Switch LT-Serie

Software User's Manual V2.8

Content

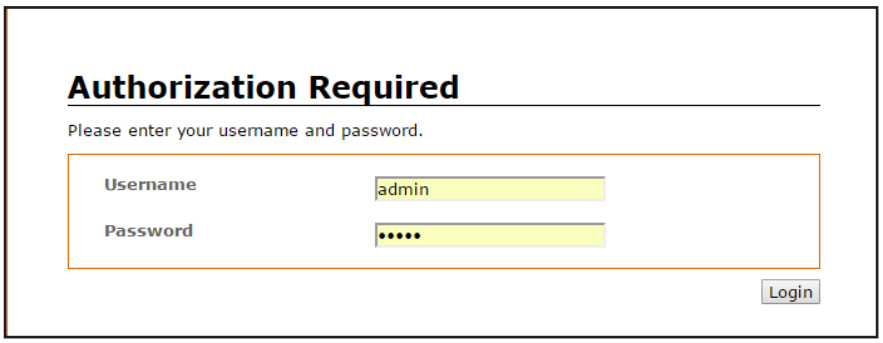
Web Management

This section describes the Web console interface for a series Industrial Management Switch. This is a **user friendly** design with advanced management features that allow you to manage switches through Internet browser.

Connecting to the Web Console Interface

1. Initiate a connection from a browser to the default IP address: http://192.168.1.254 The Login page appears.

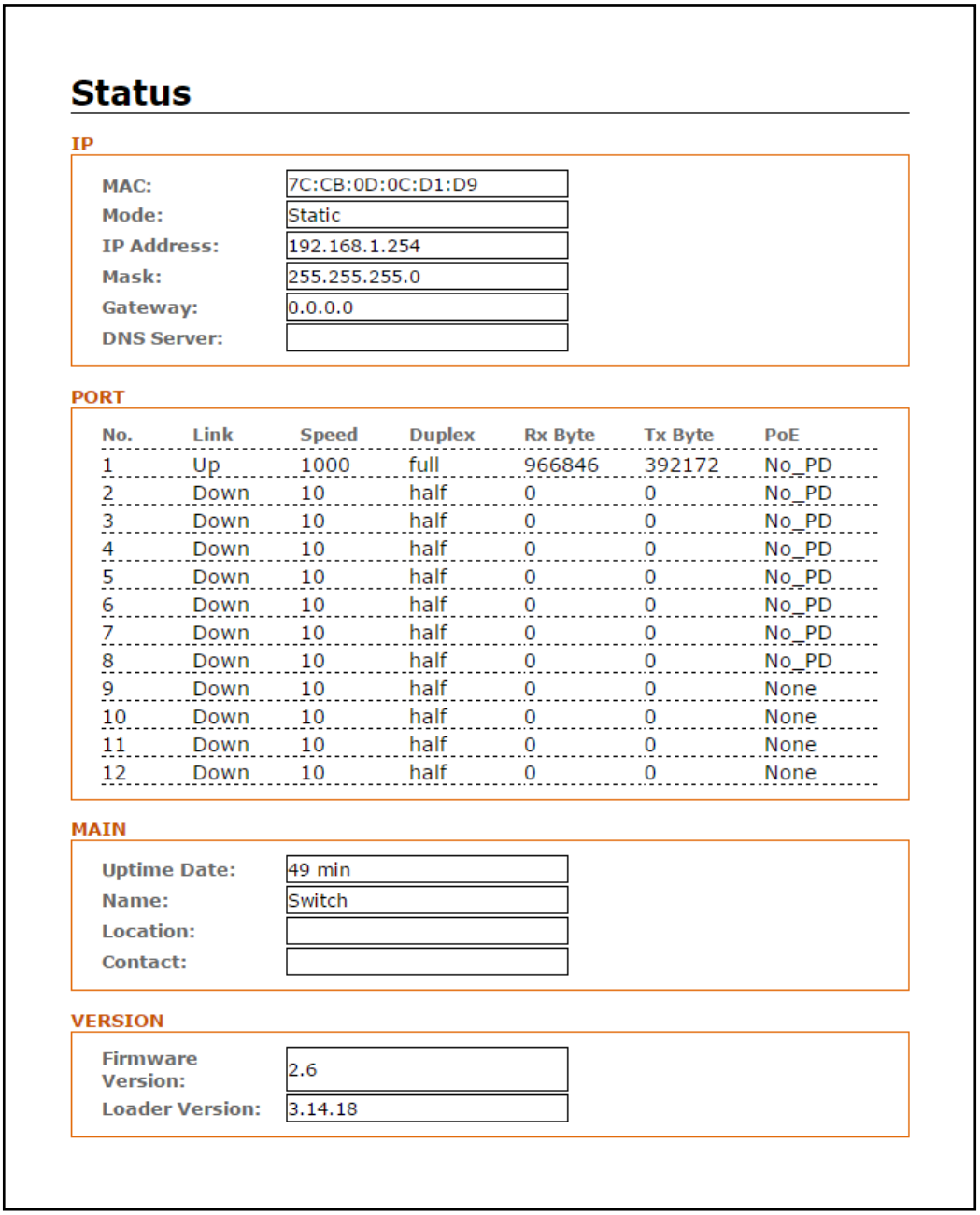
2. The administrator username/ password is admin/admin by default. Enter the username and password and then click the Login button.



NOTE: Make sure that the PC and Switches are on the same logical subnetwork.

Status

When logged into the Web Console Interface, the status page will be displayed as seen below.



Status

IP

MAC:	7C:CB:0D:0C:D1:D9
Mode:	Static
IP Address:	192.168.1.254
Mask:	255.255.255.0
Gateway:	0.0.0.0
DNS Server:	

PORT

No.	Link	Speed	Duplex	Rx Byte	Tx Byte	PoE
1	Up	1000	full	966846	392172	No_PD
2	Down	10	half	0	0	No_PD
3	Down	10	half	0	0	No_PD
4	Down	10	half	0	0	No_PD
5	Down	10	half	0	0	No_PD
6	Down	10	half	0	0	No_PD
7	Down	10	half	0	0	No_PD
8	Down	10	half	0	0	No_PD
9	Down	10	half	0	0	None
10	Down	10	half	0	0	None
11	Down	10	half	0	0	None
12	Down	10	half	0	0	None

MAIN

Uptime Date:	49 min
Name:	Switch
Location:	
Contact:	

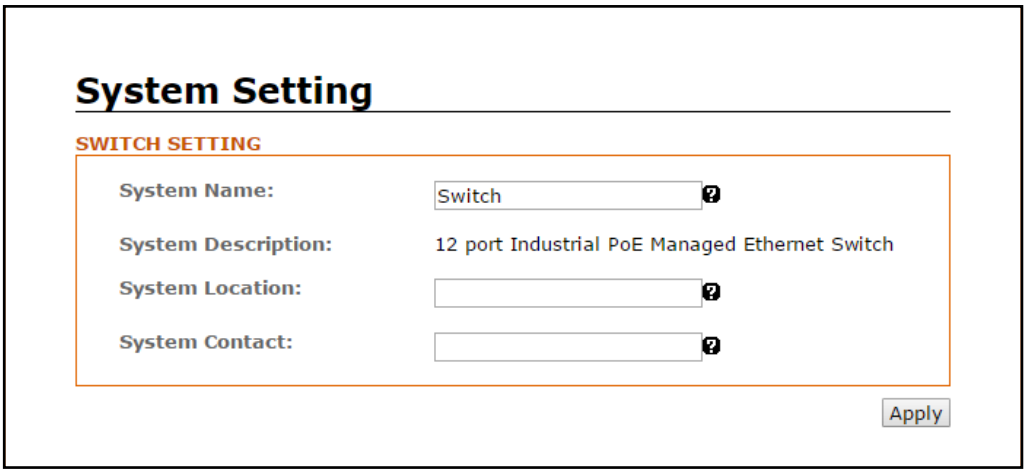
VERSION

Firmware Version:	2.6
Loader Version:	3.14.18

Basic Settings

The basic settings contain the most common settings for maintenance and control.

Basic Settings > System



System Name

Setting	Description	Factory Default
Max. 32 Characters	The name for identifying different devices.	Switch

System Description

Setting	Description	Factory Default
Fixed	Describe this device	According to the device

System Location

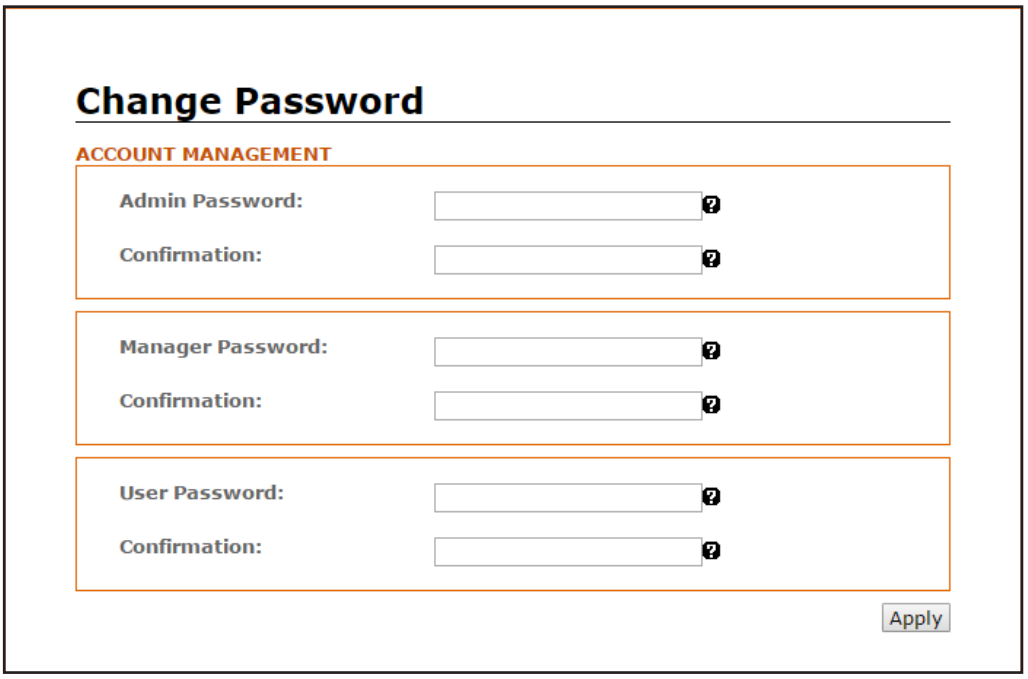
Setting	Description	Factory Default
Max. 32 Characters	The physical location of this device (e.g., telephone closet, 3rd floor).	None

System Contact

Setting	Description	Factory Default
Max. 32 Characters	Maintenance contact information	None

Basic Settings > Change Password

The system provides three level configuration access. The Admin account has read/write access to all configuration parameters. The Manager account can modify the configuration, but can not reset to default or update the firmware. The User account can view the configuration but can not make changes.



Account

User Account Type	Description
Admin	The administrator has full privileges.
Manager	The manager can modify configuration but can not reset to default or update the firmware though software method.
User	The user can view status and configuration but can not change the configuration in any way.

Password

Setting	Description	Factory Default
Password (Max. 20 alphanumeric characters)	Enter a new password.	admin manager user
Confirmation (Max. 20 alphanumeric characters)	Type the new password again to confirm.	admin manager user

Basic Settings > IP Setting

This page is used to set the device's IP address; you can use DHCP to allocate IP addresses or use static IP addresses.

DHCP Client

Check box	Description	Factory Default
Unchecked	Configure IP address, Subnet mask, Gateway and DNS of this device manually.	Unchecked
Checked	The IP address, Subnet mask, Gateway, and DNS will be assigned to this device automatically by the DHCP server.	

IP Address

Setting	Description	Factory Default
IP address of this device	Manually configure an IP address to this device	192.168.1.254

Subnet Mask

Setting	Description	Factory Default
Subnet mask of this device	Manually configure the subnet mask to the IP address. (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	255.255.255.0

Gateway

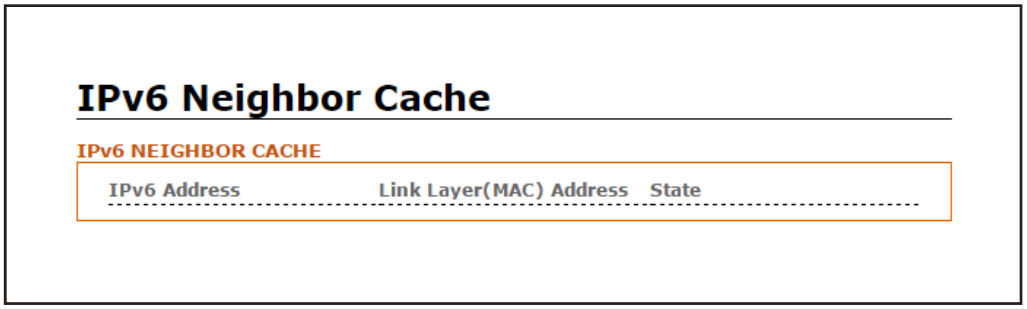
Setting	Description	Factory Default
IP address of the router	Manually configure the IP address of the gateway router	0.0.0.0

DNS

Setting	Description	Factory Default
IP address of the DNS server	Manually configure the IP address of the DNS server	None

Basic Settings > IPv6 Neighbor Cache

The following information provides the current IPv6 neighbors and their states.

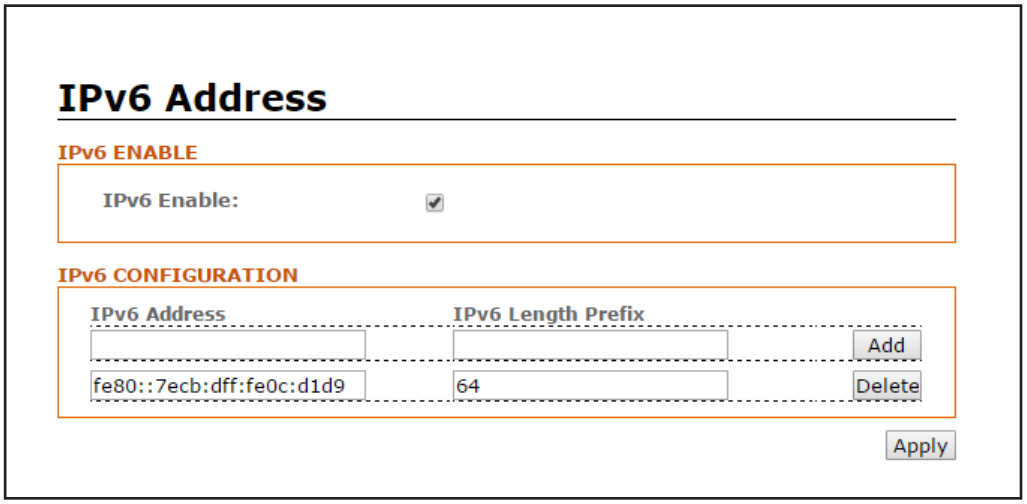


Account

Permission	Description
IPv6 Address	The IPv6 address of nodes attached to the same link
Link Layer(MAC) Address	The address at the link layer
State	Indicates if the neighbor is functioning properly.

Basic Settings > IPv6 Setting

This page is used to enable/ disable the IPv6 support.



IPv6 Enable

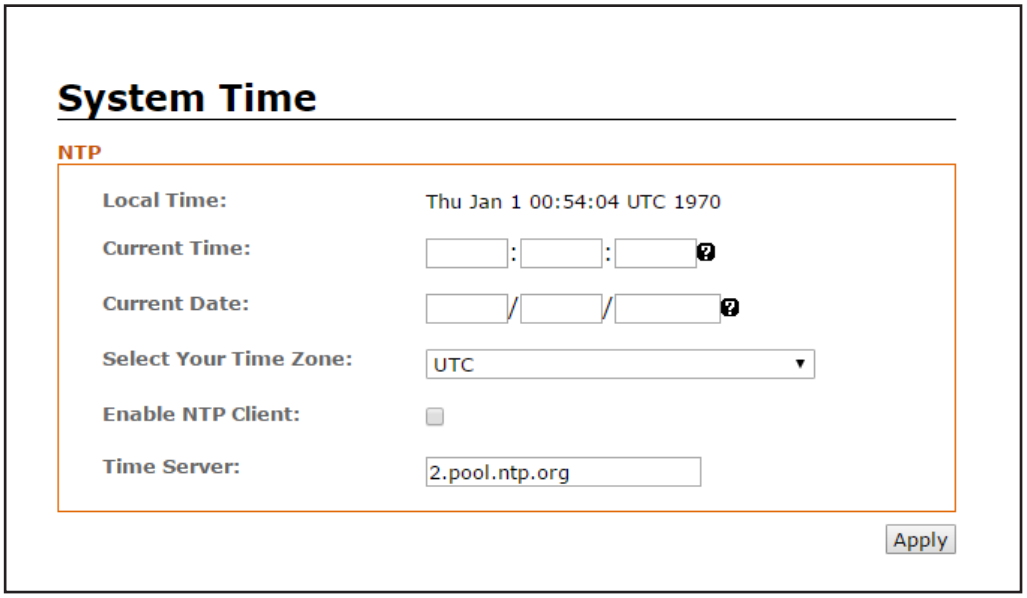
Check box	Description	Factory Default
Checked	Enables IPv6 support	Checked
Unchecked	Disables IPv6 support	

IPv6 Configuration

Setting	Description	Factory Default
IPv6 Address	Manually configure an IPv6 address on this device. You can add IPv6 addresses by clicking the **Add** button and use the **Delete** button to remove them.	Depended on MAC address
IPv6 Length Prefix	Configure the bit-length of the prefix	64

Basic Settings > System Time

This page allows you to configure the system time and Network Time Protocol (NTP).



Local Time
Displays the local time of the device.

Current Time

Setting	Description	Factory Default
User-specified time	Configure the local time in 24-hour HH:MM:SS format.	None

Current Date

Setting	Description	Factory Default
User-specified time	Configure the local date in DD:MM:YY format.	None

Select Your Time Zone

Setting	Description	Factory Default
Time zone	Select your time zone, which is used to determine the local time offset from GMT (Greenwich Mean Time).	UTC (Coordinated Universal Time)

Enable NTP Client

Setting	Description	Factory Default
Unchecked	Disables time calibration function	Unchecked
Checked	Enables time calibration function based on information from an NTP server	

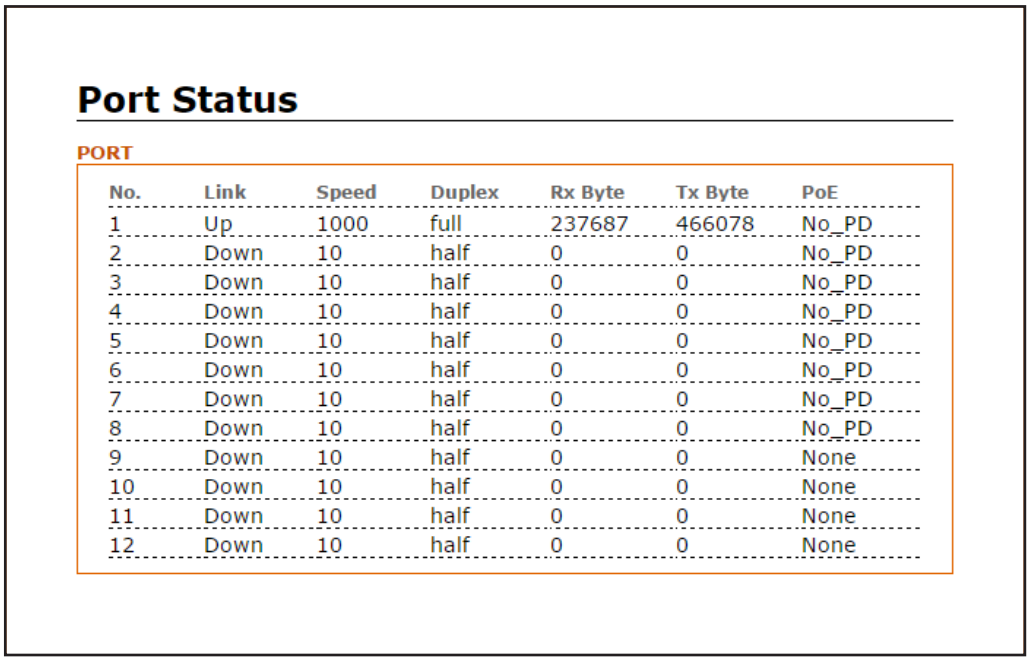
Time Server

Setting	Description	Factory Default
Domain name	Assign the NTP server	2.pool.ntp.org

Port Management

Port Management > Port Status

This page shows current port status.

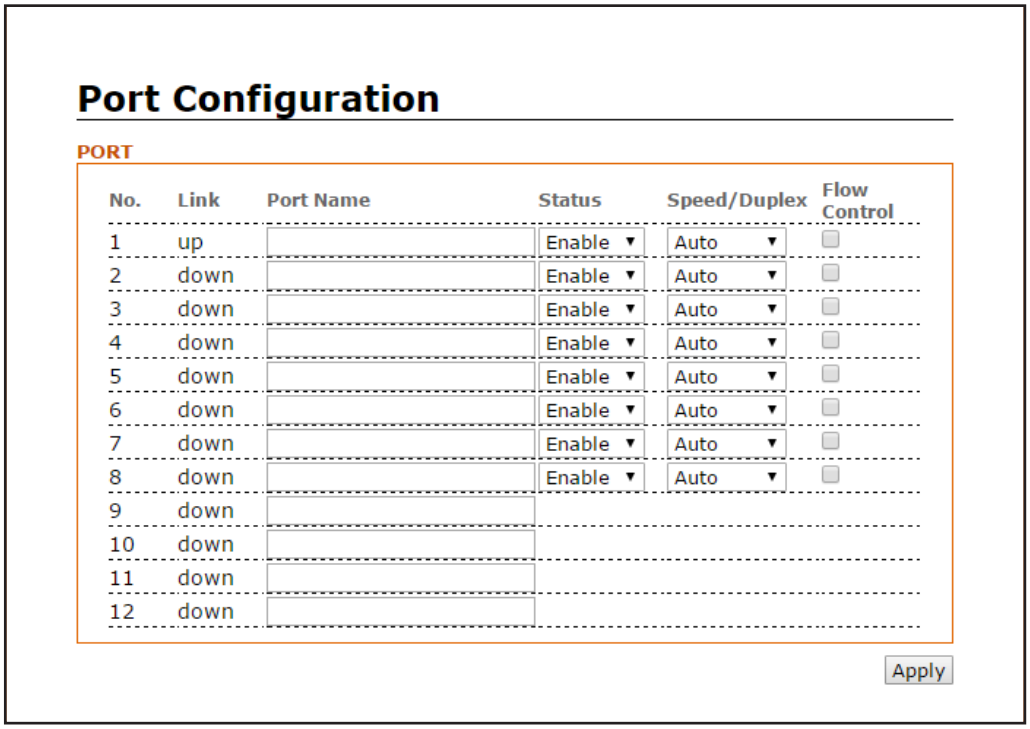


Port Status

Item	Description
No.	Port Number
Link	Shows if the port is connected. Up is for Link-up (connected) status, and Down is for Link-down (non-connected) status.
Speed	Displays 10 Mbps, 100 Mbps, or 1000 Mbps speed of the connected device.
Duplex	Displays full or half duplex mode of the connected device.
Rx Byte	Number of bytes received (download) by the port.
Tx Byte	Number of bytes transmitted (upload) by the port.
PoE	Indicates the PoE status of the port.

Port Configuration

This page allows you to configure the ports name, speed, and function.



Port

Item	Description
No.	Port number on the switch.
Link	Shows if the port is connected or not. Up is for Link-up (connected) status, and Down is for Link-down (non-connected) status.

Port Name

Setting	Description	Factory Default
Max. 32 alphanumeric characters	Used to identify the port	None

Status

S	Description	F

etting		actoryDefault
Enable	Allows data transfer via the port.	Enable
Disable	Turns off the access through the port.	

Speed/Duplex

Setting	Description	FactoryDefault
Auto	Allows the port to negotiate with the connected device using the IEEE 802.3u protocol. The port and the connected device will determine the optimum speed for the connection.	Auto
100FDX	Manually select line speed of 100 Mbps full duplex	
100HDX	Manually select line speed of 100 Mbps half duplex	
10FDX	Manually select line speed of 10 Mbps full duplex	
1	Manually select line speed of 10 Mbps half duplex	

0 H D X		

Flow Control

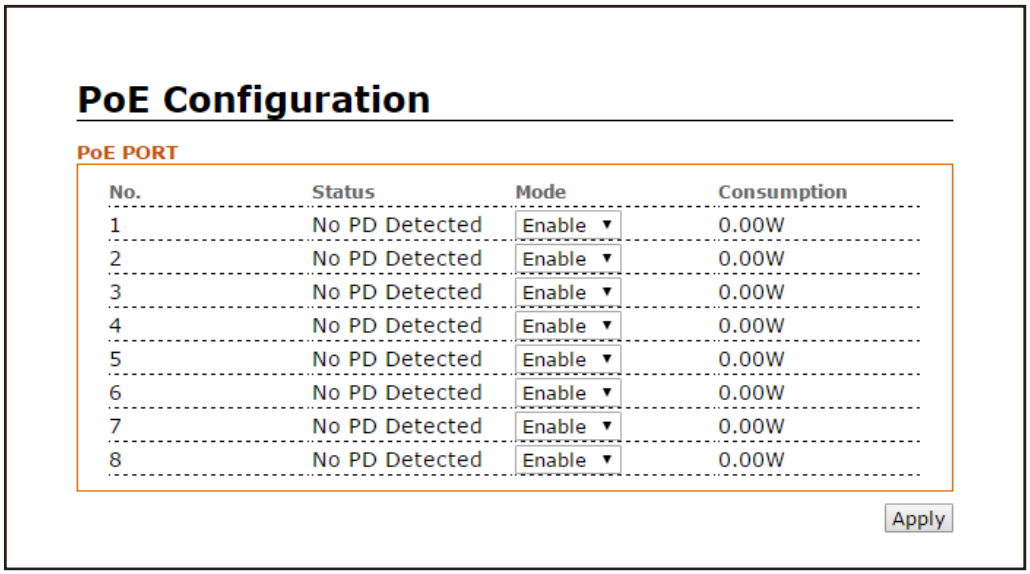
Check box	Description	Factory Default
Unchecked	Disable the Flow Control function	Unchecked
Checked	Enable Flow Control when **Speed/Duplex** is set to Auto.	

PoE

Power over Ethernet (PoE) is a technology that uses network cables carry electrical power and data to Powered Devices (PD).

PoE > PoE Configuration

This page allows you to control PoE for each port and monitor PD status.

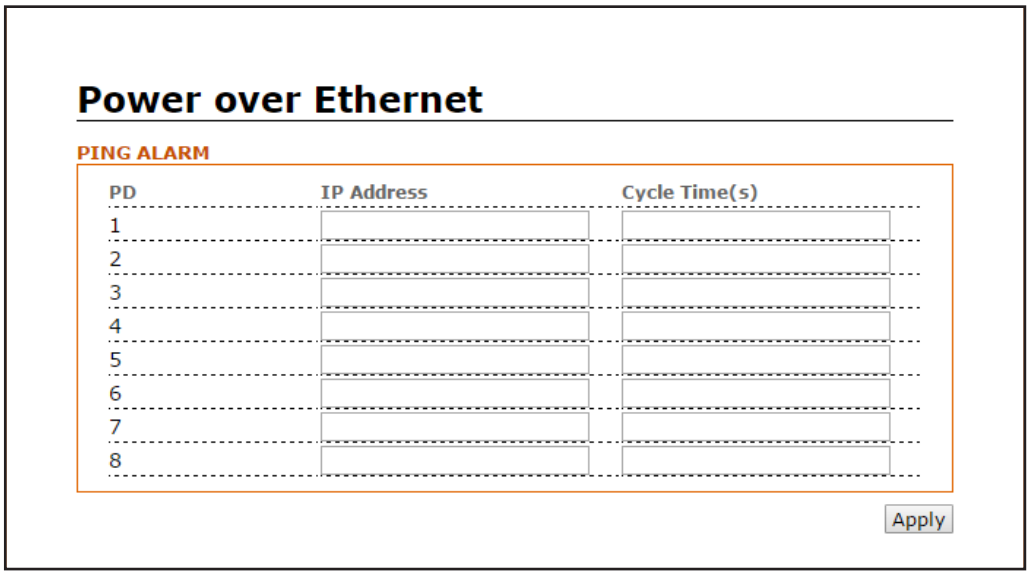


PoE Port

Item	Description
No.	Port Number
Status	Indicates the PoE port status
Mode	Enable/ Dsiable PoE on the port. The default configuration is Enable.
Consumption	Shows the PoE consumption on the port.

PoE > Ping Alarm

The PoE ping alarm function is that uses the ping command to recycle any PoE port. Insert any powered device's IP address and set the interval time between pings for each port. After 3 pings are not returned, PoE power will recycle for that individual port.



Ping Alarm

Item	Description
PD	The powered device which is connected on the PoE/PSE port.

IP Address

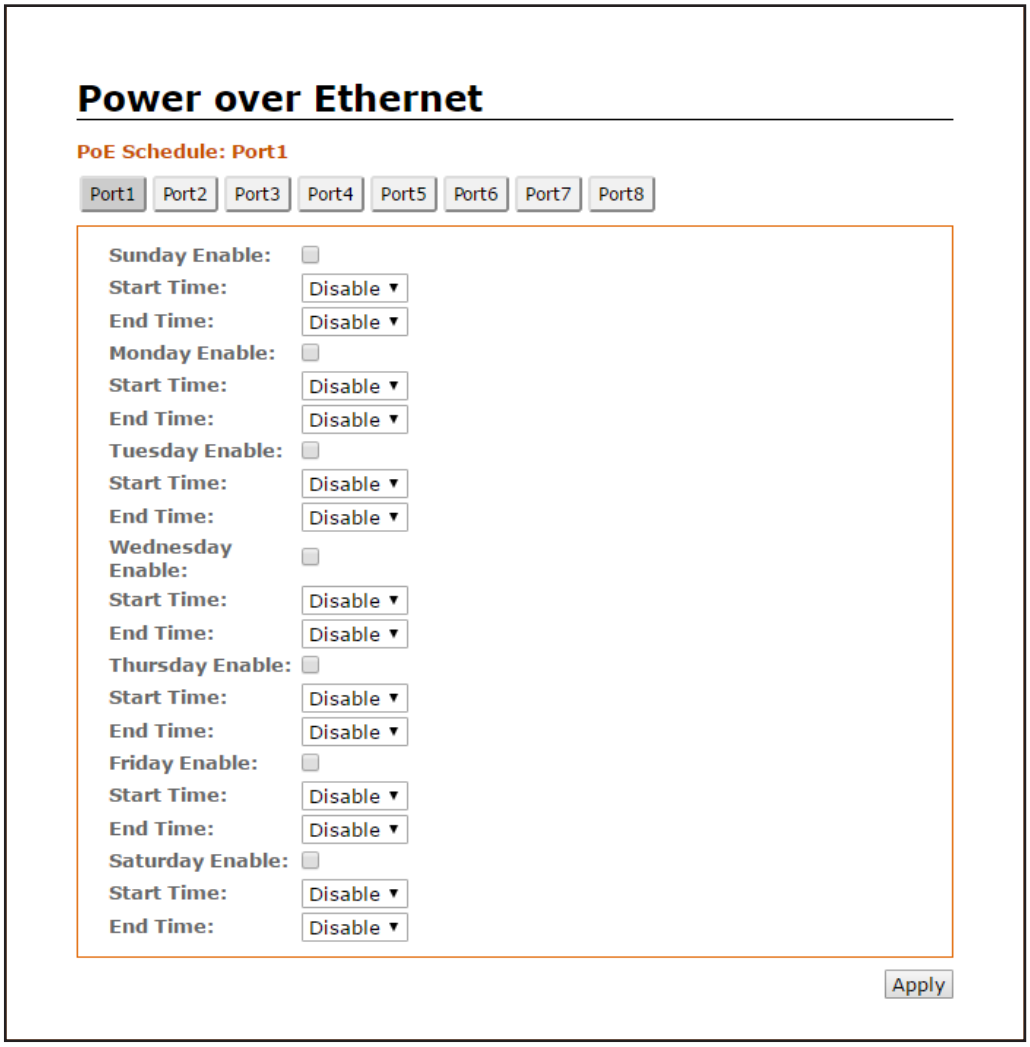
Setting	Description	Factory Default
IP address	Insert IP address of Powered Device	None

Cycle Times

Setting	Description	Factory Default
0~65535	Set the interval time (second) between pings for individual port.	None

PoE > PoE Schedule

This page allows you to create a schedule for enabling / disabling PoE.



PoE Schedule Tabs

Buttons	Description	Factory Default
Port1 ~8 buttons	Switch the PoE schedule settings menu from port1 to port8	Port1

Sunday / Monday / Tuesday / Wednesday / Thursday / Friday / Saturday Enable

Check box	Description	Factory Default
Unchecked	Disables the schedule for day selected	Unche
Check	Enables the schedule for day selected	

ed		ck ed

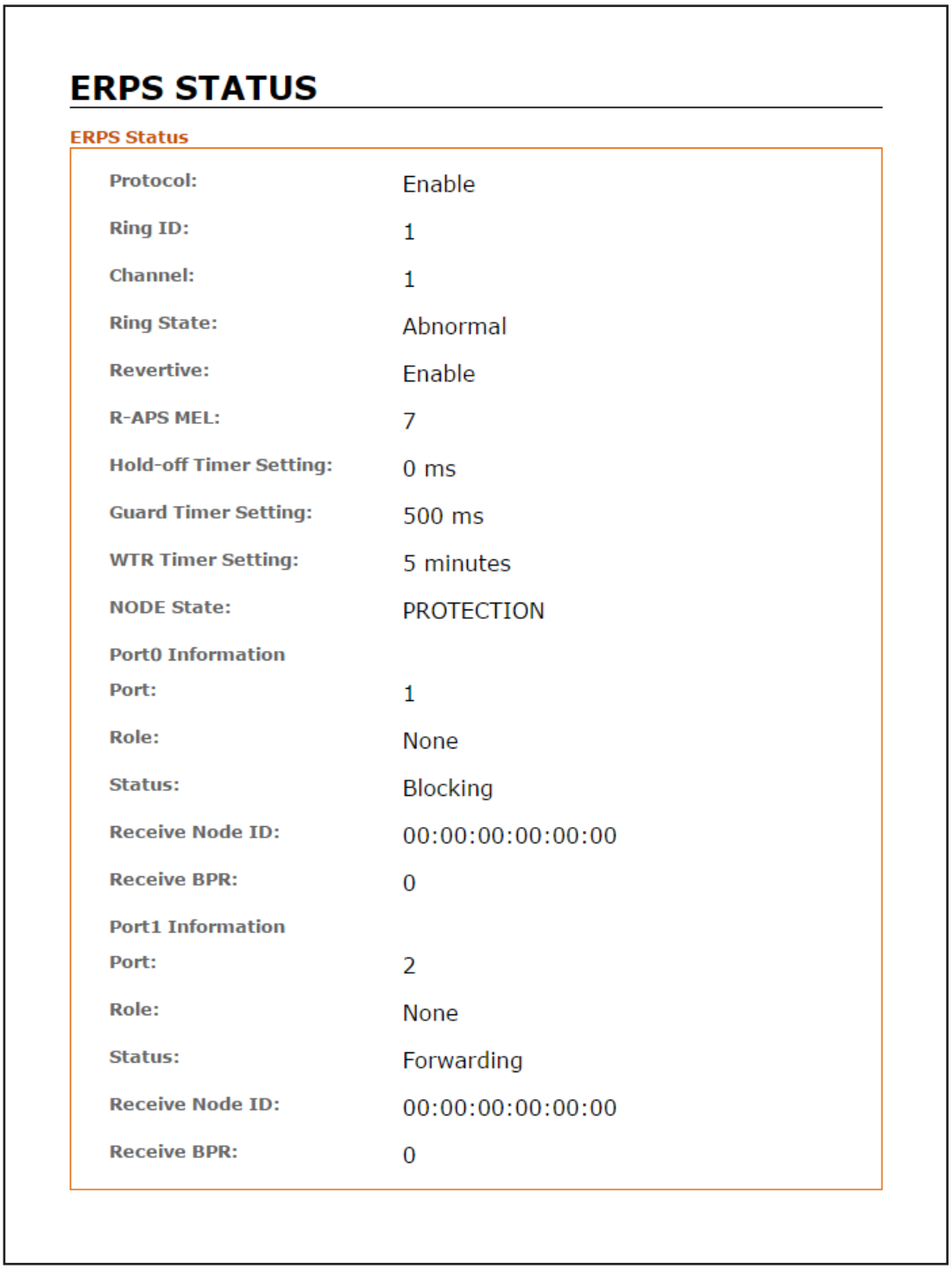
Start/ End Time

Setting	Description	Factory Default
Disable	PoE schedule is disabled	Disable
0~23	Select the start and end time for the Powered Device	

ERPS

Ethernet Ring Protection Switching (ERPS), defined in ITU-T G8032, implements a protection switching mechanism for Ethernet traffic in a ring topology. By performing the ERPS function, potential loops in a network can be avoided by blocking traffic to flow to the ring protection link (RPL) to protect the entire Ethernet ring. There can be only one RPL owner and neighbor for each ring. Owner and Neighbor ports must be connected for ring to function properly.

ERPS > ERPS STATUS



Item	Description
Protocol	Indicate ERPS protocol is enabled or disabled

Item	Description
Ring ID	ERPS ring ID, ranges from 1 to 239. Ring ID distinguishes different Ring topology.
Channel	ERPS Channel ID, ranges from 1 to 4094. It's a channel to send PDUs of ERPS.
Ring State	Displays ring port status.
Revertive	Indicates if Revertive Mode is enabled or disabled
R-APS MEL	Displays the R-APS MEL value
Hold-off Timer Settings	Displays the Hold-off Timer expiration setting
Guard Timer Setting	Displays the Guard Timer expiration setting
WTR Timer Setting	Displays the WTR (Wait to Restore) Timer expiration setting
NODE State	The following are the different states for each node of a specific ring: INIT - Not a participant of a specific ring. IDLE - No failure on the ring; the node is performing normally. For a normal node, traffic is unblocked on both ring ports. For the RPL owner or RPL neighbor, traffic is blocked on the ring port that connects to the RPL and unblocked on the other ring port. PROTECTION - A failure occurred on the ring. For a normal node, traffic is blocked on the ring port that connects to the failing link and unblocked on working ring ports. For the RPL owner, traffic is unblocked on both ring ports if they connect to non-failure links. PENDING - The node is recovering from a failure or its state after a clear command is used to remove the previous manual command. When a protection group is configured, the node enters the pending state. When a node is in pending state, the WTR or WTB timer will be running. All nodes are in pending state till WTR or WTB timer expiry. FORCE SWITCH - A force switch is issued. When a force switch is issued on a node in the ring, all nodes in the ring will move into the force switch state. MANUAL SWITCH - A manual switch is issued. When a manual switch is issued on a node in the ring all nodes in the ring will move into the manual switch state.

Port(x) Information

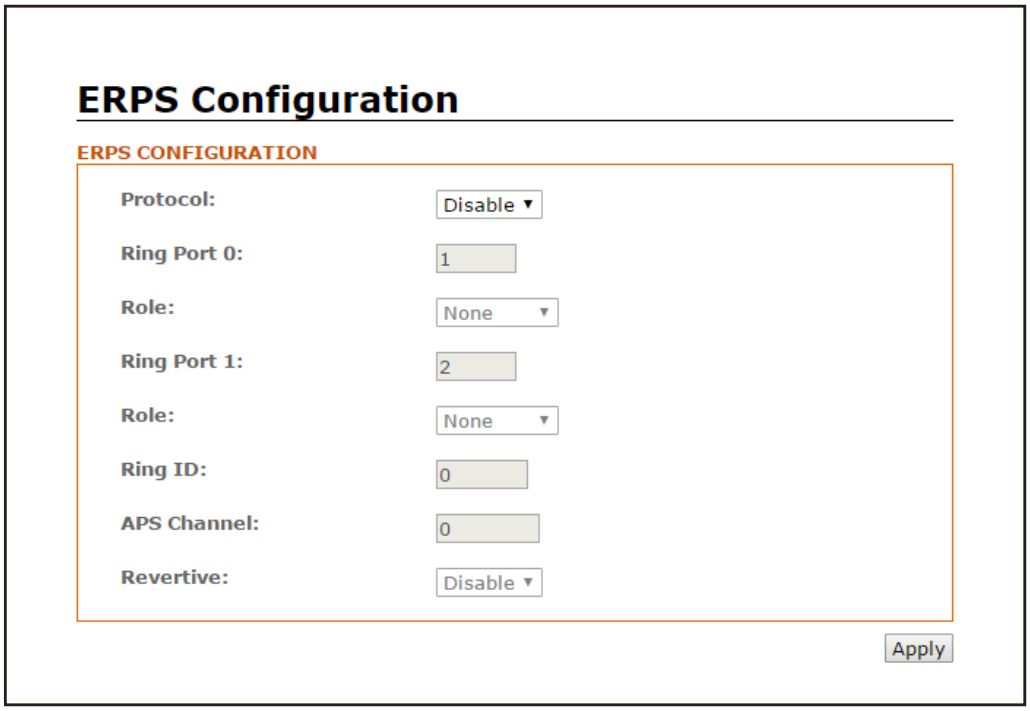
Item	Description
Port	Port number that is participating in the ring
Role	The following are the different states for ERPS role: Owner - In charge of blocking one side of RPL link. It will prevent the packet flow from its blocked port. Neighbor - In charge of blocking one side of RPL link. It will prevent the packet flow from its blocked port. None - Besides Owner and Neighbor node, all other nodes are defined as None node.
Status	Display the port status information
Receive	The MAC address of message source node

Node ID	
Receive BPR	Display the Receive BPR value

ERPS > ERPS Configuration

This page allows you to enable / disable ERPS and configure the ERPS settings.

NOTE: Before configuring ERPS, rapid spanning tree protocol (RSTP), or multiple spanning tree protocol is required to disabled. Only one protocol can be running within a switch at once.



Protocol

Setting	Description	Factory Default
Disable	Disables ERPS protocol	Disable
Enable	Enables ERPS protocol	

Ring Port 0

Setting	Description	Factory De

		fault
Port number	Switch port number that is participating in the ERPS ring.	1

Ring Port 1

Setting	Description	FactoryDefault
Port number	Switch port number that is participating in the ERPS ring.	2

NOTE: Ring port 1 and Ring port 0 must use different ports on switch.

Role

Setting	Description	FactoryDefault
None	Besides Owner and Neighbor node, all other of nodes are defined as None nodes.	None
Owner	In charge of blocking one side of the RPL link. This prevents packet flow from the blocked port.	
Neighbor	In charge of blocking one side of the RPL link. This prevents packet flow from the blocked port.	

Ring ID

Setting	Description	Factory Default
1~239	ERPS ring ID, ranges from 1 to 239. Ring ID distinguishes different Rings.	0

APS Channel

Setting	Description	Factory Default
1~4094	ERPS Channel ID, ranges from 1 to 4094. This is the channel set to send PDU (protocol data units) for the ERPS ring.	0

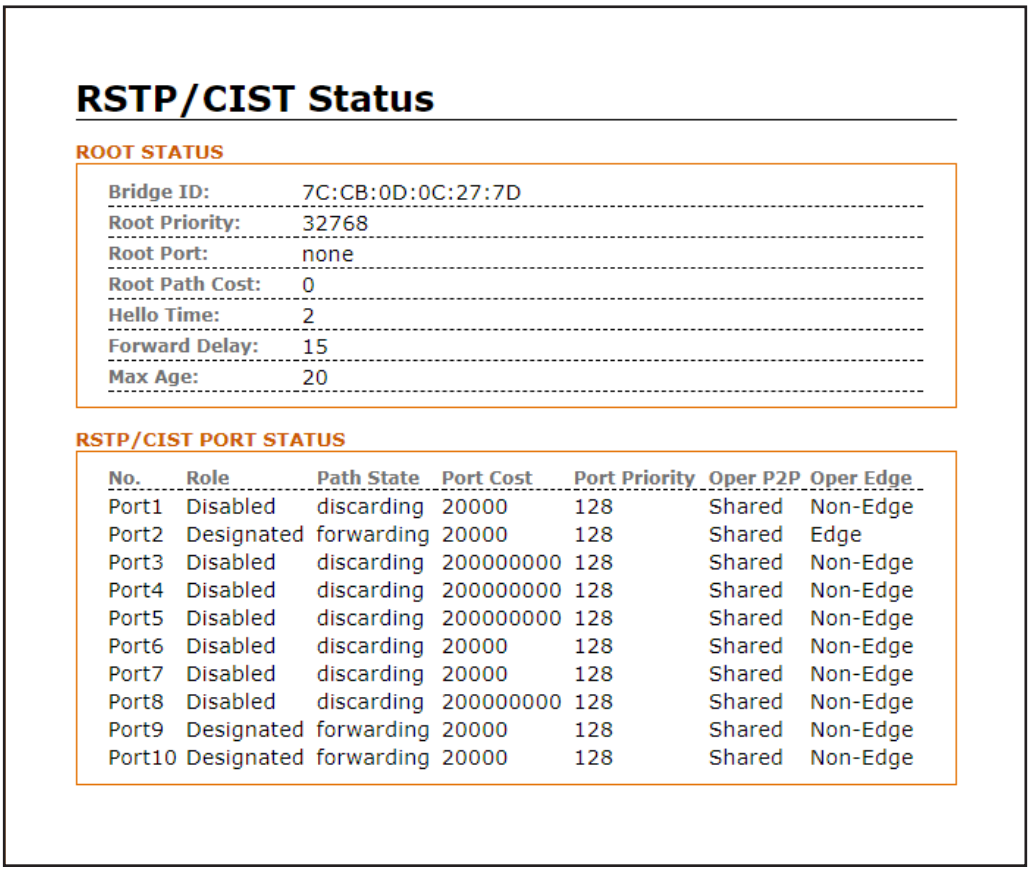
Revertive

Setting	Description	Factory Default
Disable	The failed ring link the port attached to it will remain blocked even the situation is eliminated.	Disable
Enable	The RPL link will be blocked for the time interval set by WTR timer after recovery from link failure situation. Otherwise, it will remain unchanged from the blocking state. That is, the failed link port will block permanently until the next event happen.	

Spanning Tree

Rapid Spanning Tree Protocol (RSTP), is defined by IEEE 802.1w. RSTP is an enhanced version of STP STP (Spanning Tree Protocol). It shares most of its basic operation characteristics, and creates a cascading effect away from the root bridge where each designated bridge proposes to its neighbors to determine if it should disable traffic to prevent a loop.

Spanning Tree > RSTP Status



Root Status

Item	Description
Bridge ID	The Bridge MAC address
Root Priority	The lowest priority will become the Root Bridge
Root Port	The port receiving traffic from the Root Bridge
Root Path Cost	The STP cost between this switch and the current root
Hello Time	Time interval between each Bridge Protocol Data Unit (BPDU) that is sent on a port
Forward Delay	Delay time in seconds unit network converts to forwarding state
Max Age	Maximum length of time that passes before a bridge port saves its configuration

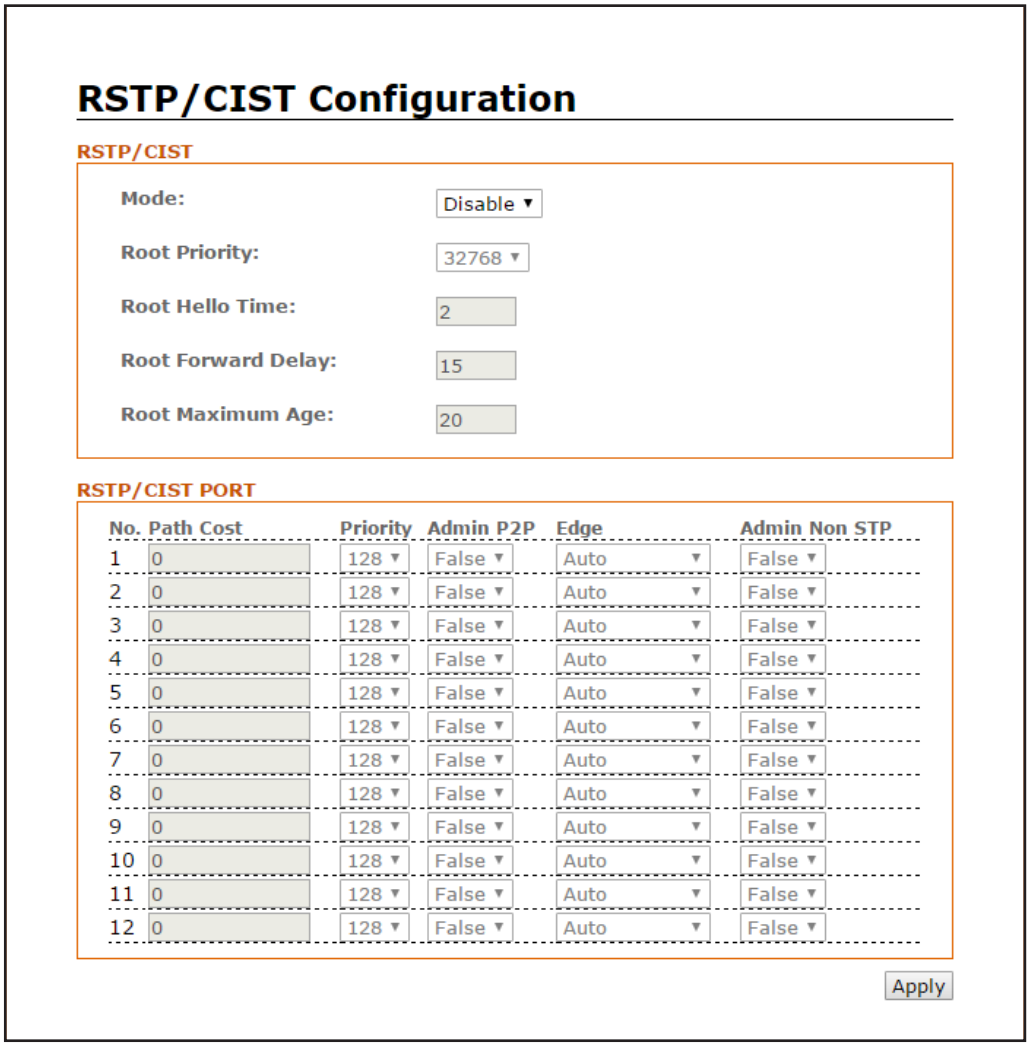
RSTP/CIST Port Status

Item	Description
No.	Port number of the switch

Item	Description
Role	The role of the port [Root] The port closest to the root bridge in terms of least path cost (based on BPDU) is determined to be the root port. [Designated] The designated port is the port that can send the best BPDU on the segment to which it is connected. [Alternate] The alternate port roles correspond to the blocking state of RSTP. [Disabled] There is no link on the port
Path State	The path to the Root Bridge. Forwarding indicates that traffic is moving across the port. Discarding indicates that the port is blocking traffic to prevent a loop
Port Cost	The Root Path Cost of the port
Port Priority	The Root Priority of the port
Oper P2P	The P2P status of the port
Oper Edge	The Edge status of the port

Spanning Tree > RSTP Configuration

This page allows you to enable / disable the RSTP function and configure the settings for each port.



Mode

Setting	Description	Factory Default
Disable	Disables RSTP function	Disable
RSTP	Enables RSTP function	
MSTP	Enables MSTP function	

Root Priority

Setting	Description	Factory Default

0~6144 0	The value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If there is any change of the value, the switch must be power cycled. The value must be multiple of 4096 according to the standard rule of the protocol.	32768

Root Hello Time

Setting	Description	Factory Default
1~10	Controls the time interval to send out the BPDU packet for checking RSTPs current status.	2

Root Forward Delay

Setting	Description	Factory Default
4~30	Enter a value between 4 and 30 for the number of seconds a port is to wait before changing from its learning and listening states to the forwarding state.	15

Root Maximum Age

Setting	Description	Factory Default
6~40	Enter a value between 6 and 40 for the number of seconds a bridge waits without receiving STP configuration messages before attempting a reconfiguration.	20

Path Cost

Setting	Description	Factory Default
0~200000000	Enter a value from 1 through 200000000 to define the path cost for the other switch from this transmitting switch at the specified port. When path cost is set to 0, the switches will be setup as automatic data transmitting.	0

Priority

Setting	Description	Factory Default
0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240	Enter a number 0 through 240 to decide which port should be blocked by priority. The value of priority must be the multiple of 16.	128

Admin P2P

Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other switch (i.e. It is served by a point-to-point LAN segment), or it can be connected to two or more switches (i.e. It is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively.

Setting	Description	Factory Default
False	Disables P2P function	False
True	Enables P2P function	

Edge

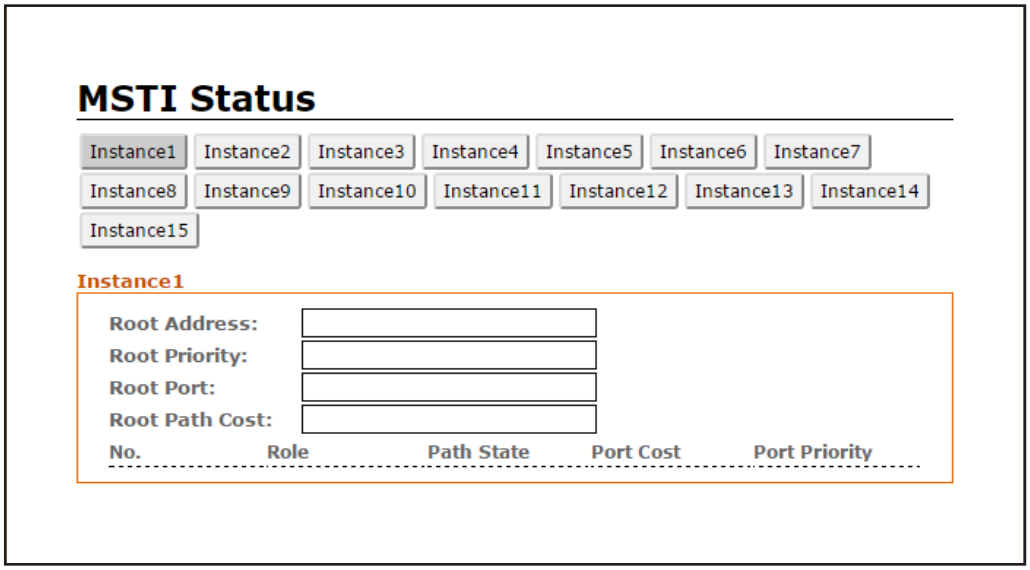
Setting	Description	Factory Default
Auto	If any incoming RST BPDU is received from a previously configured Edge port, 802.1W automatically makes the port as a non-edge port.	Auto
Admin True	Enables Admin Edge Port	
Admin False	Disables Admin Edge Port	

Admin Non STP

Setting	Description	Factory Default
False	Includes the STP mathematic calculation.	False
True	Not includes STP mathematic calculation.	

Spanning Tree > MSTI Status

This page shows Multiple Spanning Tree Instance (MSTI) status.



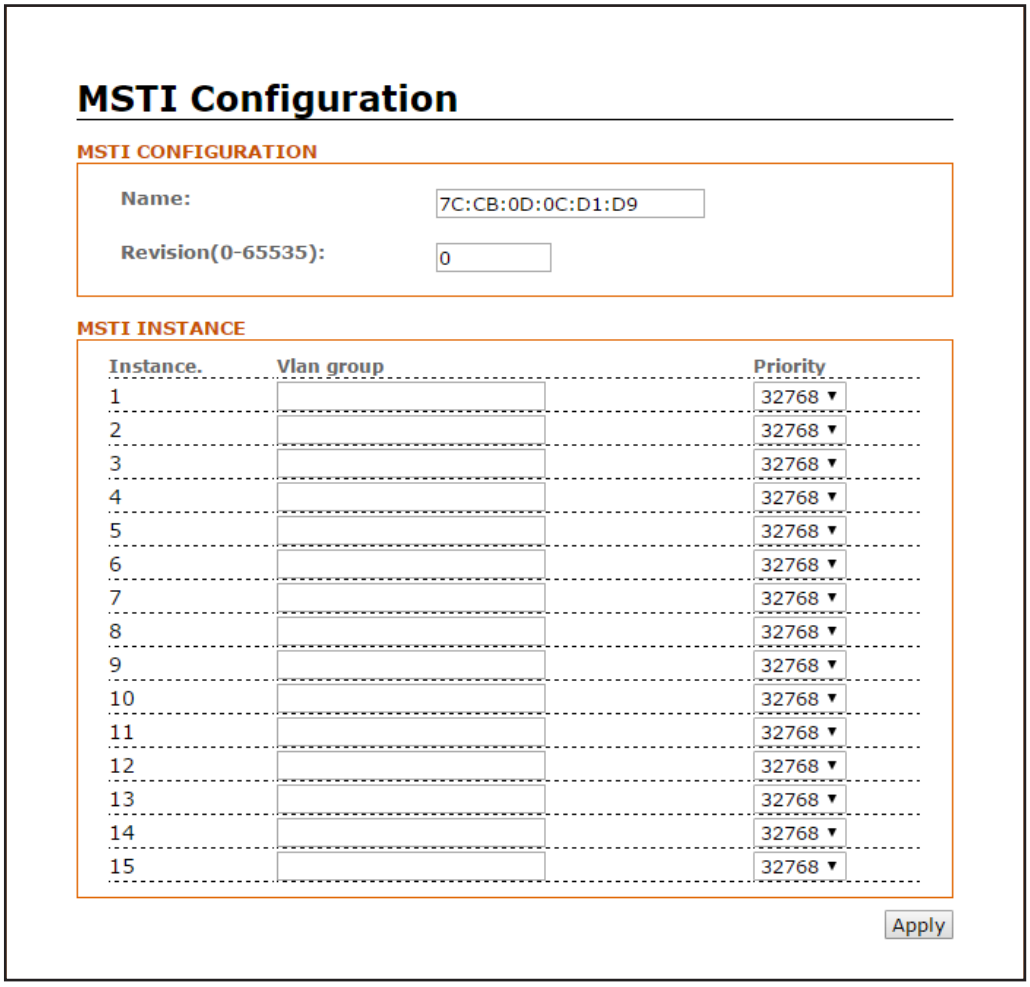
Instance1~15 buttons

These buttons allow you to select Instance Tab #1~#15 to configure each MSTI port **Cost** & **Priority** value.

Instance1~15

Item	Description
Root Address	The root address of the MST instance
Root Priority	The switch priority for the designated instance
Root Port	The root port for the designated instance
Root Path Cost	The root cost for the MST instance

Spanning Tree > MSTI Configuration



MSTI Configuration

Item	Description
Name	The MAC address of the bridge switch.
Revision (0-65535)	Specifies the revision level for MSTP that you are configuring on the switch. The default revision number is 0.

MSTI Instance

Item	Description
Instance	Instance number

Vlan group

Setting	Description	Factory Default
Vlan Numb	Enter Vlan information of the instance. Max value is 4094.	None

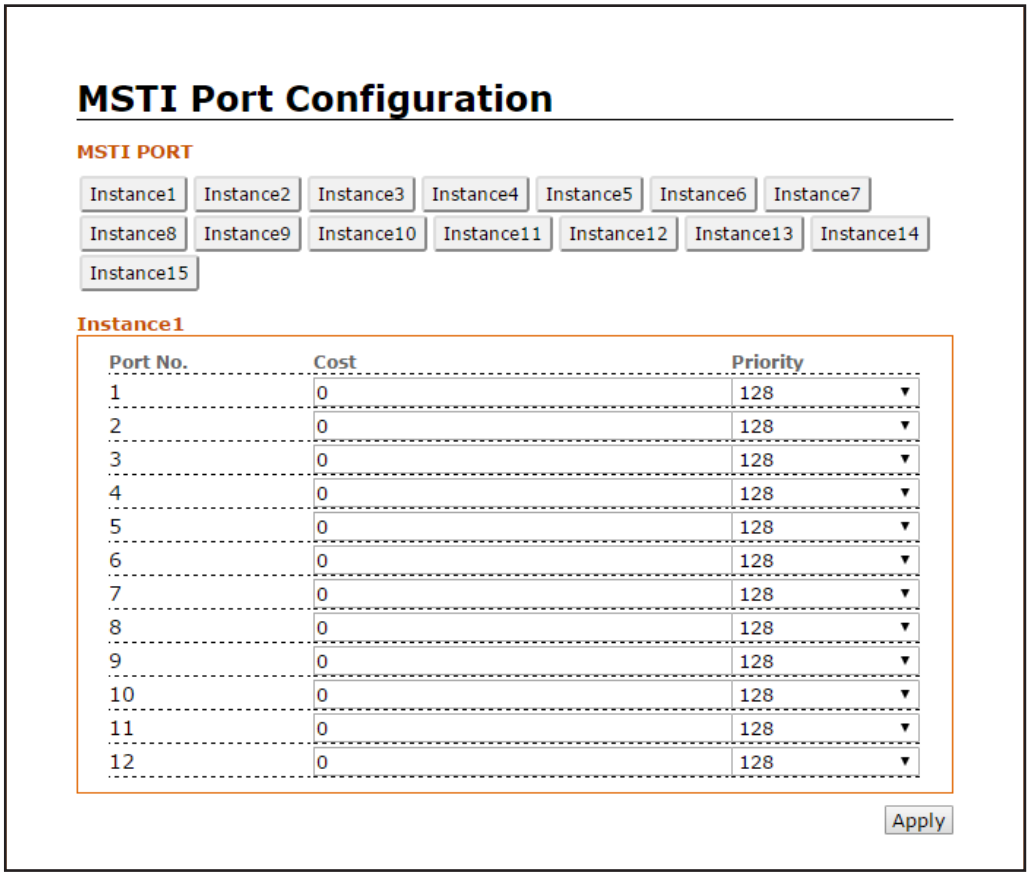
er		

Priority

Setting	Description	Factory Default
0 ~ 61440	Used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. The switch is required to reboot when there is a value change. The value must be a multiple of 4096 according to the standard rule of the protocol.	32768

Spanning Tree > MSTI Port Configuration

This page allows you to configure and view parameters per MST Instance.



Instance

Item	Description
No.	Port number of the switch

Cost

Setting	Description	Factory Default
0~200000000	Defines the path cost value from 1 through 200000000 to the other bridge from this transmitting bridge at the specified port.	0

Priority

Setting	Description	Factory Default
0, 16, 3	Enter a number 0 through 240 to decide which port should be blocked by priority. The value of priority must be the multiple of 16.	128

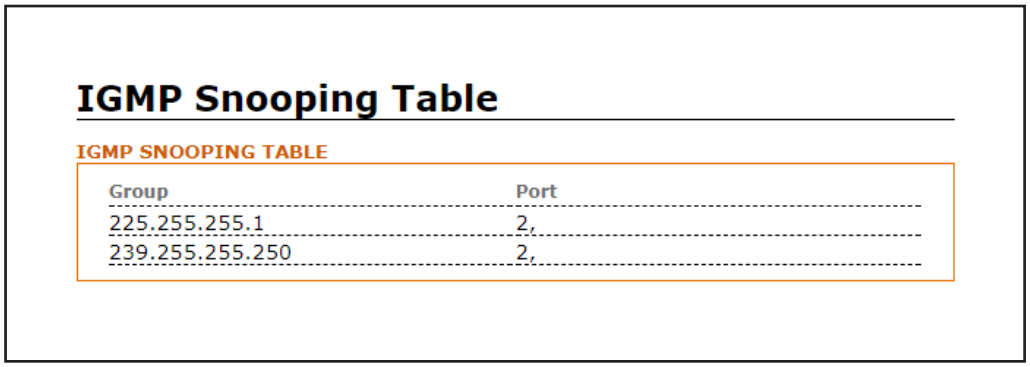
2,48,64,80,96,112,128,144,160,176,192,208,224,240		

IGMP Snooping

The Internet Group Management Protocol (IGMP) 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.

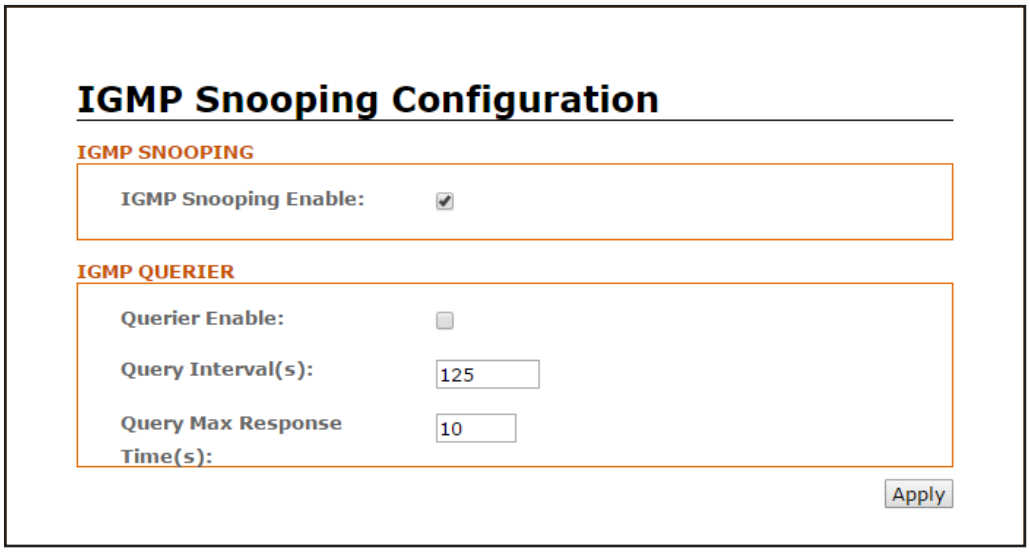
IGMP Snooping > IGMP Snooping Stream Table

Multicast filtering is the system by which end stations only receive multicast traffic if they register to join specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end stations.



IGMP Snooping > IGMP Snooping Configuration

This page allows you to enable / disable the IGMP Snooping function and configure the settings.



IGMP Snooping Enable

Setting	Description	Factory Default
Checked	Enables the IGMP Snooping function	Checked
Unchecked	Disables the IGMP Snooping function	

Query Enable

Setting	Description	Factory Default
Checked	Enables the Querier	Unchecked
Unchecked	Disables the Querier	

Query Interval(s)

Setting	Description	Factory Default
1 ~ 3600	The frequency at which the querier sends query messages. These messages are used to build the IGMP snooping tables.	125

Query Max Response Time(s)

Set	Description	Factory Default

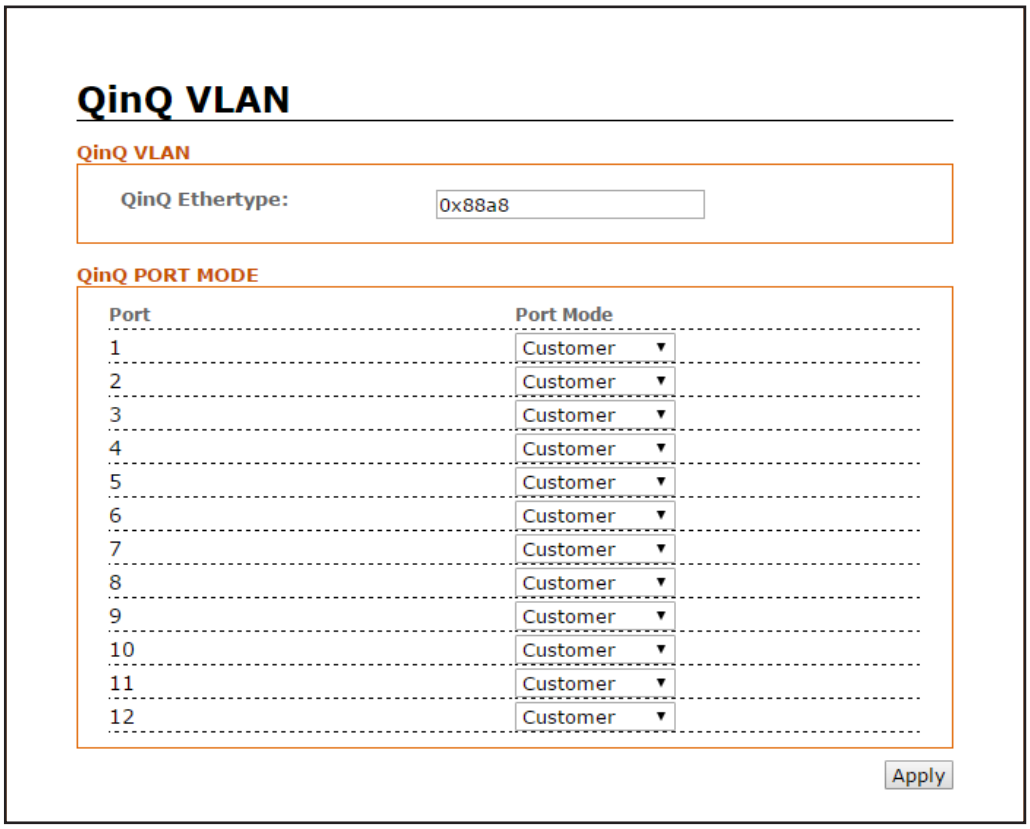
ing		
1 ~ 12	The maximum response time advertised.	10

VLAN

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which allows users to isolate network traffic. Only the members of a VLAN will receive traffic from the same members on that VLAN. Creating a VLAN on a switch is the equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still physically plugged into the same switch.

VLAN > QinQ VLAN

This page allows you to configure IEEE 802.1Q-in-Q (Q-in-Q) VLAN.



QinQ Ethertype

Setting	Description	Factory Default
0x0001~0xFFFF	It is used to indicate which protocol is encapsulated in the payload of the frame. The same field is also used to indicate the size of some Ethernet frames. Ethertype was first defined by the Ethernet II framing standard, and later adapted for the IEEE 802.3 standard.	0x88a8

Port

Item	Description
Port No.	Port Number on switch

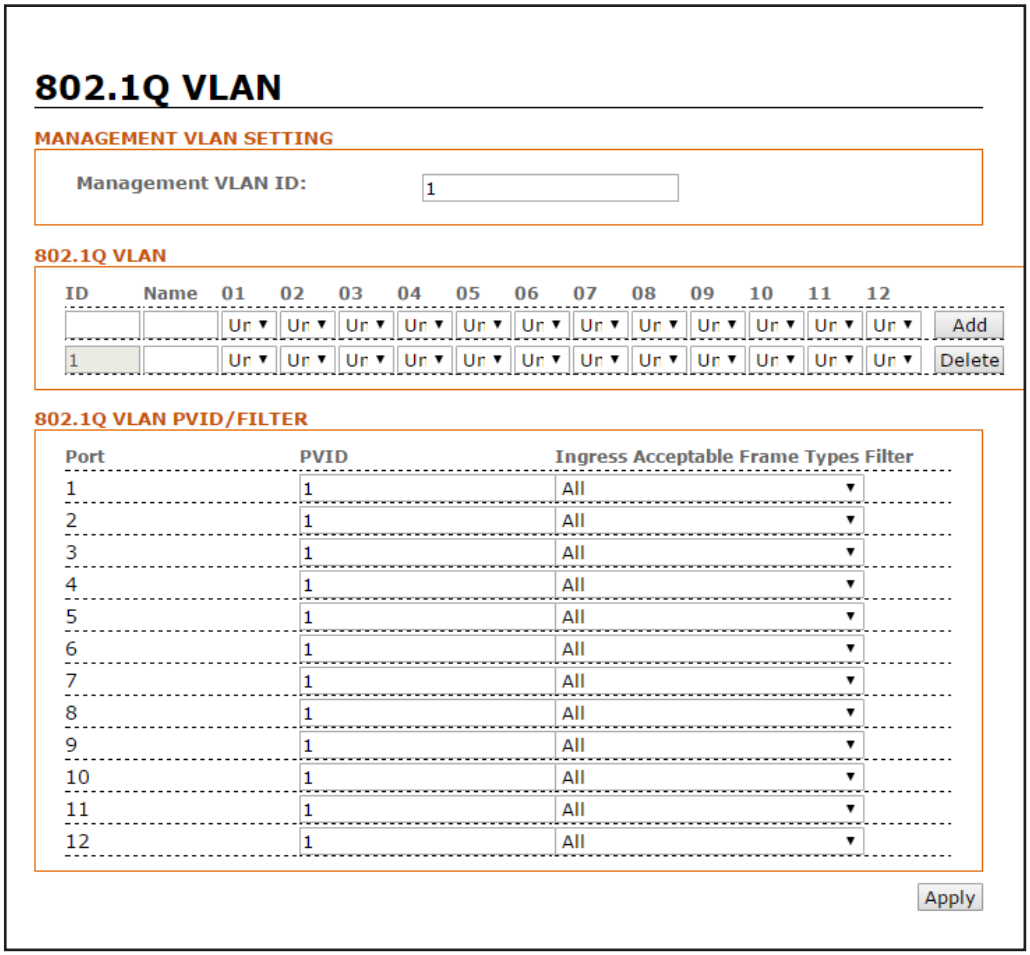
Port Mode

Setting	Description	Factory Default
Custo	Specifics the port to the general port	Cus

mer		tom er
Dot1q - tunnel	Specifics the port to the client port	
Provi der	Specifics the port to the ISP port	

802.1Q VLAN

This page allows you to configure Vlan (IEEE 802.1Q) protocol.



Management VLAN ID

Setting	Description	Factory Default
1 ~ 4094	Set the VLAN ID of management VLAN. The management VLAN is the VLAN on which the switch expects to receive management traffic.	1

802.1Q VLAN

Item	Description	Factory Default
ID	Vlan ID. VLANs that have the same ID will treated as if on the same network, devices with different Vlan IDs will not be able to see each other.	None
Name	The name of this VLAN. VLAN names can be different in each switch.	None

802.1Q VLAN PVID/ Filter

Item	Description	Factory Default
Port	Port Number on the switch	None
PVID	When a frame comes into the port, it will be tagged with the PVID if the frame is without VLAN tag.	1

Item	Description	Factory Default
Ingress Acceptable Frame Types Filter	An incoming frame will be dropped or forwarded according to the port filter. [All] All frames are forwarded. [Tagged] Only the frames with 802.1Q tags can be forwarded, untagged frames will be dropped. [Untagged] Only the frames without a 802.1Q tag can be forwarded, tagged frames will be dropped.	All

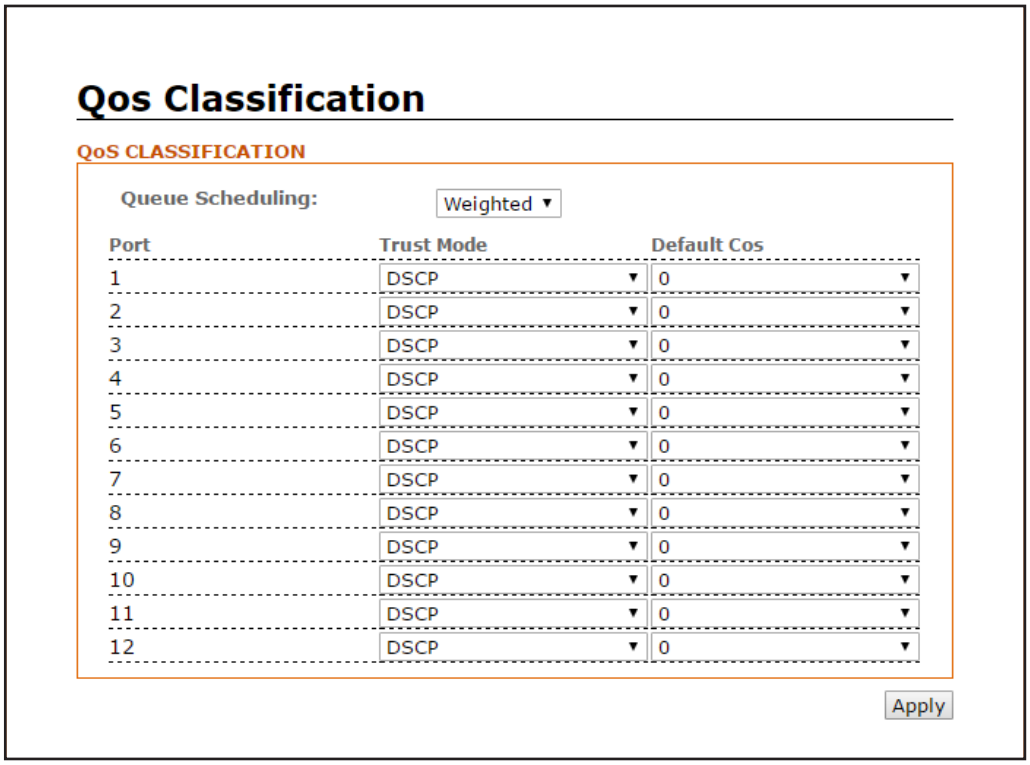
QoS

QoS provides the ability to assign different priorities to different devices which can be improved through traffic shaping methods. These methods include prioritization of packets and device classification. A priority queue is a data type which identifies an item with the highest priority in a system. The CoS Mapping is used to map each CoS value to a QoS priority queue. The purpose of this is to prioritize the type of traffic at congestion points of the network.

Some devices provide QoS based IEEE 802.1p class of service (CoS) values and Differentiated Services Code Point (DSCP) values for implementing Quality of Service (QoS) at the Media Access Control level.

QoS > QoS Classification

This page allows you to configure QoS Classification.



Queue Scheduling

Setting	Description	Factory Default
Weighted	Weighting applies a round robin priority to the queues. The queues are emptied from highest to lowest priority by frame rates of 8, 4, 2, 1.	Weighted
Strict	Gives egress queues with higher priority to be transmitted first before lower priority queues are serviced. An entire queue must be emptied before moving to the next set.	

Trust Mode

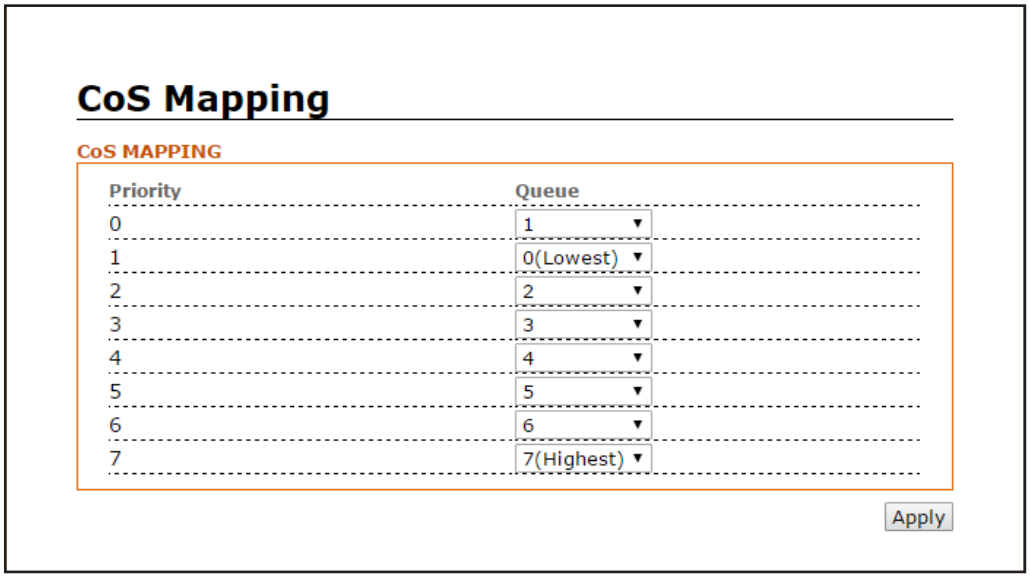
Setting	Description	Factory Default
DSCP	Only trusted DSCP (Differentiated Services Code Point) values are mapped to a specific QoS class and drop precedence level (DPL). Frames with untrusted DSCP values are treated as non-IP frames.	DSCP
CoS	(Class Of Service) is known as 802.1p. It describes that the output priority of a packet is determined by user priority field in 802.1Q VLAN tag. The priority value supports 0 to 7 CoS values maped to 4 priority levels.	
Queues	Highest, SecHigh, SecLow, and Lowest.	

Default CoS

Setting	Description	Factory Default
0~7	Set each port's priority queue from 0 to 7. By default 0 is the highest, and 7 is the lowest.	0

QoS > CoS Mapping

This page allows you to configure Class of Service (CoS) Mapping.



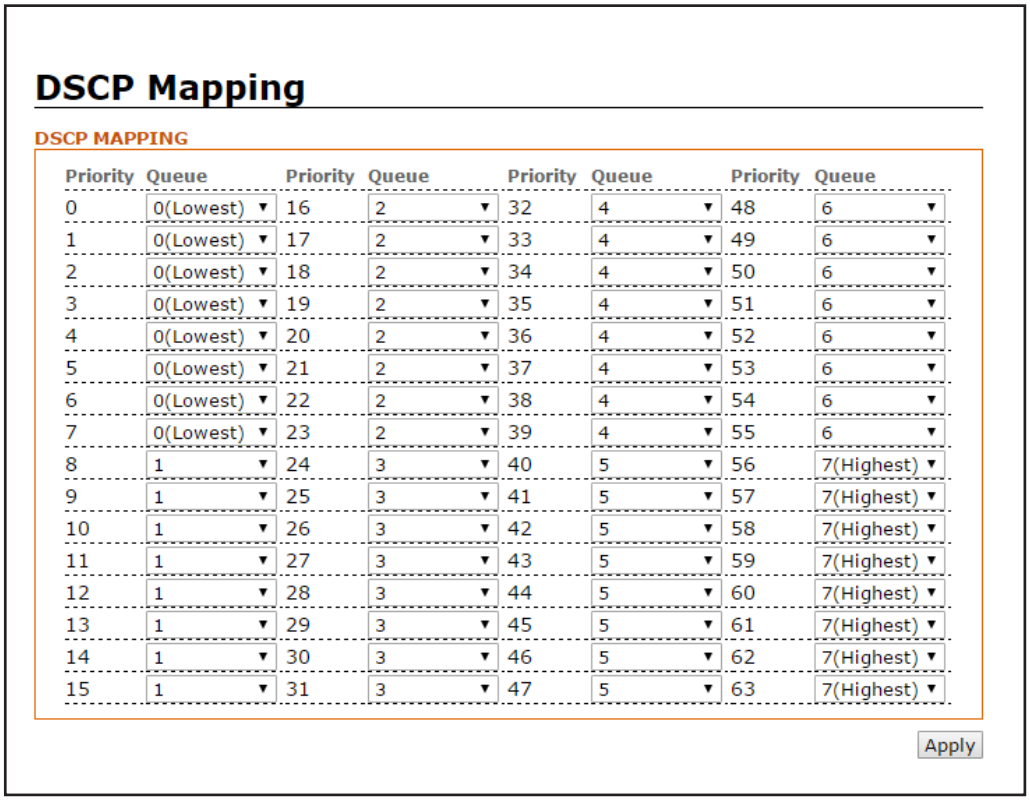
CoS Mapping

Setting	Description	Factory Default
0(Lowest)~7(Highest)	Maps different CoS values to 0~7 designated egress queues.	0: 1 1: 0(Lowest) 2: 2 3: 3 4: 4
		5: 5
		6: 6 7: 7(Highest)

NOTE: Priority 0 is set as queue 1 so unprioritized packets are given some weight in the network.

QoS > DSCP Mapping

This page allows you to configure Differentiated Services Code Point (DSCP) Mapping.



DSCP Mapping

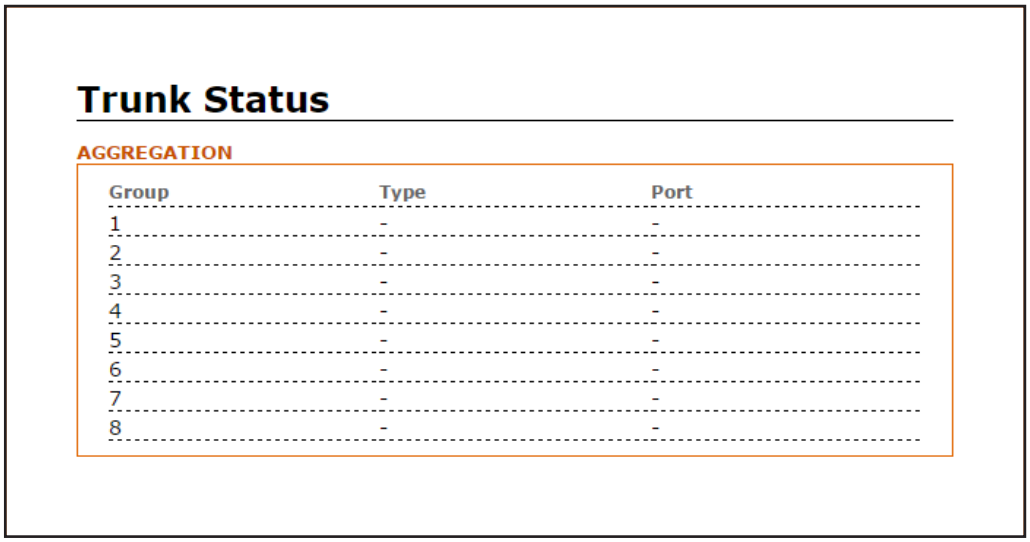
Setting	Description	Factory Default
0(Lowest)~7(Highest)	Maps different DSCP values to 0~7 designated egress queues.	0~7: 0(Lowest) 8~15: 1 16~23: 2 24~31: 3 32~39: 4 40~47: 5 48~55: 6 56~63: 7(Highest)

Port Trunk

Port Trunk, also called Link Aggregation, is a method of combining multiple network connections in parallel. It is to increase throughput beyond what a single connection could sustain. For example, if the application requires a 5-Gigabit link, and each port supports only 1-Gigabit link, the Port Trunk allows users to link 5
1- Gigabit ports together to obtain a 5-Gigabit trunk. There are 2 types of Port Trunk. One is LACP (dynamic) and the other is Static.

- LACP mode is more flexible, and it can change modes, either trunk or single port.
- Dynamic Port Trunk also provides a redundancy function, in case one of the links fail. If one of the trunk members has failed, it will still work well in LACP mode, but it will show link down if using static mode. Although not advised. Static mode is still necessary, some devices only support static trunks.

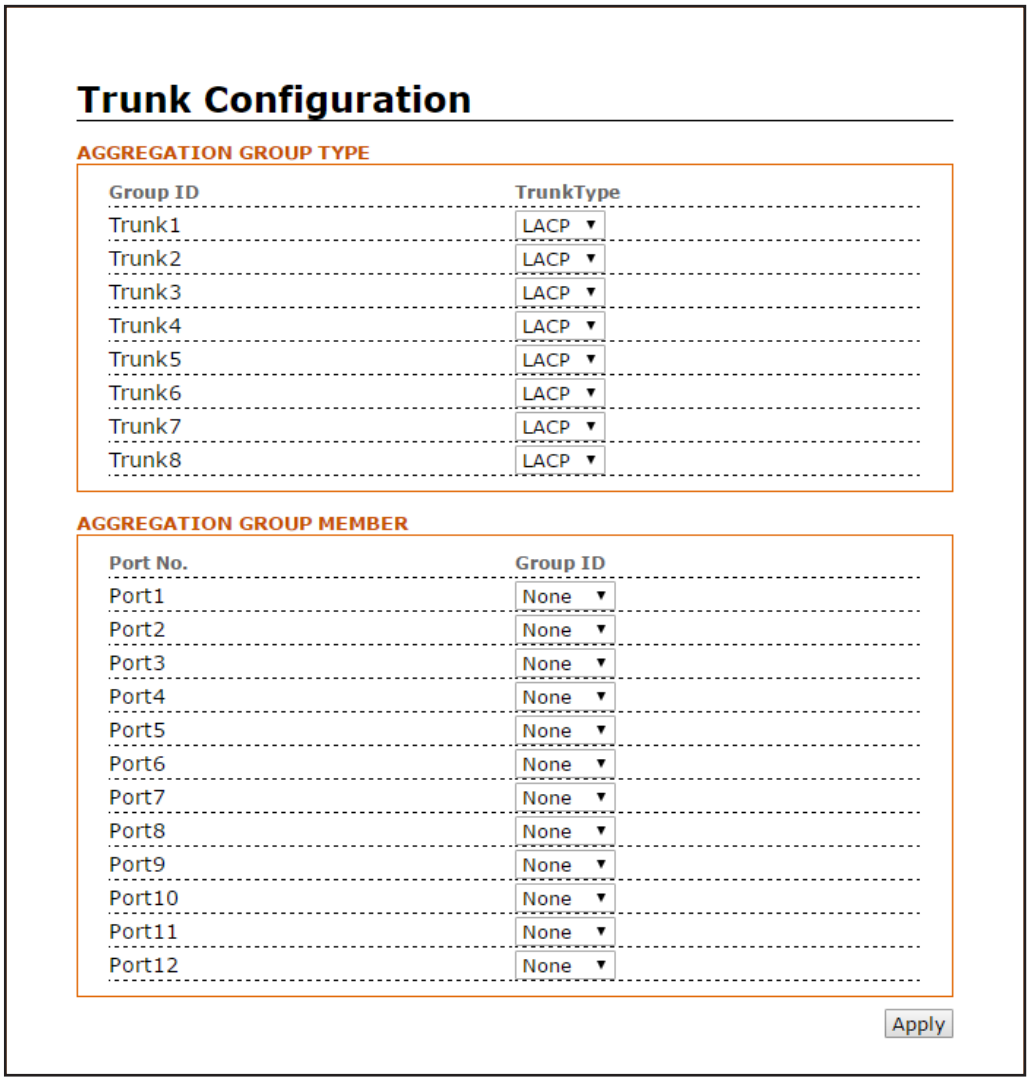
Port Trunk > Trunk Status



Aggregation

Item	Description
Group	Trunk group number.
Type	Truck type of aggregated group (LACP or static)
Port	The port numbers of aggregated group members

Port Trunk > Trunk Configuration



Aggregation Group Type

Item	Description
Group ID	Name of aggregated ports.

DSCP Mapping

Setting	Description	Factory Default
LACP	Dynamic trunking. If a link in a trunk goes down, the traffic will be routed to the remaining links.	LACP
Static	Static trunking. If any link goes down in the trunk the entire trunk will go down.	

Aggregation Group Member

Item	Description
Port No.	The port number on the switch being aggregated into a group.

Group ID

Setting	Description	Factory Defa

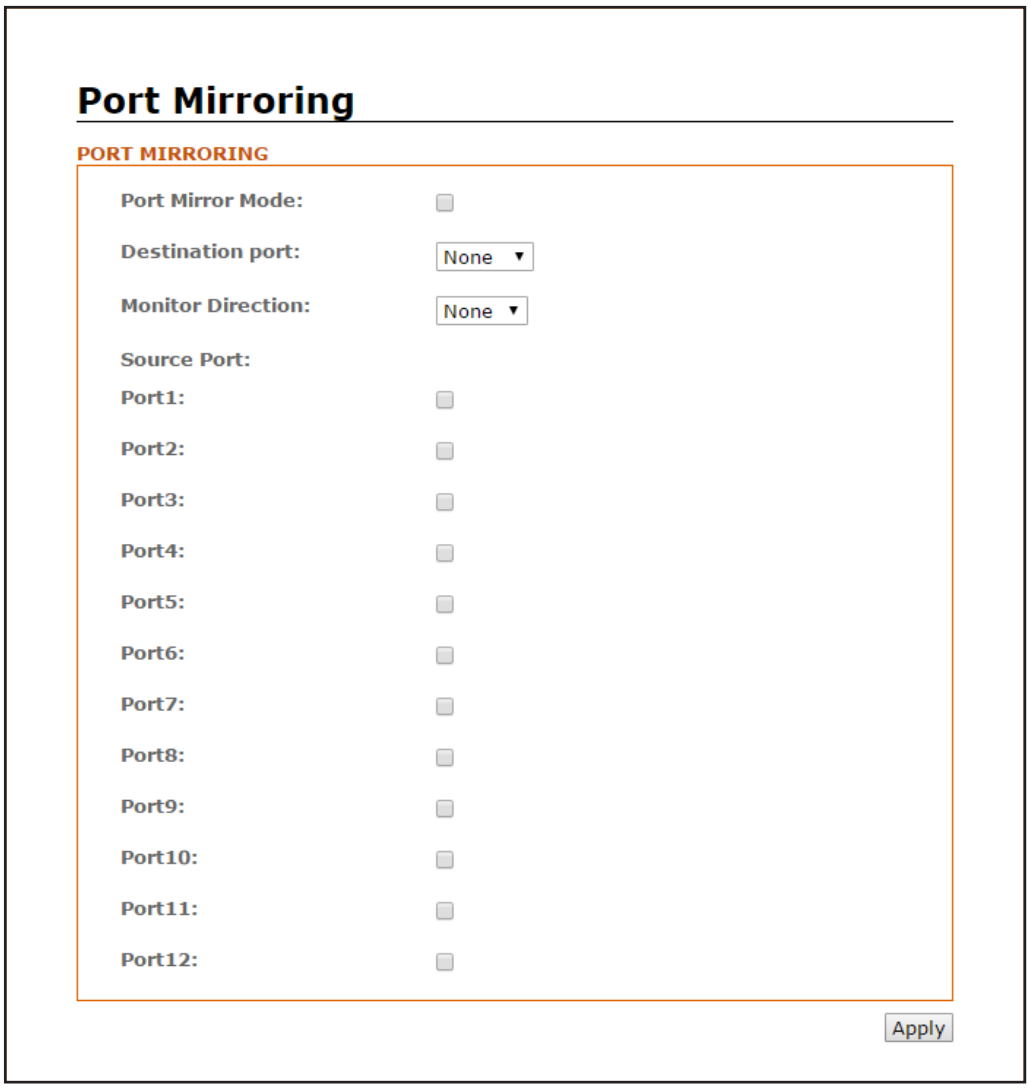
		ult
None	Disables the mapping function.	Non e
Trunk1~ Trunk8	Assigns port to Trunk1~Trunk8.	

Port Mirroring

Port mirroring is an approach to monitoring network traffic that involves forwarding a copy of each packet from one network switch port to another.

Port Mirroring > Port Mirroring

This page allows you to enable / disable port mirroring feature. When enabled, a matching copy of frames will be mirrored to the destination port specified in the port mirroring interface.



Port Mirroring Mode

Setting	Description	Factory Default
Unchecked	Disables Port Mirroring function.	Unchecked
Checked	Enables Port Mirroring function.	

Destination Port

Setting	Description	Factory Default
None	No destination port	None

Port number	Select one port to be the destination (mirroring) port for monitoring both RX and TX traffic coming from the source port.	

Monitor Direction

Setting	Description	Factory Default
None	Disables monitor function	None
Tx	Monitors Tx traffic coming (outgoing traffic)	
Rx	Monitors Rx traffic coming (incoming traffic)	
Tx/Rx	Monitors Tx/Rx traffic coming (Bi directional traffic)	

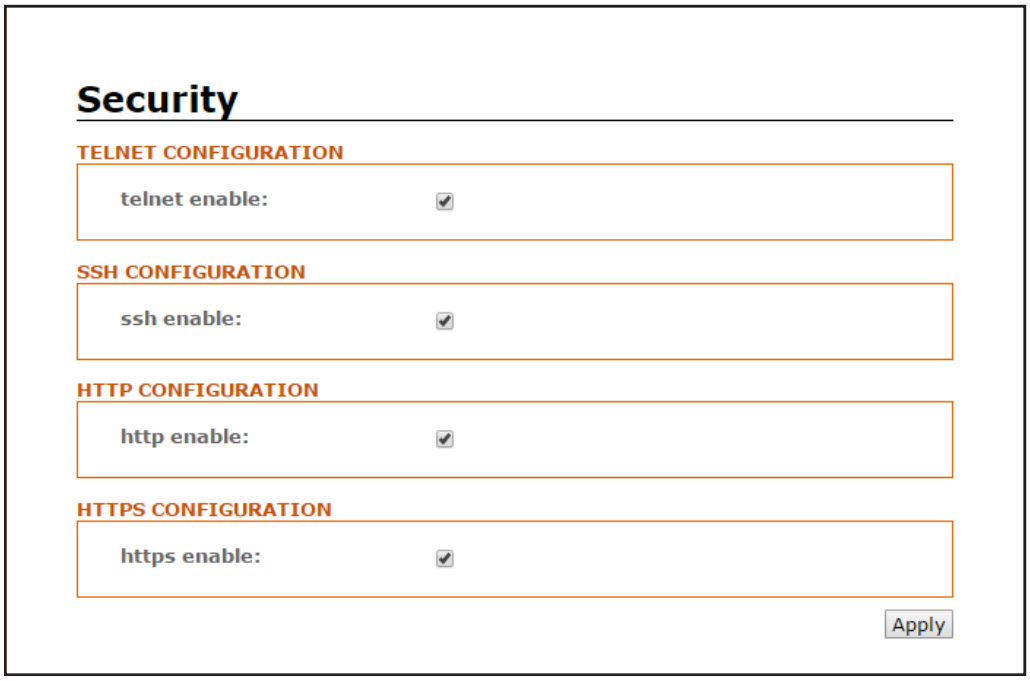
Source Port: Port1 ~ Port12

Setting	Description	Factory Default
Unchecked	Disables Port Mirroring function of the port.	Unchecked
Checked	Enables Port Mirroring function of the port to send traffic to the destination port.	

Security

You can access the command-line interface and web interface on the device over the network. This page allows you to enable / disable the Telnet, SSH, HTTP and HTTPS access.

Security > Security



telnet enable

Setting	Description	Factory Default
Checked	Allows telnet access	Checked
Unchecked	Denies telnet access	

ssh enable

Setting	Description	Factory Default
Checked	Allows ssh access	Checked
Unchecked	Denies ssh access	

http enable

Setting	Description	Factory Default
Checked	Allows http access	Checked
Unchecked	Denies http access	

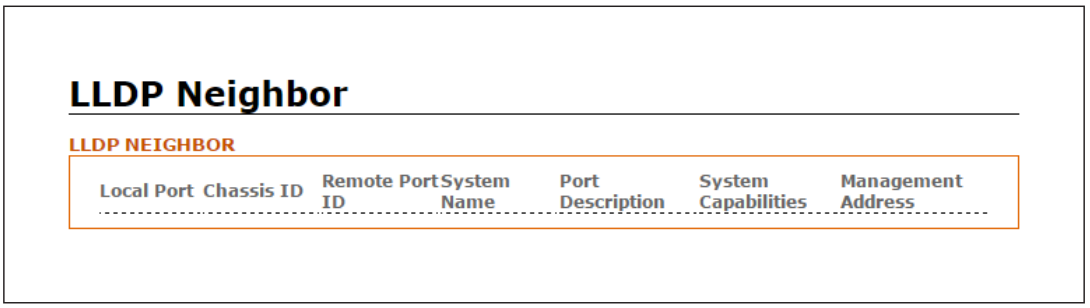
https enable

Setting	Description	Factory Default
Checked	Allows https access	Checked
Unchecked	Denies https access	

LLDP

LLDP is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.

LLDP > LLDP Neighbor

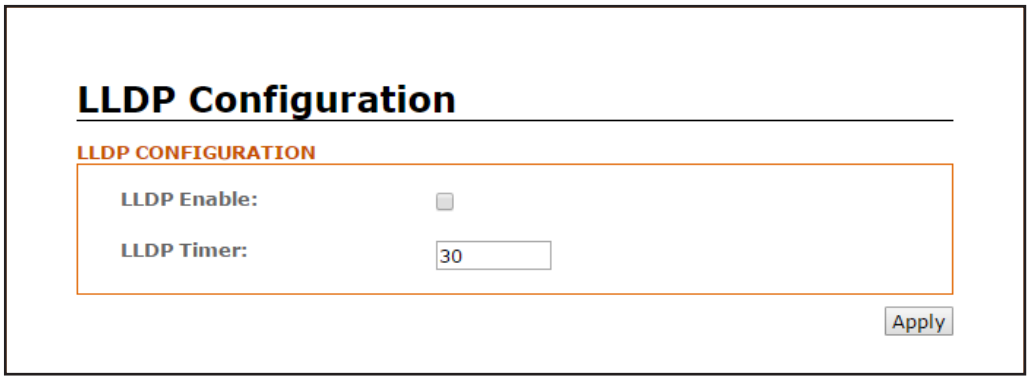


LLDP Neighbor

Item	Description
Local Port	The port which connects directly/ indirectly to the LLDP device, used to transmit/ receive LLDP packets.
Chassis ID	The MAC address of the LLDP neighbor.
Remote Port ID	The number of the port which connects directly/ indirectly to this local switch.
System Name	The device name defined on the LLDP neighbor.
Port Description	The description for the port defined on the LLDP neighbor.
System Capabilities	The capabilities of the LLDP neighbor, including: 1. Bridge: Layer 2 devices, like switches, used in LAN 2. Router: Layer 3 devices which used to connect to Internet 3. WLAN Access Point: Wireless devices Capabilities always follows by a (+) or (-). (+) means **enabled** and (-) means **disabled**.
Management Address	The IP address of the LLDP neighbor. User can access and configure the system by this management address.

LLDP > LLDP Configuration

This page allows you to enable / disable the LLDP function and configure the settings.



LLDP Enable

Setting	Description	Factory Default
Unchecked	Disables LLDP function	Unchecked
Checked	Enables LLDP function	

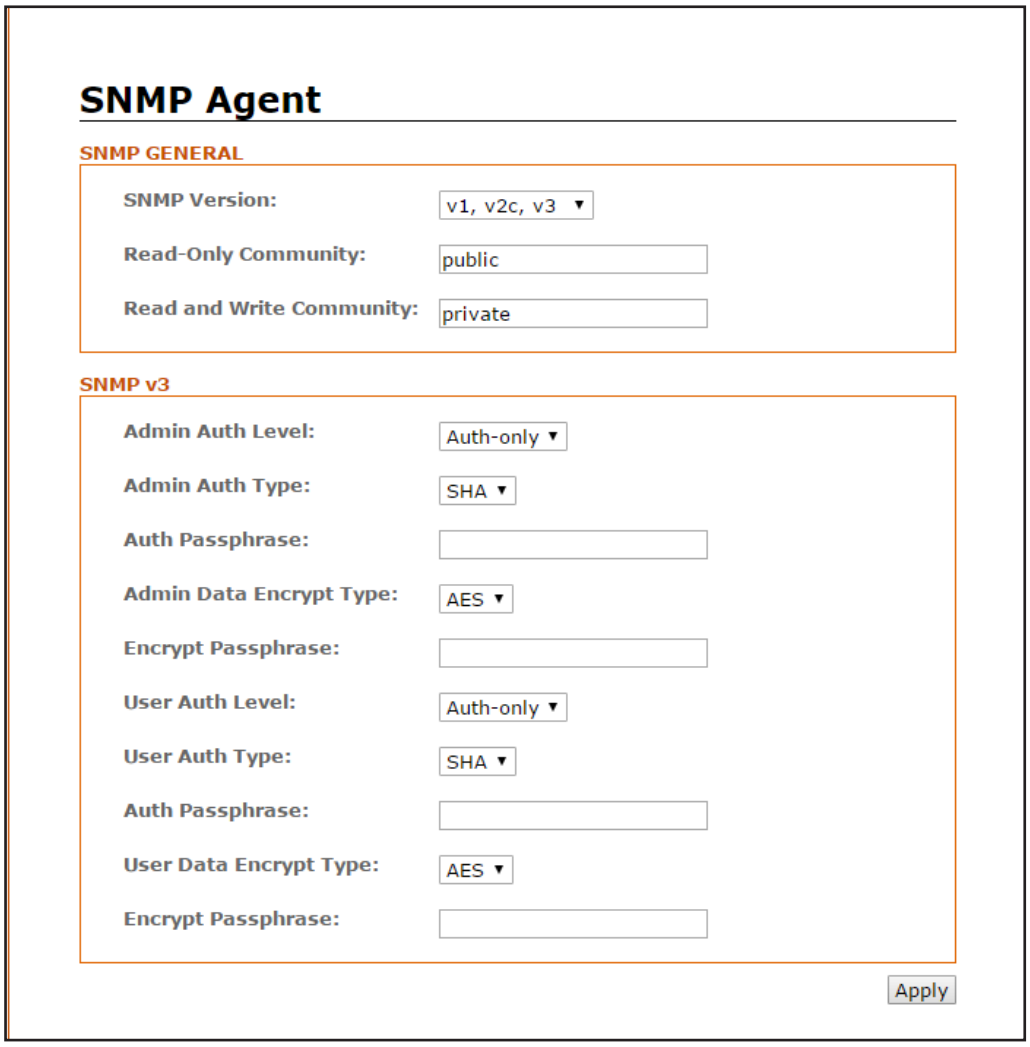
LLDP Timer

Setting	Description	Factory Default
5~32768	Sets the transmit interval of LLDP messages, in seconds.	30

SNMP

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

SNMP > SNMP Agent



SNMP Version

Setting	Description	Factory Default
v1, v2c, v3	Specifies the SNMP protocol compatible v1, v2c & v3 versions.	v1, v2c, v3
v1, v2c-only	Specifies the SNMP protocol compatible v1 & v2c versions.	
v3-only	Specifies the SNMP protocol compatible only v3 version.	
None	Disables the SNMP agent	

Read-Only Community

Setting	Description	Factory Defa

		ult
Max. 32 characte rs	Specifies the community string to verify read-only access to the SNMP agent. The SNMP agent will use this community string to access all objects with read-only permissions.	publi c

Read and Write Community

Setting	Description	Factory Default
Max. 32 characters	Specifies the community string to verify read and write access to the SNMP agent. The SNMP agent will use this community string to access all objects with read and write permissions.	private

Admin Auth Level

Setting	Description	Factory Default
Auth-only	Authentication without encryption	Auth-only
Both	Authentication with encryption	
None	No authentication	

Admin Auth Type

Setting	Description	Factory Default
SHA	Authentication is performed by using a SHA privKey	SHA
MD5	Authentication is performed by using a MD5 privKey	

Auth Passphrase

Setting	Description	Factory Default
8~32 characters	The string is used to authenticate (Admin and Manager)	None

Admin Data Encrypt Type

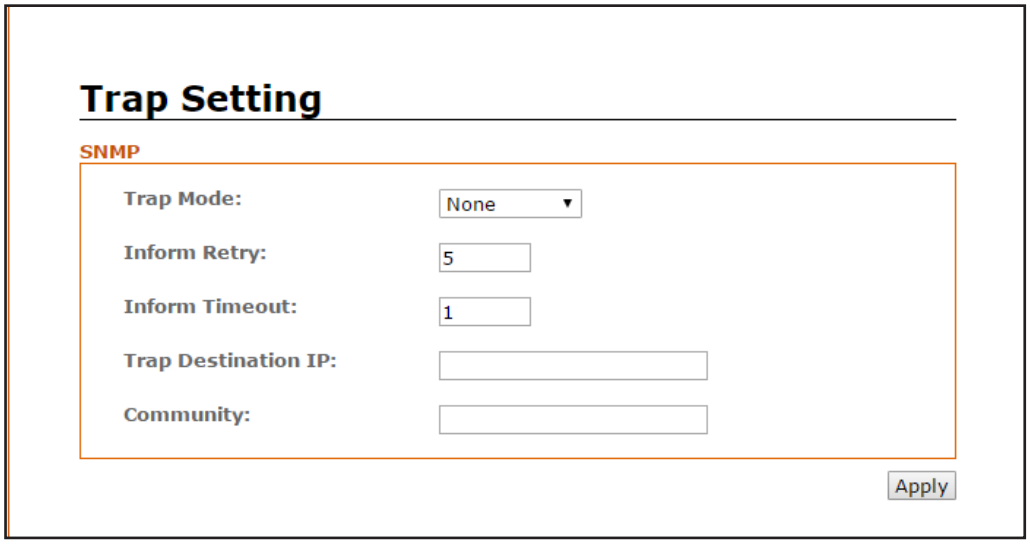
Setting	Description	Factory Default
AES	Encrypts administrator's data with AES algorithm	AES
DES	Encrypts administrator's data with DES algorithm	

Encrypt Passphrase

Setting	Description	Factory Default
8~32 characters	This string is used to encrypt data (Admin)	None

SNMP > Trap Setting

This page allows you to enable / disable the SNMP Trap function and configure the settings.



Trap Mode

Setting	Description	Factory Default
None	Disables SNMP Trap	None
Trap v1	Send SNMP v1 trap message once	
Trap v2c	Send SNMP v2c trap message once	
Inform (v2c)	Retry to send SNMP v2c trap message based on the number of **Inform Retry** settings	

Inform Retry

Setting	Description	Factory Default
1~100	Specifies the number of times the SNMP agent should resend the inform if it does not get the acknowledgment after sending of inform once. This field is valid only when **Trap Mode** is set to **Inform**.	5

Inform Timeout

Setting	Description	Factory Default
1~300 (in second)	Specifies the time that the agent should wait after sending a confirmation request. This field is valid only when **Trap Mode** is set to **Inform**.	1

Trap Destination IP

Setting	Description	Factory Default

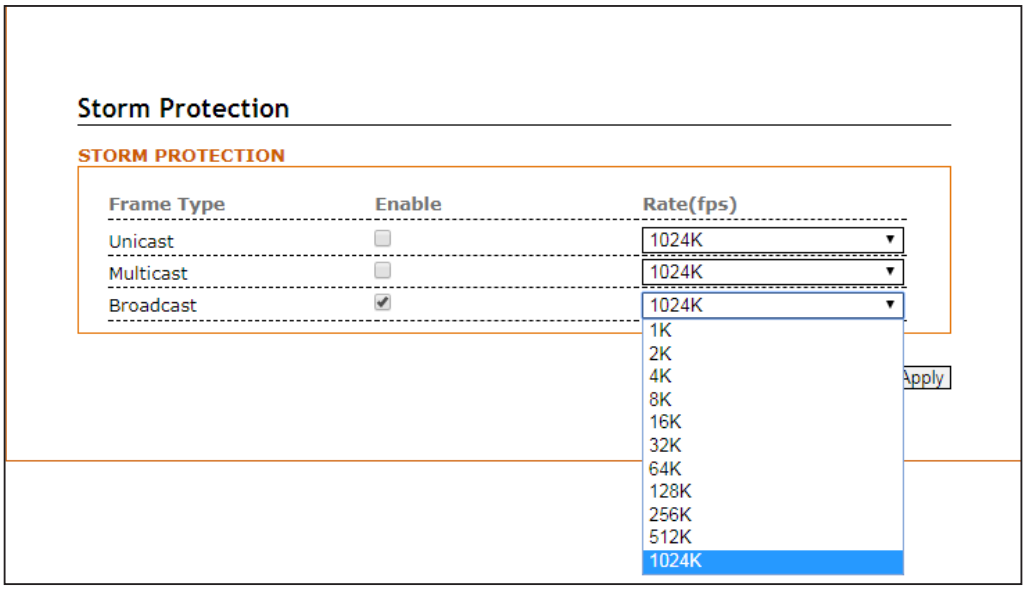
IP address	The IP address of the SNMP Server where the trap will be sent.	None

Community

Setting	Description	Factory Default
Max. 32 characters	The community string used for authentication	None

Storm Protection

Storm Protection > Strom Protection



Frame Type

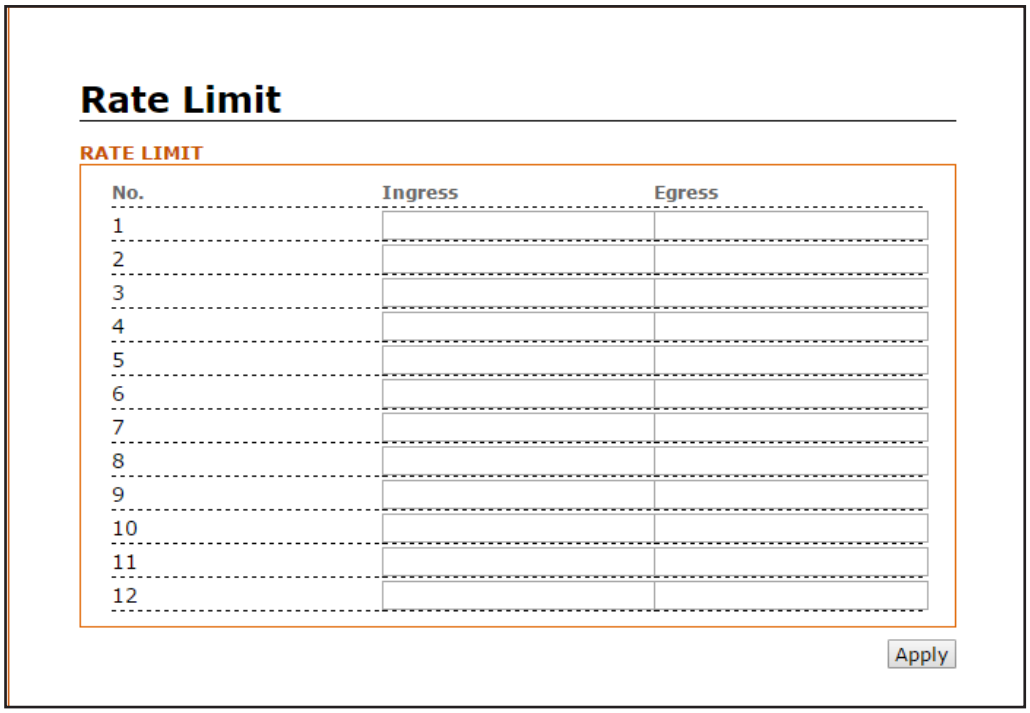
Item	Description	Factory Default
Uni Cast	Enables or disables UniCast traffic storm control	Disabled
Multicast	Enables or disables Multicast traffic storm control	Disabled
Broadcast	Enables or disables Broadcast traffic storm control	Enabled

Rate(fps)

Setting	Description	Factory Default
1K~1024K selection menu (per second)	Specifics maximum rate at which packet type is forwarded	1024K

Rate Limit

Rate Limit > Rate Limit



Rate Limit

Item	Description
No.	The number of ports

Ingress

Setting	Description	Factory Default
1~10000 (*100kbps)	Ingress Rate Limiting restricts the speed of incoming traffic from a particular device to the switch port.	None

Egress

Setting	Description	Factory Default
1~10000 (*100kbps)	Egress Rate Limiting restricts the speed of outgoing traffic from witch port to a particular device.	None

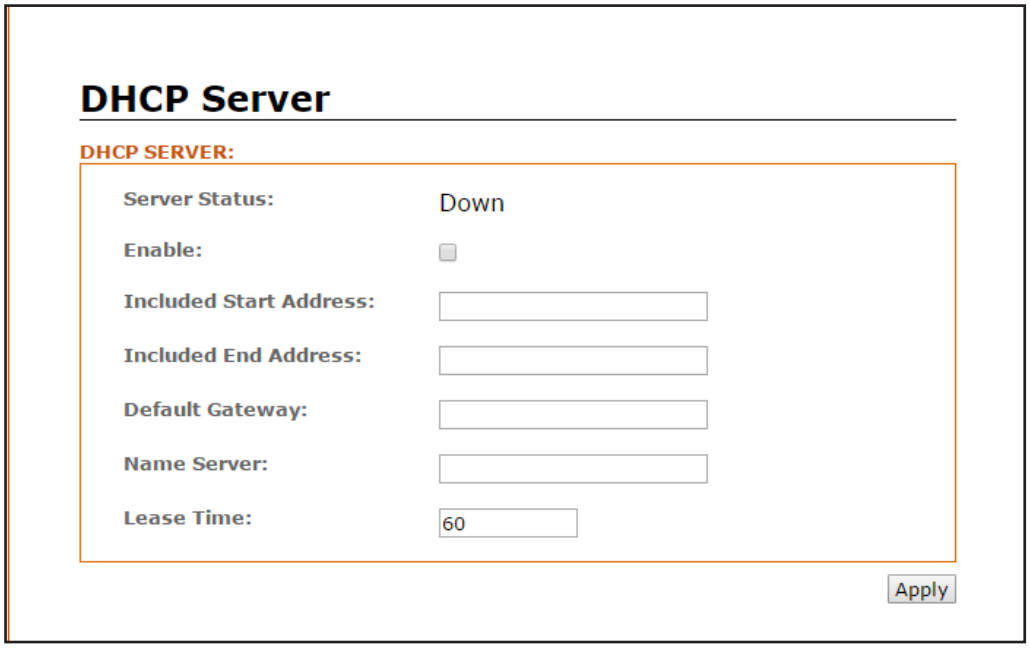
DHCP Server/Relay

Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol. It is used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters. For example, devices can request IP addresses for interfaces from a DHCP server. Using DHCP can also reduce the need for a network administrator or a user to configure these settings manually.

The protocol operates based on the client-server model. When DHCP Clients connect to a network, they will send a broadcast query to request necessary information from a DHCP server. DHCP Servers manage a pool of IP address and network configuration information. If they get queries from DHCP Clients, they will automatically distribute IP address and network parameters to them.

DHCP Server/Relay > DHCP Server

This page allows you to enable / disable the DHCP Server function and configure the settings.



Server Status

Status	Description
Down	The DHCP Server is disabled
Up	The DHCP Server is enabled

Enable

Setting	Description	Factory Default
Unchecked	Disables the DHCP Server feature	Unchecked
Checked	Enables the DHCP Server feature	

Included Start Address

Setting	Description	Factory Default
IP address	The starting IP address of the pool that DHCP Server managed	None

Included End Address

Setting	Description	Factory Default
IP address	The ending IP address of the pool that DHCP Server managed	None

Default Gateway

Setting	Description	Factory Default
IP address	The default gateway IP address	None

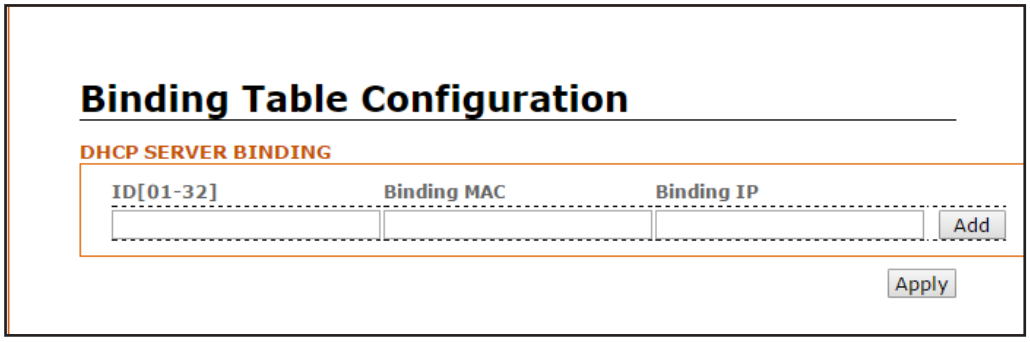
Name Server

Setting	Description	Factory Default
IP address	The DNS server IP address	None

Lease Time

Setting	Description	Factory Default
IP address	Sets the time period for the server to lease an address to a device.	60

DHCP Server/Relay > DHCP Server Binding

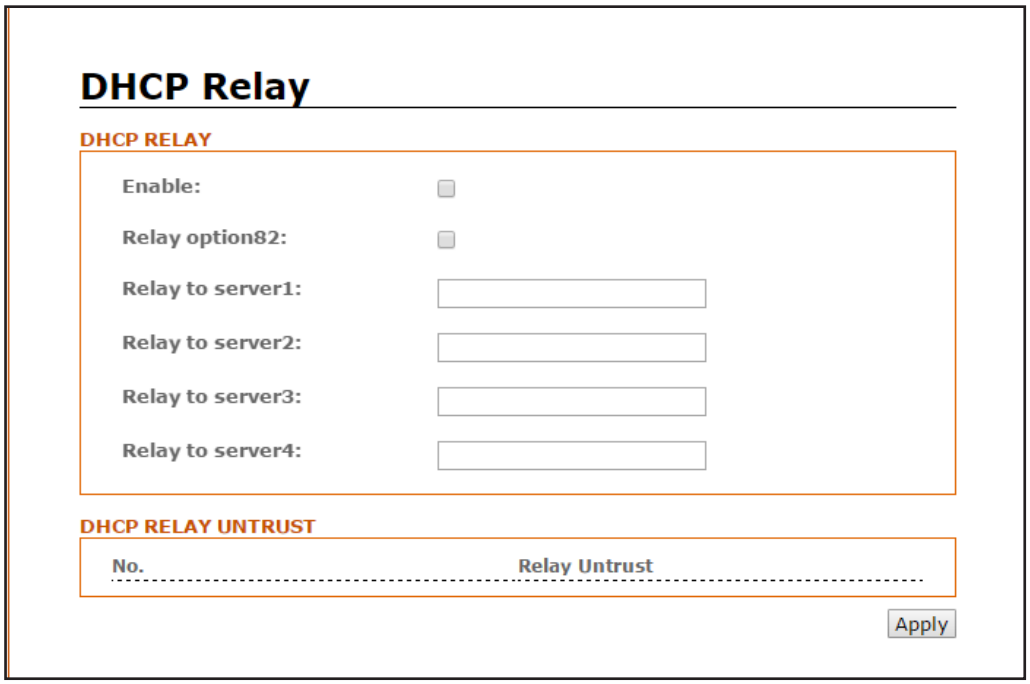


DHCP Server Binding

There are 32 Binding MAC settings available. You can enter ID from 01 to 32 to verify Binding MAC and Binding IP. And you can also add Binding ID by click the **Add** button and use the **Delete** button to remove them.

DHCP Server/Relay > DHCP Relay

DHCP Relay Agents help DHCP Clients forwarding request to DHCP Servers. With DHCP Relay Agents, DHCP Servers and Clients will not know each other. A Relay Agent can connect to more than 1 DHCP Server, so that DHCP Clients will have more resources.



Enable

Setting	Description	Factory Default
Unchecked	Disables the DHCP Relay agent	Unchecked
Checked	Enables the DHCP Relay agent	

Relay Option 82

Setting	Description	Factory Default
Unchecked	Disables the DHCP Relay Option 82	Unchecked
Checked	Enables the DHCP Relay Option 82	

Relay to server1

Setting	Description	Factory Default
IP address	The IP address of the first DHCP server that Relay Agent connect to	None

Relay to server2

Setting	Description	Factory Default

IP address	The IP address of the second DHCP server that Relay Agent connect to	None

Relay to server3

Setting	Description	Factory Default
IP address	The IP address of the third DHCP server that Relay Agent connect to	None

Relay to server4

Setting	Description	Factory Default
IP address	The IP address of the fourth DHCP server that Relay Agent connect to	None

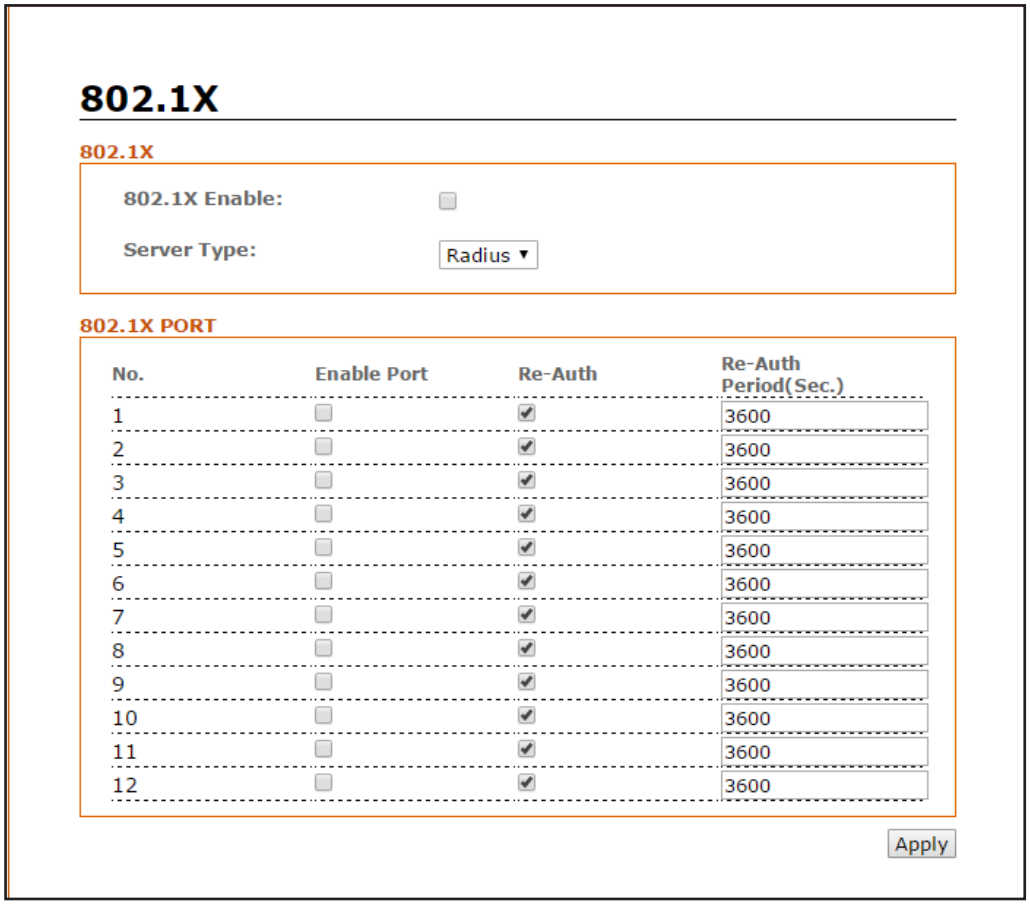
DHCP Relay Untrust

Terms	Description
No.	Port number of the switch
Relay Untrust	Per-port **Enable** or **Disable** Relay Trust. DHCP frames can pass that port when it set to **Enable** only.

802.1X

802.1X is an IEEE Standard for Port-based Network Access Control. It provides an authentication mechanism to devices that wish to attach to a LAN or WLAN. This port-based network access control protocol contains 3 parts, supplicant, authenticator, and authentication server. With 802.1X authentication, we can link a user-name with an IP address, MAC address, and port. This provides greater visibility into the network. 802.1X also provides more security because it only allows traffic transmitting on authenticated ports or MAC addresses. Although the IEEE standard defined it as a Port-based control, to provide more robust service.

802.1X > 802.1X



802.1X Enable

Setting	Description	Factory Default
Unchecked	Disables the 802.1X protocol	Unchecked
Checked	Enables the 802.1X protocol	

Server Type

Setting	Description	Factory Default
Radius	Use the **RADIUS Server** settings for authentication	Radius
Local	Use the **Local Database** settings for authentication	

Enable Port

Setting	Description	Factory Default
Unchecked	Disables authentication before connecting to a LAN or WAN	Unchecked
Checked	Enables authentication before connecting to a LAN or WAN	

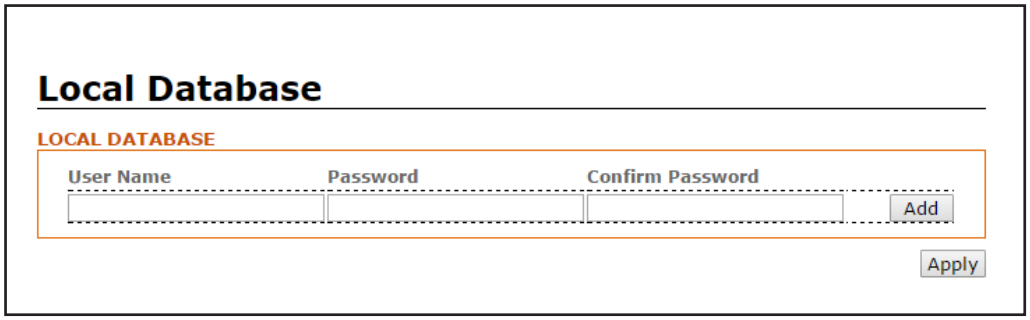
Re-Auth

Setting	Description	Factory Default
Checked	Enables waiting for a period of time before re-authentication	Checked
Unchecked	Disables waiting for a period of time before re-authentication	

Re-Auth Period (Sec.)

Setting	Description	Factory Default
60~65535	Specifics a period of seconds for re-authentication	3600

802.1X > Local Database



Local Database

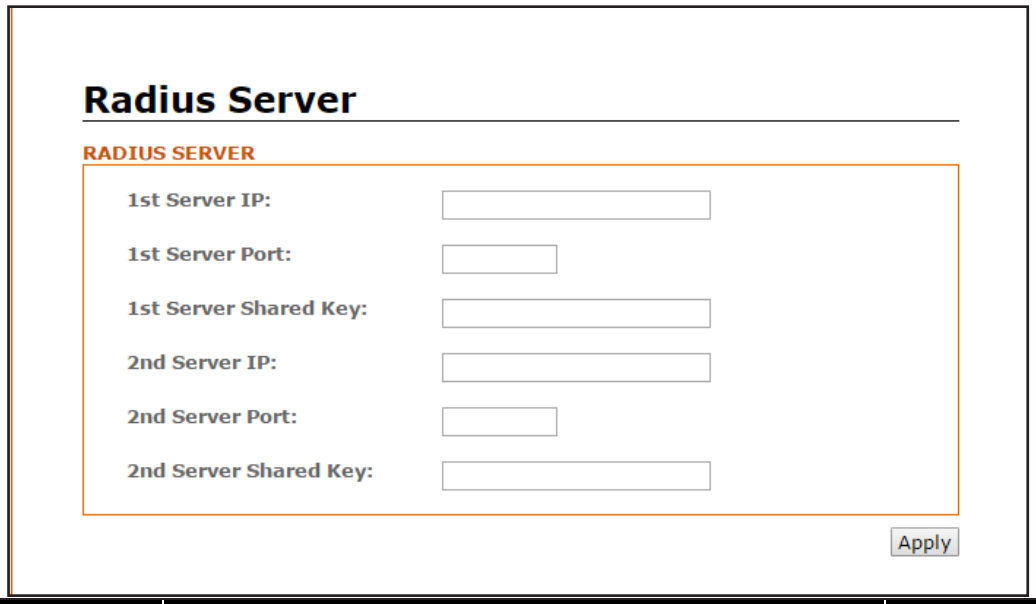
Terms	Description
User Name	The user name use to authenticate in 802.1X when server set to **Local**
Password	The password use to authenticate in 802.1X when server set to **Local**
Confirm Password	Type the password again to confirm

You can add local database by click the **Add** button and use the **Delete** button to remove them.

802.1X > RADIUS Server

RADIUS is used in the authentication process. Database of authorized users is maintained on a RADIUS server. There is an authenticator, our switch enabling 802.1X, to forward the authentication requests between authentication (RADIUS) server and client. Allowing or denying the requests decides if the client can connect to a LAN/WAN or not.

1st Server IP



Setting	Description	Factory Default
IP address	The IP address of the first RADIUS server	None

1st Server Port

Setting	Description	Factory Default
Numerical	The UDP port of the first RADIUS Server	None

1st Server Shared Key

Setting	Description	Factory Default
1~32 characters	A key to be shared with the first RADIUS server. It must be the same key of the first RADIUS server.	None

2nd Server IP

Setting	Description	Factory Default
IP address	The IP address of the second RADIUS server	None

2nd Server Port

Setting	Description	Factory Default
Numerical	The UDP port of the second RADIUS Server	None

2nd Server Shared Key

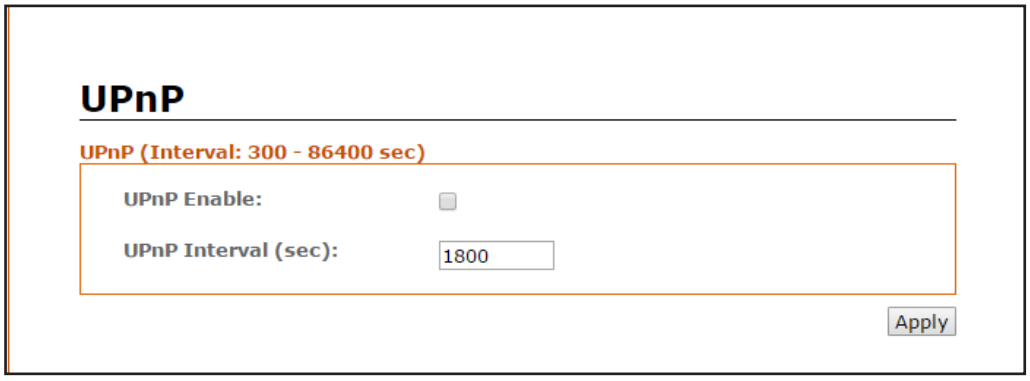
Setting	Description	Factory Default
1~32 characters	A key to be shared with the second RADIUS server. It must be the same key of the first RADIUS server.	None

UPnP

Universal Plug and Play (UPnP) is a set of networking protocols that were promoted by the UPnP Forum. UPnP Protocol permits networked devices to discover each other's presence on the network and seamlessly establish functional network services for data sharing, communications, and entertainment.

The concept of UPnP is an extension of plug-and-play, a technology for dynamically attaching devices directly to a computer. But UPnP is not directly related to the earlier plug-and-play technology any more. UPnP devices are plug-and-play in that when connected to a network they automatically establish working configurations with other devices.

UPnP > UPnP



UPnP Enable

Setting	Description	Factory Default
Unchecked	Disables the UPnP protocol	Unchecked
Checked	Enables the UPnP protocol	

UPnP Interval (sec)

Setting	Description	Factory Default
300~86400	Specifics a timeout interval in seconds	1800

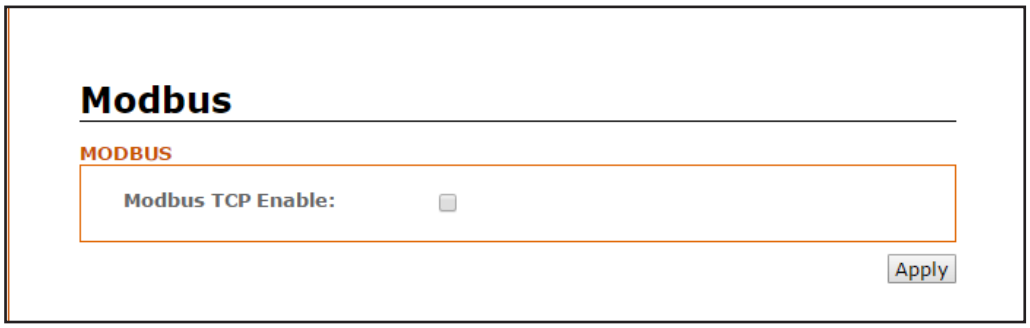
Modbus

Modbus is a serial communications protocol that is used with industrial automation equipment, such as programmable logic controllers (PLCs), sensors, and meters. It is a common, simple, and robust method of connecting industrial devices.

MODBUS TCP is a variant of the MODBUS family. This vendor-neutral communication protocol is commonly used for the integration of a SCADA system.

According to the standard, Modbus TCP encapsulates the message with an Ethernet TCP/IP wrapper.

Modbus > Modbus



Modbus TCP Enable

Setting	Description	Factory Default
Unchecked	Disables Modbus TCP	Unchecked
Checked	Enables Modbus TCP	

System Warning

The System Warning function is very important for managing a switch. Users can manage the switch by Syslog, System Event Log, SMTP and Fault Alarms. By setting up all these system warning features, users will receive warnings, when events occurs. It increases the flexibility and capability for the user to monitor the remote site network and device statuses.

System Warning > Syslog Setting

Syslog Mode

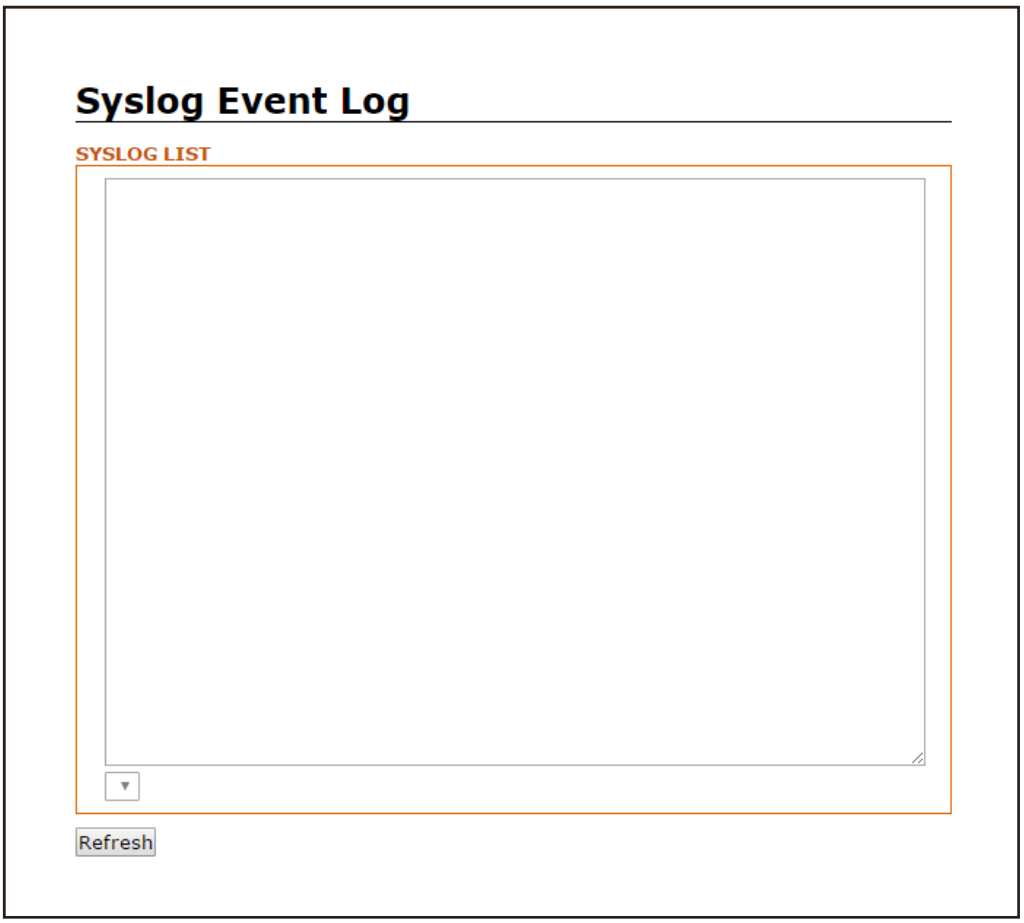
Setting	Description	Factory Default
Disable	Disables Syslog event notifications.	Disable
Local Only	Transmits event notification messages to the local system.	
Remote Only	Transmits event notification messages to the remote Syslog server.	
Local And Remote	Transmits event notification messages to both of the local system and the remote Syslog server.	

Syslog Server IP Address

Setting	Description	Factory Default
IP address	The IP address of the Syslog server	None

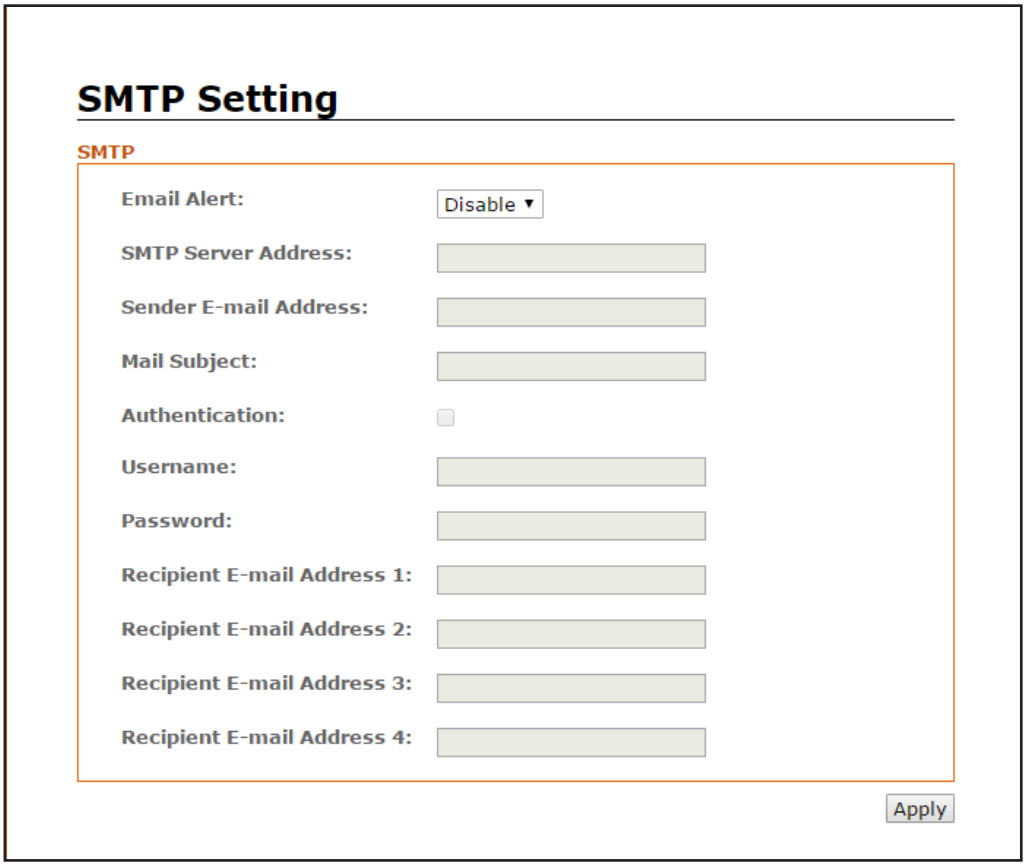
System Warning > System Event Log

The system list window displays up to 5 pages of system event log information. You can click the **Refresh** button to update system event log information.



System Warning > SMTP Setting

The Simple Mail Transfer Protocol (SMTP) is for e-mail transmission.



Email Alert

Setting	Description	Factory Default
Disable	Disables transmission system warning events by e-mail.	Disable
Enable	Enables transmission system warning events by e-mail.	

SMTP Server Address

Setting	Description	Factory Default
IP address	The IP address of the SMTP server	None

Sender E-mail Address

Setting	Description	Factory Default
E-mail address	The recipients will see in the From field of Email alert	None

Mail Subject

Setting	Description	Factory Default
Max. 320 characters	The subject of the Email alert	None

Authentication

Setting	Description	Factory Default
Unchecked	Send Emails alert without SMTP authentication	Unchecked
Checked	Send Emails alert with SMTP authentication	

Username

Setting	Description	Factory Default
Max. 320 characters	The authentication username	None

Password

Setting	Description	Factory Default
Max. 320 characters	The authentication password	None

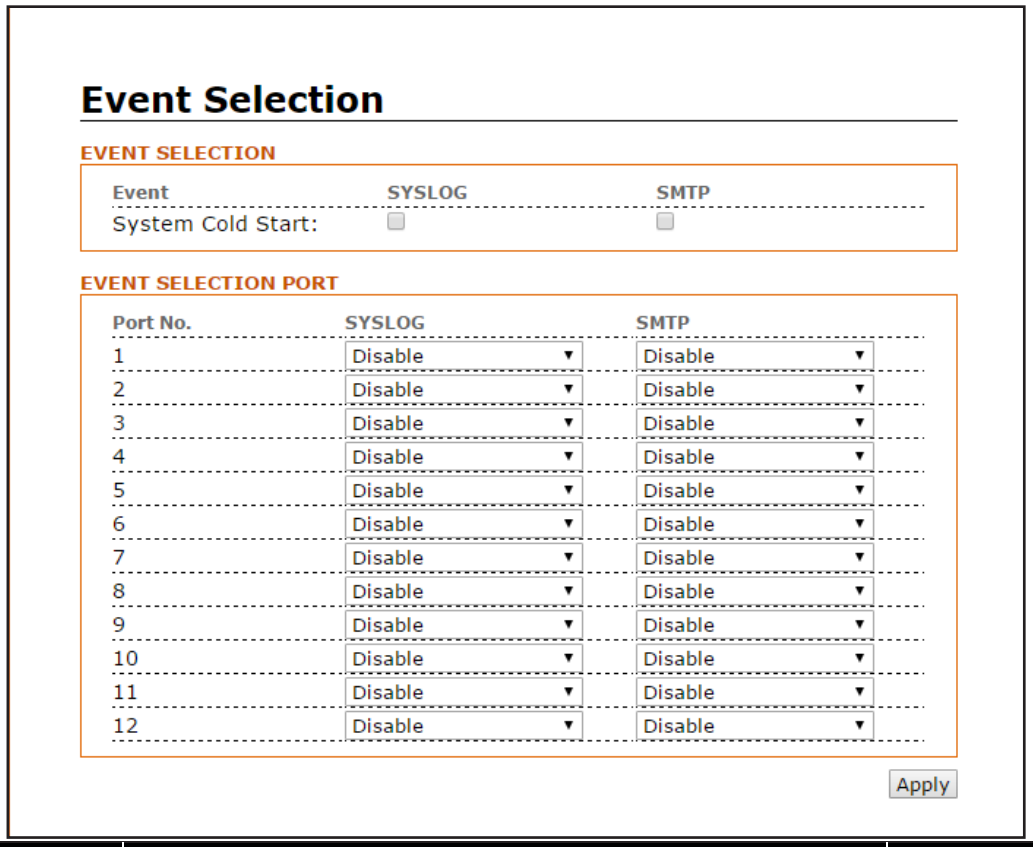
Recipient E-mail Address 1~4

Setting	Description	Factory Default
E-mail address	You can setup up to 4 recipient E-mail addresses to receive any system warning message	None

System Warning > Event Selection

This page allows you to select event type, such as System Cold Start, Link Up, Link Down, Link Up and Down Link, and send a system warning message to SYSLOG or SMTP. Cold start indicates that the unit had been rebooted.

System Cold Start - Syslog



Setting	Description	Factory Default
Unchecked	Disables recording system cold start events to Syslog	Unchecked
Checked	Enables recording system cold start events to Syslog	

System Cold Start - SMTP

Setting	Description	Factory Default
Unchecked	Disables recording system cold start events to SMTP	Unchecked
Checked	Enables recording system cold start events to SMTP	

Port - Syslog

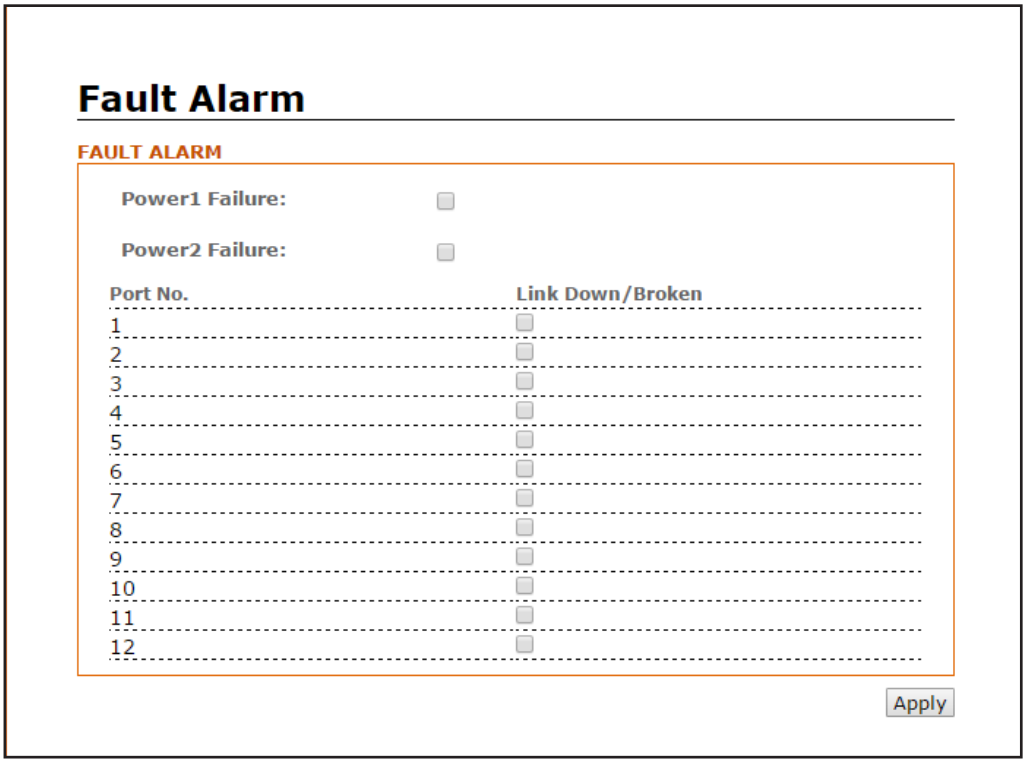
Setting	Description	Factory Default
Disable	Disables recording port Link Up/ Link Down events to Syslog	Disable
Enable	Enables recording port Link Up/ Link Down event to Syslog	

Port - SMTP

Setting	Description	Factory Default
Disable	Disables recording port Link Up/ Link Down events to SMTP	Disable
Enable	Enables recording port Link Up/ Link Down event to SMTP	

System Warning > Fault Alarm

This page allows you to select the fault alarms you want to receive.



Power1 Failure

Setting	Description	Factory Default
Unchecked	Disables Power1 Failure LED indicator on the device's front panel	Unchecked
Checked	Enables Power1 Failure LED indicator on the device's front panel	

Power2 Failure

Setting	Description	Factory Default
Unchecked	Disables Power2 Failure LED indicator on the device's front panel	Unchecked
Checked	Enables Power2 Failure LED indicator on the device's front panel	

Link Down/ Broken

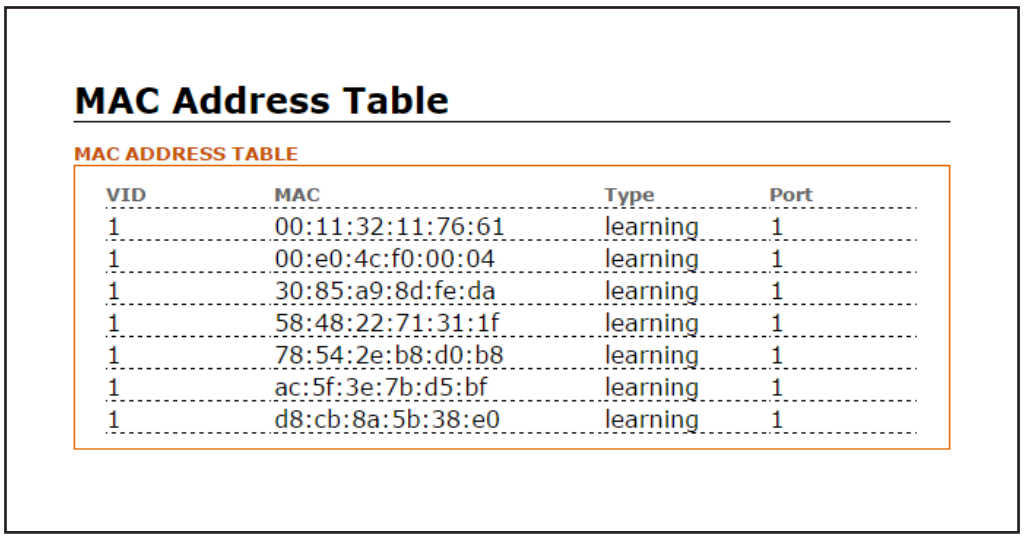
Setting	Description	Factory Defa

		ult
Unchecked	Disables Link Down/ Broken LED indicator on the LAN port jack	Unchecked
Checked	Enables Link Down/ Broken LED indicator on the LAN port jack	

MAC Table

MAC Table > MAC Address Table

The MAC address table is the filtering database that supports queries by the forwarding process, as to whether a frame received by a given port with a given destination MAC address is to be forwarded through a given potential transmission port.

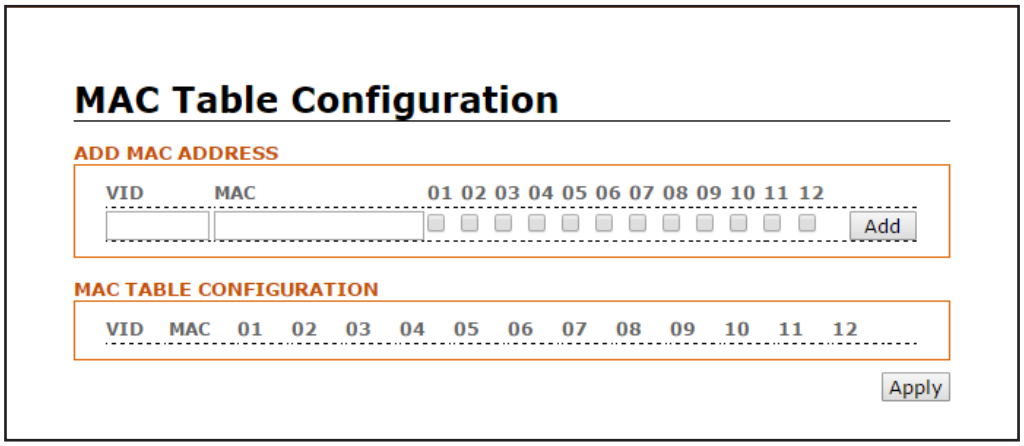


MAC Address Table

Terms	Description
VID	The ID of VLAN
MAC	The MAC address
Type	The type of this MAC address
Port	The port on the switch to which the MAC address belongs

MAC Table > MAC Table Configuration

This page allows you to configure the MAC Table.



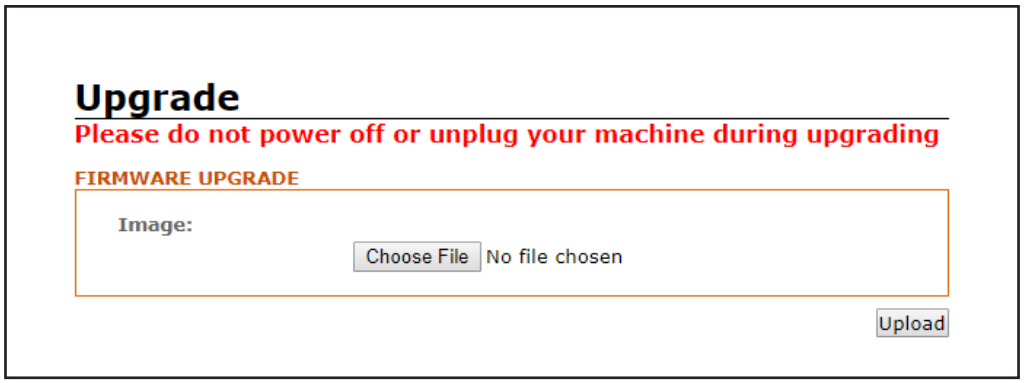
Add MAC Address

Terms	Description
VID	Specifics the ID of VLAN
MAC	Specifics the MAC address
01~12 (numbers depend on the device)	Specifics list of ports on the switch

Maintenance

In the Maintenance menu, you can upgrade the firmware, reboot and restore the default value.

Maintenance > Upgrade

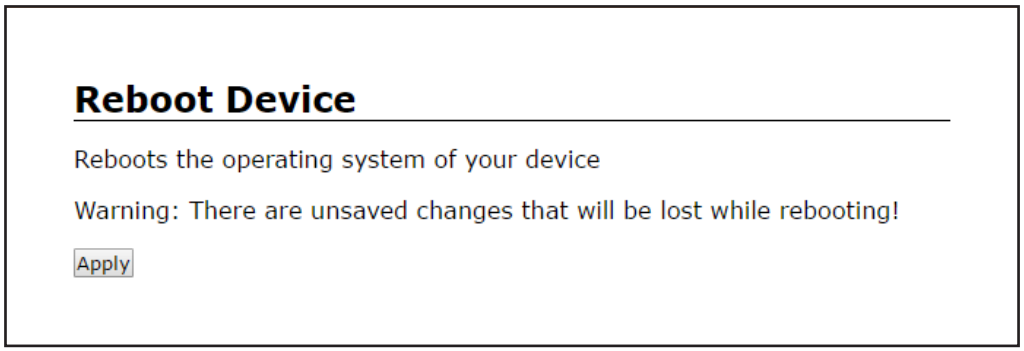


Upgrading the firmware

To upgrade firmware on the device

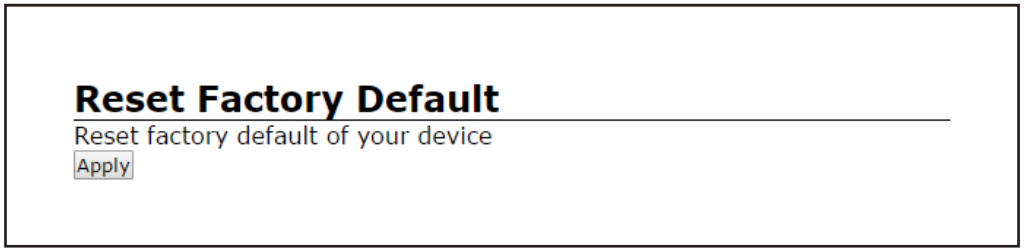
1. Download the firmware file store to your PC.
2. Log into the Admin user on the device
3. Go to **Maintenance > Upgrade** page
4. Click **Choose File** button to select the file you have downloaded.
5. Click **Upload** button. It may take a few minutes. Do not turn off the device.

Maintenance > Reboot



You can reboot the device by clicking the Apply button on **Maintenance > Reboot** page.

Maintenance > Default

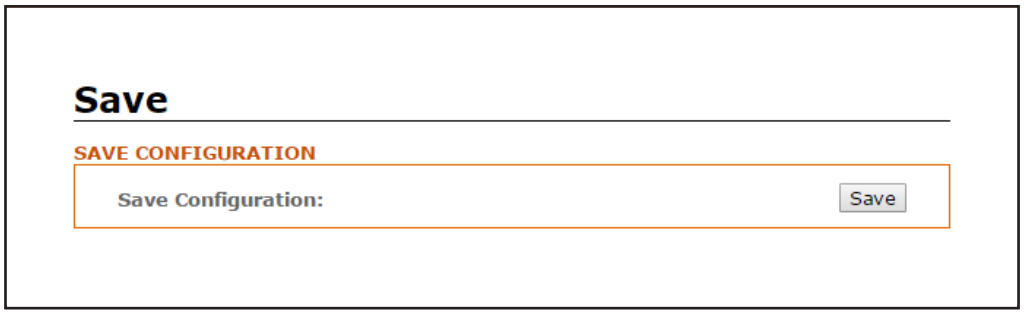


You can reset the switch to Factory Default values by clicking the **Apply** button on **Maintenance > Default** page.

Configuration

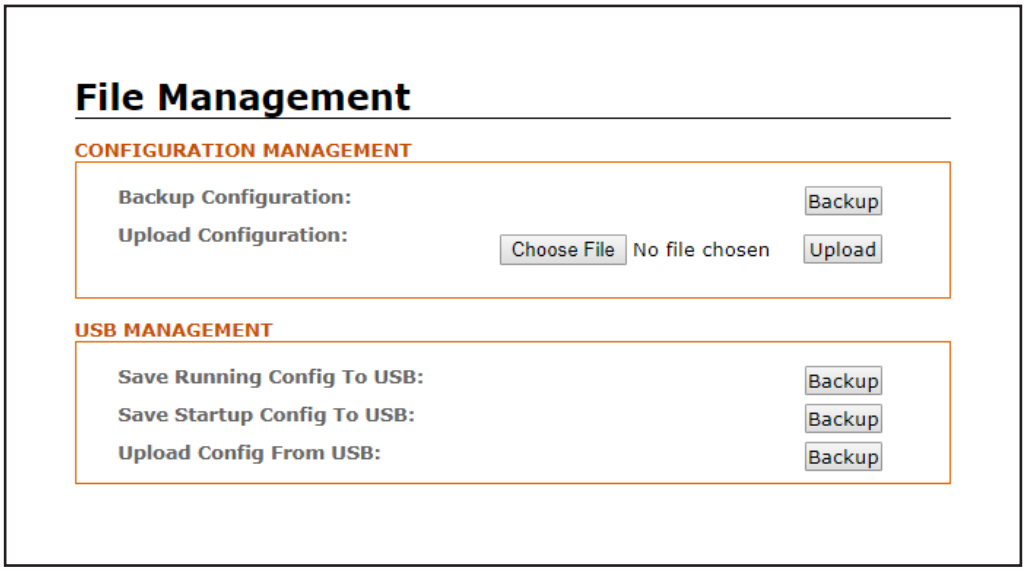
In the Configuration menu, you can save, backup and restore settings.

Configuration > Save



You can click the **Save** button on **Configuration > Save** page, once all the settings had been configured.

Configuration > Backup & Restore



Configuration Management

Feature	Description
Backup Configuration	Stores the configuration backup file
Upload Configuration	Restore the configuration backup from the backup file

User Management

Feature	Description
Save Running Config to USB	Stores the running-config file to the USB drive
Save Startup Config to USB	Stores the startup-config file to the USB drive
Upload Config from USB	Restore the startup-config file from the USB drive

Log out

You can logout of the web management by clicking **Log out** from the menu.

Command Line Management

You can configure the switch using command line.

Configuration by serial console

1. Connect your PC to the switches' Console port.
2. Launch the serial terminal program.
3. Configure the port settings of the serial terminal program to match the console port:

- 115200 baud
- 8 data bits
- No parity
- 1 stop bit
- No flow control

4. The administrator username/ password are admin/admin by default. Enter the username and password to login the serial console.

```
User Access Verification

Username: admin
Password:

SWES> en

SWES# configure terminal
```

Configuration by Telnet console

1. Connect your PC and the switches on the same logical subnetwork.
2. Launch the Telnet program.
3. Configure the switches default settings of the Telnet program:

- IP Address: 192.168.1.254
- Subnet Mask: 255.255.255.0
- Default Gateway: none

4. The administrator username/ password are admin/admin by default. Enter the username and password to login the Telnet console.

```
User Access Verification

Username: admin
Password:

SWES> en

SWES# configure terminal
```

Commander Groups

System Group

Command	Mode
hostname [Switch]	configure
no hostname	configure
system location [none]	configure
system contact [none]	configure
no system location	configure
no system contact	configure
show system uptime	c

	configure
show system mac	configure
show system version firmware	configure
show system version loader	configure
Username [admin | manager | user] password [PASSWORD]	configure

IP Group

Command	Mode
boot host dhcp	configure
ip address [ip_addr] [ip_mask]	conf

	igure
ip default-gateway [ip_router]	configure
ip name-server [ip_addr_string]	configure
no boot host dhcp	configure
no ip default-gateway	configure
no ip name-server	configure
show boot host dhcp	configure
show ip address	confi

	guree
show ip default-gateway	configure
show ip name-server	configure
show ip mode	configure

Time Group

Command	Mode
ntp time update	configure
ntp client timeserver [ip_addr_string]	configure
clock time [hh:mm:ss] [day] [month] [year]	configur

	e
clock timezone [area] [city]	c o n f i g u r e
ntp client sync [minute | hour | day | month | year] [NUMBER]	c o n f i g u r e
no ntp client timeserver	c o n f i g u r e
no clock timezone	c o n f i g u r e
no ntp client sync [minute | hour | day | month | year] [NUMBER]	c o n f i g u r e
show ntp client timeserver	c o n f i g u r e
show clock timezone	c o n f i g u r

	e
show ntp client sync [minute | hour | day | month | year] [NUMBER]	c o n f i g u r e

Port Group

Command	Mode
speed_duplex [10 | 100 | 1000] [full | halp]	interface
flowcontrol [on | off]	interface
name [string]	interface
shutdown	interface
no speed_duplex	interface
no flowcontrol	interface
no name	int

	e r f a c e
no shutdown	i n t e r f a c e
show speed_duplex	i n t e r f a c e
show flowcontrol	i n t e r f a c e
show name	i n t e r f a c e
show link rx	i n t e r f a c e
show link tx	i n t e r f a c e
show link summary	i n t e

	r f a c e
rate-limit [egress | ingress] [RATE VALUE]	i n t e r f a c e
no rate-limit egress	i n t e r f a c e
no rate-limit ingress	i n t e r f a c e
show link status	i n t e r f a c e
show interface transceiver	c o n f i g u r e

VLAN Group

Command	Mode
management vlan [vlan_id]	c o n f i g u

	re
name [vlan_name]	vlan
member [member_portlist] [<untag_portlist>]	vlan
switchport pvid [vlan_id]	interface
switchport filter [tagged | untagged]	interface
no name	vlan
no member	vlan
no switchport pvid	interface
no switchport filter	interface
show name	vlan
show member	vlan
show switchport pvid	i

	interface
show switchport filter	interface
switchport mode [d(dot1q-tunnel) | c(customer) | p(provider)]	interface

ERPS Group

Command	Mode
ethernet ring erps major	configure
enable	erps
disable	erps
rpl [port0 | port1] [owner | neighbor]	erps
aps-channel [channel ID]	erps
revertive	erps

Command	Mode
clear	erps
port0 interface [interface name]	erps
port1 interface [interface name]	erps
fs [port0 | port1]	erps
ms [port0 | port1]	erps
ring-id [erps ring ID]	erps
timer hold-off [0~1000]	erps
timer guard [10~2000]	erps
timer wtr [1~12]	erps
no rpl [port0 | port1]	erps
no aps-channel	erps
no revertive	erps
no port0	erps
no port1	erps
no ring-id	e

	erps
no timer hold-off	erps
no timer guard	erps
no timer wtr	erps
show status	erps
show brief	erps
show port status	erps
show configuration	erps
mel [0~7]	erps
no fs	erps
no ms	erps

PoE Group

Command	Mode
power inline never	interface
keepalive ip [IP_Address]	inte

	r f a c e
keepalive time [Seconds]	i n t e r f a c e
schedule [monday~sunday] enable	i n t e r f a c e
schedule [monday~sunday] starttime [Hour]	i n t e r f a c e
schedule [monday~sunday] endtime [Hour]	i n t e r f a c e
no power inline never	i n t e r f a c e
no keepalive ip	i n t e r f a c e
no keepalive time	i n t e r

	face
no schedule [monday~sunday] enable	interface
no schedule [monday~sunday] starttime	interface
no schedule [monday~sunday] endtime	interface
show power inline status	interface
show keepalive ip	interface
show keepalive time	interface
show schedule [monday~sunday] enable	interf

	ace
show schedule [monday~sunday] starttime	interface

Command	Mode
show schedule [monday~sunday] endtime	interface

STP Group

Command	Mode
spanning-tree mode [rstp | mst]	configure
spanning-tree priority [priority_value]	configure
spanning-tree forward-time [forward time]	configure
spanning-tree hello-time [hello_time]	configure
spanning-tree max-age [max_age]	configu

	re
spanning-tree cost [link_cost_value]	interface
spanning-tree port-priority [port_priority]	interface
spanning-tree link-type [point-to-point | point-to-multiple]	interface
spanning-tree auto-edge off	interface
spanning-tree admin-edge on	interface
spanning-tree stp disable	interface
no spanning-tree mode	configur

	e
no spanning-tree priority	c o n f i g u r e
no spanning-tree forward-time	c o n f i g u r e
no spanning-tree hello-time	c o n f i g u r e
no spanning-tree max-age	c o n f i g u r e
no spanning-tree mst [instance_ID] priority	c o n f i g u r e
no spanning-tree cost	i n t e r f a c e
no spanning-tree port-priority	i n t e r f a c

	e
no spanning-tree link-type	interface
no spanning-tree auto-edge	interface
no spanning-tree admin-edge	interface
no spanning-tree stp	interface
show spanning-tree mode	configure
show spanning-tree priority	configure
show spanning-tree forward-time	configur

	e
show spanning-tree hello-time	configure
show spanning-tree max-age	configure
show spanning-tree cost	interface
show spanning-tree port-priority	interface
show spanning-tree link-type	interface
show spanning-tree auto-edge	interface
show spanning-tree admin-edge	interfac

	e
show spanning-tree stp	interface
spanning-tree mst [instance_ID] priority [priority]	configure
spanning-tree mst name [NAME]	configure
spanning-tree mst revision [REVISION]	configure
spanning-tree mst instance [instance_ID] vlan [vlan_grp]	configure
spanning-tree mst [instance_ID] cost [cost_value]	interface
spanning-tree mst [instance_ID] port-priority [priority]	interfac

no spanning-tree mst name	configure

Command	Mode
no spanning-tree mst revision	configure
no spanning-tree mst instance [instance_ID] vlan	configure
no spanning-tree mst [instance_ID] cost	interface
no spanning-tree mst [instance_ID] port-priority	interface
show spanning-tree mst name	configure
show spanning-tree mst revision	configure
show spanning-tree mst instance [instance_ID] vlan	conf

	igure
show spanning-tree mst [instance_ID] priority	configure
show spanning-tree mst [instance_ID] cost	interface
show spanning-tree mst [instance_ID] port-priority	interface

Event Group

Command	Mode
event smtp power1 enable	configure
event smtp power2 enable	configure
event smtp cold-start enable	configu

	re
event smtp warm-start enable	configure
event smtp authentication-failure enable	configure
event smtp erps-change enable	configure
event smtp interface [INTERFACE_NAME] up	configure
event smtp interface [INTERFACE_NAME] down	configure
no event smtp power1	configure
no event smtp power2	configur

	e
no event smtp cold-start	configure
no event smtp warm-start	configure
no event smtp authentication-failure	configure
no event smtp erps-change	configure
no event smtp interface [INTERFACE_NAME] up	configure
no event smtp interface [INTERFACE_NAME] down	configure
show event smtp power1	configur

	e
show event smtp power2	configure
show event smtp cold-start	configure
show event smtp warm-start	configure
show event smtp authentication-failure	configure
show event smtp erps-change	configure
show event smtp interface [INTERFACE_NAME] up	configure
show event smtp interface [INTERFACE_NAME] down	configur

	e
event syslog power1 enable	configure
event syslog power2 enable	configure
event syslog cold-start enable	configure
event syslog warm-start enable	configure
event syslog authentication-failure enable	configure
event syslog erps-change enable	configure
event syslog interface [INTERFACE_NAME] up	configur

	e
event syslog interface [INTERFACE_NAME] down	c o n f i g u r e

Command	Mode
no event syslog power1	configure
no event syslog power2	configure
no event syslog cold-start	configure
no event syslog warm-start	configure
no event syslog authentication-failure	configure
no event syslog erps-change	configure
no event syslog interface [INTERFACE_NAME] up	conf

	i g u r e
no event syslog interface [INTERFACE_NAME] down	c o n f i g u r e
show event syslog power1	c o n f i g u r e
show event syslog power2	c o n f i g u r e
show event syslog cold-start	c o n f i g u r e
show event syslog warm-start	c o n f i g u r e
show event syslog authentication-failure	c o n f i g u r e
show event syslog erps-change	c o n f i

	gure
show event syslog interface [INTERFACE_NAME] up	configure
show event syslog interface [INTERFACE_NAME] down	configure
event alarm power1 enable	configure
event alarm power2 enable	configure
event alarm interface [INTERFACE_NAME] down	configure
no event alarm power1	configure
no event alarm power2	config

	u r e
no event alarm interface [INTERFACE_NAME] down	c o n f i g u r e
show event alarm power1	c o n f i g u r e
show event alarm power2	c o n f i g u r e
show event alarm interface [INTERFACE_NAME] down	c o n f i g u r e
event apply	c o n f i g u r e

Syslog Group

Command	Mode
syslog server [IP_address]	c o n f i g u r e

syslog mode [all | local | remote]	configure
no syslog server	configure
no syslog mode	configure
show syslog server	configure
show syslog mode	configure
show syslog log	configure
syslog apply	configure

SMTP Group

Command	Mode
smtp enable	configure
smtp sender [E-MAIL_ADDR]	configure
smtp subject [subject_text]	configure
smtp server address [GMAIL_SMPT_SERVER]	configure
smtp server port [GMAIL_SMPT_SERVER]	configure
smtp authentication enable	configure

Command	Mode
smtp authentication username [GMAIL_ACCOUNT]	configure
smtp authentication password [GMAIL_PASS]	configure
smtp receive [1 | 2 | 3 | 4] [e-mail_address]	configure
no smtp enable	configure
no smtp sender	configure
no smtp subject	configure
no smtp server address	conf

	igure
no smtp server port	configure
no smtp authentication enable	configure
no smtp authentication username	configure
no smtp authentication password	configure
no smtp receive [1 | 2 | 3 | 4]	configure
show smtp state	configure
show smtp sender	confi

	guree
show smtp subject	configure
show smtp server address	configure
show smtp server port	configure
show smtp authentication enable	configure
show smtp authentication username	configure
show smtp receive [1 | 2 | 3 | 4]	configure

SNMP Group

Command	Mod

snmp server enable [<v1-v2c-only | v3-only>]	configure
snmp server community [ro | rw] [community_name]	configure
snmp server v3 level [admin | user] [auth | noauth | priv]	configure
snmp server v3 auth [admin | user] [md5 | sha] [PWD]	configure
snmp server v3 encryption [admin | user] [des | aes] [PWD]	configure
no snmp server enable	configure
no snmp server community [ro | rw]	configur

	e
no snmp server v3 level [admin | user]	configure
no snmp server v3 auth [admin | user]	configure
no snmp server v3 encryption [admin | user]	configure
show snmp server enable	configure
show snmp server community [ro | rw]	configure
show snmp server v3 level [admin | user]	configure
show snmp server v3 auth [admin | user]	configur

	e
show snmp server v3 encryption [admin | user]	c o n f i g u r e
snmp trap enable	c o n f i g u r e
snmp trap host [DESTINATION_IP]	c o n f i g u r e
snmp trap version [1 | 2c | 3] [traps | inform]	c o n f i g u r e
snmp trap community [trap_community_name]	c o n f i g u r e
snmp trap inform retry [retry_time]	c o n f i g u r e
snmp trap inform timeout [retry_interval]	c o n f i g u r

	e
snmp trap v3 user [user_ID]	c o n f i g u r e

Command	Mode
snmp trap v3 level [auth | noauth | priv]	configure
snmp trap v3 engine-ID [engineID]	configure
snmp trap v3 auth [md5 | sha] [PASSWORD]	configure
snmp trap v3 encryption [des | aes] [PASSWORD]	configure
no snmp trap enable	configure
no snmp trap host	configure
no snmp trap version	conf

	igure
no snmp trap community	configure
no snmp trap inform retry	configure
no snmp trap inform timeout	configure
no snmp trap v3 user	configure
no snmp trap v3 level	configure
no snmp trap v3 engine-ID	configure
no snmp trap v3 auth	confi

	g u r e
no snmp trap v3 encryption	c o n f i g u r e
show snmp trap enable	c o n f i g u r e
show snmp trap host	c o n f i g u r e
show snmp trap version	c o n f i g u r e
show snmp trap community	c o n f i g u r e
show snmp trap inform retry	c o n f i g u r e
show snmp trap inform timeout	c o n f i g

	u r e
show snmp trap v3 user	c o n f i g u r e
show snmp trap v3 level	c o n f i g u r e
show snmp trap v3 engine-ID	c o n f i g u r e
show snmp trap v3 auth	c o n f i g u r e
show snmp trap v3 encryption	c o n f i g u r e

File Group

Command	Mode
copy running-config startup-config	configure

copy startup-config running-config	configure
copy usb startup-config	configure

Port Mirror Group

Command	Mode
monitor enable	configure
monitor source [rx | tx | both] [port_list]	configure
monitor destination [dest_port_number]	configure
no monitor enable	configure
no monitor source	con

	figure
no monitor destination	configure
show monitor enable	configure
show monitor source	configure
show monitor destination	configure

QoS Group

Command	Mode
qos queue-schedule [strict | wrr]	configure
qos map cos [priority_type] to tx-queue [queue]	configure
qos map dscp [[priority_type] to tx-queue [[queue]	configure
qos trust [cos | dscp]	interface
qos default cos [cos_default_value]	interface
no qos queue-schedule	configure
no qos map cos [priority_type]	con

	figure
no qos map dscp [priority_type]	configure
no qos trust	interface
no qos default cos	interface
show qos queue-schedule	configure
show qos map cos [priority_type]	configure
show qos map dscp [priority_type]	configure
show qos trust	inte

	r f a c e
show qos default cos	i n t e r f a c e

IGMP Group

Command	Mode
igmp snooping enable	c o n f i g u r e
igmp snooping query max-respond-time [1..12]	c o n f i g u r e
igmp snooping query interval [1..3600]	c o n f i g u r e
igmp snooping last-member count [2..10]	c o n f i g u r e
igmp snooping last-member interval [60..300]	c o n f i g u

	re
igmp snooping querier enable	configure
igmp snooping fast-leave enable	interface
no igmp snooping enable	configure
no igmp snooping query max-respond-time	configure
no igmp snooping query interval	configure
no igmp snooping last-member count	configure
no igmp snooping last-member interval	configur

	e
no igmp snooping querier	configure
no igmp snooping fast-leave	interface
show igmp snooping mdb	configure
show igmp snooping all	configure
show igmp snooping fast-leave	interface

Trunk Group

Command	Mode
trunk group [group] [static | lacp] [interface_list]	configure
show trunk group	co

	nfigure
show trunk group [1-8]	configure

DHCP Server/Relay Group

Command	Mode
dhcp service server	configure

Command	Mode
dhcp server included-address [IP_START] [IP_END]	configure
dhcp server default-gateway [router_ip]	configure
dhcp server name-server [dns_ip]	configure
dhcp server lease [dhcp_lease_time]	configure
dhcp server binding [bind_num] [MAC] [bind_IP]	configure
dhcp service relay	configure
dhcp relay server [server_number] [IP]	conf

	igure
dhcp relay information option	configure
dhcp relay untrust	interface
no dhcp service server	configure
no dhcp server included-address	configure
no dhcp server default-gateway	configure
no dhcp server name-server	configure
no dhcp server lease	confi

	g u r e
no dhcp server binding [bind_num]	c o n f i g u r e
no dhcp service relay	c o n f i g u r e
no dhcp relay server [server_number]	c o n f i g u r e
no dhcp relay information option	c o n f i g u r e
no dhcp relay untrust	c o n f i g u r e
show dhcp service	i n t e r f a c e
show dhcp server status	c o n f i g

	u r e
show dhcp server included-address	c o n f i g u r e
show dhcp server default-gateway	c o n f i g u r e
show dhcp server name-server	c o n f i g u r e
show dhcp server lease	c o n f i g u r e
show dhcp server binding [bind_num] [MAC] [bind_IP]	c o n f i g u r e
show dhcp relay enable	c o n f i g u r e
show dhcp relay server [server_number]	c o n f i g u

	r e
show dhcp relay information option	c o n f i g u r e
show dhcp relay untrust	i n t e r f a c e

UPnP Group

Command	Mode
upnp enable	c o n f i g u r e
upnp advertisement interval [SEC]	c o n f i g u r e
no upnp enable	c o n f i g u r e
no upnp advertisement interval	c o n f i g u r e
show upnp enable	c

	configure
show upnp advertisement interval	configure

Modbus Group

Command	Mode
modbus tcp server	configure
no modbus tcp server	configure
show modbus tcp server	configure

802.1X Group

Command	Mode
dot1x enable	configure
dot1x authentication server type [local | radius]	configure
dot1x authentication server 1 ip [IP]	configure
dot1x authentication server 1 port [PORT]	configure
dot1x authentication server 1 share-key [KEY]	configure
dot1x authentication server 2 ip [IP]	configure
dot1x authentication server 2 port [PORT]	con

	figure
dot1x authentication server 2 share-key [KEY]	configure
dot1x local-db [USER] [PASSWORD]	configure
dot1x authenticator enable	interface
dot1x reauthentication enable	interface
dot1x reauthentication period [SEC]	interface
no dot1x enable	configure
no dot1x authentication server type	conf

	i g u r e
no dot1x authentication server 1 ip	c o n f i g u r e
no dot1x authentication server 1 port	c o n f i g u r e
no dot1x authentication server 1 share-key	c o n f i g u r e
no dot1x authentication server 2 ip	c o n f i g u r e
no dot1x authentication server 2 port	c o n f i g u r e
no dot1x authentication server 2 share-key	c o n f i g u r e
no dot1x local-db [USER] [PASSWORD]	c o n f i

	guree
no dot1x authenticator enable	interface
no dot1x reauthentication enable	interface
no dot1x reauthentication period	interface
show dot1x enable	configure
show dot1x authentication server type	configure
show dot1x authentication server 1 ip	configure
show dot1x authentication server 1 port	config

	u r e
show dot1x authentication server 1 share-key	c o n f i g u r e
show dot1x authentication server 2 ip	c o n f i g u r e
show dot1x authentication server 2 port	c o n f i g u r e
show dot1x authentication server 2 share-key	c o n f i g u r e
show dot1x local-db [USER] [PASSWORD]	c o n f i g u r e
show dot1x brief	c o n f i g u r e
show dot1x server brief	c o n f i g u

	r e
show dot1x brief	i n t e r f a c e
show dot1x server brief	i n t e r f a c e
show dot1x authenticator enable	i n t e r f a c e
show dot1x reauthentication enable	i n t e r f a c e
show dot1x reauthentication period	i n t e r f a c e

IPv6 Group

Command	Mode
ipv6 enable	c o n f i g u r e
ipv6 address add [IPV6_ADDR</PREFIX_LEN>]	c

	onfigure

Command	Mode
ipv6 neighbor flush	configure
ipv6 ping [IPV6_ADDR] [<size PKG_SIZ> | <repeat PKG_CNT>]	configure
no ipv6 enable	configure
no ipv6 address [IPV6_ADDR/PREFIX_LEN]	configure
show ipv6 enable	configure
show ipv6 address	configure
show ipv6 neighbor	conf

	igure

TFTP Group

Command	Mode
tftp upgrade	configure
tftp server ip [IP_ADDRESS]	configure
tftp file name [UPGRADE_FILE_NAME]	configure

MAC Table Group

Command	Mode
mac set [1-4094] [MAC] [PORT]	configure
no mac set [1-4094] [MAC]	configure
show mac set	c

	onfigure
clear mac address-table dynamic	configure

LLDP Group

Command	Mode
lldp enable	configure
lldp timer [5-32767] (s)	configure
no lldp	configure
no lldp timer	configure
show lldp	conf

	i g u r e
show lldp neighbor	c o n f i g u r e
show lldp timer	c o n f i g u r e

Storm Protection Group

Command	M o d e
storm protection [broadcase | multicase | unicase] enaable	c o n f i g u r e
storm protection [broadcase | multicase | unicase] rate [RATE_VALUE]	c o n f i g u r e
no storm protection [broadcase | multicase | unicase]	c o n f i g u r e
no storm protection [broadcase | multicase | unicase] rate	c o n f i g u

	re
show storm protection [broadcase | multicase | unicase]	configure
show storm protection [broadcase | multicase | unicase] rate	configure

Security Group

Command	Mode
Security [http | https | ssh | telent | usb] enable	configure
Security show [http | https | ssh | telent | usb]	configure
Security no [http | https | ssh | telent | usb]	configure

Save and Load Configuration File to/from USB

1. CLI: enable > configure terminal > copy running-config usb (path)

```
User Access Verification

Username: Admin
Password:

SWES> en

SWES# configure terminal

SWES<config># copy
running-config startup-config usb
SWES<config># copy running-config
startup-config usb

SWES<config># copy running-config usb file1

SWES<config># copy running-config usb /test/file2
```

Fill in the folder and filename behind the copy **running-config usb** command. Ex: file1, / folder /file2.

2. CLI: enable > configure terminal > copy startup-config usb (path)

```
User Access Verification

Username: Admin
Password:

SWES> en

SWES# configure terminal

SWES<config># copy
running-config startup-config usb
SWES<config># copy startup-config
runing-config usb

SWES<config># copy startup-config usb file1

SWES<config># copy startup-config usb /test/file2
```

Fill in the folder and filename behind the copy **startup-config usb** command. Ex: file1, / folder /file2.

3. CLI: enable > configure terminal > copy usb startup-config (path)

```
User Access Verification

Username: Admin
Password:

SWES> en

SWES# configure terminal

SWES<config># copy
running-config startup-config usb
SWES<config># copy usb
startup-config firmware

SWES<config># copy usb
  startup-config       destination file
  firmware             destination file

SWES<config># copy usb startup-config file1
```

Fill in the folder and filename behind the **copy usb startup-config** command. Ex: file1, / folder /file2.

Upgrade via TFTP

CLI: enable > configure terminal > tftp server ip [IP_ADDRESS] > tftp file name [UPGRADE_FILE_NAME] > tftp upgrade

```
Switch> enable

Switch# configure terminal

Switch(config)# tftp server ip 192.168.1.237

Switch(config)# tftp file name 240.dat

Switch(config)# tftp upgrade
```

Fill in the TFTP server IP and upgrade file name behind the **tftp server ip [IP_ADDRESS]** and **tftp file name [UPGRADE_FILE_NAME]**