BUFFALO™

Layer 2/Layer 3 Web Smart Gigabit Switch
BS-GS Series

# User Manual

www.buffaloamericas.com

35020643-04
2015.04

# Contents

# Chapter 1 Initial Settings

## Product Requirements

### Compatible Devices, Browsers, and OSs

#### Compatible Devices to Connect to BS-GS

1000BASE-T/100BASE-TX/10BASE-T compatible devices (PCs, Mac, NAS, switches)

#### Compatible Browsers to Enter Settings

Internet Explorer 8/9/10/11
Mozilla Firefox
Google Chrome
Safari
Refer to our website to confirm the latest information of the compatible browser versions.

#### Business Switch Configuration Tool's Compatible OSs

Windows 8.1 (64-bit/32-bit), Windows 8 (64-bit/32-bit),
Windows 7 (64-bit/32-bit), Windows Vista (64-bit/32-bit), Windows XP (32-bit)

## Install Business Switch Configuration Tool

Install "Business Switch Configuration Tool" before you perform the following procedure. (Compatible with Windows only.)

**Note:** You can download the latest version of Business Switch Configuration Tool from the URLs below:

BS-GS2008: http://d.buffalo.jp/BS-GS2008/

BS-GS2008P: http://d.buffalo.jp/BS-GS2008P/

BS-GS2016: http://d.buffalo.jp/BS-GS2016/

BS-GS2016P: http://d.buffalo.jp/BS-GS2016P/

BS-GS2024: http://d.buffalo.jp/BS-GS2024/

BS-GS2024P: http://d.buffalo.jp/BS-GS2024P/

BS-GS2048: http://d.buffalo.jp/BS-GS2048/

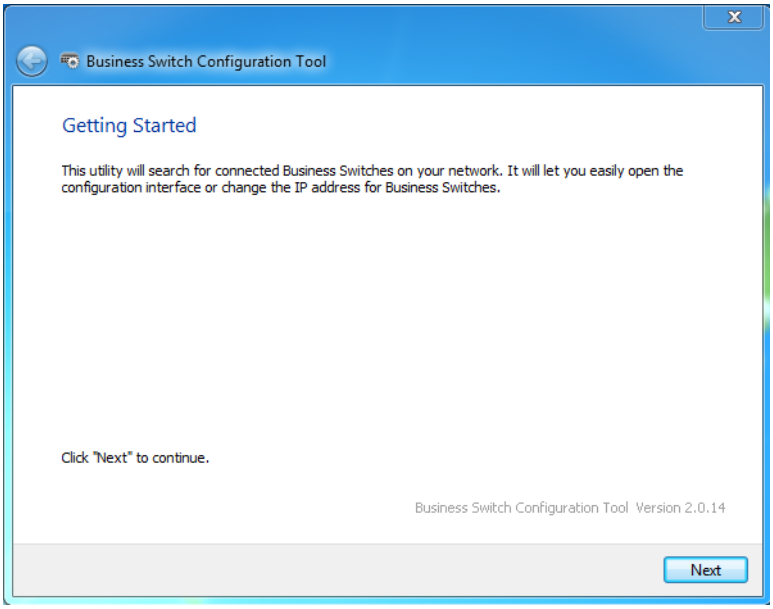
## Change Switch's IP Address

To enter Settings, the switch's web user interface, the switch's IP address should belong to the same segment as your PC's IP address.

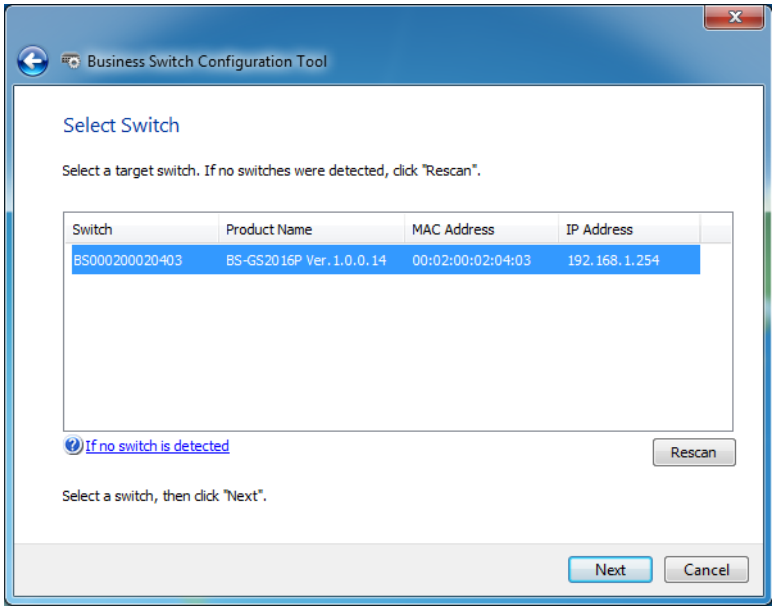
**1** Connect the switch to your PC and your network with an Ethernet cable (sold separately). Confirm that link/act LED of the connected port is on.

**2** Double-click the "Business Switch Configuration Tool" icon to open Business Switch Configuration Tool.

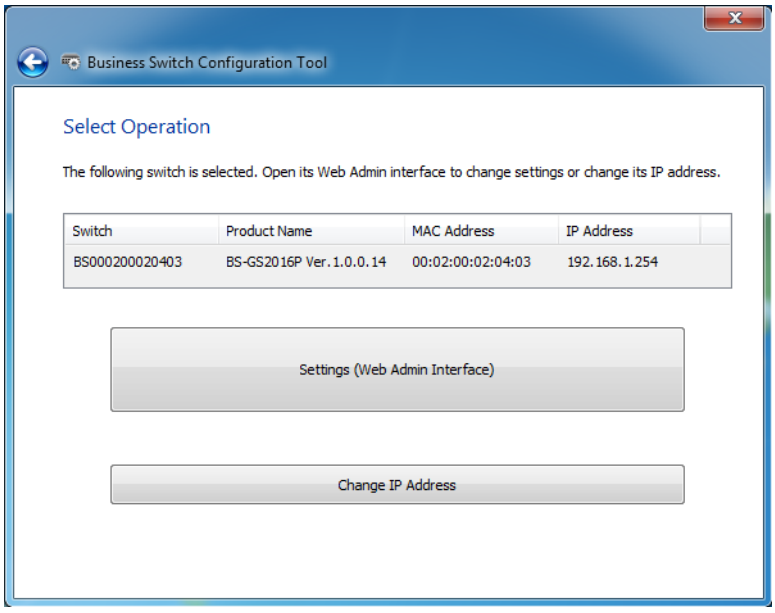
**3** Click [Next] to start searching for the switch.



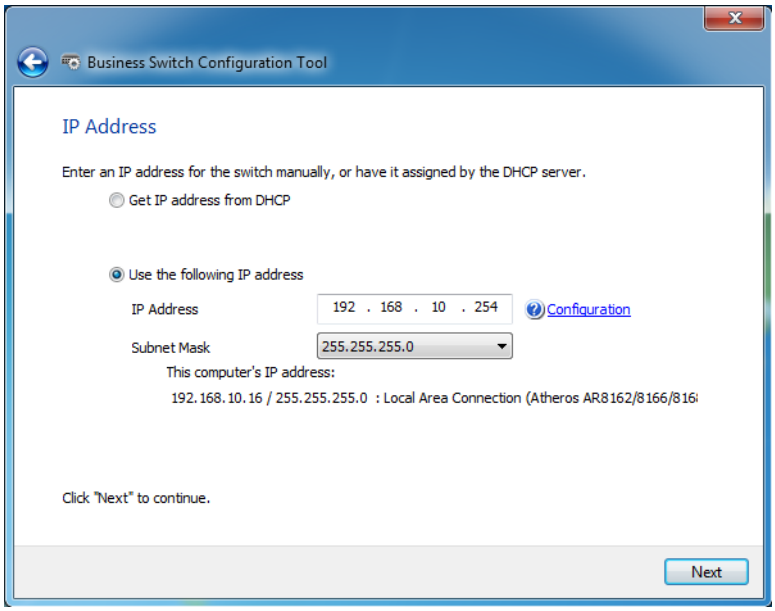
**4** Select the switch and click [Next].




**5** Click [Change IP Address].



**6** Configure the switch's IP address to match the segment of the IP address of your PC and click [Next]. If the password input screen is displayed, enter "password" and click [Next].



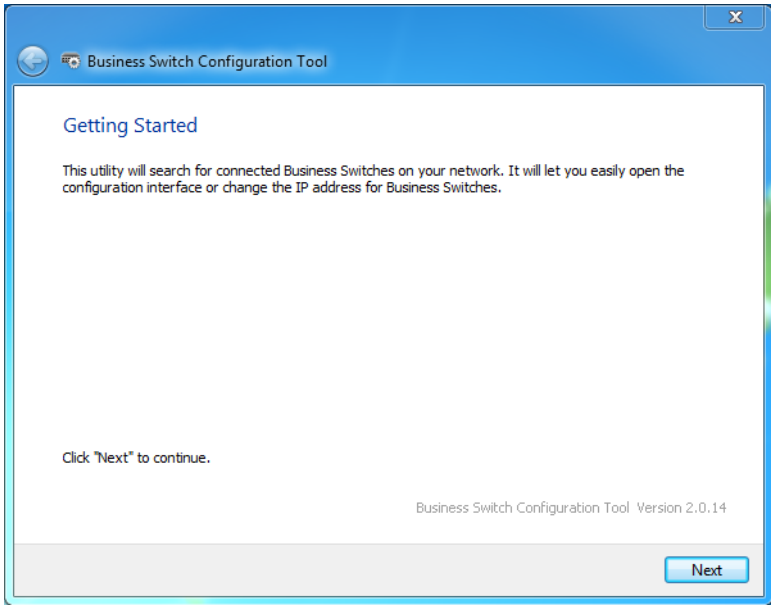

**7** Click [Back to Select Switch].

# Open Settings

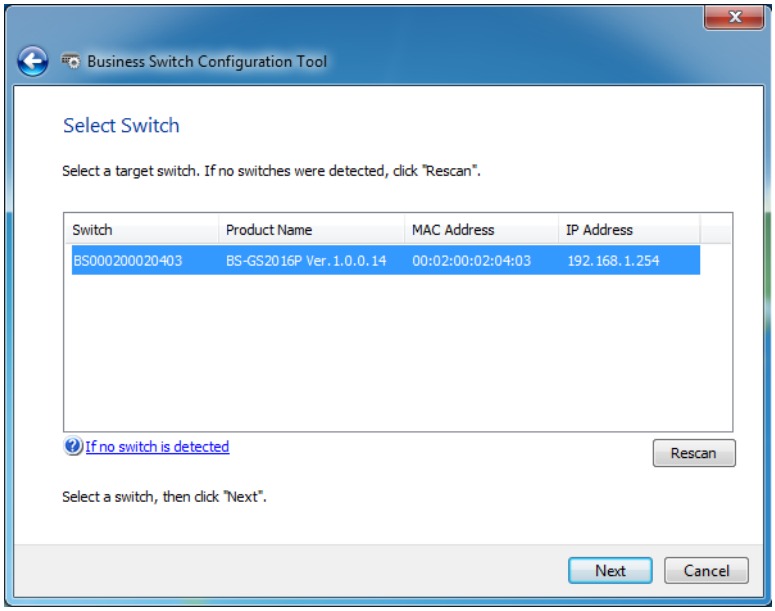
1 Configure the switch's IP address referring to "Change Switch's IP Address" above.

2 Double-click the "Business Switch Configuration Tool" icon to open Business Switch Configuration Tool.

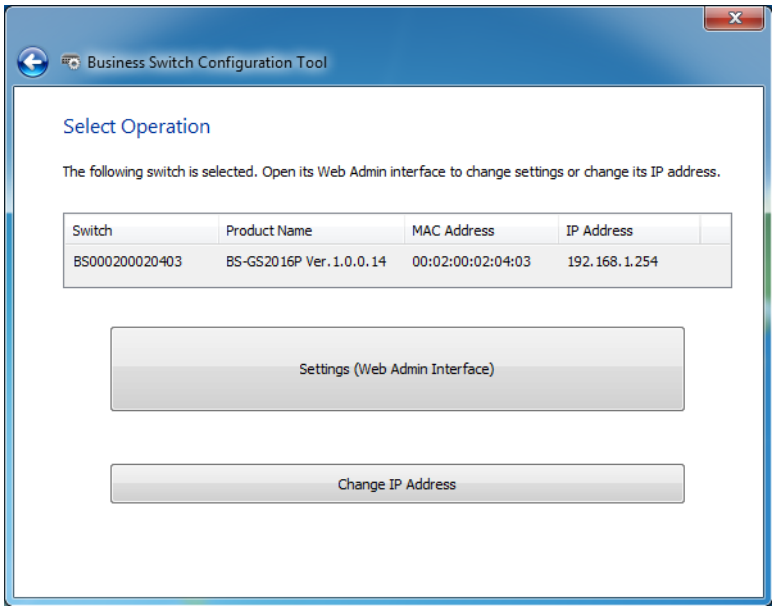
3 Click [Next] to start searching for the switch.



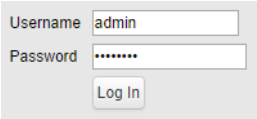

4 Select the switch and click [Next].



**5** Click [Settings (Web Admin Interface)].




**6** Click OK to launch a web browser and display the login screen. Enter "admin" as the username and "password" as the password, then click [Log In].



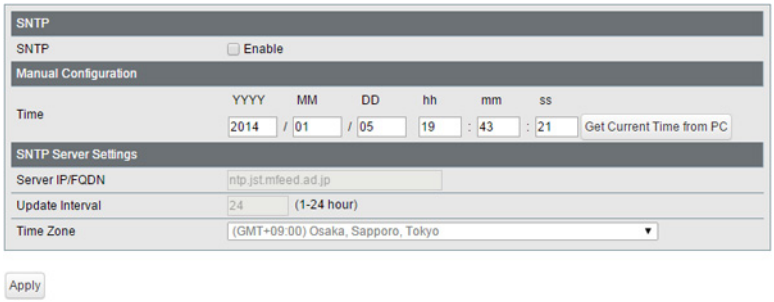

## Configure Date and Time

To configure the date and time, refer to the following procedure.

**1** Open Settings.

**2** Navigate to [Basic] - [Date & Time].

**3** Configure each settings and click [Apply].




**Note:** Enter the IP address or FQDN of the NTP server to change the NTP server. You may enter 4-255 characters. To use FQDN, you have to configure DNS settings separately.

# Change Username and Password

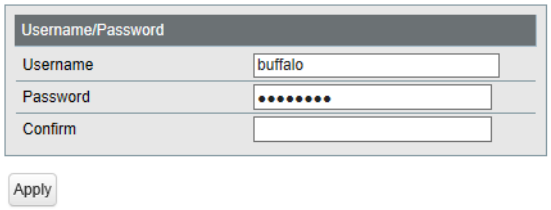
To change the default username and password from "admin" and "password", refer to the following procedure.

**1** Open Settings.

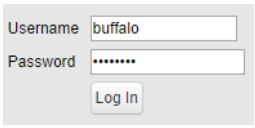
**2** Navigate to [Basic] - [System Security] - [Administration Account].

**3** Enter your new username and password (also fill the "Confirm" field), then click [Apply].

**Note:** You may enter up to 8 alphanumeric characters, hyphens (-), and underscores (_) for the new username and password.



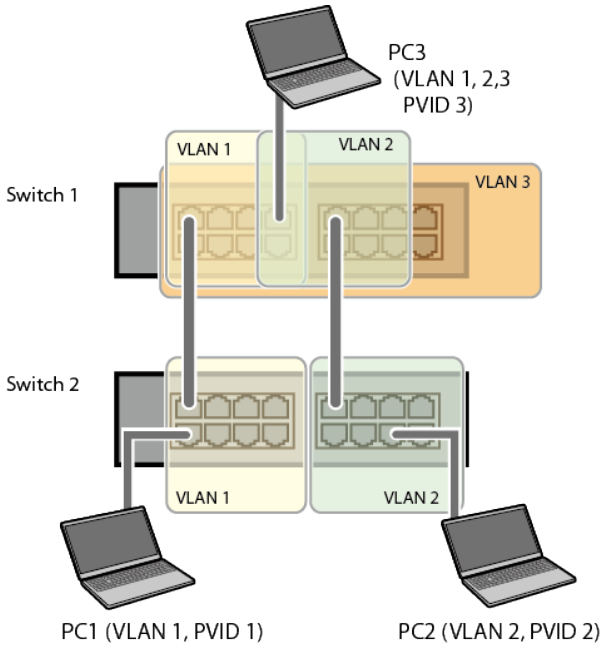

**4** Enter the new username and password, then click [Log In].



# MAC Address Learning

This switch uses SVL (Shared VLAN Learning) to learn MAC addresses. SVL is a method that retains a shared MAC address table for the entire switch. It differs from IVL, which retains a MAC address table for each VLAN. Be sure you understand how SVL works before you create a VLAN with the switch.

## Differences between Operation of SVL and IVL




**SVL**

When PC 1 and PC 3 communicate, PC 3 is learned by port 1 on switch 2 so PC 2 and PC 3 cannot communicate.

**IVL**

When PC 1 and PC 3 communicate, PC 3 is learned by both VLAN 1 and VLAN 2 so PC 2 and PC 3 can communicate. However, frames sent from PC 3 to PC 1 are also delivered to PC 2.

# Chapter 2 Settings

Refer to the "Open Settings" section in chapter 1 to access Settings.

## Menu

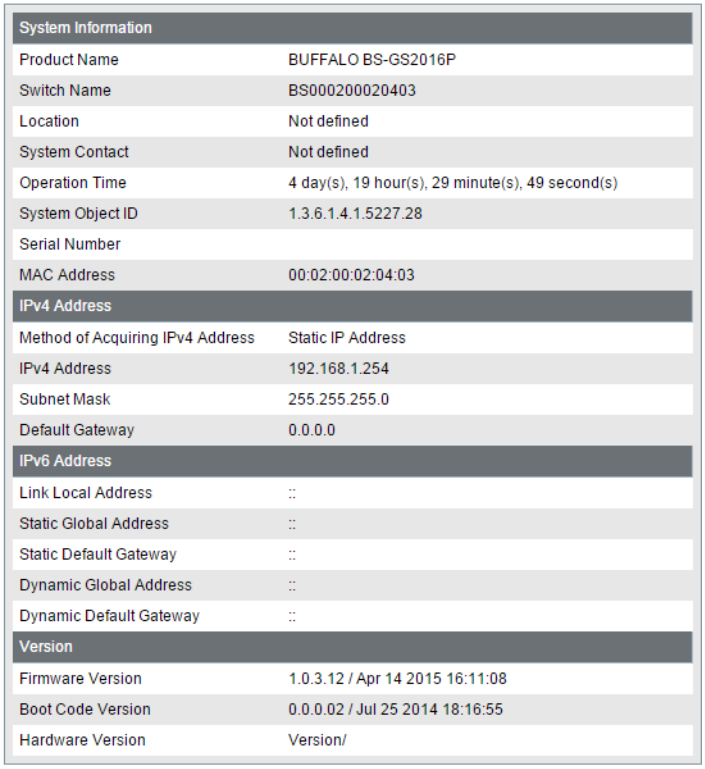
| | | |
|---|---|---|
| **System Information** | | Displays the switch's information. |
| **Basic** | | |
| **System** | | Configure the switch's name, location, and contact. |
| **VLAN** | **VLAN Settings** | Confirm VLAN status and create new VLAN. This switch's IP address can also be configured on this page. |
| | **VLAN Ports** | Configure PVID (Port VLAN ID). |
| **Routing** | **L2/L3 Settings** | Switch between L2 mode and L3 mode. |
| | **Static Routing** (L3 mode only) | Configure the gateway to access the specific destination. |
| **SNMP** | **SNMP Community Table** | Configure SNMP community table. |
| | **SNMP Host Table** | Configure SNMP host table. |
| | **SNMP Trap** | Configure SNMP trap. |
| | **SNMPv3 User** | Configure SNMPv3 user information. |
| **LLDP** | **LLDP Properties** | Configure LLDP. |
| | **LLDP Port** | Configure LLDP for each port. |
| | **LLDP-MED Port** | Configure LLDP-MED for each port. |
| | **Neighbor Table** | Displays the information of LLDP-compatible products connected to the switch. |
| **MAC Addresses** | **Static MAC Filtering** | Configure static MAC address-based filtering. |
| | **Dynamic MAC Filtering** | Configure dynamic MAC address-based filtering. |
| | **Convert MAC Address** | Add dynamic MAC addresses to static MAC address table to filter them in static MAC filtering. |
| | **Static MAC Address** | Register static MAC addresses to MAC address table. |
| | **MAC Address Aging** | Configure MAC address aging time. |
| **Port Settings** | **Status** | Displays port status. |
| | **Speed/Mode Settings** | Configure transmission rate and flow control for each port. |
| **System Security** | **Administration Account** | Configure administration username and password. |
| | **Access Management** | Configure each administration interface. |
| | **Certificate** | Configure certificate. |
| **Date & Time** | | Configure date and time by using SNTP or manually. |
| **PoE** (PoE-compatible switches only) | **Status** | Displays PoE status. |
| | **PoE Profiles** | Configure PoE settings. |
| | **Power Profiles** | Configure power saving schedules. |
| **Advanced** | | |

| | | |
|---|---|---|
| **QoS** | **QoS Settings** | Configure QoS priority. |
| | **QoS Mapping** | Configure QoS mapping for each priority. |
| | **VoIP Auto Priority** | Configure priority for SIP, H.323, SCCP. |
| | **DiffServ** | |
| | **IPv4/MAC Policy** | Create DiffServ policies based on IPv4 or MAC addresses. |
| | **IPv6 Policy** | Create DiffServ policies based on IPv6 addresses. |
| | **Port Settings** | Configure ports to assign each DiffServ policy. |
| | **IPv4/MAC Priority** | Configure priority of each DiffServ policy based on IPv4 or MAC address. |
| | **IPv6 Priority** | Configure priority of each DiffServ policy based on IPv6 address. |
| | **Status** | Displays DiffServ status. |
| **Security** | **Auto DoS Attack Prevention** | Configure to drop specified packets. |
| | **DHCP Snooping** | Configure DHCP snooping. |
| | **DHCP Table** | Displays the list of DHCP clients that obtain IP addresses from a DHCP server via the switch. |
| **Authentication** | **Status** | Displays authentication server status. |
| | **RADIUS** | Configure authentication (RADIUS) server. |
| | **Port Authentication** | Configure authentication for each port. |
| **Port Trunking** | | Configure port trunking. |
| **Traffic Control** | | Configure traffic storm control. |
| **Mirroring** | | Configure to monitoring traffic. |
| **Spanning Tree Protocol** | **STP Settings** | Configure STP/RSTP/MSTP. |
| | **Status** | Displays STP/RSTP/MSTP status of each port. |
| | **Ports** | Configure STP/RSTP/MSTP priority for each port. |
| **IGMP** | **Status** | Displays IGMP status. |
| | **IGMP Settings** | Configure IGMP snooping. |
| | **IGMP Querier** | Configure IGMP querier. |
| | **IGMP Router Port** | Specify ports to connect to multicast routers. |
| **MLD** | **Status** | Displays MLD status. |
| | **MLD Settings** | Configure MLD snooping. |
| | **MLD Querier** | Configure MLD querier. |
| | **MLD Router Port** | Specify ports to connect to multicast routers. |
| **ACL** | **ACL Wizard** | Configure ACL with wizard. |
| | **MAC ACL** | Create MAC address-based ACL. |
| | **IPv4 ACL** | Create IPv4 address-based ACL. |
| | **IPv6 ACL** | Create IPv6 address-based ACL. |
| | **Ports** | Configure ports to assign each ACL group. |
| | **IPv4/MAC Priority** | Configure priority of each IPv4 or MAC ACL group. |
| | **IPv6 Priority** | Configure priority of each IPv6 ACL group. |
| | **Status** | Displays ACL status. |
| **Loop Prevention** | | Configure loop prevention settings. |
| **DHCP Relay** (L3 mode only) | | Configure DHCP relay settings. |
| **Management** | | |
| **Update Firmware** | | Update firmware from a local file. |
| **Dual Image** | | Select a firmware image to be read when booting. |
| **Back Up and Restore Settings** | | Save settings to a file or restore settings from a file. |

| | | |
|---|---|---|
| **Reboot** | | Reboot the switch. |
| **Initialize** | | Initialize the switch. |
| **ARP Table** (L3 mode only) | **Port Order** | Displays the ARP table ordered by ports. |
| | **IP Address Order** | Displays the ARP table ordered by IP addresses. |
| **MAC Address Table** | **Port Order** | Displays the MAC address table ordered by ports. |
| | **MAC Order** | Displays the MAC address table ordered by MAC addresses. |
| **Statistics** | | Displays the switch's statistics. |
| **Logs** | | Displays log information. |
| **Syslog Settings** | | Configure to transfer logs to syslog server. |
| **Network Diagnostics** | | Execute communication test to the specified IP address. |
| **Cable Diagnostics** | | Confirm abnormalities of each Ethernet cable connected to the switch. |

# System Information

Displays the switch's information.



| System Information | |
|---|---|
| Product Name | BUFFALO BS-GS2016P |
| Switch Name | BS000200020403 |
| Location | Not defined |
| System Contact | Not defined |
| Operation Time | 4 day(s), 19 hour(s), 29 minute(s), 49 second(s) |
| System Object ID | 1.3.6.1.4.1.5227.28 |
| Serial Number | |
| MAC Address | 00:02:00:02:04:03 |
| **IPv4 Address** | |
| Method of Acquiring IPv4 Address | Static IP Address |
| IPv4 Address | 192.168.1.254 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 0.0.0.0 |
| **IPv6 Address** | |
| Link Local Address | :: |
| Static Global Address | :: |
| Static Default Gateway | :: |
| Dynamic Global Address | :: |
| Dynamic Default Gateway | :: |
| **Version** | |
| Firmware Version | 1.0.3.12 / Apr 14 2015 16:11:08 |
| Boot Code Version | 0.0.0.02 / Jul 25 2014 18:16:55 |
| Hardware Version | Version/ |

| | |
|---|---|
| **System Information** | Displays system information such as the switch name, serial number, and MAC address. |
| **IPv4 Address** | Displays information such as the switch's IPv4 address, subnet mask, and default gateway. |
| **IPv6 Address** | Displays information such as the switch's IPv6 addresses and default gateways. |
| **Version** | Displays the switch's firmware, boot code, and hardware version. |

# System

Configure the switch's name, location, and contact.

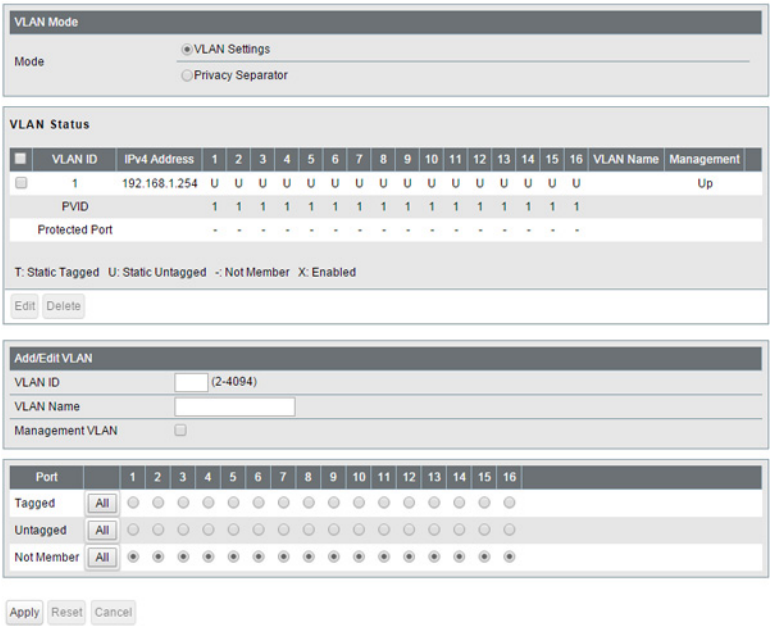

| | |
|---|---|
| **Switch Name** | Enter the switch's name. You may enter up to 50 alphanumeric characters, hyphens, and underscores. |
| **Location** | Enter the location of the switch. You may enter up to 50 alphanumeric characters, hyphens, underscores, and spaces. |
| **Contact** | Enter the contact information of the switch. You may enter up to 50 alphanumeric characters, hyphens, underscores, and spaces. |

# VLAN

## VLAN Settings

Confirm VLAN status and configure new VLAN. The switch's IP address, default gateway, and DNS server can also be configured on this page.

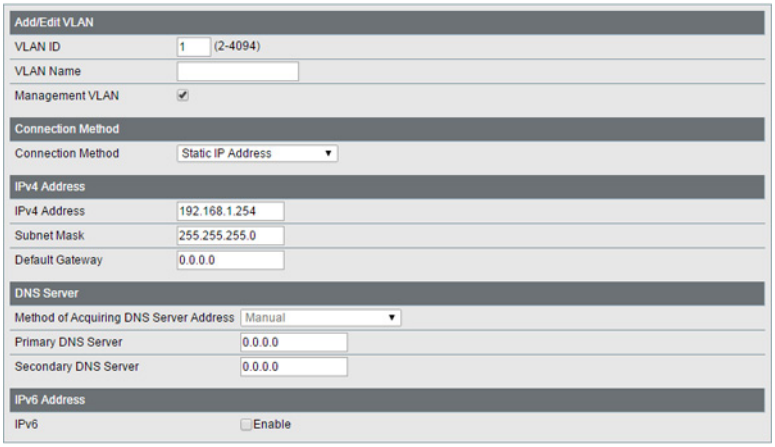
### In L2 mode



| | |
|---|---|
| **Mode** | Select a VLAN mode from "VLAN Settings" or "Privacy Separator". Privacy separator is a mode that enables communication to the router from a port but blocks communication between ports.<br>**Note:** VLAN and privacy separator cannot be used at the same time. |
| **VLAN Status** | Displays current VLAN and PVID (Port VLAN ID) status. Click [Edit] to edit the VLAN selected. Click [Delete] to delete the VLAN selected. VLAN 1 cannot be deleted. |
| **VLAN ID** | Specify VLAN ID from 2-4094. |
| **VLAN Name** | Enter the VLAN name. You may enter up to 17 alphanumeric characters, hyphens, and underscores. |
| **Management VLAN** | Check it if the VLAN is a management VLAN. Only devices which belong to the management VLAN can open Settings. |
| **Tagged** | Select when you assign the port to tag member. |
| **Untagged** | Select when you assign the port to untag member. |
| **Not Member** | Select when you do not assign the port to any member. |
| **Reset** | Click to reset the changes to the previous settings. |
| **Uplink** | Appears when "Privacy Separator" is selected.<br>A router should be connected to the uplink port to connect to the Internet. Uplink ports can communicate with all downlink ports. Specify at least 1 port to an uplink port. |
| **Downlink** | Appears when "Privacy Separator" is selected.<br>Downlink ports are the ones which each device connected to. Downlink ports can communicate with uplink ports, but cannot communicate with each downlink port. |

**Note:** In privacy separator mode, only the device connected to an uplink port can open Settings. If you configure the port that your PC is connected as a downlink port, you cannot open Settings any more.

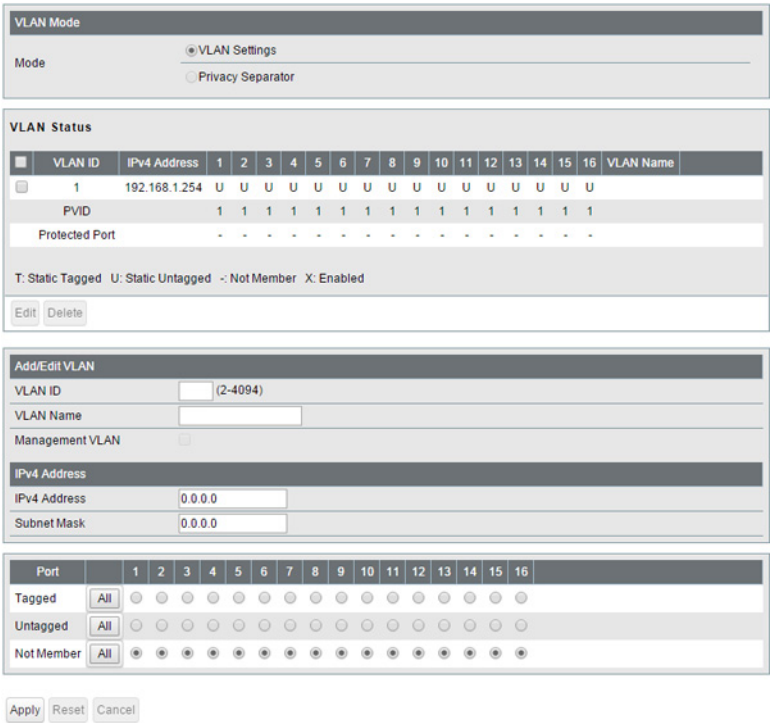
The following screen is displayed when you select VLAN 1 and click [Edit] or click [Edit] next to the IP address field in privacy separator mode.




| | |
|---|---|
| **Connection Method** | Select a method of obtaining the switch's IP address.<br><br>**Static IP Address**<br>Enter the IP address manually.<br>**Obtain from DHCP Server**<br>Obtain the switch's IP address from DHCP server. |
| **IPv4 Address** | Enter the switch's IPv4 address if you select [Static IP Address] as the connection method. |
| **Subnet Mask** | Enter the switch's subnet mask if you select [Static IP Address] as the connection method. |

| | |
|---|---|
| **Default Gateway** | Enter the switch's default gateway if you select [Static IP Address] as the connection method. |
| **Method of Acquiring DNS Server Address** | Select a method of obtaining the DNS server's IP address. |
| **Primary DNS Server** | Enter the primary DNS server's IP address. |
| **Secondary DNS Server** | Enter the secondary DNS server's IP address. |
| **IPv6** | Check "Enable" to enable IPv6. |
| **Obtain IPv6 address automatically** | Check "Enable" if the switch need to obtain router advertisement from IPv6-compatible router. |
| **DHCPv6 Client** | Check "Enable" if using DHCPv6 client. When "Rapid Commit" is checked, the communication speed with DHCPv6 server will be increased if the DHCPv6 server is also compatible with rapid commit. |
| **Link Local Address** | Displays the switch's link local address. This is generated automatically when IPv6 is enabled. |
| **Static Global Address** | Enter the global address and prefix length to configure an IPv6 address manually. The prefix length may contain 1-128. When "EUI-64" is checked, the bottom 64 bit of the IPv6 address will be generated automatically based on the switch's MAC address, in accordance with Modified EUI-64 (RFC4291). |
| **Static Default Gateway** | Enter the default gateway to configure an IPv6 default gateway manually. The default gateway prefix should be the same as the static global address. |
| **Dynamic Global Address** | Displays the dynamic global address obtained from DHCPv6 or router advertisement. The address with the trailing "SF" means that the address was obtained from DHCPv6. The address with the trailing "SL" means that the address was obtained from router advertisement. |
| **Dynamic Default Gateway** | Displays the default gateway obtained from router advertisement. |

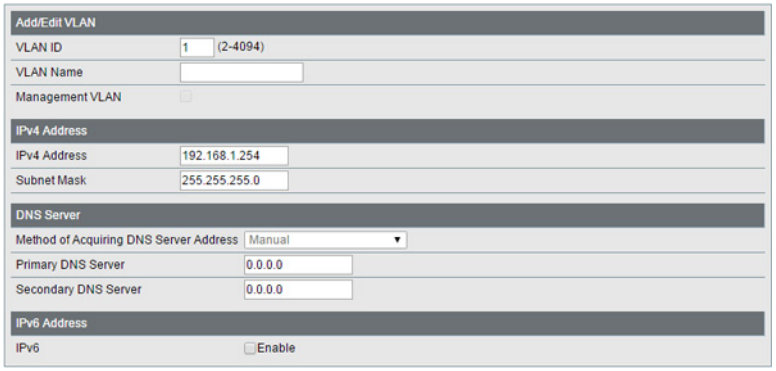
## In L3 mode




| | |
|---|---|
| **Mode** | Privacy separator cannot be used when the switch is in L3 mode. |
| **VLAN Status** | Displays current VLAN and PVID (Port VLAN ID) status. Click [Edit] to edit the VLAN selected. Click [Delete] to delete the VLAN selected. VLAN 1 cannot be deleted. |
| **VLAN ID** | Specify the VLAN ID from 2-4094. |
| **VLAN Name** | Enter the VLAN name. You may enter up to 17 alphanumeric characters, hyphens, and underscores. |
| **Management VLAN** | If an IP address is assigned to the VLAN, that VLAN will become a management VLAN in L3 mode. |
| **IPv4 Address** | Enter an IPv4 address and a subnet mask to assign them to the VLAN. Up to 32 VLANs that a unique IPv4 addresses is assigned can be created. |
| **Tagged** | Select when you assign the port to tag member. |
| **Untagged** | Select when you assign the port to untag member. |
| **Not Member** | Select when you do not assign the port to any member. |
| **Reset** | Click to reset the changes to the previous settings. |
| **Uplink** | Appears when "Privacy Separator" is selected.<br>A router should be connected to the uplink port to connect to the Internet. Uplink ports can communicate with all downlink ports. Specify at least 1 port to an uplink port. |
| **Downlink** | Appears when "Privacy Separator" is selected.<br>Downlink ports are the ones which each device connected to. Downlink ports can communicate with uplink ports, but cannot communicate with each downlink port. |

**Note:** In privacy separator mode, only the device connected to an uplink port can open Settings. If you configure the port that your PC is connected as a downlink port, you cannot open Settings anymore.

The following screen is displayed when you select VLAN 1 and click [Edit].

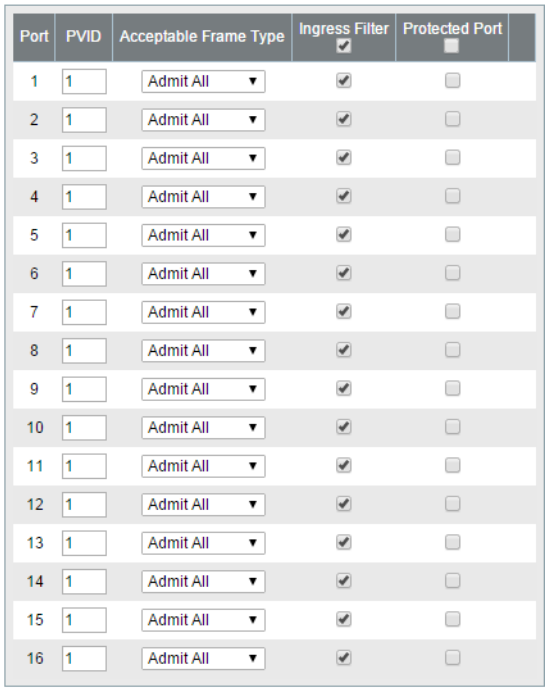



| | |
|---|---|
| **Method of Acquiring DNS Server Address** | Select a method of obtaining the DNS server's IP address. |
| **Primary DNS Server** | Enter the primary DNS server's IP address. |
| **Secondary DNS Server** | Enter the secondary DNS server's IP address. |
| **IPv6** | Check "Enable" to enable IPv6. |
| **Obtain IPv6 address automatically** | Check "Enable" if the switch need to obtain router advertisement from IPv6-compatible router. |
| **DHCPv6 Client** | Check "Enable" if using DHCPv6 client. When "Rapid Commit" is checked, the communication speed with the DHCPv6 server will be increased if the DHCPv6 server is also compatible with rapid commit. |
| **Link Local Address** | Displays the switch's link local address. This is generated automatically when IPv6 is enabled. |
| **Static Global Address** | Enter the global address and prefix length to configure an IPv6 address manually. The prefix length may contain 1-128. When "EUI-64" is checked, the bottom 64 bit of the IPv6 address will be generated automatically based on the switch's MAC address, in accordance with Modified EUI-64 (RFC4291). |
| **Static Default Gateway** | Enter the default gateway to configure an IPv6 default gateway manually. The default gateway prefix should be the same as the static global address. |
| **Dynamic Global Address** | Displays the dynamic global address obtained from DHCPv6 or router advertisement. The address with the trailing "SF" means that the address was obtained from DHCPv6. The address with the trailing "SL" means that the address was obtained from router advertisement. |
| **Dynamic Default Gateway** | Displays the default gateway obtained from router advertisement. |

**Note:** In L3 mode, you can configure the default gateway from the [Routing] - [Static Routing] page.

# VLAN Ports

Configure PVID (Port VLAN ID).

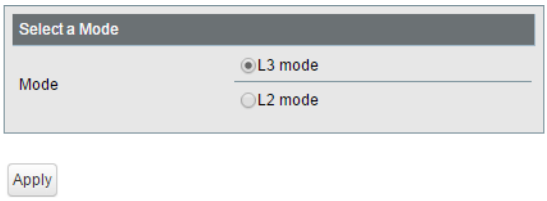



| | |
|---|---|
| **PVID** | Specify the port VLAN ID. The received untagged frames will be recognized as the specified VLAN ID. (1-4094) |
| **Acceptable Frame Type** | **Admit All**<br>Receive both untagged and tagged frames.<br>**Tag Only**<br>Receive tagged frames only and drop untagged frames. |
| **Ingress Filter** | **Enable**<br>Drop frames if the received frame's VLAN ID is not a member of incoming port's VLAN.<br>**Disable**<br>All tagged and untagged frames will be received. |
| **Protected Port** | "Protected Port" enabled ports cannot communicate with each other. |

# Routing

## L2/L3 Settings

Configure the layer mode of the switch.

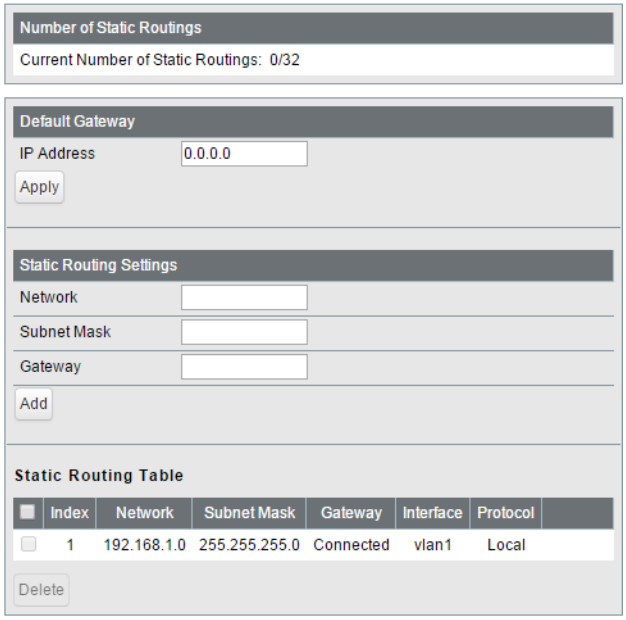



| | |
|---|---|
| **Mode** | Specify the layer mode from the following.<br><br>**L3 mode**<br>The switch works as a layer 3 switch.<br>**L2 mode**<br>The switch works as a layer 2 switch. |

**Note:** Switching the mode will delete static routing settings and all VLANs except VLAN 1.

## Static Routing

Displayed only when the switch is in L3 mode. Configure the gateway to reach the specified network.




| | |
|---|---|
| **Number of Static Routings** | Displays the number of enabled static routings. |
| **Default Gateway** | Enter the IP address of the gateway to reach an unspecified network. |

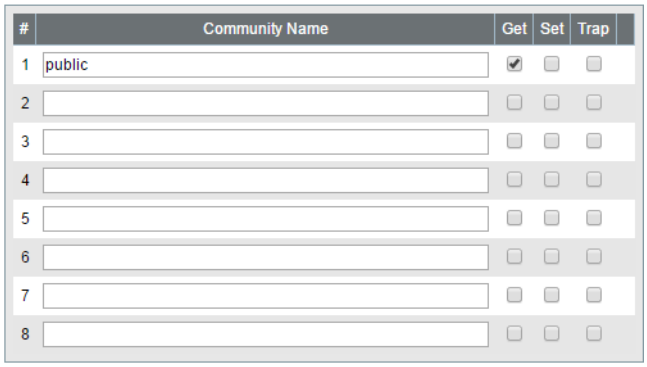
| | |
|---|---|
| **Static Routing Table Setting** | Add the static routing setting to the table by entering the following items. Up to 32 static routes can be created.<br><br>**Network**<br>Enter the IP address of the network that you need to configure the static routing for.<br>**Subnet Mask**<br>Enter the subnet mask of the network.<br>**Gateway**<br>Enter the IP address of the gateway to reach the specified network. |
| **Static Routing Table** | Displays the static routing information. |

# SNMP Settings

To use SNMP, SNMP monitoring software is needed.

## SNMP Community Table

Configure SNMP community table.

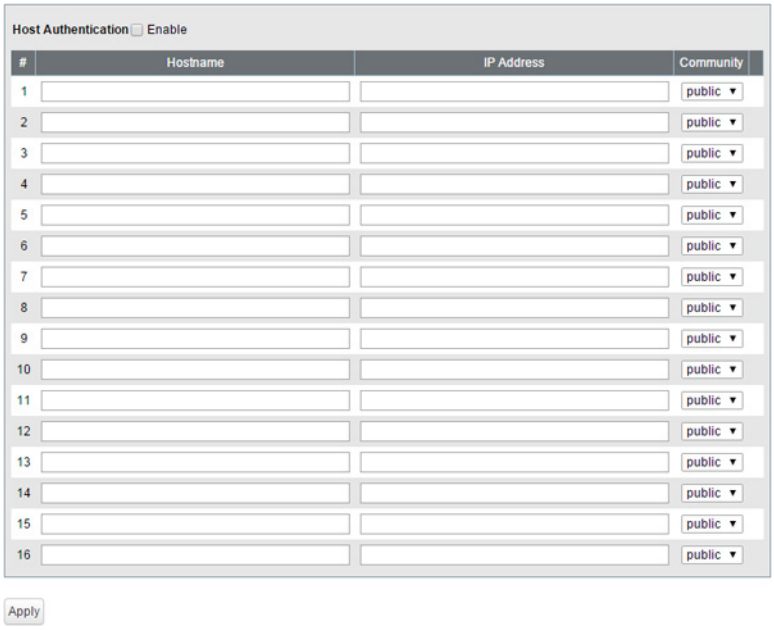



| | |
|---|---|
| **Community Name** | Enter the community name. You may enter up to 31 alphanumeric characters, hyphens, and underscores. |
| **Get** | If checked, community members are allowed to read the switch's SNMP information. |
| **Set** | If checked, community members are allowed to write the switch's SNMP information. |
| **Trap** | If checked, communication members can receive SNMP traps. |

# SNMP Host Table

Configure the SNMP host table.

**Note:** To delete the registered host, make "Hostname" and "IP Address" field blank and click [Apply].

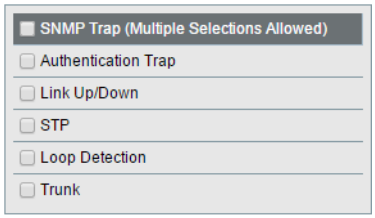



| | |
|---|---|
| **Host Authentication** | Enable/disable SNMP host authentication.<br>**Enable**<br>SNMP service will be provided from SNMP manager only. Read/write authority depends on the community.<br><br>**Disable**<br>Receive SNMP requests from any hosts. Read/write authority depends on the community. |
| **Hostname** | Enter a hostname to permit SNMP requests. You may enter 1-31 alphanumeric characters, hyphens, and underscores. |
| **IP Address** | Enter an IPv4/IPv6 address of the host. To communicate with the host using an IPv6 address, enable IPv6 in advance. |
| **Community** | Select the host's community. Communities should be configured on the [SNMP Community Table] page in advance. |

# SNMP Trap

Configure SNMP traps.

**Note:** To use SNMP traps, register the host to the host table on the [Basic] - [SNMP] - [SNMP Host Table] page and enable "trap" for that community.




Compatible traps:

0 coldStart

1 warmStart

2 LinkDown (Link Up/Down)

3 LinkUp (Link Up/Down)

4 authenticationFailure (Authentication Trap)

6 topoligyChange (STP)

7 Loop detection (Loop Detection)

Private MIB OID: 1.3.6.1.4.1.5227.28.1.1.1

8 Trunk (Trunk)

Private MIB OID: 1.3.6.1.4.1.5227.28.1.1.2 (the value differs depending on the trunk's link status as below)

1.3.6.1.4.1.5227.28.1.2.1 (trunk key 1-8)

1.3.6.1.4.1.5227.28.1.2.2 (link up: 1, link down: 2)

All traps can be enabled/disabled except "coldStart" and "warmStart".

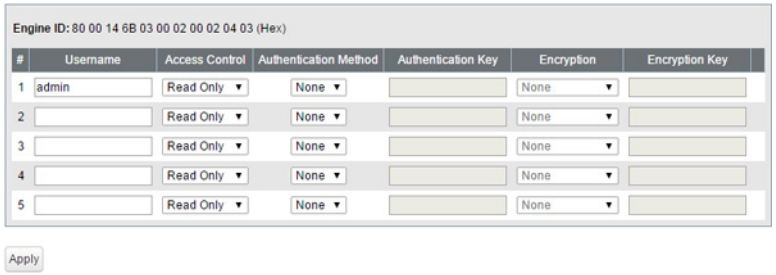
| | |
|---|---|
| **SNMP Trap** | Enable or disable all of the following traps. |
| **Authentication Trap** | If enabled, the trap will be sent when SNMP is requested from an unallowed IP address. |
| **Link Up/Down** | If enabled, the trap will be sent when link up/down of the port is detected. |
| **STP** | If enabled, the trap will be sent when STP/RSTP/MSTP topology change is occurred. |
| **Loop Detection** | If enabled, the trap will be sent when the loop is detected. |
| **Trunk** | If enabled, the trap will be sent when the trunk is configured or unconfigured. |

# SNMPv3 User

Configure information of users who are authenticated with SNMPv3. SNMPv3 will authenticate users using username and the authentication can be encrypted. This switch is compatible with the following authentication and encryption method.

Authentication method: HMAC-MD5-96/HMAC-SHA-96

Encryption method: CBC-DES/CFB-AES-128

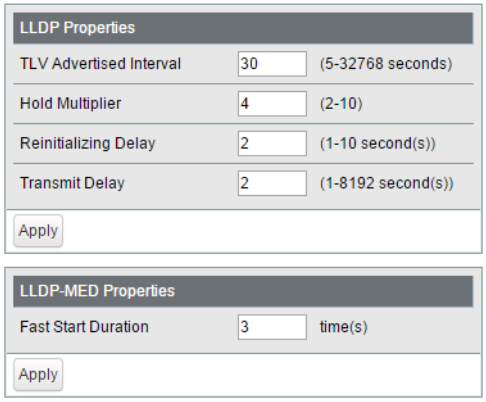



| | |
|---|---|
| **Engine ID** | This is the switch's unique ID to identify SNMP engine. This ID will be notified to other side when SNMPv3 communication is done. |
| **Username** | Enter the username to authenticate. The username should be up to 32 alphanumeric characters, hyphens (-), and underscores (_). |
| **Access Control** | Limit the access depending on the user.<br><br>**Read Only**<br>Prohibit writing.<br>**Read/Write**<br>Permit any access. |
| **Authentication Method** | Configure the authentication method. |
| **Authentication Key** | Enter the key phrase compatible with the authentication method. |
| **Encryption** | Configure the encryption method. |
| **Encryption Key** | Enter the key phrase compatible with the encryption method. |

# LLDP

## LLDP Properties

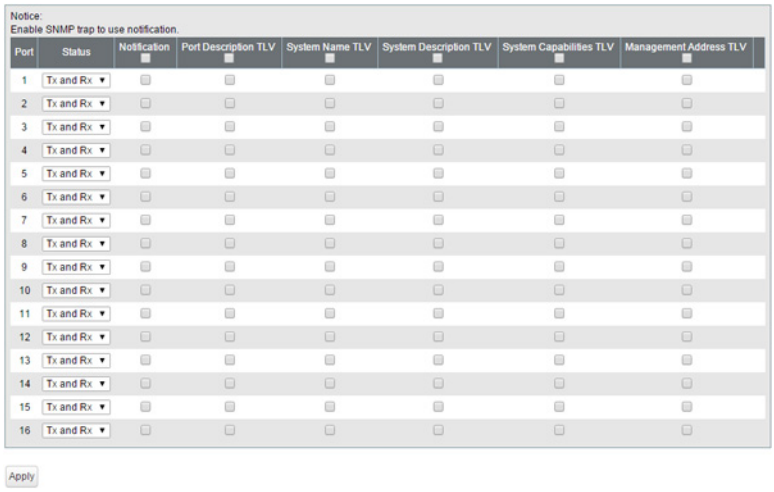
Configure LLDP.




| | |
|---|---|
| **TLV Advertised Interval** | Enter the interval of sending LLDP packets. (5-32768 seconds) |
| **Hold Multiplier** | Enter the amount of time of TTL (Time To Live: the time that LLDP packets are held before the packets are discarded) measured in multiples of the TLV advertised interval. (2-10) |
| **Reinitializing Delay** | Enter the time that passes between disabling and reinitializing LLDP. (1-10 seconds) |
| **Transmit Delay** | Enter the time that passes between changing the LLDP settings and transmitting LLDP frame. (1-8192 seconds) |
| **Fast Start Duration** | Enter the number of times that LLDP packets are sent when the LLDP-MED-compatible device is detected. |

# LLDP Port

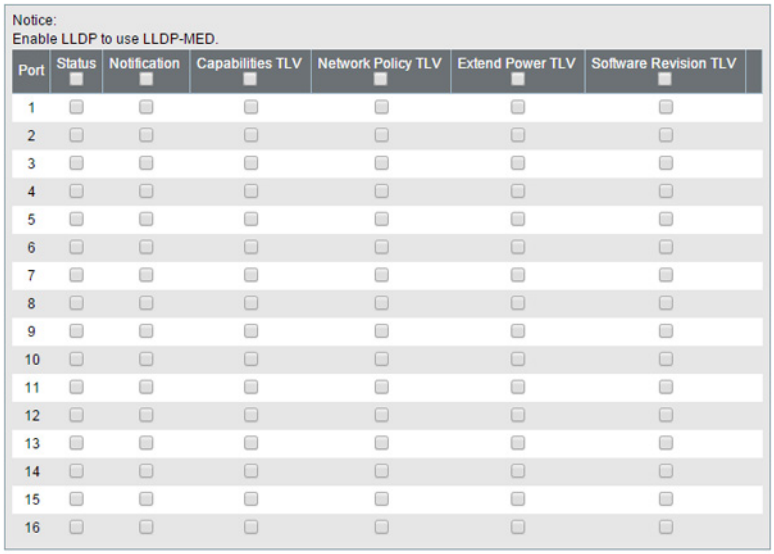
Configure LLDP for each port.




| | |
|---|---|
| **Status** | **Disable**<br>Disable LLDP.<br>**Tx Only**<br>Enable transmitting LLDP packets only.<br>**Rx Only**<br>Enable receiving LLDP packets only.<br>**Tx and Rx**<br>Enable transmitting and receiving LLDP packets. |
| **Notification** | If enabled, SNMP traps will be sent to the SNMP server when the neighbor table is updated.<br>**Note:** To use notification, configure SNMP manager and SNMP trap settings. |
| **Port Description TLV** | If enabled, the port information (port number) will be included in LLDP packets. |
| **System Name TLV** | If enabled, the switch name will be included in LLDP packets.<br>**Note:** The switch name can be configured on the [Basic] - [System] page. |
| **System Description TLV** | If enabled, the product name will be included in LLDP packets. |
| **System Capabilities TLV** | If enabled, the system capabilities will be included in LLDP packets. |
| **Management Address TLV** | If enabled, the switch's IP address will be included in LLDP packets. |

## LLDP-MED Port

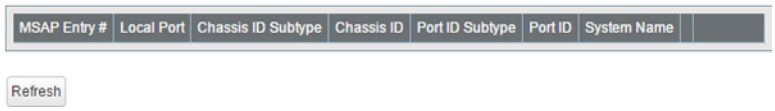
Configure LLDP-MED for each port.




| | |
|---|---|
| **Status** | If enabled, LLDP-MED will be transmitted.<br>**Note:** To use this functionality, configure the status to [Tx Only] or [Tx and Rx] on the [LLDP Port] page. |
| **Notification** | If enabled, the SNMP trap will be sent to the SNMP server when the LLDP-MED information in the neighbor table is updated.<br>**Note:** To use notification, configure SNMP manager and SNMP trap settings. |
| **Capabilities TLV** | If enabled, the capabilities will be included in LLDP packets. |
| **Network Policy TLV** | If enabled, the network policy will be included in LLDP packets. |
| **Extend Power TLV** | If enabled, the extend power will be included in LLDP packets.<br>**Note:** This functionality is compatible with PoE switches only. |
| **Software Revision TLV** | If enabled, the firmware version will be included in LLDP packets. |

## Neighbor Table

Displays the information of the LLDP-compatible devices connected to the switch.




| | |
|---|---|
| **MSAP Entry #** | Displays the entry number of the detected devices. |
| **Local Port** | Displays port number that the detected devices are connected to. |
| **Chassis ID Subtype** | Displays the chassis ID subtype of the detected devices. |
| **Chassis ID** | Displays the chassis ID of the detected devices. |
| **Port ID Subtype** | Displays the port ID subtype of the detected devices. |
| **Port ID** | Displays the port ID of the detected devices. |

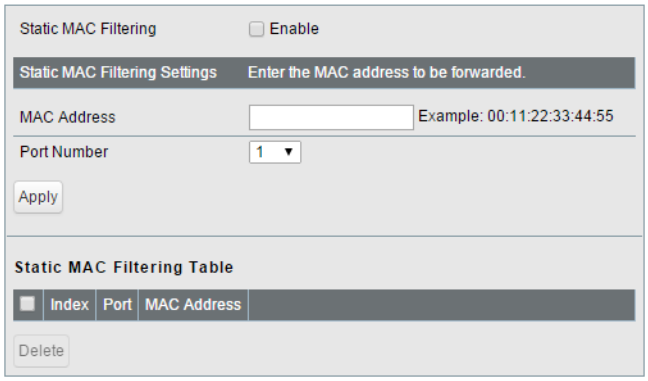
| | |
|---|---|
| **System Name** | Displays the system name of the detected devices. |

**Note:** To use this functionality, configure the status to [Rx Only] or [Tx and Rx] on the [Basic] - [LLDP] - [LLDP Port] page.

# MAC Addresses

## Static MAC Filtering

Configure the filtering of MAC addresses that are registered manually. Only the frames with registered MAC address as a source MAC address can pass through the ports that the MAC address is registered to.

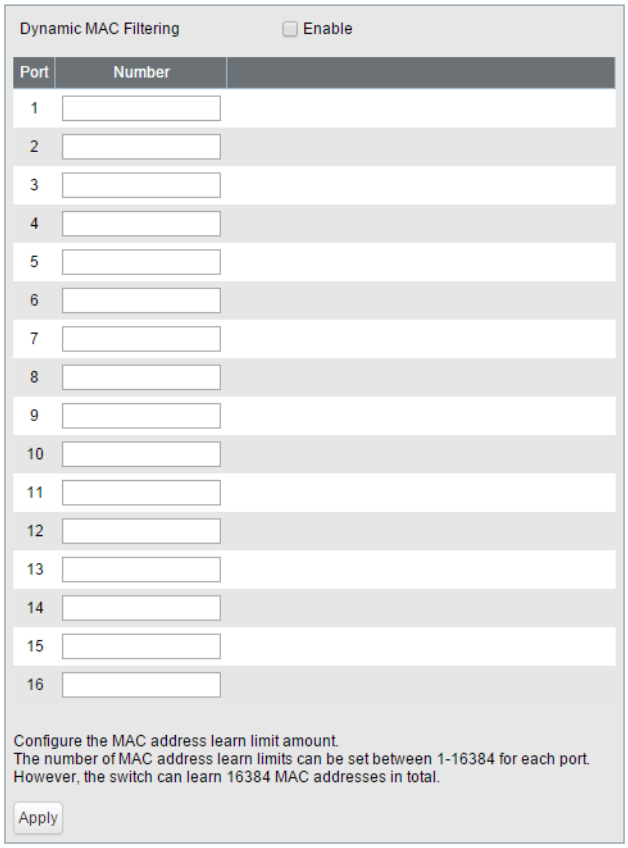



| | |
|---|---|
| **Static MAC Filtering** | Check "Enable" to enable static MAC filtering. |
| **MAC Address** | Enter the MAC address you want to filter. (Example: 00:11:22:aa:bb:cc)<br>Up to 16 addresses can be registered per port. |
| **Port Number** | Select a port to apply the static MAC filter. |
| **Static MAC Filtering Table** | Displays the registered MAC addresses and port numbers. |

**Note:** This function is not compatible with multicast MAC addresses, VRRP MAC addresses (00:00:5E:00:01:XX), and broadcast MAC addresses.

# Dynamic MAC Filtering

Configure the dynamic MAC filtering that enables you to set the number of MAC address learn limits for each port.



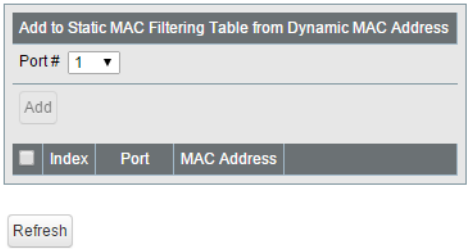

| | |
|---|---|
| **Dynamic MAC Filtering** | Check "Enable" to enable dynamic MAC filtering. |
| **Number** | Enter the number of MAC address learning limits of each port. (1-16384) |

**Notes:**

- If the port's "Number" field is left blank, all MAC addresses can pass through that port.
- The number of MAC address learn limits can be set between 1-16384 for each port. However, the switch can learn 16384 MAC addresses in total. If the number of MAC address is over 16384, MAC addresses will never be learned and will be dropped.
- When both static and dynamic MAC filtering are enabled, MAC addresses in the static MAC address table are not counted towards the number of dynamic MAC address.

# Convert MAC Address

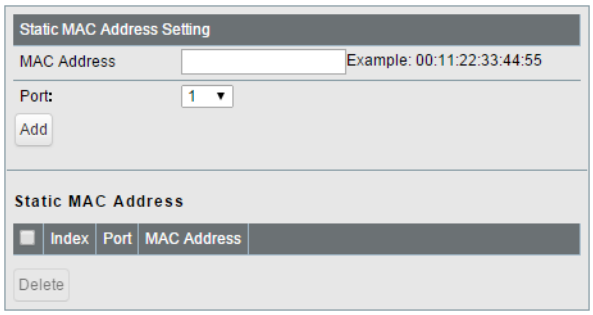
Add dynamic MAC addresses to static MAC filtering table to filter them in static MAC filtering.




| | |
|---|---|
| **Add to Static MAC Filtering Table from Dynamic MAC Address** | Select a port number to display the dynamic MAC addresses that was learned from the port. Select MAC addresses to add to the static MAC filtering table and click [Add]. |

# Static MAC Address

Register the static MAC address to the MAC address table. The device with a registered MAC address can communicate only when it is connected to the specified port. You can confirm the status of static MAC addresses registration in [Management] - [MAC Address Table].




| | |
|---|---|
| **MAC Address** | Enter a MAC address. Up to 256 MAC addresses can be registered to the switch in total. |
| **Port** | Specify the port number to register the static MAC address. |
| **Static MAC Address** | Displays the registered static MAC addresses. |

**Notes:**

- This function is not compatible with multicast MAC addresses, VRRP MAC addresses (00:00:5E:00:01:XX), and broadcast MAC addresses.
- The registered device cannot communicate when it is not connected to the specified port.

## MAC Address Aging

Configure MAC address aging time. MAC address aging time is the time between the last reference of the MAC address and deleting MAC address.

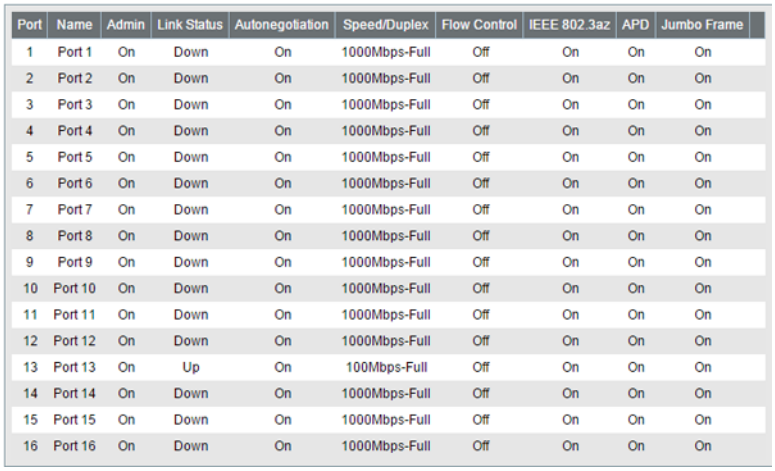

Apply

| | |
|---|---|
| **Aging Time** | Enter the aging time. |

# Port Settings

## Status

Displays the port status.

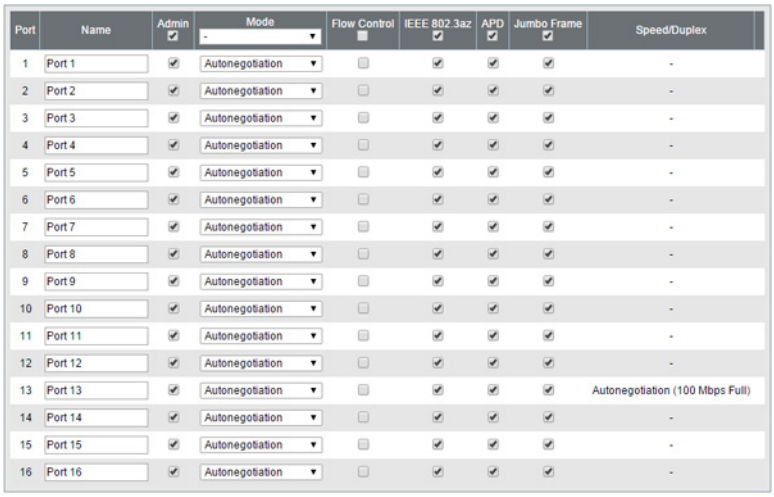


| Port | Name | Admin | Link Status | Autonegotiation | Speed/Duplex | Flow Control | IEEE 802.3az | APD | Jumbo Frame |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Port 1 | On | Down | On | 1000Mbps-Full | Off | On | On | On |
| 2 | Port 2 | On | Down | On | 1000Mbps-Full | Off | On | On | On |
| 3 | Port 3 | On | Down | On | 1000Mbps-Full | Off | On | On | On |
| 4 | Port 4 | On | Down | On | 1000Mbps-Full | Off | On | On | On |
| 5 | Port 5 | On | Down | On | 1000Mbps-Full | Off | On | On | On |
| 6 | Port 6 | On | Down | On | 1000Mbps-Full | Off | On | On | On |
| 7 | Port 7 | On | Down | On | 1000Mbps-Full | Off | On | On | On |
| 8 | Port 8 | On | Down | On | 1000Mbps-Full | Off | On | On | On |
| 9 | Port 9 | On | Down | On | 1000Mbps-Full | Off | On | On | On |
| 10 | Port 10 | On | Down | On | 1000Mbps-Full | Off | On | On | On |
| 11 | Port 11 | On | Down | On | 1000Mbps-Full | Off | On | On | On |
| 12 | Port 12 | On | Down | On | 1000Mbps-Full | Off | On | On | On |
| 13 | Port 13 | On | Up | On | 100Mbps-Full | Off | On | On | On |
| 14 | Port 14 | On | Down | On | 1000Mbps-Full | Off | On | On | On |
| 15 | Port 15 | On | Down | On | 1000Mbps-Full | Off | On | On | On |
| 16 | Port 16 | On | Down | On | 1000Mbps-Full | Off | On | On | On |

| | |
|---|---|
| **Name** | Displays the port name. |
| **Admin** | Displays whether the port is enabled (on) or disabled (off). |
| **Link Status** | Displays whether the link is up or down. |
| **Autonegotiation** | Displays whether the autonegotiation is enabled (on) or disabled (off). |
| **Speed/Duplex** | Displays the speed and duplex status. |
| **Flow Control** | Displays whether the flow control is enabled (on) or disabled (off). |
| **IEEE 802.3az** | Displays whether IEEE 802.3az is enabled (on) or disabled (off). |
| **APD** | Displays whether APD is enabled (on) or disabled (off). |
| **Jumbo Frame** | Displays whether jumbo frame is enabled (on) or disabled (off).<br>**Note:** Jumbo frames of up to 9216 frames (including header 14 bytes + FCS 4 bytes) can be forwarded. |

# Speed/Mode Settings

Configure ports settings such as the transmission rate or flow control.

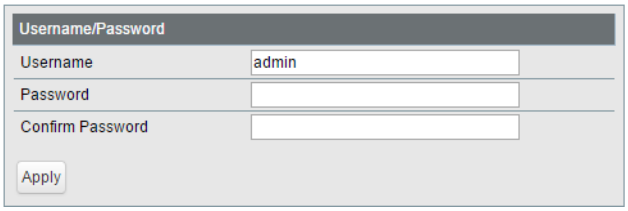



| | |
|---|---|
| **Name** | Enter the port name. You may enter up to 15 alphanumeric characters, hyphens, underscores, and spaces. |
| **Admin** | Check to enable the port. |
| **Mode** | Select the transmission rate and duplex. |
| **Flow Control** | Check to enable flow control. |
| **IEEE 802.3az** | Check to enable IEEE802.3az. |
| **APD** | Check to enable APD (auto power down). If enabled, power consumption of link down ports can be reduced. |
| **Jumbo Frame** | Check to enable jumbo frame settings. |
| **Speed/Duplex** | Displays the current transmission rate and duplex. |

# System Security

## Administration Account

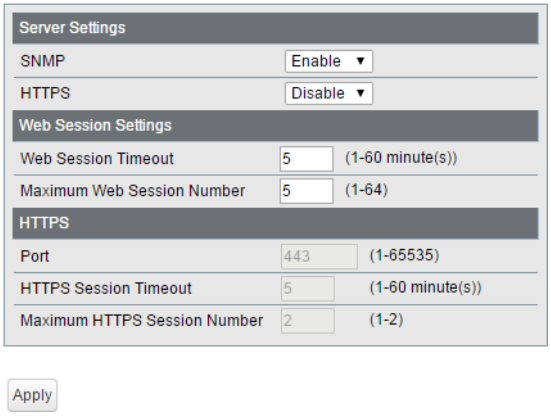
Configure the username and password.




| | |
|---|---|
| **Username** | Enter the new username. You may enter up to 8 alphanumeric characters, hyphens, and underscores. |
| **Password** | Enter the new password. You may enter up to 8 alphanumeric characters, hyphens, and underscores. |
| **Confirm** | Enter the new password again. |

## Access Management

Configure each administration interface.




| | |
|---|---|
| **SNMP** | Enable or disable SNMP administration interface. |
| **HTTPS** | Enable or disable HTTPS administration interface.<br>**Note:** To use this functionality, upload SSL certificate on the [Basic] - [System Security] - [Certificate] page. |
| **Web Session Timeout** | Enter the timeout period for accessing Settings using HTTP. |
| **Maximum Web Session Number** | Enter the number of users who can access Settings using HTTP at the same time. |
| **Port** | Specify the port number for HTTPS connections. |
| **HTTPS Session Timeout** | Enter the timeout period for accessing Settings using HTTPS. |
| **Maximum HTTPS Session Number** | Enter the number of users who can access Settings using HTTPS at the same time. |

# Certificate

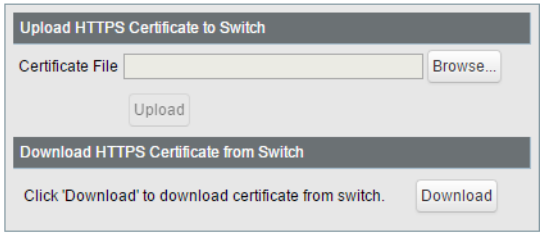
Upload or download the certificate. You have to prepare a certificate for HTTPS communication by yourself.

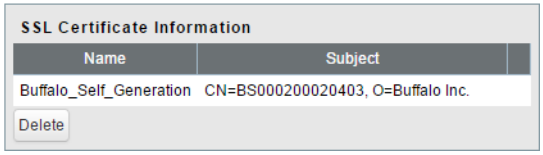
The compatible certificate types are:

| | |
|---|---|
| Certificate Type | X.509 |
| Private Key | RSA up to 2048-bit (no encryption only) |
| Hash Algorithm | SHA1, SHA256, SHA384, SHA512 |

The certificate must include the private key as the following:

```
-----BEGIN CERTIFICATE-----
…
…
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
…
…
-----END RSA PRIVATE KEY-----
```

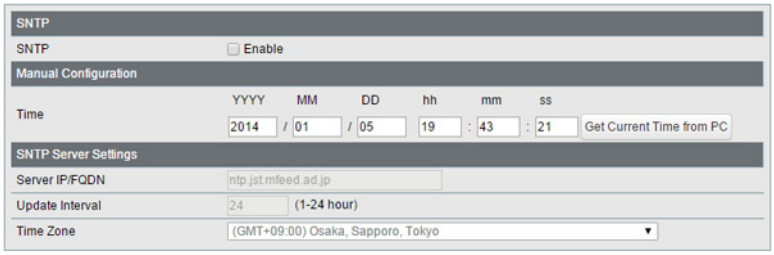



| | |
|---|---|
| **Upload HTTPS Certificate to Switch** | Upload HTTPS certificate. |
| **Download HTTPS Certificate from Switch** | Download HTTPS certificate. |
| **SSL Certificate Information** | Displays the uploaded certificate information. Click [Delete] to delete the uploaded certificate.<br>**Note:** If the certificate is deleted, a certificate will be automatically created next time the switch reboots. |

# Date & Time

Configure whether to manually set the date and time or automatically using a SNTP server.



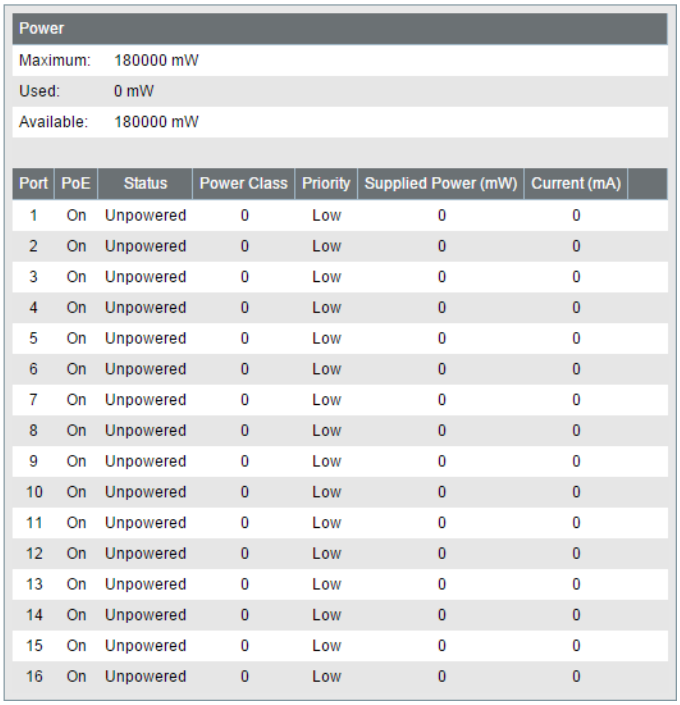

| | |
|---|---|
| **SNTP** | Enable to automatically obtain the time from SNTP server. |
| **Time** | Configure the time when SNTP is disabled. |
| **Server IP/FQDN** | Enter the SNTP server IP address or FQDN. To enter the FQDN, DNS settings must be configured. |
| **Update Interval** | Enter the interval which time is obtained from the SNTP server. |
| **Time Zone** | Configure the time zone. |

# PoE

This functionality is for PoE-compatible switches only.

## Status

Displays the PoE status.



Power

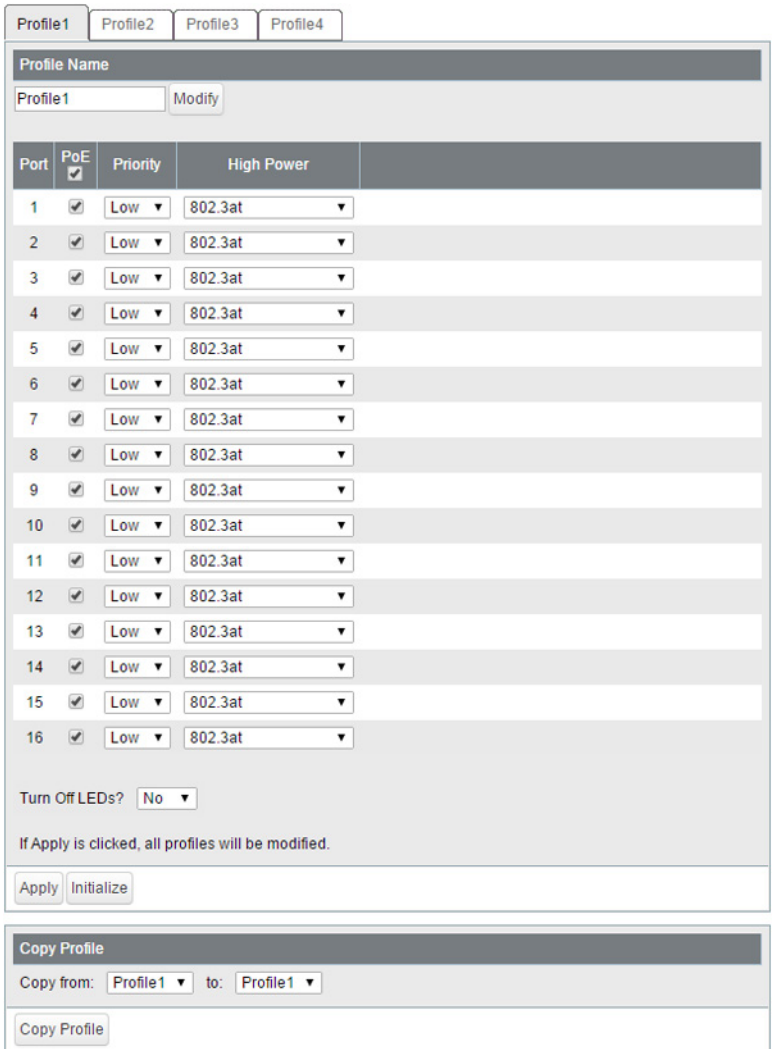
| | |
|---|---|
| Maximum: | 180000 mW |
| Used: | 0 mW |
| Available: | 180000 mW |

| Port | PoE | Status | Power Class | Priority | Supplied Power (mW) | Current (mA) |
|---|---|---|---|---|---|---|
| 1 | On | Unpowered | 0 | Low | 0 | 0 |
| 2 | On | Unpowered | 0 | Low | 0 | 0 |
| 3 | On | Unpowered | 0 | Low | 0 | 0 |
| 4 | On | Unpowered | 0 | Low | 0 | 0 |
| 5 | On | Unpowered | 0 | Low | 0 | 0 |
| 6 | On | Unpowered | 0 | Low | 0 | 0 |
| 7 | On | Unpowered | 0 | Low | 0 | 0 |
| 8 | On | Unpowered | 0 | Low | 0 | 0 |
| 9 | On | Unpowered | 0 | Low | 0 | 0 |
| 10 | On | Unpowered | 0 | Low | 0 | 0 |
| 11 | On | Unpowered | 0 | Low | 0 | 0 |
| 12 | On | Unpowered | 0 | Low | 0 | 0 |
| 13 | On | Unpowered | 0 | Low | 0 | 0 |
| 14 | On | Unpowered | 0 | Low | 0 | 0 |
| 15 | On | Unpowered | 0 | Low | 0 | 0 |
| 16 | On | Unpowered | 0 | Low | 0 | 0 |

| | |
|---|---|
| **Power** | Displays the maximum power, power being used, and available power. |
| **PoE** | Displays if PoE is enabled (on) or disabled (off). |
| **Status** | Displays the power feeding status. |
| **Power Class** | Displays the connected device's class. |
| **Priority** | Displays the priority of each port. |
| **Supplied Power** | Displays the supplied power of each port. |
| **Current** | Displays the supplied current of each port. |

# PoE Profiles

Configure PoE settings of each profile that is used in [Power Profile] page.




| | |
|---|---|
| **Profile Name** | To change the profile name, enter a new profile name and click [Modify]. |
| **PoE** | Enable or disable PoE functionality. |
| **Priority** | Configure the priority of PoE power feeding. When the supplied power exceeds maximum power, the switch will supply power to the ports in the order of priority. |
| **High Power** | Configure the high-powered power feeding function.<br><br>**Disable**<br>The switch will supply power up to 15.4 W to the 802.3af-compatible devices. High-powered power feeding is disabled.<br>**802.3af High Power**<br>This is the expansion of 802.3af standard. The switch will supply power up to 15.4 W to the class 0-3 devices and up to 30 W to the class 4 devices.<br>**802.3at**<br>The switch will supply power up to 30 W to the 802.3at-compatible devices. |
| **Turn Off LEDs?** | Select "Yes" to turn off all LEDs except the power LED. |
| **Initialize** | Click to initialize the selected profile. |

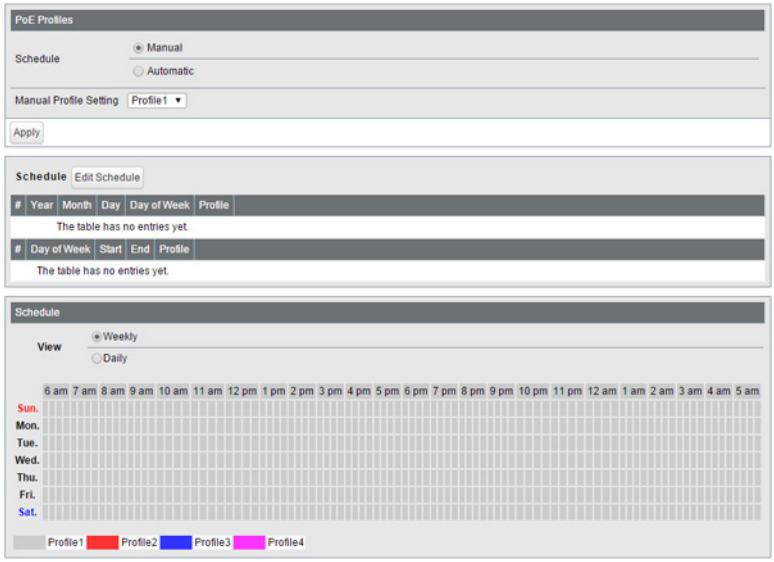
| | |
|---|---|
| **Copy Profile** | Select the source and destination profiles and click [Copy Profiles] to copy them. |

**Notes:**

- Click [Apply] to apply the current settings to all profiles.
- To use dynamic power feeding by LLDP, configure the status to [Tx and Rx] on the [Basic] - [LLDP] - [LLDP Port] page.
- If the supplied power exceeds the maximum power, the switch will supply power to the port in the order of the port number.

# Power Profile

Configure the power saving schedule.



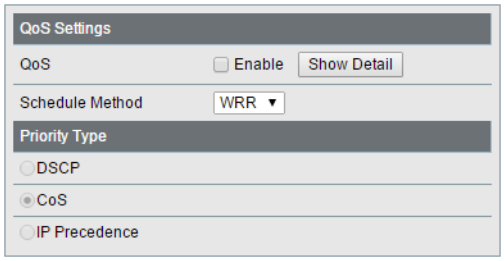

| | |
|---|---|
| **Schedule** | **Manual**<br>Switch the profile manually.<br>**Automatic**<br>Switch the profile automatically in accordance with the settings below.<br>**Note:** To set to [Automatic], SNTP must be enabled. If the time cannot be obtained from SNTP server, the configured profile will be applied in accordance with the switch's internal clock. |
| **Manual Profile Setting** | Select a profile to be used when the schedule is set to [Manual]. |
| **Profiles** | Displays the list of the profiles. Click [Edit Profiles] to edit the profile.<br>**Note:** To edit the profile, set the schedule to [Manual]. |
| **Schedule** | Displays the list of the schedule. Click [Edit Schedule] to edit the schedule. |
| **View** | **Weekly**<br>Displays the weekly schedule.<br>**Daily**<br>Displays the daily schedule. |
| **The screen appears when [Edit Schedule] is clicked** | |
| **Unscheduled Profile** | Select a profile to be used when no schedules are configured. |
| **Specify by** | Select a timetable type. |

| | |
|---|---|
| **Date** | Enter the date to add to the schedule if "Date" is selected as the timetable type. |
| **Day of Week** | Select the day of week to add to the schedule if "Day of week and time" is selected as the timetable type. |
| **Period** | Select the time frame while the schedule is enabled if "Day of week and time" is selected as the timetable type. |
| **Select Profile** | Select a method of specifying the profile. "Copy profile from a different day" cannot be selected when "Day of week and time" is selected as the timetable type. |
| **Profile** | Select a profile name if "Use profile below" is selected as the method of specifying the profile. Click [Check] to confirm each profile's settings. |
| **Use profile from** | Select a day of week to copy the profile if "Copy profile from a different day" is selected as the method of specifying the profile. |
| **Schedule** | Displays the list of configured schedule. |

# QoS

## QoS Settings

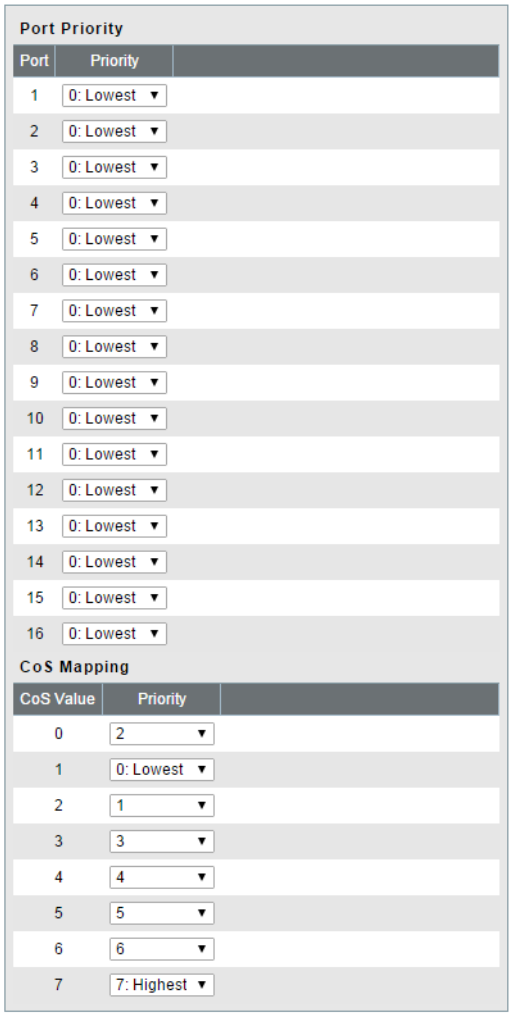
Configure the priority.




| | |
|---|---|
| **QoS** | Check to enable QoS. Click [Show Detail] to enable/disable QoS for each port. |
| **Schedule Method** | Configure the queue scheduling type.<br>**Strict**<br>Execute the queue scheduling based on strict priority. High-prioritized queues are always forwarded strictly; low-prioritized queue will never be forwarded if any data remains in the high prioritized queue.<br>**WRR**<br>Execute the queue scheduling based on WRR (Weighted Round Robin). This will forward queues in order of a round robin; even lower priority queues will be forwarded at a constant rate. The priority can be specified from 0 (lowest) to 7 (highest).<br><br>**Note:** Packets without VLAN tag will belong to the lowest priority queue. |
| **Priority Type** | Select a priority parameter from DSCP, CoS, and IP precedence. |

# QoS Mapping

Configure port-based priority for DSCP, CoS, and IP precedence.

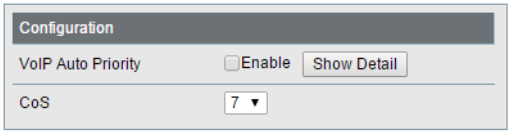



| | |
|---|---|
| **Port Priority** | Configure the priority of each port. |
| **DSCP Mapping** | Configure the DSCP priority value from 0-63. |
| **CoS Mapping** | Configure the CoS priority value from 0-7. |
| **IP Precedence Mapping** | Configure the IP precedence priority value from 0-7. |
| **Priority** | Configure the priority from 0-7. |

**Note:** DSCP mapping, CoS mapping, and IP precedence mapping is displayed when each type is selected.

## VoIP Auto Priority

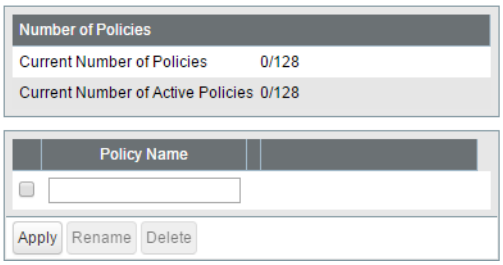
Configure the priority of SIP, H.323, SCCP.




| | |
|---|---|
| **VoIP Auto Priority** | Check to enable VoIP auto priority. Click [Show Detail] to enable or disable this functionality for each port. |
| **CoS** | Applied to the VoIP packets of SIP, H.323, SCCP only. If QoS is enabled, it is handled in accordance with CoS priority. |

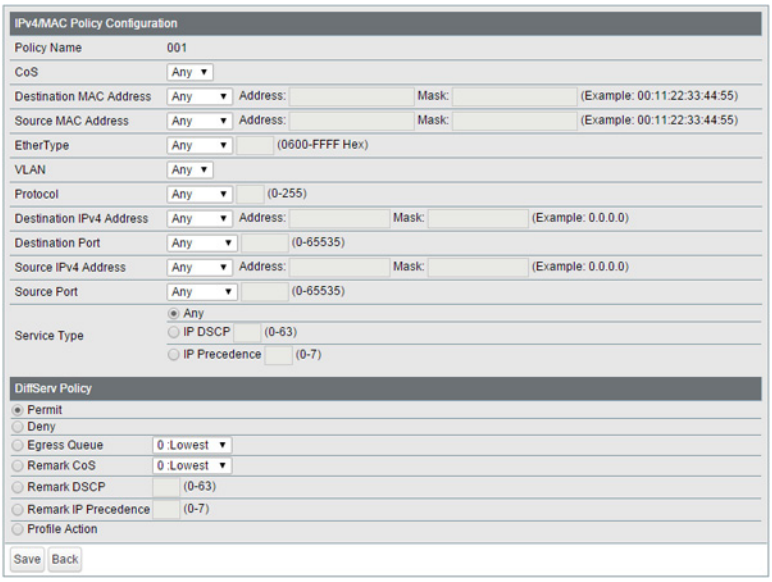
## IPv4/MAC Policy

Create DiffServ policies. IPv4 and MAC addresses can be specified here. The enabled policies will be applied when the packet or frame enters to the switch.




| | |
|---|---|
| **Current Number of Policies** | Displays the number of created policies. |
| **Current Number of Active Policies** | Displays the number of active policies. |
| **Policy Name** | Enter the policy name into the blank field and click [Apply] to create a new policy. Click [Show Detail] to configure the policy in detail.<br>Check the created policy name, enter the new name and click [Rename] to rename the policy. |

The following screen appears when [Show Detail] is clicked.




| | |
|---|---|
| **Policy Name** | Displays the selected policy name. |
| **CoS** | Adds the CoS value to the policy condition. |
| **Destination MAC Address** | Adds the frame's destination MAC address to the policy condition. For instructions on how to enter the address, refer to "About Address and Mask" section below. |
| **Source MAC Address** | Adds the frame's source MAC address to the policy condition. For instructions on how to enter the address, refer to "About Address and Mask" section below. |
| **EtherType** | Adds the frame's ether type to the policy condition. |
| **VLAN** | Adds the frame's VLAN ID to the policy condition. |
| **Protocol** | Adds the packet's protocol to the policy condition. |
| **Destination IPv4 Address** | Adds the packet's destination IPv4 address to the policy condition. For instructions on how to enter the address, refer to "About Address and Mask" section below. |
| **Destination Port** | Adds the packet's destination port to the policy condition. |
| **Source IPv4 Address** | Adds the packet's source IPv4 address to the policy condition. For instructions on how to enter the address, refer to "About Address and Mask" section below. |
| **Source Port** | Adds the packet's source port to the policy condition. |
| **Service Type** | Adds the packet's service type to the policy condition. Only 1 value can be specified when "IP DSCP" or "IP Precedence" is selected. |

| | |
|---|---|
| **DiffServ Policy** | Select the action for when the frames satisfy the condition.<br><br>**Permit**<br>Permits forwarding the frames and packets.<br>**Deny**<br>Discards the frames and packets.<br>**Egress Queue**<br>Changes the processing priority of the frames and packets.<br>**Remark CoS**<br>Rewrites CoS value of the frames and packets.<br>**Remark DSCP**<br>Rewrites DSCP value of the frames and packets.<br>**Remark IP Precedence**<br>Rewrites IP precedence value of the frames and packets.<br>**Profile Action**<br>Processes the frames and packets depending on the committed rate. If the rate of the frames and packets is less than the committed rate, the switch will process the frames and packets in accordance with the in-profile action. Otherwise, the switch will process the frames and packets in accordance with the out-of-profile action.<br>**Committed Rate**<br>Specify the rate to determine the process method.<br>**Committed Burst**<br>Specify the burst size that the switch processes in accordance with the in-profile action when the rate of frames and packets exceeds the committed rate instantaneously. When the burst size exceeds the committed burst, the switch will process in accordance with the out-of-profile action.<br>**In-Profile Action**<br>Specify the action when the rate of frames and packets is less than the committed rate.<br>**Out-of-profile Action**<br>Specify the action when the rate of frames and packets exceeds the committed rate. |

**About Address and Mask**

This product adopts "wildcard masks".

To configure the source MAC address or destination MAC address, refer to the following example.

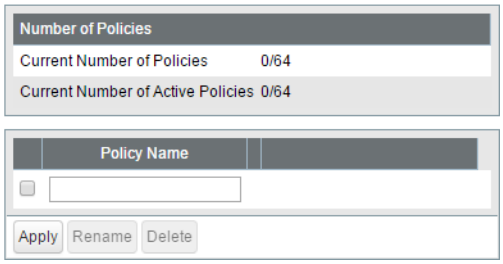
- To specify the range of "00:11:22:33:ab:cd:00" to "00:11:22:33:ab:cd:ff"
  Enter "00:11:22:33:ab:cd:00" in the address field and also enter "00:00:00:00:00:ff" in the mask field.
- To specify only "00:11:22:33:ab:cd:ef"
  Enter "00:11:22:33:ab:cd:ef" in the address field and also enter "00:00:00:00:00:00" in the mask field.

To configure the source IPv4 address or destination IPv4 address, refer to the following example.

- To specify the range of "192.168.1.0" to "192.168.1.254"
  Enter "192.168.1.0" in the address field and also enter "0.0.0.255" in the mask field.
- To specify only "192.168.1.1"
  Enter "192.168.1.1" in the address field and also enter "0.0.0.0" in the mask field.

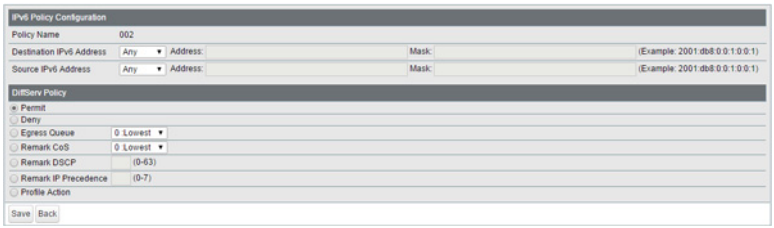
# IPv6 Policy

Create DiffServ policies. IPv6 addresses can be specified here. The enabled policies will be applied when the packet or frame enters the switch.




| | |
|---|---|
| **Current Number of Policies** | Displays the number of created policies. |
| **Current Number of Active Policies** | Displays the number of active policies. |
| **Policy Name** | Enter the policy name into the blank field and click [Apply] to create a new policy. Click [Show Detail] to configure the policy in detail.<br>Check the created policy name, enter the new name and click [Rename] to rename the policy. |

The following screen appears when [Show Detail] is clicked.




| | |
|---|---|
| **Policy Name** | Displays the selected policy name. |
| **Destination IPv6 Address** | Adds the packet's destination IPv6 address to the policy condition. For instructions on how to enter the address, refer to "About Address and Mask" section below. |
| **Source IPv6 Address** | Adds the packet's source IPv6 address to the policy condition. For instructions on how to enter the address, refer to "About Address and Mask" section below. |

| | |
|---|---|
| **DiffServ Policy** | Select the action for when the frames satisfy the condition.<br><br>**Permit**<br>Permits forwarding the frames and packets.<br>**Deny**<br>Discards the frames and packets.<br>**Egress Queue**<br>Changes the processing priority of the frames and packets.<br>**Remark CoS**<br>Rewrites CoS value of the frames and packets.<br>**Remark DSCP**<br>Rewrites DSCP value of the frames and packets.<br>**Remark IP Precedence**<br>Rewrites IP precedence value of the frames and packets.<br>**Profile Action**<br>Processes the frames and packets depending on the committed rate. If the rate of the frames and packets is less than the committed rate, the switch will process the frames and packets in accordance with the in-profile action. Otherwise, the switch will process the frames and packets in accordance with the out-of-profile action.<br>**Committed Rate**<br>Specify the rate to determine the process method.<br>**Committed Burst**<br>Specify the burst size that the switch processes in accordance with the in-profile action when the rate of frames and packets exceeds the committed rate instantaneously. When the burst size exceeds the committed burst, the switch will process in accordance with the out-of-profile action.<br>**In-Profile Action**<br>Specify the action when the rate of frames and packets is less than the committed rate.<br>**Out-of-profile Action**<br>Specify the action when the rate of frames and packets exceeds the committed rate. |

**About Address and Mask**

This product adopts "wildcard masks". To configure the source IPv6 address or destination IPv6 address, refer to the following example.

- To specify the range of "2001:db8::" to "2001:db8::ffff"
  Enter "2001:db8::" in the address field and also enter "::ffff" in the mask field.
- To specify only "2001:db8::"
  Enter "2001:db8::" in the address field and also enter "::" in the mask field.

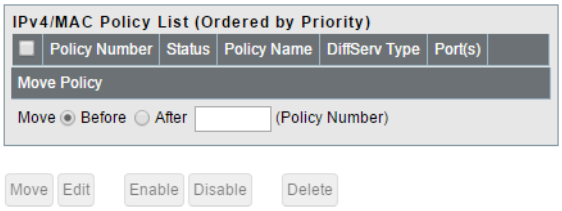
# Port Settings

Configure the ports to apply DiffServ policies. The ports specified by ACL rules cannot be specified.


| | |
|---|---|
| **Current Number of Active Policies** | Displays the number of active IPv4 and MAC address-based policies. |
| **Current Number of Active IPv6 Policies** | Displays the number of active IPv6 address-based policies. |
| **Port Settings** | Select a policy name and ports, then click [Apply]. |
| **IPv4/MAC (IPv6) ACL Rule List** | Displays the selected policy's conditions. |

# IPv4/MAC Priority

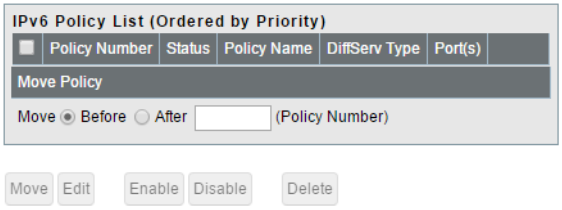
Configure IPv4 and MAC address-based policies priority.




| | |
|---|---|
| **IPv4/MAC Policy List** | Displays the list of IPv4 and MAC address-based policy. Policies are listed in order of the priority. |
| **Move Policy** | Select a policy and enter the policy number that the selected policy moves to before (or after). Select [Before] or [After] and click [Move] to change the priority of the policy. |

# IPv6 Priority

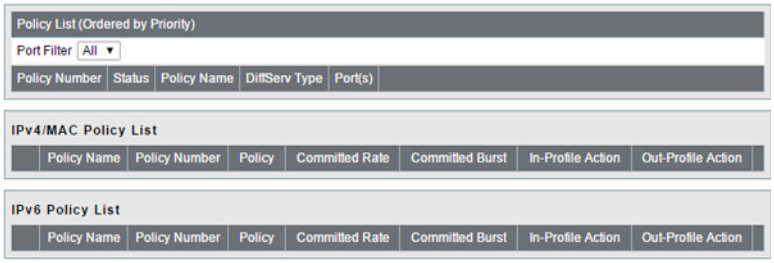
Configure IPv6 address-based policies priority.



| | |
|---|---|
| **IPv6 Policy List** | Displays the list of IPv6 address-based policies. Policies are listed in order of the priority. |
| **Move Policy** | Select a policy and enter the policy number that the selected policy moves to before (or after). Select [Before] or [After] and click [Move] to change the priority of the policy. |

## Status

Displays the DiffServ status.

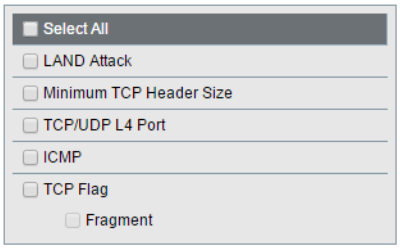



| | |
|---|---|
| **Policy List** | Displays the list of policies. Policies are listed in order of the priority. Select a port from [Port Filter] to display only the policies that the selected port belongs to. |
| **IPv4/MAC Policy List** | Displays the list of IPv4 and MAC address-based policies. Click [+] next to a policy to show its conditions. Conditions are listed in order of the priority. |
| **IPv6 Policy List** | Displays the list of IPv6 address-based policies. Click [+] next to a policy to show its conditions. Conditions are listed in order of the priority. |

# Security

## Auto DoS Attack Prevention

Configure packets to be dropped.





| | |
|---|---|
| **LAND Attack** | If enabled, the packets whose source IP address and destination IP address are the same will be dropped. |
| **Minimum TCP Header Size** | If enabled, the packets whose TCP header size is less than 20 bytes will be dropped. |
| **TCP/UDP L4 Port** | If enabled, the packets whose source port number and destination port number are the same will be dropped. Disable when using SNTP and RADIUS. |
| **ICMP** | If enabled, the ICMP packets whose ICMP header+data is more than 512 bytes. |

| | |
|---|---|
| **TCP Flag** | If enabled, the illegal TCP flagged packets will be dropped. This will not be applied to the fragment packets. |
| **Fragment** | If checked, the configuration of [TCP Flag] will be applied also to the fragment packets. |

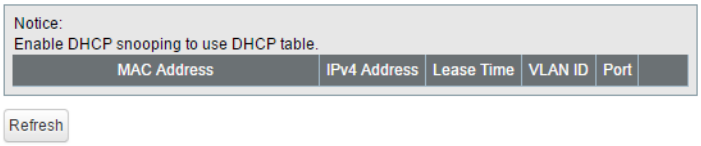
## DHCP Snooping

Configure DHCP snooping. DHCP snooping is a function to prevent leasing IP addresses when an illegal DHCP server is connected.


| | |
|---|---|
| **DHCP Snooping** | Check to enable DHCP snooping. |
| **DHCP Option 82** | Add option 82 to the DHCP packets received from DHCP clients. To obtain an IP address from the DHCP server using this functionality, the DHCP server should be compatible with option 82. |
| **Rate Limit (pps)** | Limits the rate of the DHCP packets received from DHCP clients to all ports per a second. Exceeded DHCP packets from DHCP clients will be discarded. |
| **Status** | **Trusted**<br>The DHCP server connected to the trusted port can lease IP addresses.<br>**Untrusted**<br>The DHCP packet from the DHCP server connected to the untrusted port will be blocked. |

## DHCP Table

Displays the DHCP clients that obtained an IPv4 address from the DHCP server via the switch. Up to 256 clients can be listed.



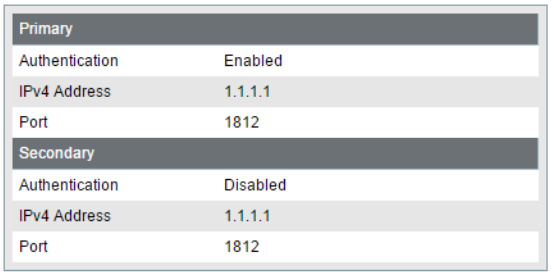

**Note:** DHCP table can be used only when DHCP snooping is enabled.

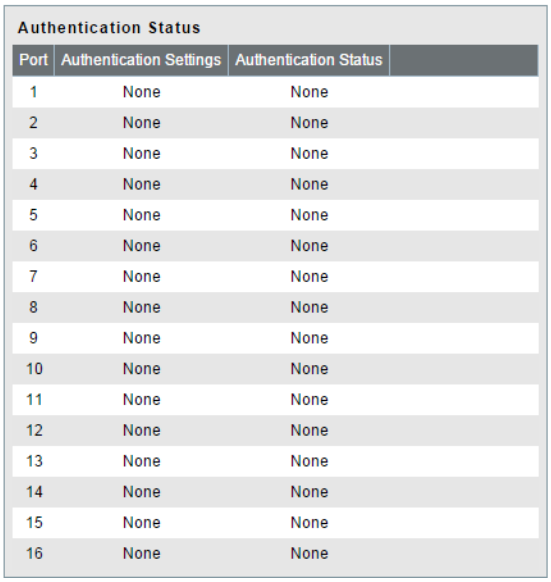
| | |
|---|---|
| **MAC Address** | Displays the DHCP client's MAC address. |
| **IPv4 Address** | Displays the IPv4 address that DHCP client obtained. |
| **Lease Time** | Displays the lease period of the IPv4 address. |
| **VLAN ID** | Displays the VLAN ID that the DHCP client belongs to. |
| **Port** | Displays the port number that the DHCP client is connected to. |

# Authentication

## Status

Displays the authentication server and port authentication status.

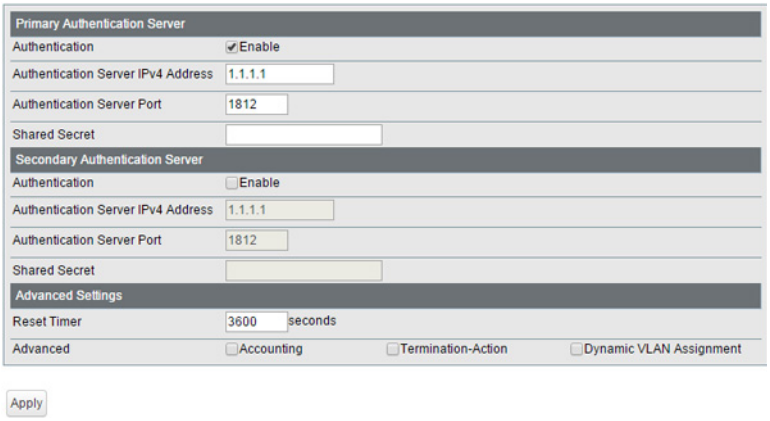


| | |
|---|---|
| **Primary/Secondary** | Displays if each server is enabled or disabled, and the server's IP address and port number. |
| **Authentication Status** | Displays the authentication status of each port. |

# RADIUS

Configure RADIUS server.




| | |
|---|---|
| **Authentication** | Check to enable authentication server. |
| **Authentication Server IP** | Enter the authentication server's IP address. |
| **Authentication Server Port** | Enter the authentication server's port number. (1-65535) |
| **Shared Secret** | Enter the shared secret of the authentication server. You may enter up to 20 alphanumeric characters, hyphens, and underscores. |
| **Reset Timer** | Enter the time that passes before re-authentication. |
| **Advanced** | **Accounting**<br>If enabled, notify the connection status to the RADIUS server.<br>**Termination-Action**<br>If you follow the termination-action notified by the server, enable this.<br>**Dynamic VLAN Assignment**<br>If enabled, the VLAN to which the port belongs to can change dynamically based on the authentication information received from the RADIUS server. You need to add attributes in the RADIUS server settings in advance to use dynamic VLAN . For more information, refer to "RADIUS Server Settings to Use Dynamic VLAN" section below.<br>**Note:** This product's dynamic VLAN can only be used with 802.1X port authentication. |

**Notes:**

- Use only the primary authentication server under normal conditions. Use the secondary server when a backup server is used.
- Session-timeout is fixed to 5 seconds and the number of confirmation times is fixed to 3 times.
- To delete configured shared secret, initialize the switch. You do not have to initialize the switch when you change the shared secret.

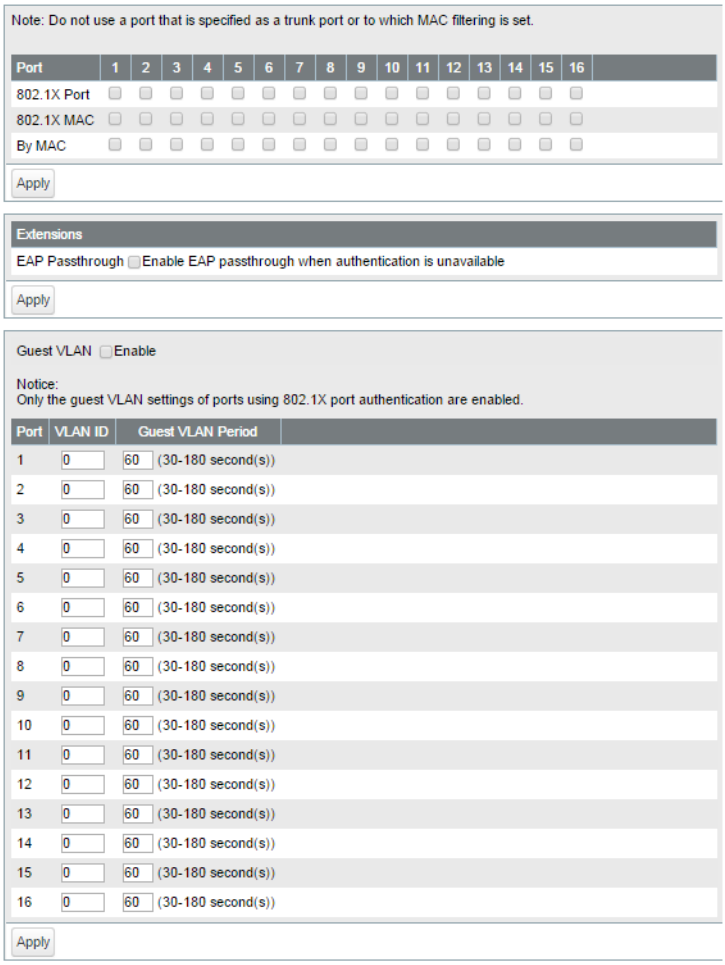
### RADIUS Server Settings to Use Dynamic VLAN

When dynamic VLAN is enabled, add the following attributes to the RADIUS server.

| Attribute | Value |
|---|---|
| Tunnel-Type | 13 (VLAN) |
| Tunnel-Medium-Type | 6 (IEEE-802) |
| Tunnel-Private-Group-ID | VLAN ID that the authenticated user will belong to |

## Port Authentication

Configure authentication settings for each port. Prepare an authentication server (RADIUS server) separately.




| | |
|---|---|
| **802.1X Port** | Authenticate 802.1X based on the port. All devices connected to the port can communicate after the authentication. |
| **802.1X MAC** | Authenticate 802.1X based on the MAC address. Only the authenticated devices can communicate. Up to 12 MAC addresses can be authenticated per port. |
| **By MAC** | Enables MAC authentication. Up to 12 MAC addresses can be authenticated per port. |
| **EAP Passthrough** | If the authentication of all ports is disabled or received EAP frames should be transmitted, enable this. |

| | |
|---|---|
| **Guest VLAN** | Click "Enable" to enable guest VLAN functionality. Enter each port's guest VLAN period and the VLAN ID to be assigned to users who could not be authenticated by the time the guest VLAN period expires.<br>**Notes:**<br>• Only the guest VLAN settings of ports using 802.1X port authentication are enabled.<br>• If the port's guest VLAN ID is "0", guest VLAN of that port is disabled. |

The MAC authentication port authenticates using the source MAC address when it receives IP packets. Use the following username and password to authenticate to the RADIUS server.

Username: source MAC address

Password: source MAC address

Example: If the source MAC address of the IP packet is 00:11:22:33:AA:BB, the username and password is the following.

Username: 00112233aabb

Password: 00112233aabb

Enter letters in lower case.

RADIUS requests will be sent to the RADIUS server with this information. On the RADIUS server side, user registration is needed in advance.

**Note:** MAC authentication will not authenticate the same MAC address twice in a row. If MAC authentication fails, disconnect and reconnect the Ethernet cable or authenticate others, then try again.

This product's authentication is compatible with the following encryption method.

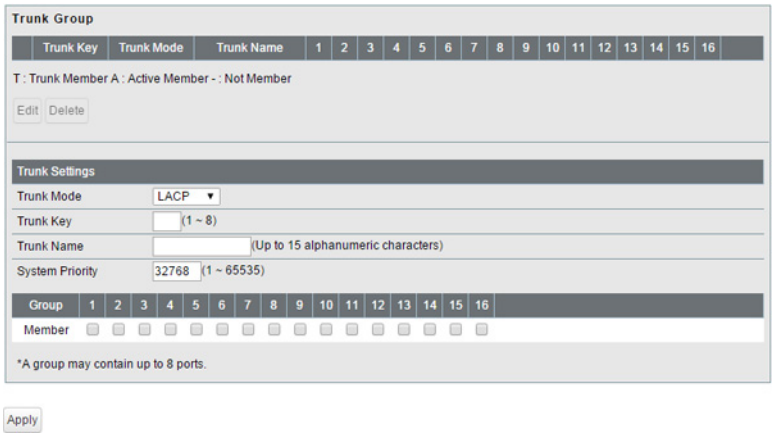
| | | |
|---|---|---|
| 802.1X Port | 802.1X (EAP-MD5, TLS, PEAP) | Cannot use with other methods at the same time |
| 802.1X MAC | 802.1X (EAP-MD5, TLS, PEAP) | Can use with other methods at the same time |
| By MAC | PAP | Can use with other methods at the same time |

**Notes:**

- If 802.1X MAC is enabled, EAPOL-Start should be issued by the supplicant.
- You cannot use MAC filtering for the port that enables 802.1X port authentication.
- You cannot select a authentication type for the port that enables MAC filtering or trunk.

# Port Trunking

Configure port trunking settings.



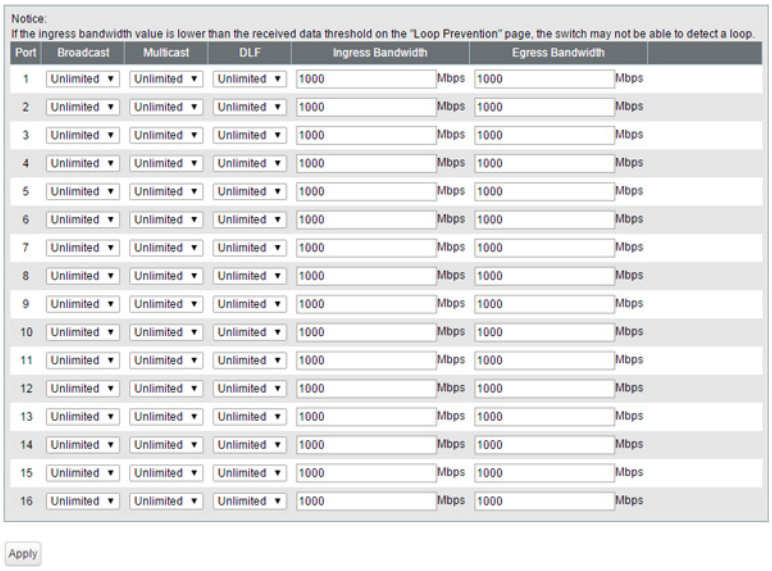
| | |
|---|---|
| **Trunk Mode** | Select a trunk mode. |
| **Trunk Key** | Enter the key to identify the trunk group. |
| **Trunk Name** | Enter the trunk name. |
| **System Priority** | Enter the priority that is used to decide whose settings are used when the trunk is constructed. The settings of the device whose system priority is the minimum will be used. If the system priorities are the same, the settings of the device whose MAC address is smaller will be used. |
| **Member** | Select ports to join the trunk member. |

**Notes:**

- 8 groups can be created in total between LACP and manual creation. Up to 8 port can be set to a group.
- The ports in the same trunk group should belong to the same VLAN.
- If you construct the trunk group using LACP, the opposing switch can set the LACP to both active and passive.

# Traffic Control

Configure storm settings. If each packet exceeds the threshold configured on this page, exceeded packets will be dropped.

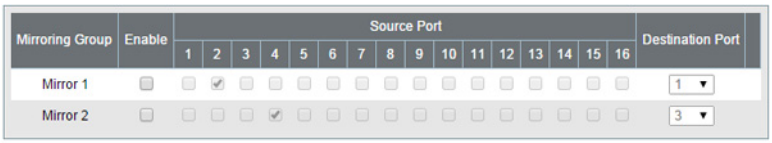



| | |
|---|---|
| **Broadcast** | Select a rate to allow passing broadcasts. |
| **Multicast** | Select a rate to allow passing multicasts. |
| **DLF** | Select a rate to allow passing DLF (destination lookup failure) unicasts. |
| **Ingress Bandwidth** | Limits the bandwidth of ingress (input to the switch) speed as the configured value. **Note:** If the ingress bandwidth value is lower than the received data threshold on the "Loop Prevention" page, the switch may not be able to detect a loop. |
| **Egress Bandwidth** | Limits the bandwidth of egress (output from the switch) speed as the configured value. |

**Note:** If the rate is configured based on broadcasts, multicasts, or DLF unicasts that sometimes cannot pass due to the difference of traffic, configure the minimum rate of frames for normal use.

# Mirroring

Configure to monitor the traffic (copy the contents of communication from source to destination).

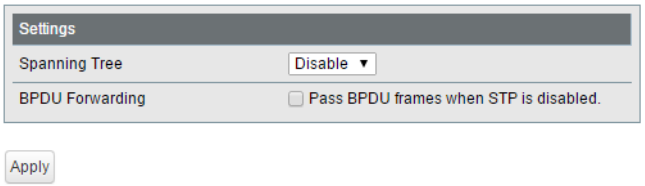



| | |
|---|---|
| **Enable** | Check to enable mirroring. |
| **Source Port** | Select ports to be monitored. |
| **Destination Port** | Select ports to monitor the traffic. |

# Spanning Tree Protocol

## STP Settings

Configure STP settings.




| | |
|---|---|
| **STP Version** | Select a STP version from STP, RSTP or MSTP.<br>**Note:** MSTP cannot be enabled when LDF is enabled. To disable LDF, navigate to [Advanced] - [Loop Prevention]. |
| **BPDU Forwarding**<br>(Only when STP is disabled) | Enable to forward BPDU frames when STP is disabled. |
| **Hello Time** | Enter the interval of BPDU transmission when this switch is the root bridge. |
| **Max Age** | Enter the maximum time that passes before trying to reconfigure when this switch doesn't receive BPDU. |
| **Forward Delay** | Enter the time spent in the status changes (listening-learning-forwarding) of the switch before forwarding packets. |
| **Max Hop Count**<br>(MSTP only) | Specify the maximum hop count of BPDU. |
| **Bridge Priority** | Enter the priority of this switch for selecting the root bridge. |
| **MST Configuration Name**<br>(MSTP only) | Enter an MST region name. The same name should be configured for all devices that belong to the same region. |
| **MST Revision Level**<br>(MSTP only) | Configure MST revision. The same value should be configured for all devices that belong to the same region. |

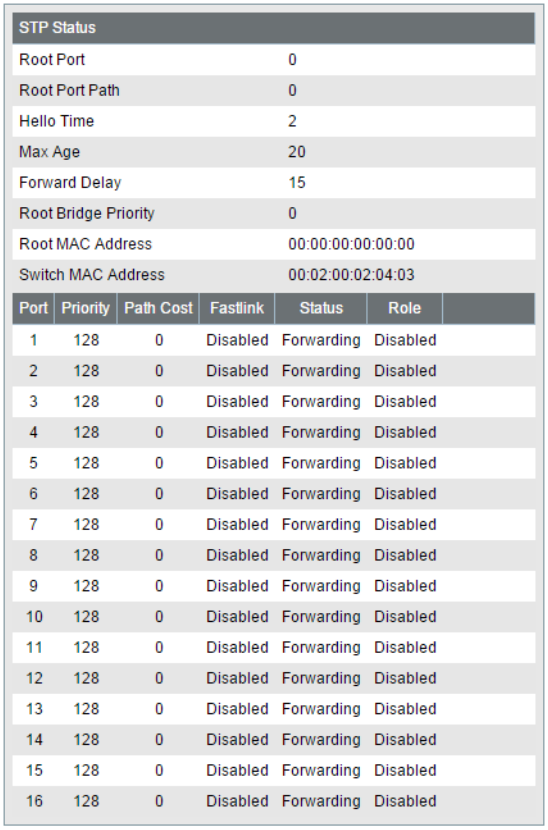
| | |
|---|---|
| **Configuration Digest** (MSTP only) | Displays the MSTI status as MD5 digest message. |
| **MSTI Settings** (MSTP only) | To add MSTI ID, enter the MSTI ID and bridge priority, select VLAN ID(s) to belong to, then click [Add]. |
| **MSTP Status** (MSTP only) | Displays the MSTI configuration status. Select an MSTI ID and click [Edit] to add or delete the VLAN ID(s) and change the bridge priority value. |

**Note:**

- To use spanning tree, all devices in the segment must be compatible with spanning tree.
- To configure each items, the following relational expression must be true.
  2 x (Forward Delay - 1) ≥ Max Age
  Max Age ≥ 2 x (Hello Time + 1)

# Status

Displays the STP status of each port.



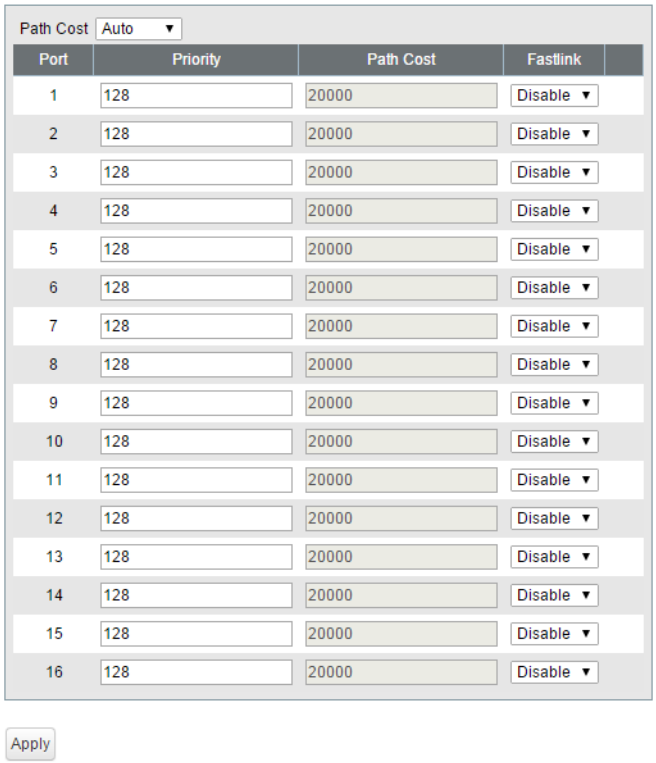
| STP Status | | | | | |
|---|---|---|---|---|---|
| Root Port | 0 | | | | |
| Root Port Path | 0 | | | | |
| Hello Time | 2 | | | | |
| Max Age | 20 | | | | |
| Forward Delay | 15 | | | | |
| Root Bridge Priority | 0 | | | | |
| Root MAC Address | 00:00:00:00:00:00 | | | | |
| Switch MAC Address | 00:02:00:02:04:03 | | | | |
| **Port** | **Priority** | **Path Cost** | **Fastlink** | **Status** | **Role** |
| 1 | 128 | 0 | Disabled | Forwarding | Disabled |
| 2 | 128 | 0 | Disabled | Forwarding | Disabled |
| 3 | 128 | 0 | Disabled | Forwarding | Disabled |
| 4 | 128 | 0 | Disabled | Forwarding | Disabled |
| 5 | 128 | 0 | Disabled | Forwarding | Disabled |
| 6 | 128 | 0 | Disabled | Forwarding | Disabled |
| 7 | 128 | 0 | Disabled | Forwarding | Disabled |
| 8 | 128 | 0 | Disabled | Forwarding | Disabled |
| 9 | 128 | 0 | Disabled | Forwarding | Disabled |
| 10 | 128 | 0 | Disabled | Forwarding | Disabled |
| 11 | 128 | 0 | Disabled | Forwarding | Disabled |
| 12 | 128 | 0 | Disabled | Forwarding | Disabled |
| 13 | 128 | 0 | Disabled | Forwarding | Disabled |
| 14 | 128 | 0 | Disabled | Forwarding | Disabled |
| 15 | 128 | 0 | Disabled | Forwarding | Disabled |
| 16 | 128 | 0 | Disabled | Forwarding | Disabled |

| | |
|---|---|
| **MSTI/CIST** (MSTP only) | When MSTP is enabled, this page shows the status of each MSTI ID or CIST. Select an MSTI ID or CIST to display the status. |
| **Root Port** | Displays the root port. If this switch is the root bridge, "0" is displayed. |
| **Root Port Path** | Displays the path cost to the root bridge. If this switch is the root bridge, "0" is displayed. |
| **Regional Root Port Path** (MSTP only) | Displays the path cost to the CIST root bridge in the MST region. |
| **Hello Time** | Displays the interval of BPDU transmission when this switch is the root bridge. |

| | |
|---|---|
| **Max Age** | Displays the maximum time that passes before trying to reconfigure when this switch doesn't receive BPDU. |
| **Forward Delay** | Displays the time spent in the status changes (listening-learning-forwarding) of the switch before forwarding packets. |
| **Max Hop Count** (STP/RSTP only) | Displays the maximum hop count of BPDU. |
| **Root Bridge Priority** (STP/RSTP only) | Select a root bridge priority of this switch. |
| **Root MAC Address** (MSTP only) | Displays the root bridge's MAC address. |
| **CIST Root Bridge Priority** (MSTP only) | Displays the CIST root bridge's bridge priority. |
| **CIST Root MAC Address** (MSTP only) | Displays the CIST root bridge's MAC address. |
| **Regional Root Bridge Priority** (MSTP only) | Displays the bridge priority of the root bridge in the MST region. |
| **Regional Root MAC Address** (MSTP only) | Displays the MAC address of the root bridge in the MST region. |
| **Switch MAC Address** | Displays this switch's MAC address. |
| **Priority** | Displays the port priority. |
| **Path Cost** | Displays the path cost. |
| **Fastlink** | Displays if fastlink is enabled or disabled. |
| **Status** | Displays the port status. |
| **Role** | Displays the port role. |

# Ports

Configure STP settings for each port. Path cost can be switched between "Auto" and "Manual".



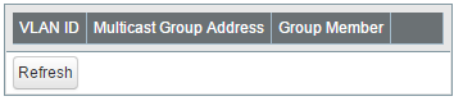

| | |
|---|---|
| **Priority** | Enter the port priority in hexadecimal format. This is used to decide the path to the root bridge. |
| **Path Cost** | If path cost is set to "Manual", you can edit the value. This is used to decide the path to the root bridge. |
| **Fastlink** | If enabled, the port will be in forwarding status immediately. It is recommended to enable fastlink to the port a PC is connected to. Disable it if the switch using STP is connected to the port.<br>**Note:** Fastlink is disabled when the port trunking is configured. |

# IGMP

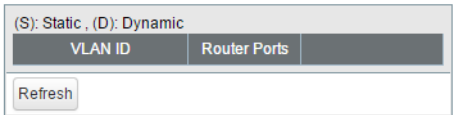
## Status

Displays the IGMP status.

**IGMP Status**



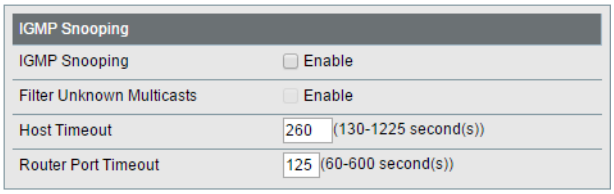

**Router Port Status**




| | |
|---|---|
| **IGMP Status** | Displays the multicast address table. |
| **Router Port Status** | Displays the port connected to the multicast router (server). |

## IGMP Settings

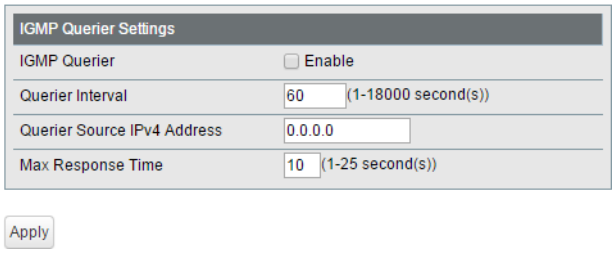
Configure IGMP snooping. This product is compatible with IGMP snooping v1, v2, and v3.




| | |
|---|---|
| **IGMP Snooping** | Check to enable IGMP snooping.<br>If enabled, you can prevent the flooding of multicast packets except for the port connected to the host which joins the multicast group.<br>**Note:** The addresses in the range of 224.0.0.1-224.0.0.255 will be excepted from IGMP snooping. |
| **Filter Unknown Multicasts** | If checked, the packets of the multicast that is not learned will be discarded except for 224.0.0.1-224.0.0.255. |
| **Host Timeout** | Enter the host timeout period for receiving multicast. |
| **Router Port Timeout** | Enter the timeout length for the multicast router (server). |

# IGMP Querier

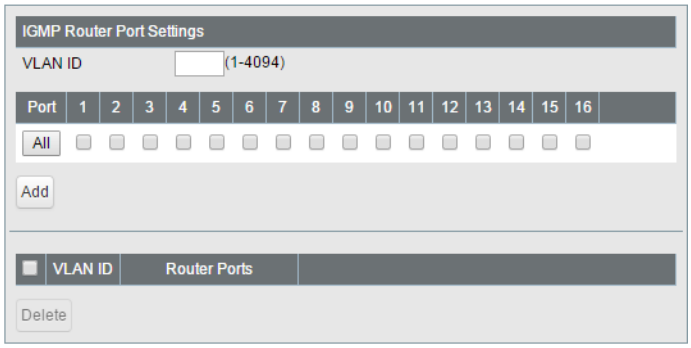
If IGMP querier is enabled, IGMP snooping can be enabled even if no multicast router is connected.




| | |
|---|---|
| **IGMP Querier** | Check to enable IGMP querier. IGMP queries will be forwarded from each VLAN. |
| **Querier Interval** | Configure the transmit interval for the querier that confirms the existence of multicast group's member. |
| **Querier Source IPv4 Address** | Enter the source IPv4 address of the querier. |
| **Max Response Time** | Configure the time between transmitting the querier and response from the member. If the member responds to the querier by this time, the querier determines that the member is connected. |

# IGMP Router Port

Specify the port connected to the multicast router (server) for each VLAN.



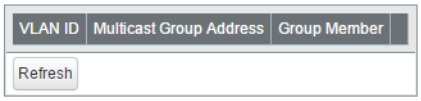

| | |
|---|---|
| **IGMP Router Port Settings** | Enter the VLAN ID and specify the port connected to the multicast router (server), then click [Add]. |

# MLD

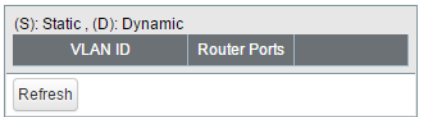
## Status

Displays the MLD status.

**MLD Status**



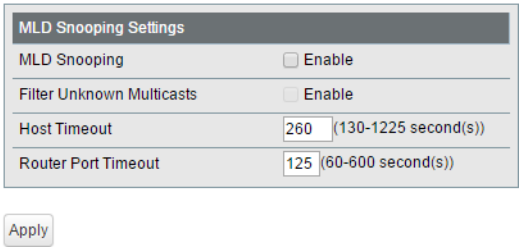

**Router Port Status**




| | |
|---|---|
| **MLD Status** | Displays the multicast address table. |
| **Router Port Status** | Displays the port connected to the multicast router (server). |

## MLD Settings

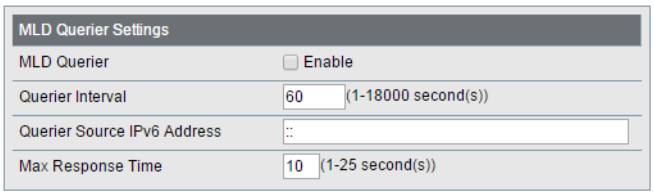
Configure MLD snooping.




| | |
|---|---|
| **MLD Snooping** | Check to enable MLD snooping.<br>If enabled, you can prevent the flooding of multicast packets except for the port connected to the host which joins the multicast group.<br>**Note:** FF02::-FF02::FF and FF0X:: will be excepted from MLD snooping. |
| **Filter Unknown Multicasts** | If checked, the packets of the multicast that is not learned will be discarded except for FF02::-FF02::FF and FF0X::. |
| **Host Timeout** | Enter the host timeout period for receiving multicast. |
| **Router Port Timeout** | Enter the timeout length for the multicast router (server). |

# MLD Querier

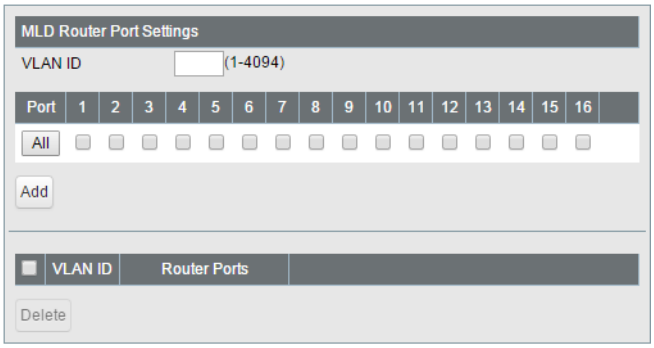
If MLD querier is enabled, MLD snooping can be enabled even if no multicast router is connected.




| | |
|---|---|
| **MLD Querier** | Check to enable MLD querier. MLD queries will be forwarded from each VLAN. |
| **Querier Interval** | Configure the transmit interval for the querier that confirms the existence of multicast group's member. |
| **Querier Source IPv6 Address** | Enter the source IPv6 address of the querier. |
| **Max Response Time** | Configure the time between transmitting the querier and response from the member. If the member responds to the querier by this time, the querier determines that the member is connected. |

# MLD Router Port

Specify the port connected to the multicast router (server) for each VLAN.

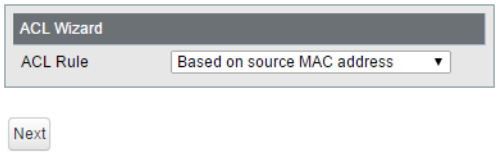



| | |
|---|---|
| **MLD Router Port Settings** | Enter the VLAN ID and specify the port connected to the multicast router (server), then click [Add]. |

# ACL

## ACL Wizard

Configure ACLs with the wizard. Follow the directions on the screen.



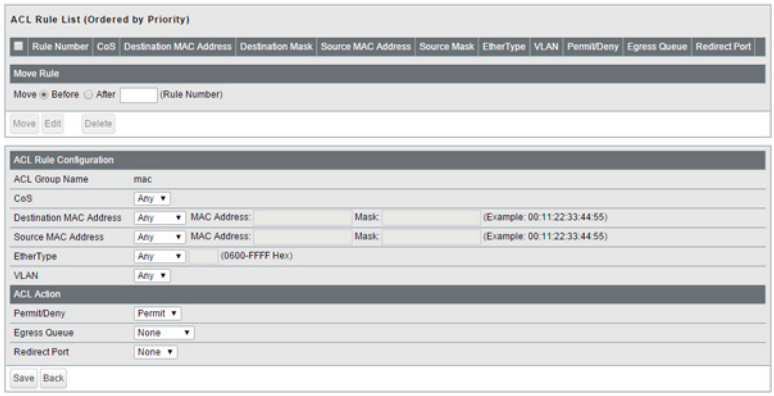

| | |
|---|---|
| **Based on source MAC address** | Configure to permit or deny the specified source MAC address. |
| **Based on destination MAC address** | Configure to permit or deny the specified destination MAC address. |
| **Based on source IPv4 address** | Configure to permit or deny the specified source IPv4 address. |
| **Based on destination IPv4 address** | Configure to permit or deny the specified destination IPv4 address. |
| **Based on source IPv6 address** | Configure to permit or deny the specified source IPv6 address. |
| **Based on destination IPv6 address** | Configure to permit or deny the specified destination IPv6 address. |

## MAC ACL

Create MAC address-based ACLs.


| | |
|---|---|
| **Current Number of Groups** | Displays the number of ACL groups. |
| **Current Number of Active Rules** | Displays the number of active rules for ACLs. |
| **ACL Group Name** | Displays the ACL group name. To create new ACLs, enter the group name and click [Apply]. Click [Show Detail] to add rules to the ACL group. To change the group name, select a group, enter the new name and click [Rename]. |
| **Number of Rules** | Displays the number of rules of each ACL group. |

The following screen is displayed when [Show Detail] is clicked. Up to 10 rules can be configured per group.




| | |
|---|---|
| **ACL Rule List** | Displays the list of rules in the ACL group. Rules are listed in order of the priority. |
| **Move Rule** | Select a rule and enter the rule number that the selected rule moves to before (or after). Select [Before] or [After] and click [Move] to move the priority of the rule. |
| **ACL Group Name** | Displays the selected ACL group name. |
| **CoS** | Configure the filtering rule based on the frame's class of service value. |
| **Destination MAC Address** | Configure the filtering rule based on the frame's destination MAC address. For instructions on how to enter the address, refer to "About Address and Mask" section below. |
| **Source MAC Address** | Configure the filtering rule based on the frame's source MAC address. For instructions on how to enter the address, refer to "About Address and Mask" section below. |
| **Ether Type** | Configure the filtering rule based on the Ether Type of the frame. |
| **VLAN** | Configure the filtering rule based on the frame's VLAN ID. |
| **Permit/Deny** | Select whether the frames that satisfy the requirements can be forwarded to the other port or not.<br><br>**Permit**<br>Forwards the incoming frames to the other port. Any packets or frames out of the range of permitted MAC addresses will be dropped.<br>**Deny**<br>Drops the incoming frames. |
| **Egress Queue** | Apply the scheduling to the frames that satisfy the requirement and configure the priority. Select the priority from 0 (lowest) to 7 (highest).<br>The scheduling is executed based on strict or WRR. It depends on the settings on the [Advanced] - [QoS] page. If QoS is disabled, it will be based on WRR. |
| **Redirect Port** | Forwards the frames that satisfy the requirements to the specified port. If enabled, the frames will not be forwarded to the primary destination port.<br>If the rule is set to [Deny], the frames will be dropped and will not be forwarded to the primary destination port. |

### About Address and Mask

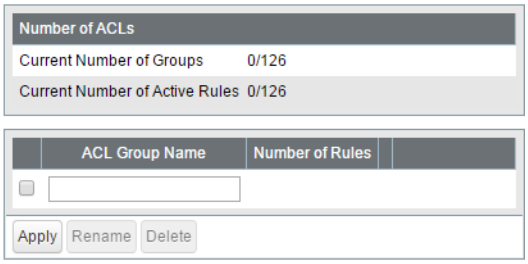
This product adopts "wildcard masks". To configure the source MAC address or destination MAC address, refer to the following example.

- To specify the range of "00:11:22:33:ab:cd:00" to "00:11:22:33:ab:cd:ff"
  Enter "00:11:22:33:ab:cd:00" in the address field and also enter "00:00:00:00:00:ff" in the mask field.
- To specify only "00:11:22:33:ab:cd:ef"

Enter "00:11:22:33:ab:cd:ef" in the address field and also enter "00:00:00:00:00:00" in the mask field.

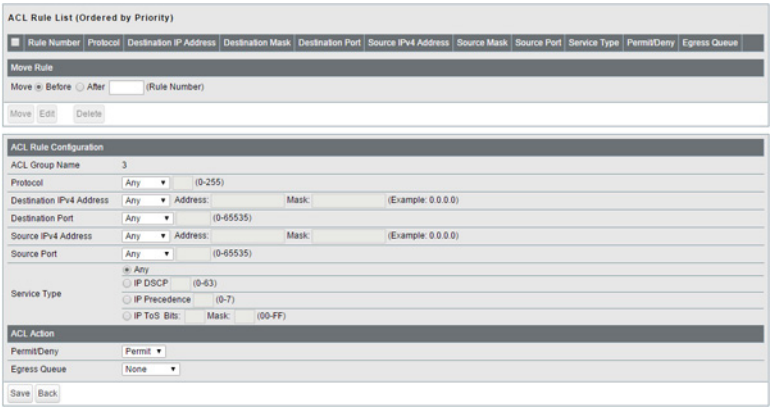
# IPv4 ACL

Create IPv4 address-based ACLs.




| | |
|---|---|
| **Current Number of Groups** | Displays the number of ACL groups. |
| **Current Number of Active Rules** | Displays the number of active rules for ACLs. |
| **ACL Group Name** | Displays the ACL group name. To create new ACLs, enter the group name and click [Apply]. Click [Show Detail] to add rules to the ACL group. To change the group name, select a group, enter the new name and click [Rename]. |
| **Number of Rules** | Displays the number of rules of each ACL group. |

The following screen is displayed when [Show Detail] is clicked. Up to 10 rules can be configured per group.




| | |
|---|---|
| **ACL Rule List** | Displays the list of rules in the ACL group. Rules are listed in priority order. |
| **Move Rule** | Select a rule and enter the rule number that the selected rule moves to before (or after). Select [Before] or [After] and click [Move] to change the priority of the rule. |
| **ACL Group Name** | Displays the selected ACL group name. |
| **Protocol** | Configure the filtering rule based on the packet's protocol. |
| **Destination IPv4 Address** | Configure the filtering rule based on the frame's destination IPv4 address. For instructions on how to enter the address, refer to "About Address and Mask" section below. |
| **Destination Port** | Configure the filtering rule based on the frame's destination port. |
| **Source IPv4 Address** | Configure the filtering rule based on the frame's source IPv4 address. For instructions on how to enter the address, refer to "About Address and Mask" section below. |
| **Source Port** | Configure the filtering rule based on the frame's source port. |

| | |
|---|---|
| **Service Type** | Configure the filtering rule based on the frame's service type.<br>If [IP DSCP] or [IP Precedence] is selected, only 1 value can be permitted or denied. If [IP ToS] is selected, you can specify the range of values which is permitted or denied. Refer to "About IP ToS Mask" section below for details. |
| **Permit/Deny** | Select if the frames that satisfy the requirement can be forwarded to the other port or not.<br><br>**Permit**<br>Forwards the incoming frames to the other port. Any packets or frames out of the range of permitted IP addresses will be dropped.<br>**Deny**<br>Drops the incoming frames. |
| **Egress Queue** | Apply the scheduling to the frames satisfy the requirement and configure the priority. Select the priority from 0 (lowest) to 7 (highest).<br>The scheduling is executed based on strict or WRR. It depends on the settings on the [Advanced] - [QoS] page. If QoS is disabled, it will be based on WRR. |

**About Address and Mask**

This product adopts "wildcard masks". To configure the source IP address or destination IP address, refer to the following example.

- To specify the range of "192.168.1.0" to "192.168.1.254"
  Enter "192.168.1.0" in the address field and also enter "0.0.0.255" in the mask field.
- To specify only "192.168.1.1"
  Enter "192.168.1.1" in the address field and also enter "0.0.0.0" in the mask field.

**About IP ToS Mask**

IP ToS mask also adopts "wildcard mask". If [IP ToS] is selected for [Service Type], you can specify the range of IP DSCP values or IP precedence values. To specify the range of values, refer to the following example.

To specify DSCP value 1-7,
Enter "0" in [Bits] field and also enter "1C" in [Mask] field.

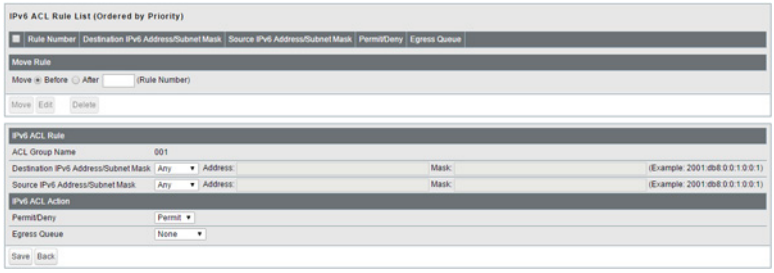
# IPv6 ACL

Create IPv6 address-based ACLs.


| | |
|---|---|
| **Current Number of Groups** | Displays the number of ACL groups. |
| **Current Number of Active Rules** | Displays the number of active rules for ACLs. |

| | |
|---|---|
| **ACL Group Name** | Displays the ACL group name. To create new ACLs, enter the group name and click [Apply]. Click [Show Detail] to add rules to the ACL group. To change the group name, select a group, enter the new name and click [Rename]. |
| **Number of Rules** | Displays the number of rules of each ACL group. |

The following screen is displayed when [Show Detail] is clicked. Up to 10 rules can be configured per group.




| | |
|---|---|
| **IPv6 ACL Rule List** | Displays the list of rules in the ACL group. Rules are listed in priority order. |
| **Move Rule** | Select a rule and enter the rule number that the selected rule moves to before (or after). Select [Before] or [After] and click [Move] to move the priority of the rule. |
| **ACL Group Name** | Displays the selected ACL group name. |
| **Destination IPv6 Address/Subnet Mask** | Configure the filtering rule based on the frame's destination IPv6 address. For instructions on how to enter the address, refer to "About Address and Mask" section below. |
| **Source IPv6 Address/ Subnet Mask** | Configure the filtering rule based on the frame's source IPv6 address. For instructions on how to enter the address, refer to "About Address and Mask" section below. |
| **Permit/Deny** | Select if the frames that satisfy the requirement can be forwarded to the other port or not.<br><br>**Permit**<br>Forwards the incoming frames to the other port. Any packets or frames out of the range of permitted IP addresses will be dropped.<br>**Deny**<br>Drops the incoming frames. |
| **Egress Queue** | Apply the scheduling to the frames satisfy the requirement and configure the priority. Select the priority from 0 (lowest) to 7 (highest).<br>The scheduling is executed based on strict or WRR. It depends on the settings on the [Advanced] - [QoS] page. If QoS is disabled, it will be based on WRR. |

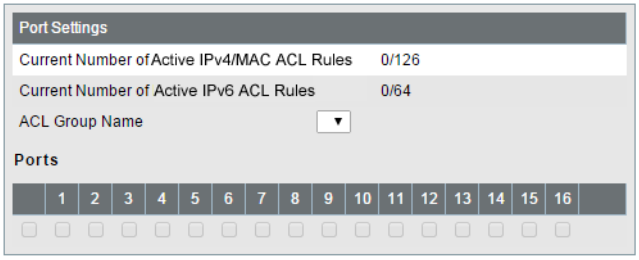
**About Address and Mask**

This product adopts "wildcard masks". To configure the source IPv6 address or destination IPv6 address, refer to the following example.

- To specify the range of "2001:db8::" to "2001:db8::ffff"
  Enter "2001:db8::" in the address field and also enter "::ffff" in the mask field.
- To specify only "2001:db8::"
  Enter "2001:db8::" in the address field and also enter "::" in the mask field.

# Ports

Configure the ports to apply ACL groups. A total of up to 126 MAC ACL and IP ACL rules may be applied to the ports.

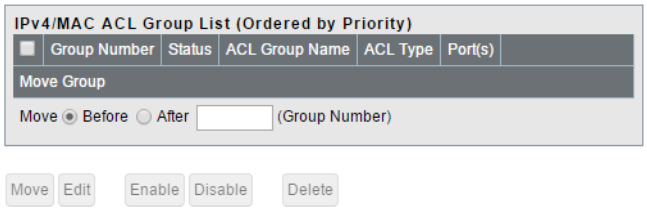



| | |
|---|---|
| **Current Number of Active IPv4/MAC ACL Rules** | Displays the number of active rules for IPv4/MAC ACLs. |
| **Current Number of Active IPv6 ACL Rules** | Displays the number of active rules for IPv6 ACLs. |
| **Port Settings** | Select an ACL group name and ports, then click [Apply]. |
| **MAC (IPv4/IPv6) ACL Rule List** | Displays the selected ACL group's rules. |

**Note:** If the group has no rules, the ports that the group belongs to will permit and forward all packets and frames. If the group has any rules, the ports that the group belongs to will drop all packets and frames that don't belong to any rules.

# IPv4/MAC Priority

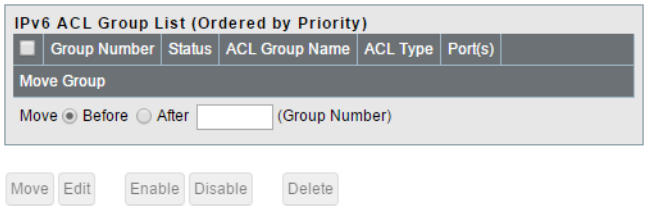
Configure IPv4 and MAC ACL group's priority. MAC ACL will be applied to both of the IPv4 and IPv6 packets. Filtering The destination and source ports for IPv4 ACL will not be applied to IPv6 packets.




| | |
|---|---|
| **IPv4/MAC ACL Group List** | Displays the list of ACL groups. Groups are listed in order of the priority. |
| **Move Group** | Select a group and enter the group number that the selected group moves to before (or after). Select [Before] or [After] and click [Move] to move the priority of the group. |

# IPv6 Priority

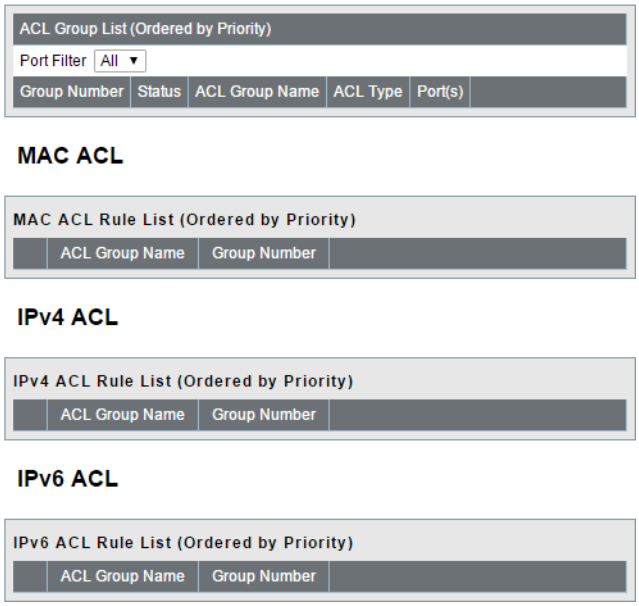
Configure IPv6 ACL group's priority. IPv6 ACL takes a priority than MAC and IPv4 ACL.




| | |
|---|---|
| **IPv6 ACL Group List** | Displays the list of ACL groups. Groups are listed in order of the priority. |
| **Move Group** | Select a group and enter the group number that the selected group moves to before (or after). Select [Before] or [After] and click [Move] to move the priority of the group. |

# Status

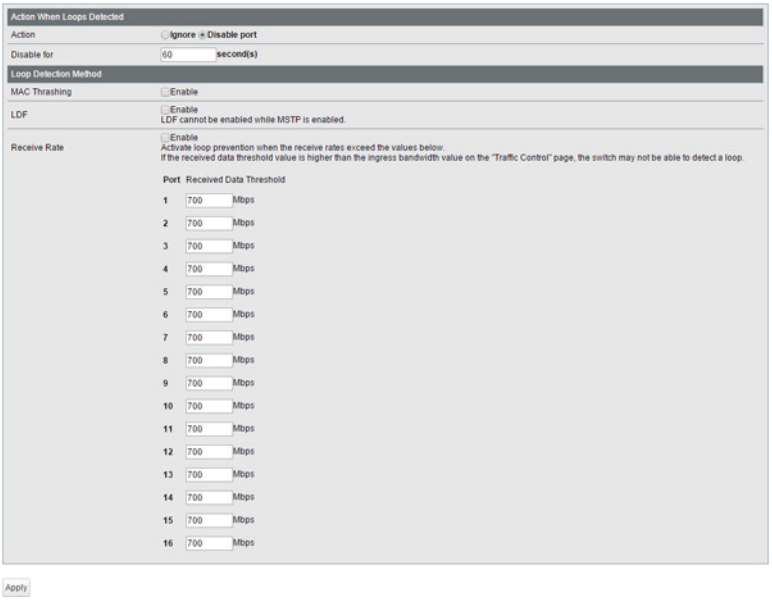
Displays the ACL status.




| | |
|---|---|
| **ACL Group List** | Displays the list of ACL groups. Groups are listed in order of the priority. Select a port from [Port Filter] to display only the groups that the selected port belongs to. |
| **MAC ACL Rule List** | Displays the list of MAC ACL groups. Click [+] next to a group to show its rules. Rules are listed in order of the priority. |
| **IPv4 ACL Rule List** | Displays the list of IPv4 ACL groups. Click [+] next to a group to show its rules. Rules are listed in order of the priority. |
| **IPv6 ACL Rule List** | Displays the list of IPv6 ACL groups. Click [+] next to a group to show its rules. Rules are listed in order of the priority. |

# Loop Prevention

Configure loop prevention functionality.




| | |
|---|---|
| **Action** | Configure the switch's action when a loop is detected.<br><br>**Ignore**<br>When a loop is detected, the switch will do nothing for the port itself; the diag LED and loop-detected port's LED will blink for the time configured in [Disable for] section. If a loop is detected again, it will blink and continue until the loop is resolved.<br>**Disable port**<br>The switch will disable the loop-detected port for the time configured in [Disable for] section. At the same time, the diag LED and loop-detected port's LED will blink for the time configured in [Disable for] section. If a loop is detected again after the time configured in [Disable for] section is passed, the switch will disable the loop-detected port and continue until the loop is resolved. |
| **Disable for** | Configure the period to disable the loop-detected port when [Disable port] is selected as the action. |
| **MAC Thrashing** | Check to enable MAC thrashing loop detection method, which assumes that a loop occurs when the switch's MAC address learn limit exceeds the configured threshold in one second. |
| **LDF** | Check to enable LDF loop detection method. The switch will transmit the LDF packet once per second. If the transmitted LDF packet is received, this will assume that a loop is occurring.<br>**Note:** LDF cannot be used when MSTP is enabled. |
| **Receive Rate** | Check to enable receive rate loop detection method. If the port's threshold exceeds the configured receive rate, this will assume that a loop is occurring. |
| **Received Data Threshold** | Configure the threshold to assume that a loop is occurring. (1-1000 Mbps)<br>**Note:** If the received data threshold value is higher than the ingress bandwidth value on the "Traffic Control" page, the switch may not be able to detect a loop. |

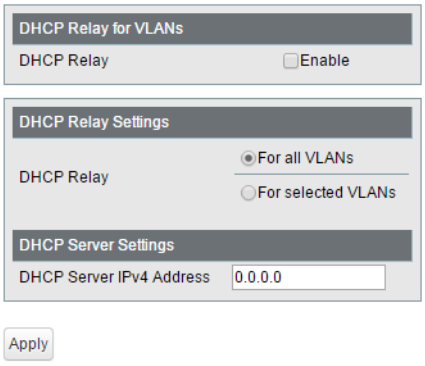
**Note:** The loop prevention functionality temporarily disables the port, but will not resolve the loop itself. On the other hand, the spanning tree functionality blocks the port when a loop is detected and switches the route automatically to prevent the network from going down. This switch has both functions; use the most appropriate

one depending on your network environment.

| | Loop Prevention | Spanning Tree |
|---|---|---|
| Action when the loop is detected | Temporarily disables the port. After the configured time passes, the port will be enabled again. | Blocks the port and switches the transmission route automatically. |
| How to resolve the loop | Resolve manually<br>Data can be transmitted temporarily while the port is disabled.<br>Data cannot be transmitted until the loop is resolved unless storm control is enabled. | Resolve automatically<br>Communication will be interrupted while the route is being switched. |
| Recommended Environment | Small-scale network | • Large or medium-scale network with existing spanning tree<br>• The environment that the loop must be prevented in |

# DHCP Relay

Displayed only when the switch is in L3 mode. Configure DHCP relay, that relays the DHCP messages in the other network to the specific VLAN.




| | |
|---|---|
| **DHCP Relay** | Check to enable DHCP relay. |
| **DHCP Relay Settings** | If only one DHCP server is configured for all VLANs, select "For all VLANs". If DHCP servers are configured for each VLAN, select "For selected VLANs".<br>If "For all VLAN" is selected, enter the DHCP server IP address. If "For selected VLANs" is selected, check "Enabled" of each VLAN that need to enable DHCP relay. Then, enter the DHCP server IP address for each VLAN. |

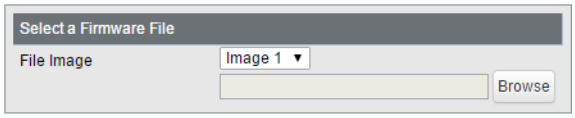
# Update Firmware

Update firmware with the local firmware file.

Select a file image to update and click [Browse] to select the firmware image, then click [Update].

**Notes:**

- Do not turn off the switch or close the browser while updating.
- To finish the update, reboot the switch.

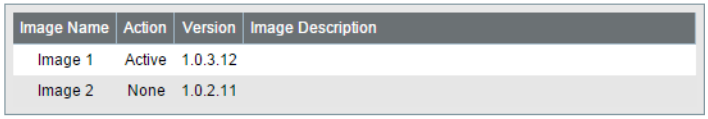


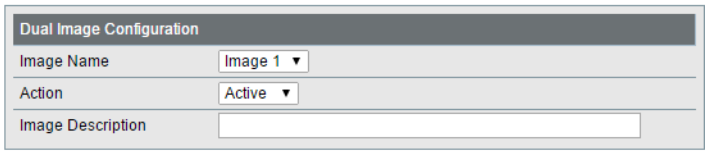


| | |
|---|---|
| **File Image** | Select a file image to update. |

# Dual Image

The switch can save up to 2 firmware files and can be configured to choose one for booting.



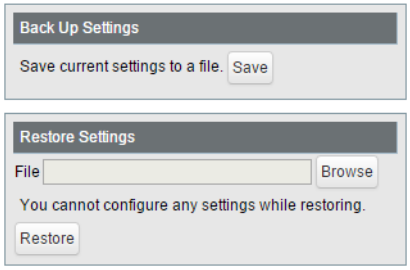


| | |
|---|---|
| **Image Name** | Select an image to change the action. |
| **Action** | **Active**<br>Reads the image when the switch boots.<br>**None**<br>The image will not be used.<br>**Delete**<br>Select [Delete] and click [Apply] to delete the image. |
| **Image Description** | Enter the image's description. You may enter up to 50 alphanumeric characters.<br>**Note:** The image description will never be initialized even if the switch is initialized. |

**Note:** Switching to the lower version image (older version firmware) may delete some settings.

# Back Up and Restore Settings

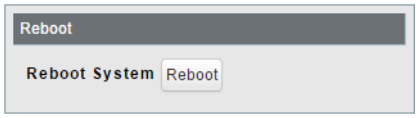
Save or restore the switch's settings.




| | |
|---|---|
| **Back Up Settings** | Click [Save] to save current settings to a file. |
| **Restore Settings** | Click [Browse] to select a settings file and click [Restore] to start restoring.<br>**Note:** To finish restoring, reboot the switch. |

# Reboot

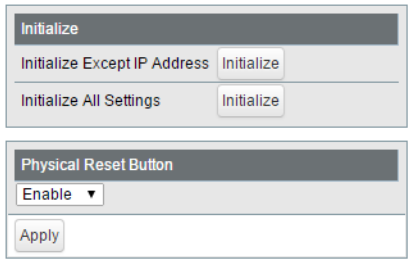
Reboot the switch.




| | |
|---|---|
| **Reboot** | Click [Reboot] to reboot the switch. |

# Initialize

Restore the switch settings to the factory default.



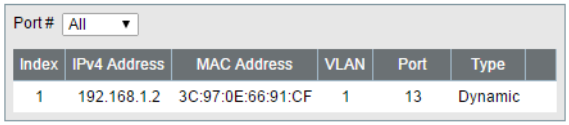

| | |
|---|---|
| **Initialize Except IP Address** | Click [Initialize] to initialize all settings except the switch's IPv4/IPv6 address. |
| **Initialize All Settings** | Click [Initialize] to initialize all switch settings. |
| **Physical Reset Button** | Enable or disable the reset button on the switch. |

# ARP Table

Displayed only when the switch is in L3 mode. ARP table can record up to 510 devices.

## Port Order

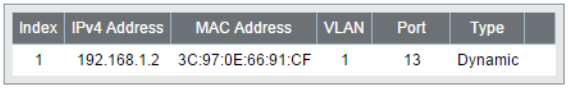
Displays the IP addresses and the MAC addresses of the connected devices with the port order. Select a port from the dropdown menu to display the devices that is connected to the selected port.




Refresh Clear

## IP Address Order

Displays the IP addresses and the MAC addresses of the connected devices with the IP address order.

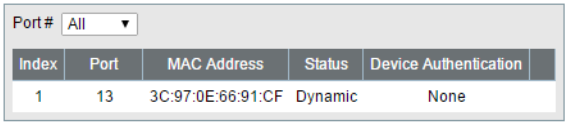



Refresh Clear

# MAC Address Table

## Port Order

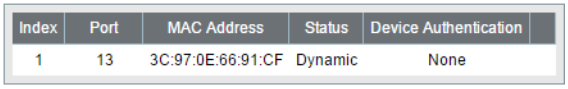
Displays the MAC address table with the port order. Select a port from the dropdown menu to display the MAC addresses that are connected to the selected port.




Refresh Clear

## MAC Order

Displays the MAC address table with the MAC address order.



| Index | Port | MAC Address | Status | Device Authentication |
|---|---|---|---|---|
| 1 | 13 | 3C:97:0E:66:91:CF | Dynamic | None |

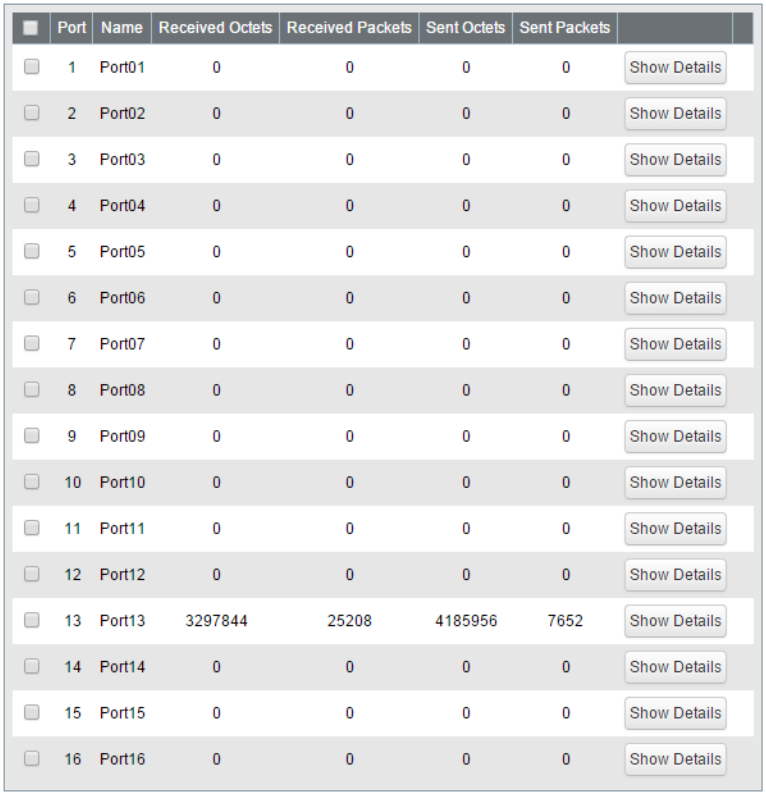
Refresh Clear

**Note:** "Authenticated" is displayed on "Device Authentication" section only when the PC is authenticated using 802.1X MAC or MAC authentication method.

# Statistics

Displays the switch's statistics.

**Note:** Each maximum value is 4,294,967,295. If this is reached or exceeded, the value will reset to 0. Rebooting the switch will also reset the value to 0.



| Port | Name | Received Octets | Received Packets | Sent Octets | Sent Packets | |
|---|---|---|---|---|---|---|
| 1 | Port01 | 0 | 0 | 0 | 0 | Show Details |
| 2 | Port02 | 0 | 0 | 0 | 0 | Show Details |
| 3 | Port03 | 0 | 0 | 0 | 0 | Show Details |
| 4 | Port04 | 0 | 0 | 0 | 0 | Show Details |
| 5 | Port05 | 0 | 0 | 0 | 0 | Show Details |
| 6 | Port06 | 0 | 0 | 0 | 0 | Show Details |
| 7 | Port07 | 0 | 0 | 0 | 0 | Show Details |
| 8 | Port08 | 0 | 0 | 0 | 0 | Show Details |
| 9 | Port09 | 0 | 0 | 0 | 0 | Show Details |
| 10 | Port10 | 0 | 0 | 0 | 0 | Show Details |
| 11 | Port11 | 0 | 0 | 0 | 0 | Show Details |
| 12 | Port12 | 0 | 0 | 0 | 0 | Show Details |
| 13 | Port13 | 3297844 | 25208 | 4185956 | 7652 | Show Details |
| 14 | Port14 | 0 | 0 | 0 | 0 | Show Details |
| 15 | Port15 | 0 | 0 | 0 | 0 | Show Details |
| 16 | Port16 | 0 | 0 | 0 | 0 | Show Details |

Refresh Clear

| | |
|---|---|
| **Name** | Displays the port name. |
| **Received Octets** | Displays the number of total received octets. |
| **Received Packets** | Displays the number of total received packets. |
| **Sent Octets** | Displays the number of total sent octets. |
| **Sent Packets** | Displays the number of total sent packets. |
| **Show Details** | Click to display the detailed information. |

| | |
|---|---|
| **Port Statistics** | Displays the number of total received/sent packets of the selected port. |
| **EAP Statistics** | Displays the number of total received/sent EAP packets of the selected port. |

The following items appear when [Show Detail] is clicked.

| | |
|---|---|
| **Received Octets** | Displays the number of total received octets. |
| **Received Unicast Packets** | Displays the number of received unicast packets. |
| **Received Multicast Packets** | Displays the number of received multicast packets. |
| **Received Broadcast Packets** | Displays the number of received broadcast packets. |
| **Discarded Received Packets** | Displays the number of packets that the switch received but did not forwarded to any port. |
| **Received Packet Error** | Displays the number of packets that was discarded because of FCS error. |
| **Sent Octets** | Displays the number of total sent octets. |
| **Sent Unicast Packets** | Displays the number of sent unicast packets. |
| **Sent Multicast Packets** | Displays the number of sent multicast packets. |
| **Sent Broadcast Packets** | Displays the number of sent broadcast packets. |
| **Discarded Sent Packets** | Displays the number of packets that could not be sent. |
| **Sent Packet Error** | Displays the number of packets that was discarded because of FCS error. |
| **Total Frames Rx** | Displays the number of total received EAP packets. |
| **Total Frames Tx** | Displays the number of total sent EAP packets. |
| **Start Frames Rx** | Displays the number of received EAPOL start packets. |
| **Logoff Frames Rx** | Displays the number of received EAPOL logoff packets. |
| **Request/ID Frames Tx** | Displays the number of EAP packets that include "Code:Request(1) Type:Identity(1)". |
| **Request Frames Tx** | Displays the number of EAP packets that do not include "Code:Request(1) Type:Identity(1)". |
| **Response/ID Frames Rx** | Displays the number of EAP packets that include "Code:Response(2) Type:Identity(1)". |
| **Response Frames Rx** | Displays the number of EAP packets that do not include "Code:Response(2) Type:Identity(1)". |
| **Invalid Frames Rx** | Displays the number of EAP packets whose types are invalid. |
| **Length Error Frames Rx** | Displays the number of EAP packets whose packet lengths are invalid. |
| **Last Frame Version** | Displays the version of the latest received EAP packet. |
| **Last Frame Source** | Displays the source MAC address of the latest received EAP packet. |

**Notes:**

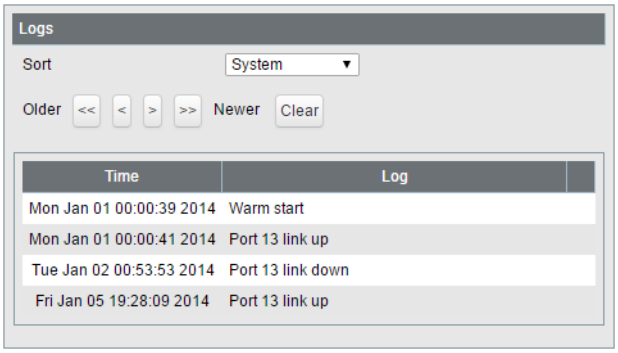
- When the switch is in L2 mode, packets that are designated to the switch (such as ping or http communication for displaying Settings) will be displayed as "received unicast packets" and "discarded received packets".
- When the switch is in L3 mode, packets that are designated to the switch are displayed as "received unicast packets".
- The target packets of this page are MAC frames, IPv4 packets, and IPv6 packets.

# Logs

Displays the switch's log information.

**Notes:**

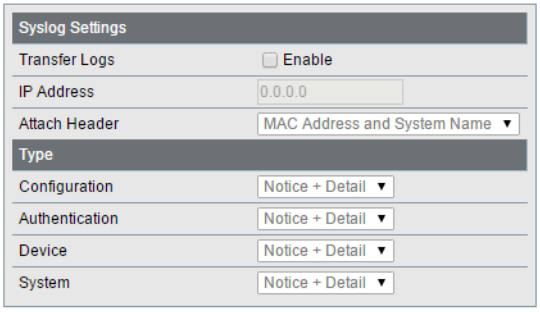
- Up to 512 logs can be recorded to this switch in total. If exceeded, logs will be deleted in order of oldest.
- When the switch is turned off, all logs will be deleted.




| | |
|---|---|
| **Sort** | Select a type of log to display. |

# Syslog Settings

Configure syslog to transfer logs.

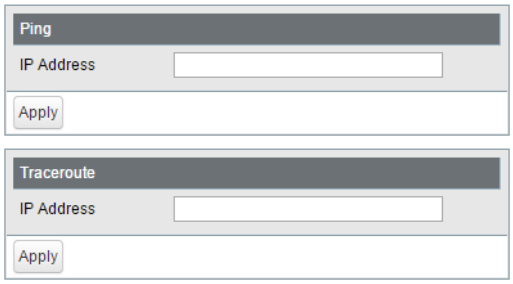




| | |
|---|---|
| **Transfer Logs** | Check to enable syslog server. |
| **IP Address** | Enter the syslog server's IP address. |
| **Attach Header** | Select an item to attach to the header of the transmitted data. |
| **Type** | Select a type of log to transfer. |

# Network Diagnostics

Execute a communication test to the specified IP address.




| | |
|---|---|
| **Ping** | Enter the IPv4/IPv6 address or FQDN and click [Apply] to execute a ping test to the destination. |
| **Traceroute** | Enter the IPv4 address or FQDN and click [Apply] to execute a traceroute test to the destination. |

To enter the FQDN, configure DNS server settings on [Basic] - [VLAN] - [VLAN Settings] page in advance.

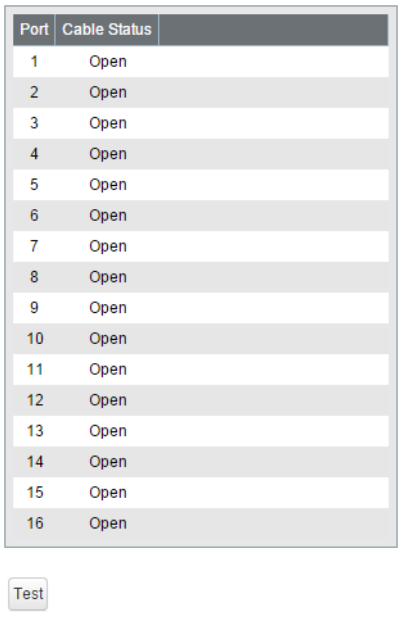
# Cable Diagnostics

Click [Test] to check whether there are any issues with the Ethernet cable connected to each port.

To check the cable status correctly, configure the following to this switch and the destination device in advance;

- Autonegotiation: enabled
- IEEE 802.3az (EEE): disabled
- Auto power down (APD): disabled

**Note:** If the destination device is not a BS-GS series switch, the result may not appear correctly.



| Port | Cable Status |
|---|---|
| 1 | Open |
| 2 | Open |
| 3 | Open |
| 4 | Open |
| 5 | Open |
| 6 | Open |
| 7 | Open |
| 8 | Open |
| 9 | Open |
| 10 | Open |
| 11 | Open |
| 12 | Open |
| 13 | Open |
| 14 | Open |
| 15 | Open |
| 16 | Open |

| | |
|---|---|
| **Cable Status** | Displays the status of each Ethernet cable.<br><br>**Open**<br>Ethernet cable is not connected.<br>**OK**<br>Ethernet cable is connected without any issues.<br>**Short**<br>Ethernet cable may be shorting out.<br>**Unknown**<br>Cannot check the cable status. |

# Chapter 3 Troubleshooting

## LED Is Not Lit, Abnormal Lighting or Blinking

| | |
|---|---|
| The power LED is not lit. | • Confirm that the AC adapter or power cable is connected to the inlet. |
| The diag LED is blinking red. | • If it blinks once per a second, a loop is detected. Check the cabling.<br>• If your switch has fans and its diag LED is blinking fast, a fan error may be occurring. Disconnect the power cable and reconnect it. If the LED keeps blinking, contact our technical support. |
| The link/act LED is not lit. | • Confirm that the Ethernet cable is connected to both the switch and the device.<br>• Confirm that the switch and the connected device are both powered on.<br>• Confirm that the Ethernet cable type and length is compatible with the switch. |
| Cannot initialize with the reset button on the switch | • Confirm whether the physical reset button is enabled in Settings.<br>• If the physical reset button is disabled and you forgot the password of Settings, contact our technical support. |

## Cannot Access Settings

- Make sure that your PC is connected to the switch.
- Access Settings with the switch's IP address (192.168.1.254 by default).
- Confirm that the username ("admin" by default) and the password ("password" by default) are correct. If you forgot the username or password, initialize the switch.
- If a proxy server is configured for the web browser, disable the proxy server or add the switch's IP address to the proxy server's exception list.
- Confirm that your PC is connected to the port which belongs to the management VLAN.

## Forgot the Password

- The password is "password" by default. If you changed the password, press the reset button to initialize.
- If the physical reset button is disabled and you forgot the password of Settings, contact our technical support.

# Appendix A Specification

## Product Specification

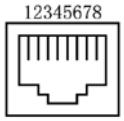
Refer to the quick setup guide to check the hardware specification.

**Note:** Only use the cables and accessories that are included in the package. Don't use other accessories or cables unless specifically instructed to in the documentation.

## Port Specification

Ethernet port specification

RJ-45 with 8 pins




| 100BASE-TX/10BASE-T | | |
|---|---|---|
| Pin Number | Signal Name | Signal Function |
| 1 | RD+/TD+ | Receive data (+)/Transmit data(+) |
| 2 | RD-/TD- | Receive data (-)/Transmit data(-) |
| 3 | TD+/RD+ | Transmit data (+)/Receive data(+) |
| 4 | (Not Use) | Not used |
| 5 | (Not Use) | Not used |
| 6 | TD-/RD- | Transmit data (-)/Receive data (+) |
| 7 | (Not Use) | Not used |
| 8 | (Not Use) | Not used |
| **1000BASE-T** | | |
| Pin Number | Signal Name | Signal Function |
| 1 | BI_DA+/BI_DB+ | Transmit and receive data A (+)/Transmit and receive data B (+) |
| 2 | BI_DA-/BI_DB- | Transmit and receive data A (-)/Transmit and receive data B (-) |
| 3 | BI_DB+/BI_DA+ | Transmit and receive data B (+)/Transmit and receive data A (+) |
| 4 | BI_DC+/BI_DD+ | Transmit and receive data C (+)/Transmit and receive data D (+) |
| 5 | BI_DC-/BI_DD- | Transmit and receive data C (-)/Transmit and receive data D (-) |
| 6 | BI_DB-/BI_DA- | Transmit and receive data B (-)/Transmit and receive data A (-) |
| 7 | BI_DD+/BI_DC+ | Transmit and receive data D (+)/Transmit and receive data C (+) |
| 8 | BI_DD-/BI_DC- | Transmit and receive data D (-)/Transmit and receive data C (-) |

PoE Port Specification (Only for PoE-compatible devices) (Alternative A)

| Pin Number | Power |
|---|---|
| 1 | Negative Vpse |
| 2 | Negative Vpse |
| 3 | Positive Vpse |
| 4 | - |
| 5 | - |
| 6 | Positive Vpse |
| 7 | - |
| 8 | - |

# Factory Default Settings

| | | | |
|---|---|---|---|
| **System** | | **Switch Name** | BS + the switch's MAC address |
| | | **Location** | Not defined |
| | | **Contact** | Not defined |
| **VLAN** | **VLAN Settings** | **VLAN Mode** | VLAN |
| | | **VLAN ID** | 1 |
| | | **VLAN Name** | None |
| | | **Management VLAN** | Enabled |
| | | **Connection Method** | Static IP Address |
| | | **IPv4 Address** | 192.168.1.254 |
| | | **Subnet Mask** | 255.255.255.0 |
| | | **Default Gateway** | 0.0.0.0 |
| | | **Method of Acquiring DNS Server Address** | Manual |
| | | **Primary DNS Server** | 0.0.0.0 |
| | | **Secondary DNS Server** | 0.0.0.0 |
| | | **IPv6** | Disabled |
| | | **Ports** | Untagged |
| | **VLAN Ports** | **PVID** | 1 |
| | | **Acceptable Frame Type** | Admit All |
| | | **Ingress Filter** | Enabled |
| | | **Protected Port** | Disabled |
| **Routing** | **L2/L3 Settings** | **Mode** | L2 mode |
| | **Static Routing** (L3 mode only) | **Default Gateway** | 0.0.0.0 |
| **SNMP Settings** | **SNMP Community Table** | **Community Name** | "public" for only #1 |
| | | **Get** | Enabled for only #1 |
| | | **Set** | Disabled |
| | | **Trap** | Disabled |
| | **SNMP Host Table** | **Host Authentication** | Disabled |

| | | | |
|---|---|---|---|
| **SNMP Settings** | **SNMP Trap** | **Authentication Trap** | Disabled |
| | | **Link Up/Down** | Disabled |
| | | **STP** | Disabled |
| | | **Loop Detection** | Disabled |
| | | **Trunk** | Disabled |
| | **SNMPv3 User** | **Username** | admin |
| | | **Access Control** | Read only |
| | | **Authentication Method** | None |
| | | **Authentication Key** | None |
| | | **Encryption** | None |
| | | **Encryption Key** | None |
| **LLDP** | **LLDP Properties** | **TLV Advertised Interval** | 30 seconds |
| | | **Hold Multiplier** | 4 |
| | | **Reinitializing Delay** | 2 seconds |
| | | **Transmit Delay** | 2 seconds |
| | | **Fast Start Duration** | 3 times |
| | **LLDP Port** | **Status** | Tx and Rx |
| | | **Notification** | Disabled |
| | | **Port Description TLV** | Disabled |
| | | **System Name TLV** | Disabled |
| | | **System Description TLV** | Disabled |
| | | **System Capabilities TLV** | Disabled |
| | | **Management Address TLV** | Disabled |
| | **LLDP-MED Port** | **Status** | Disabled |
| | | **Notification** | Disabled |
| | | **Capabilities TLV** | Disabled |
| | | **Network Policy TLV** | Disabled |
| | | **Extend Power TLV** | Disabled |
| | | **Software Revision TLV** | Disabled |
| **MAC Addresses** | **Static MAC Filtering** | **Static MAC Filtering** | Disabled |
| | **Dynamic MAC Filtering** | **Dynamic MAC Filtering** | Disabled |
| | | **Number** | None |
| | **MAC Address Aging** | **Aging Time** | 300 seconds |
| **Port Settings** | **Speed/Mode Settings** | **Name** | Port + port number |
| | | **Admin** | Enabled |
| | | **Mode** | Autonegotiation |
| | | **Flow Control** | Disabled |
| | | **IEEE 802.3az** | Enabled |
| | | **APD** | Enabled |
| | | **Jumbo Frame** | Enabled |
| **System Security** | **Administration Account** | **Username** | admin |
| | | **Password** | password |
| | **Access Management** | **SNMP** | Enabled |
| | | **HTTPS** | Disabled |
| | | **Web Session Timeout** | 5 minutes |
| | | **Maximum Web Session Number** | 5 |
| | | **Port** | 443 |

| | | | |
|---|---|---|---|
| **System Security** | **Access Management** | **HTTPS Session Timeout** | 5 minutes |
| | | **Maximum HTTPS Session Number** | 2 |
| **Date & Time** | | **SNTP** | Disabled |
| | | **Time** | 2014/01/01 00:00:00 |
| | | **Server IP/FQDN** | ntp.jst.mfeed.ad.jp |
| | | **Update Interval** | 24 hours |
| | | **Time Zone** | (GMT-06:00) Central Time (US & Canada) |
| **PoE** (PoE-compatible product only) | **PoE Profiles** | **Profile Name** | Profile 1-4 |
| | | **PoE** | Enabled |
| | | **Priority** | Low |
| | | **High Power** | 802.3at |
| | | **Turn Off LEDs?** | No |
| | **Power Profiles** | **Schedule** | Manual |
| | | **Manual Profile Setting** | Profile1 |
| | | **View** | Weekly |
| **QoS** | **QoS Settings** | **QoS** | Disabled |
| | | **Schedule Method** | WRR |
| | | **Priority Type** | CoS |
| | **QoS Mapping** | **Port Priority** | 0 |
| | | **CoS Mapping** | 2, 0, 1, 3, 5, 6, 7 in order of CoS value |
| | **VoIP Auto Priority** | **VoIP Auto Priority** | Enabled |
| | | **CoS** | 7 |
| **Security** | **Auto DoS Attack Prevention** | **LAND Attack** | Disabled |
| | | **Minimum TCP Header Size** | Disabled |
| | | **TCP/UDP L4 Port** | Disabled |
| | | **ICMP** | Disabled |
| | | **TCP Flag** | Disabled |
| | | **Fragment** | Disabled |
| | **DHCP Snooping** | **DHCP Snooping** | Disabled |
| | | **DHCP Option 82** | Disabled |
| | | **Rate Limit** | None |
| | | **Status** | Trusted |
| **Authentication** | **RADIUS** | **Authentication** | Primary authentication server: Enabled<br>Secondary authentication server: Disabled |
| | | **Authentication Server IP** | 1.1.1.1 |
| | | **Authentication Server Port** | 1812 |
| | | **Shared Secret** | None |
| | | **Reset Timer** | 3600 seconds |
| | | **Advanced** | Accounting: Disabled<br>Termination-Action: Disabled<br>Dynamic VLAN Assignment: Disabled |

| | | | |
|---|---|---|---|
| **Authentication** | **Port Authentication** | **802.1X Port** | Disabled |
| | | **802.1X MAC** | Disabled |
| | | **By MAC** | Disabled |
| | | **EAP Passthrough** | Disabled |
| | | **Guest VLAN** | Disabled |
| | | **VLAN ID** | 0 |
| | | **Guest VLAN Period** | 60 seconds |
| **Port Trunking** | | **Trunk Mode** | LACP |
| | | **Trunk Key** | None |
| | | **Trunk Name** | None |
| | | **System Priority** | 32768 |
| | | **Member** | None |
| **Traffic Control** | | **Broadcast** | Unlimited |
| | | **Multicast** | Unlimited |
| | | **DLF** | Unlimited |
| | | **Ingress Bandwidth** | 1000 Mbps |
| | | **Egress Bandwidth** | 1000 Mbps |
| **Mirroring** | | **Enable** | Mirror1: Disabled<br>Mirror 2: Disabled |
| | | **Source Port** | Mirror1: 2<br>Mirror 2: 4 |
| | | **Destination Port** | Mirror1: 1<br>Mirror 2: 3 |
| **Spanning Tree Protocol** | **STP Settings** | **STP Version** | Disabled |
| | | **Hello Time** | 2 seconds |
| | | **Max Age** | 20 seconds |
| | | **Forward Delay** | 15 seconds |
| | | **Max Hop Count** (MSTP only) | 20 |
| | | **Bridge Priority** | 32768 |
| | | **BPDU Forwarding** (Only when STP is disabled) | Disabled |
| | | **MST Configuration Name** (MSTP only) | Automatically generated from the switch's MAC address |
| | | **MST Revision Level** (MSTP only) | 0 |
| | **Ports** | **Path Cost** | Auto |
| | | **Priority** | 128 |
| | | **Path Cost** | 20000 |
| | | **Fastlink** | Disabled |
| **IGMP** | **IGMP Settings** | **IGMP Snooping** | Disabled |
| | | **Filter Unknown Multicast** | Disabled |
| | | **Host Timeout** | 260 seconds |
| | | **Router Port Timeout** | 125 seconds |
| | **IGMP Querier Settings** | **IGMP Querier** | Disabled |
| | | **Querier Interval** | 60 seconds |
| | | **Querier Source IPv4 Address** | 0.0.0.0 |
| | | **Max Response Time** | 10 seconds |

| | | | |
|---|---|---|---|
| **MLD** | **MLD Settings** | **MLD Snooping** | Disabled |
| | | **Filter Unknown Multicast** | Disabled |
| | | **Host Timeout** | 260 seconds |
| | | **Router Port Timeout** | 125 seconds |
| | **MLD Querier Settings** | **MLD Querier** | Disabled |
| | | **Querier Interval** | 60 seconds |
| | | **Querier Source IPv6 Address** | :: |
| | | **Max Response Time** | 10 seconds |
| **Loop Prevention** | | **Action** | Disable port |
| | | **Disable for** | 60 seconds |
| | | **MAC Thrashing** | Disabled |
| | | **LDF** | Disabled |
| | | **Receive Rate** | Disabled |
| | | **Received Data Threshold** | 700 Mbps |
| **DHCP Relay** | | **DHCP Relay for VLANs** | Disabled |
| | | **DHCP Relay Settings** | For all VLANs |
| | | **DHCP Server IP Address** | 0.0.0.0 |
| **Syslog Settings** | | **Transfer Logs** | Disabled |
| | | **IP Address** | 0.0.0.0 |
| | | **Attach Header** | MAC Address and System Name |
| | | **Configuration** | Notice + Detail |
| | | **Authentication** | Notice + Detail |
| | | **Device** | Notice + Detail |
| | | **System** | Notice + Detail |

# Company Information

Buffalo Americas, Inc.
11100 Metric Blvd., Suite 750
Austin, TX 78758
Office: 1-512-349-1500
Customer Service: 1-866-752-6210