNK/ACT LED on the managed switch. 2. Try another port on the managed switch. 3. Make sure the cable is installed properly. 4. Make sure the cable is the right type. 5. Turn off the power. After a while, turn on power again.
The 1000BASE-T port link LED illuminates, but the traffic is irregular	Check that the attached device is not set to dedicate full duplex. Some devices use a physical or software switch to change duplex modes. Auto-negotiation may not recognize this type of full-duplex setting.
The switch does not power up.	1. Check to ensure that the AC power cord is not faulty and that it is inserted properly. 2. If the cord is inserted correctly, replace the power cord. 3. Check that the AC power source is working by connecting a different device in place of the switch. 4. If that device does not work, check the AC power

Issue	Solution
The IP address has been changed and/or the admin password has been forgotten.	To reset the IP address to the default IP address "192.168.0.100" or reset the login password to default value, press the hardware-based reset button on the front panel for about five seconds (see "Reset button" on page 22 for the reset button locations). After the managed switch reboots, log in to the web UI within the same subnet of 192.168.0.xx.

Appendix A

Networking connection

RJ45 port pin assignments – PoE

	Pin number	RJ45 Power Assignment
	1	Power +
	2	Power +
	3	Power -
	6	Power -

RJ45 port pin assignments – 1000Mbps, 1000BASE-T

Pin number	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

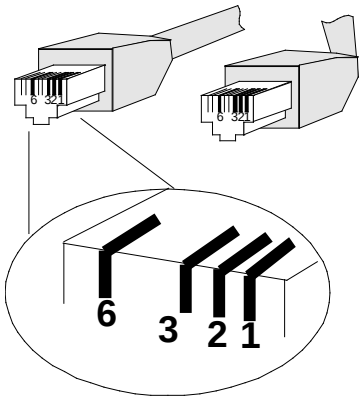
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

10/100Mbps, 10/100BASE-TX

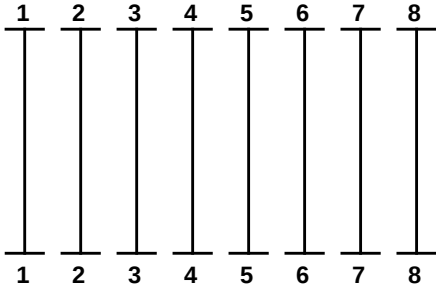
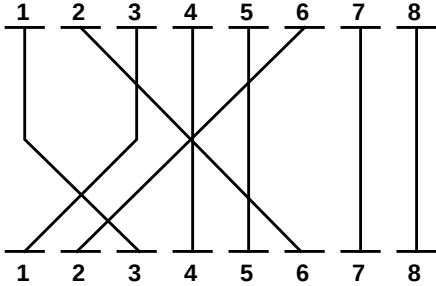
When connecting the managed switch to another Fast Ethernet switch, a bridge, or a hub, a straight or crossover cable is necessary. Each port of the managed switch supports auto-MDI (Media Dependent Interface)/MDI-X (Media Dependent Interface Cross) detection. This makes it possible to directly connect the managed switch to any Ethernet device without making a crossover cable. The following table and diagram show the standard RJ45 receptacle/ connector and their pin assignments.

Pin number	MDI	MDI-X
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx + (receive)	Tx + (transmit)
7, 8	Not used	

The standard RJ45 receptacle/connector:



There are eight wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and the color of the straight cable and crossover cable connection:

Straight Cable		SIDE 1	SIDE 2
	SIDE 1	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown
	SIDE 2		
Crossover Cable		SIDE 1	SIDE 2
	SIDE 1	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown	1 = White / Green 2 = Green 3 = White / Orange 4 = Blue 5 = White / Blue 6 = Orange 7 = White / Brown 8 = Brown
	SIDE 2		

Ensure that connected cables are with the same pin assignment and color as the above diagram before deploying the cables into the network.

Glossary

A

ACE	Access Control Entry. It describes access permission associated with a particular ACE ID. There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). ACE also contains many detailed, different parameter options that are available for individual application.
ACL	Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine if there are specific traffic object access rights. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are three web pages associated with the manual ACL configuration:

Access Control List (ACL): The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). The table is empty by default. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a policy, one ingress port, or any ingress port (the whole switch). If an ACE policy is created then that policy can be associated with a group of ports under the "Ports" web page. There are number of parameters that can be configured with an ACE. Read the web page help text to obtain further information for each of them. The maximum number of ACEs is 64.

ACL Port Configuration: The ACL ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic policy is created under the "Access Control List" page. You can also set up specific traffic properties (Action / Rate Limiter / Port copy, etc.) for each ingress port. They will only apply if the frame gets past the ACE matching without getting matched, however. In that case a counter associated with that port is incremented. See the web page help text for each specific port property.

ACL Rate Limiters: This page can be used to configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per second. The "Ports" and "Access Control List" web pages can be used to assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES	Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.
AMS	Auto Media Select. AMS is used for dual media ports (ports supporting both copper (CU) and fiber (SFP) cables. AMS automatically determines if a SFP or a CU cable is inserted and switches to the corresponding media. If both SFP and CU cables are inserted, the port will select the preferred media.
APS	Automatic Protection Switching. This protocol is used to secure that switching is done bidirectionally in the two ends of a protection group, as defined in G.8031
Aggregation	Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.
ARP	Address Resolution Protocol. It is a protocol used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP inspection	ARP inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.
Auto negotiation	Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link

C

CC	Continuity Check. This is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.
CCM	Continuity Check Message. This is an OAM frame transmitted from a MEP to its peer MEP and used to implement CC functionality.
CDP	Cisco Discovery Protocol

D

DEI	Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.
DES	Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.
DHCP	Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network. DHCP is used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server. The DHCP server ensures that all IP addresses are unique. For example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically, the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option 2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option is designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal to the DHCP relay agent's MAC address.

DHCP Snooping

DHCP snooping is used to block an intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet into a legitimate conversation between the DHCP client and server.

DNS

Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting network sites or a network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.

An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

DSCP

Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

E

EEE

Energy Efficient Ethernet as defined in IEEE 802.3az.

EPS

Ethernet Protection Switching as defined in ITU/T G.8031.

Ethernet Type	Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.
---------------	---

F

FTP	File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.
-----	--

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

H

HTTP	Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW). HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, entering a URL in a browser actually sends an HTTP command to the web server directing it to fetch and transmit the requested web page. The other main standard that controls how the World Wide Web works is HTML, which covers how web pages are formatted and displayed. Any web server machine contains, in addition to the web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.
------	--

HTTPS	Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection. HTTPS provides authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons. HTTPS is the use of Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP. SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.
-------	---

I

ICMP	Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic, or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.
IEEE 802.1X	IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.
IGMP	Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.
IGMP Querier	A router sends IGMP query messages onto a particular link. This router is called the Querier.
IMAP	Internet Message Access Protocol. It is a protocol for email clients to retrieve email messages from a mail server. IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server. The current version of the IMAP is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves email messages on the server rather than downloading them to a computer. To remove your messages from the server, use the mail client to generate local folders, copy messages to the local hard drive, and then delete and expunge the messages from the server.

IP	Internet Protocol. It is a protocol used for communicating data across a internet network. IP is a "best effort" system, which means that no packet of information sent over it is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an IP address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network. The most widely used version of the Internet protocol is IPv4, which has 32-bit IP addresses allowing for over four billion unique addresses. There is a substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bit IP addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.
IPMC	IP MultiCast
IP Source Guard	IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP	LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.
LLDP	Link Layer Discovery Protocol is an IEEE 802.1ab standard protocol. The LLDP specified in this standard allows stations attached to an IEEE 802 LAN to advertise to other stations attached to the same IEEE 802 LAN the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station's point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).
LLDP-MED	LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).
LOC	LOC is an acronym for Loss Of Connectivity and is detected by a MEP and indicates lost connectivity in the network. Can be used as a switch criteria by EPS.

M

MAC Table	Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to based upon the DMAC address in the frame. This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports. The frames also contain a MAC address (SMAC address), that shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.
MEP	MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).
MD5	Message-Digest algorithm 5. MD5 is a message digest algorithm using a cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 – The MD5 Message-Digest Algorithm.
Mirroring	For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. In this context, mirroring a frame is the same as copying the frame. Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port
MLD	Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.
MVR	Multicast VLAN Registration. It is a protocol for Layer 2 (IP) networks that enables multicast traffic from a source VLAN to be shared with subscriber VLANs. The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them.

N

NAS	Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.
-----	---

NetBIOS	Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN). The NetBIOS provides each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, as well as the session and transport services described in the Open Systems Interconnection (OSI) model.
NFS	Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems. NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.
NTP	Network Time Protocol. A network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as the transport layer.

O

OAM	Operation Administration and Maintenance. It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on this.
Optional TLVs	A LLDP frame contains multiple TLVs For some TLVs it is configurable if the switch includes the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled, the corresponding information is not included in the LLDP frame.
OUI	Organizationally Unique Identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address that forms the first 24 bits of a MAC address.

P

PCP	Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.
PD	Powered Device. In a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.
PHY	Physical Interface Transceiver. It is the device that implements the Ethernet physical layer (IEEE-802.3).

Ping	Ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected. Ping uses Internet Control Message Protocol (ICMP) packets. The ping request is the packet from the origin computer, and the ping reply is the packet response from the target.
Policer	A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.
POP3	POP3 is an acronym for Post Office Protocol version 3. It is a protocol for email clients to retrieve email messages from a mail server. POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service. An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining email on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server. POP and IMAP deal with the receiving of email and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send email with SMTP, and a mail handler receives it on the recipient's behalf. Then, the mail is read using POP or IMAP.
PPPoE	Point-to-Point Protocol over Ethernet. It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames (Wikipedia). It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks.
Private VLAN	In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.
PTP	Precision Time Protocol. A network protocol for synchronizing the clocks of computer systems.

Q

QCE	QoS Control Entry. It describes the QoS class associated with a particular QCE ID. There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of four different QoS classes: "Low", "Normal," "Medium," and "High" for individual application.
-----	--

QCL	QoS Control List. It is the list table of QCEs, containing QoS control entries that classify a specific QoS class on specific traffic objects. Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.
QL	QL In SyncE is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.
QoS	Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols. A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services, and QoS can help to provide this.
QoS Class	Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one to one mapping between QoS class, queue, and priority. A QoS class of 0 (zero) has the lowest priority.

R

RARP	Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.
RADIUS	Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization, and accounting management for people or computers to connect to and use a network service.
RDI	Remote Defect Indication. It is a OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP.
Router Port	A router port is a port on the Ethernet switch that connects it to the Layer 3 multicast device.
RSTP	In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SAMBA	Samba is a program running under UNIX-like operating systems that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking. Samba can be installed on a variety of operating system platforms, including Linux and most common Unix platforms. Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".
SHA	SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.
Shaper	A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.
SMTP	Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.
SNAP	SubNetwork Access Protocol (SNAP). It is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifiers.
SNMP	Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allows diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.
SNTP	Simple Network Time Protocol. A network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as a transport layer.
SPROUT	Stack Protocol using Routing Technology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform the shortest path forwarding within the stack.

SSID	Service Set Identifier. It is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one.
SSH	Secure Shell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality.
SSM	SSM In SyncE is an abbreviation for Synchronization Status Message and contains a QL indication.
STP	Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsoleted by RSTP.
SyncE	Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+	Terminal Access Controller Access Control System Plus. It is a networking protocol that provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting services.
Tag Priority	Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.
TCP	Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange messages between computers. The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and email server) running on the same host. The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. Common network applications that use TCP include the World Wide Web (WWW), email, and File Transfer Protocol (FTP).

TELNET	TELEtype NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client. TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.
TFTP	Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provides directory service and security features.
ToS	Type of Service. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant six bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0–63).
TLV	Type Length Value. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as a TLV.
TKIP	Temporal Key Integrity Protocol. It is used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

U

UDP	User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers. UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP. UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact. Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).
-----	---

UPnP	Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components
User Priority	User Priority is a 3-bit field that stores the priority level for the 802.1Q frame.

V

VLAN	Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications: VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags. VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames. Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.
VLAN ID	VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.
Voice VLAN	Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, QoS-related configuration for voice data can be performed, ensuring the transmission priority of voice traffic and voice quality.

W

WEP	Wired Equivalent Privacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio, so are more susceptible to eavesdropping than wired networks. When introduced, WEP was intended to provide data confidentiality comparable to that of a traditional wired network (Wikipedia).
Wi-Fi	Wireless Fidelity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA	Wi-Fi Protected Access. It was created in response to several serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).
WPA-PSK	Wi-Fi Protected Access - Pre Shared Key. WPA was designed to enhance the security of wireless networks. There are two types of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes a less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard.
WPA-Radius	Wi-Fi Protected Access - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard.
WPS	Wi-Fi Protected Setup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network.
WRED	Weighted Random Early Detection. It is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level is used as input to WRED. A higher DP level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.
WTR	Wait To Restore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource.

