IES-3000 Series

Industrial Managed Ethernet Switch

User Manual

Version 2.3

March, 2024

www.oringnet.com

COPYRIGHT NOTICE

TRADEMARKS

ORing is a registered trademark of ORing Industrial Networking Corp.
All other trademarks belong to their respective owners.

REGULATORY COMPLIANCE STATEMENT

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

WARRANTY

ORing warrants that all ORing products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). ORing will repair or replace products found by ORing to be defective within this warranty period, with shipment expenses apportioned by ORing and the distributor. This warranty does not cover product modifications or repairs done by persons other than ORing-approved personnel, and this warranty does not apply to ORing products that are misused, abused, improperly installed, or damaged by accidents.
Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

DISCLAIMER

Information in this publication is intended to be accurate. ORing shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ORing reserves the right to revise the contents of this publication without notice.

CONTACT INFORMATION

ORing Industrial Networking Corp.
3F., NO.542-2, Jhongjheng Rd., Sindian District, New Taipei City 23145, Taiwan, R.O.C.
Tel: + 886 2 2218 1066 // Fax: + 886 2 22181014
Website: www.oringnet.com

Technical Support
E-mail: support@oringnet.com

Sales Contact
E-mail: sales@oringnet.com (Headquarters) sales@oringnet.com.cn (China)

Table of Content

Management

The switch can be controlled via a built-in web server which supports Internet Explorer (Internet Explorer 5.0 or above versions) and other Web browsers such as Chrome. Therefore, you can manage and configure the switch easily and remotely. You can also upgrade firmware via a Web browser. The Web management function not only reduces network bandwidth consumption, but also enhances access speed and provides a user-friendly viewing screen.

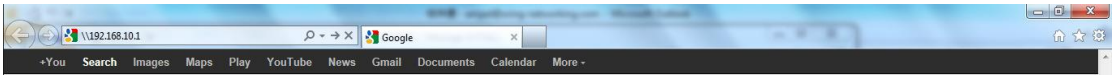
Note: By default, IE5.0 or later version do not allow Java applets to open sockets. You need to modify the browser setting separately in order to enable Java applets for network ports.

Management via Web Browser

Follow the steps below to manage your switch via a Web browser

System Login

1. Launch an Internet Explorer.
2. Type http:// and the IP address of the switch. Press **Enter**.



3. A login screen appears.
4. Type in the username and password. The default username and password is **admin**.
5. Press **Enter** or click **OK**, the management page appears.

Note: you can use the following default values:

IP Address: **192.168.10.1**

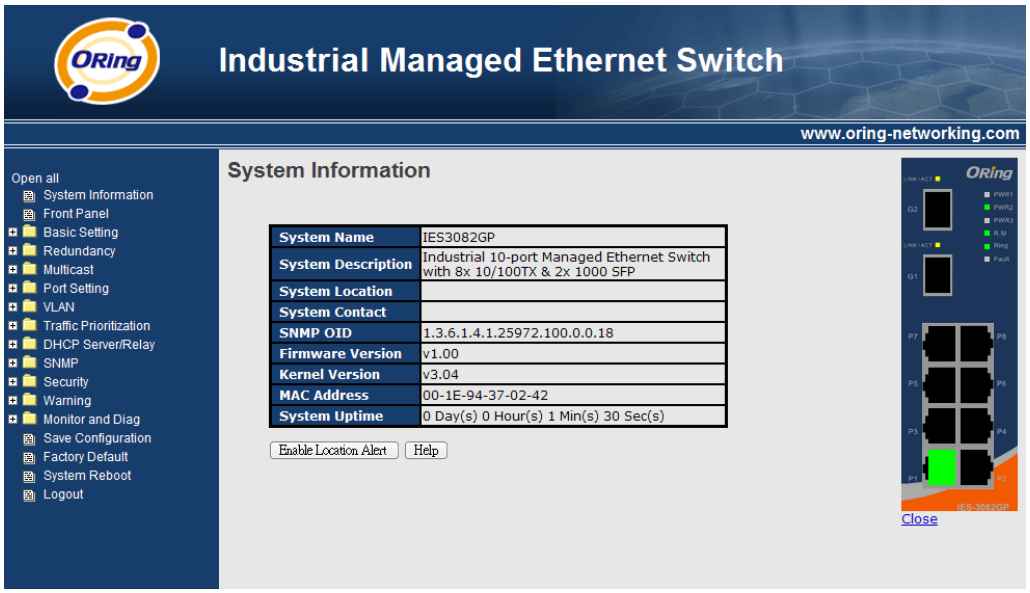
Subnet Mask: **255.255.255.0**

Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

After logging in, you will see the information of the switch as below.



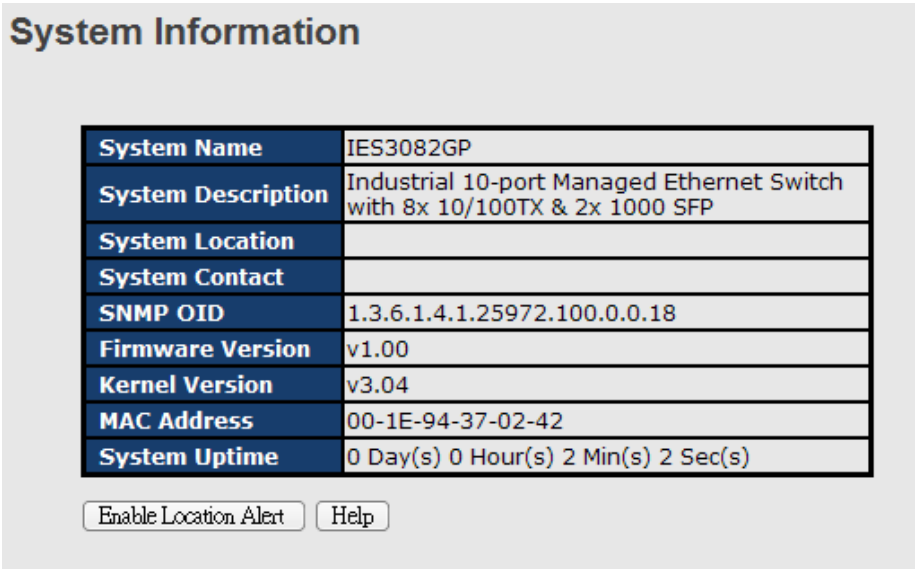
On the right hand side of the management interface shows links to various settings. Clicking on the links will bring you to individual configuration pages.

1.1 Basic Settings

The Basic Settings page allows you to configure the basic functions of the switch.

1.1.1 System Information

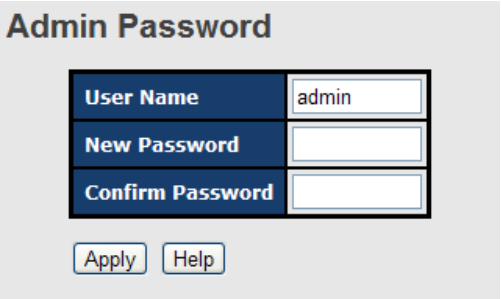
This page shows the general information of the switch.



Label	Description
System Name	An administratively assigned name for the managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string consisting of alphabets (A-Z, a-z), digits (0-9), and minus sign (-). Space is not allowed to be part of the name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
System Description	Description of the device
System Location	The physical location of the node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and only ASCII characters from 32 to 126 are allowed.
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and only ASCII characters from 32 to 126 are allowed.
System Timezone offset(minutes)	Provides the time-zone offset from UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

1.1.2 Admin & Password

This page allows you to configure the system password required to access the web pages or log in from CLI.

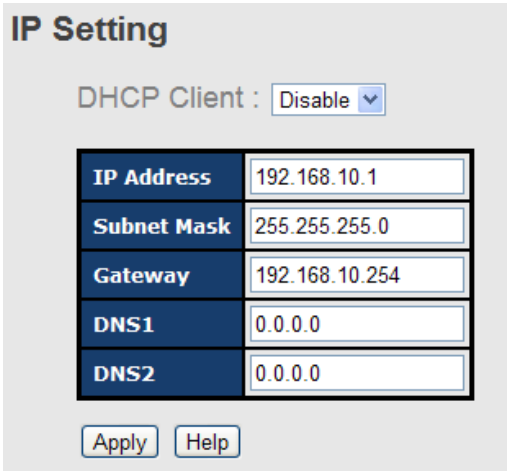


Label	Description
User name	The user name for operating the switch (default is **admin**)

New Password	The new system password (default is **admin**)
Confirm password	Re-type the new password
Apply	Click to save changes

1.1.3 IP Setting

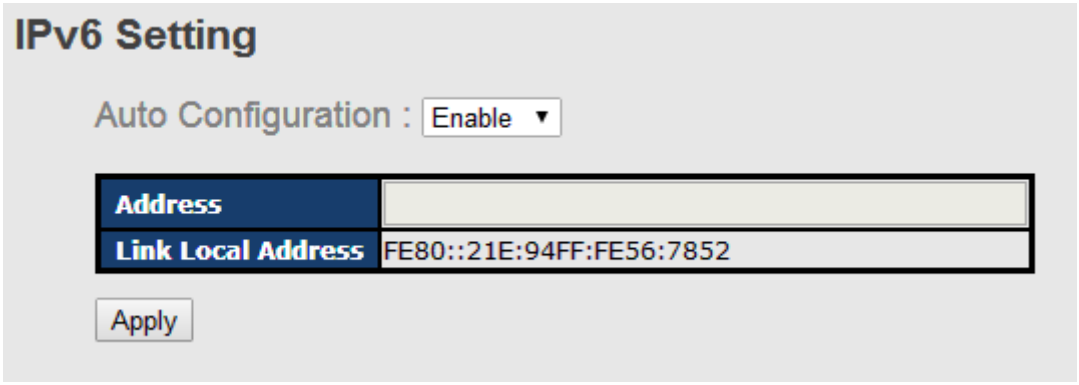
This page allows you to configure IP information for the switch. You can configure the settings manually by disabling DHCP Client. After inputting the values, click **Apply** and the new values will be applied.



Label	Description
DHCP Client	Enables or disables the DHCP client. If DHCP fails or the configured IP address is zero, DHCP will retry. If DHCP retry fails, DHCP will stop trying and the configured IP settings will be used.
IP Address	Assigns the IP address of the network in use. If DHCP client function is enabled, you do not need to assign the IP address. The network DHCP server will assign an IP address to the switch and it will be displayed in this column. The default IP is **192.168.10.1**.
Subnet Mask	Assigns the subnet mask of the IP address. If DHCP client function is enabled, you do not need to assign the subnet mask.
Gateway	Assign the network gateway for the switch. The default gateway is 192.168.10.254.
DNS1	Assign the primary DNS IP address
DNS2	Assign the secondary DNS IP address
Apply	Click to apply the changes

1.1.4 IPv6 Setting

Configure the switch-managed IPv6 information on this page.



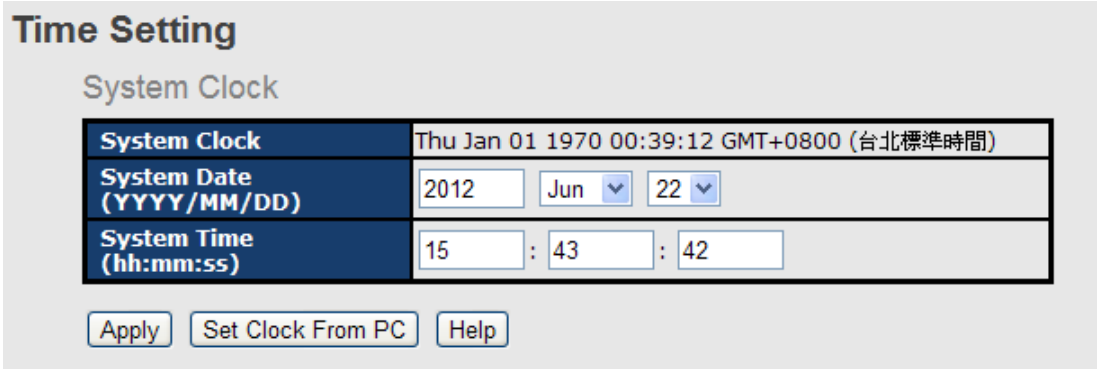
Label	Description
Auto Configuration	Enable IPv6 auto-configuration by checking this box. If system cannot obtain the stateless address in time, the configured IPv6 settings will be used. The router may delay responding to a router solicitation for a few seconds, the total time needed to complete auto-configuration can be significantly longer.
Address	Provide the IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
Link Local Address	In a computer network, a link-local address is a network address that is valid only for communications within the network segment (link) or the broadcast domain that the host is connected to.

1.1.5 Time Setting

This page allows you to configure SNTP and system clock.

System Clock

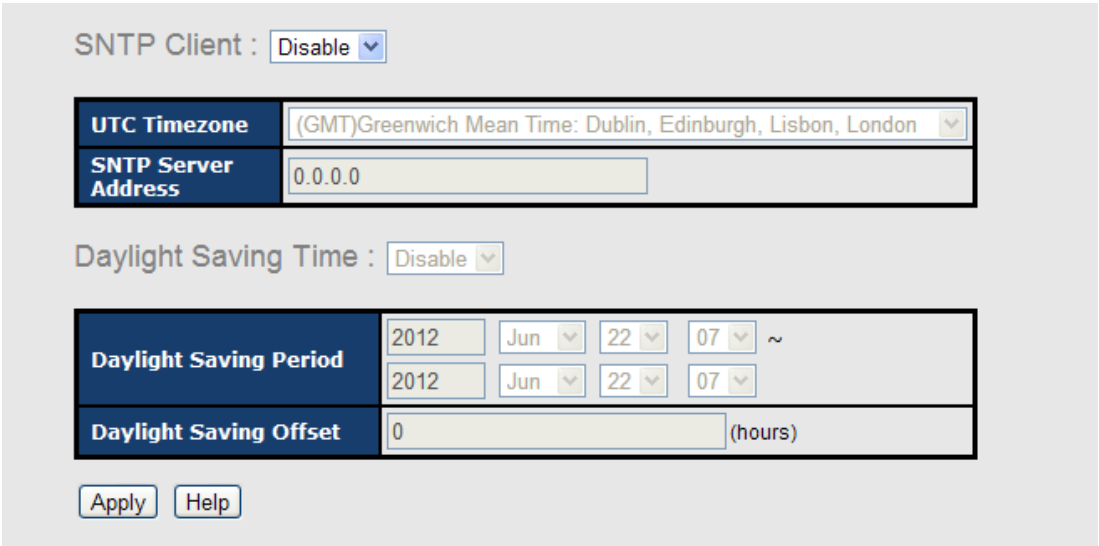
The system clock synchronizes the tasks in a computer, like loading data before manipulating it.



Label	Description
System Clock	Shows the current system time. The time stamp could be assigned manually configuration or automatically by a SNTP server.
System Date	Specifies the year, month and day of the system clock (YYYY/MM/DD). Year: 2006-2015. Month: Jan-Dec. Day:1-31(28)
System Time	Specify the hour, minute and second of the system clock (hh:mm:ss). Hour:0-24, Minute:0-59, Second:0-59

SNTP

SNTP (Simple Network Time Protocol) is a protocol able to synchronize the time on your system to the clock on the Internet. It will synchronize your computer system time with a server that has already been synchronized by a source such as a radio, satellite receiver or modem.



Label	Description

SNTP Client	Enables or disables SNTP function to retrieve the time from a SNTP server.
UTC Time zone	Selects the time zone for the switch according to its location
SNTP Sever Address	Enters the SNTP server IP address which you would like to use for time synchronization.
Daylight Saving Time	Enables or disables daylight saving time function. When it is enabled, you need to configure the daylight saving time period.
Daylight Saving Period	Configures the beginning and ending time for the daylight saving option. The values will vary each year.
Daylight Saving Offset	Configures the offset time.
Apply	Click to apply the changes

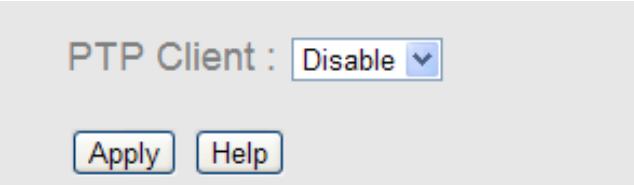
The following table lists different location time zones for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11 am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm

CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

PTP Client

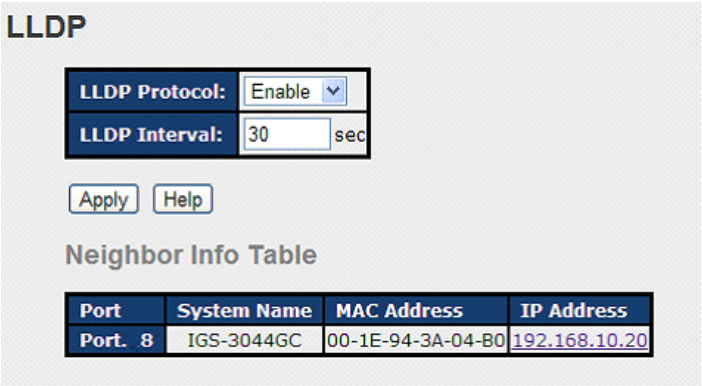
The Precision Time Protocol (PTP) is a time-transfer protocol defined in the IEEE 1588-2002 standard that allows precise synchronization of networks (e.g., Ethernet). Accuracy within the nanosecond range can be achieved with this protocol when using hardware generated timestamps.



Label	Description
PTP Client	Enables or disables PTP Client

1.1.6 LLDP

LLDP (Link Layer Discovery Protocol) provides a method for networked devices to receive and/or transmit their information to other connected devices on the network that are also using the protocols, and to store the information that is learned about other devices. This page allows you to examine and configure current LLDP port settings.

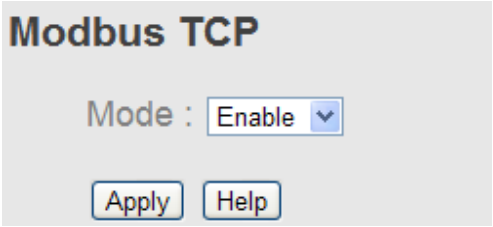


Label	Description
LLDP Protocol	Enables or disables LLDP function.
LLDP Interval	The interval of resending LLDP (30 seconds by default)

Apply	Click to apply the configurations.
Help	Shows help file.
Neighbor info table	Shows neighbor device info, including system name, MAC address, and IP address.

1.1.7 Modbus TCP

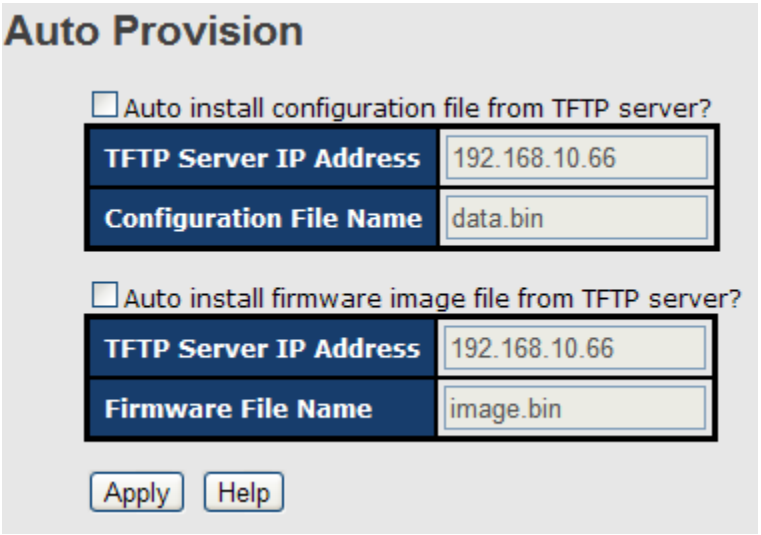
Modbus TCP uses TCP/IP and Ethernet to carry the data of the Modbus message structure between compatible devices. The protocol is commonly used in SCADA systems for communications between a human-machine interface (HMI) and programmable logic controllers. This page enables you to enable and disable Modbus TCP support of the switch.



Label	Description
Mode	Enables or disables Modbus TCP function

1.1.8 Auto Provision

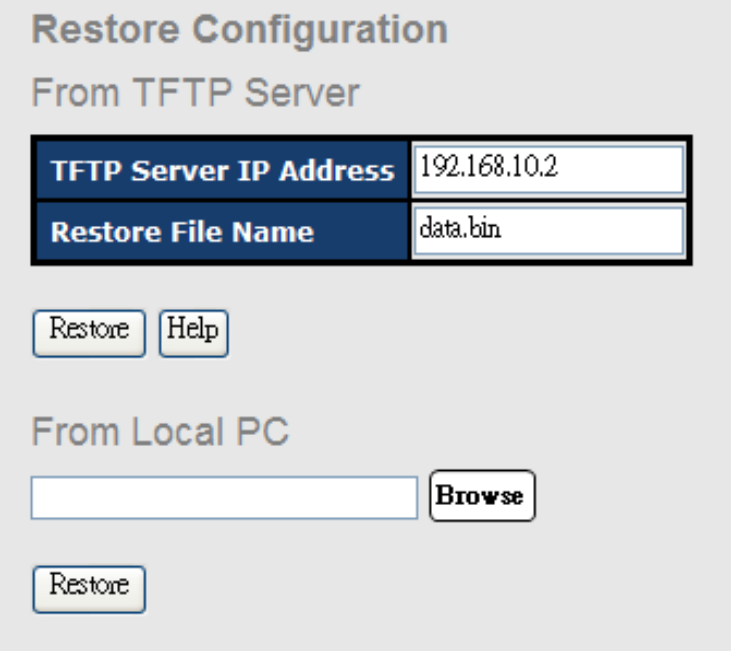
Auto Provision allows you to update switch firmware automatically. You can put the firmware or configuration file on a TFTP server. When you reboot the switch, it will upgrade firmware automatically. Before updating, make sure you have your TFTP server ready and the firmware image and configuration files are on the TFTP server.



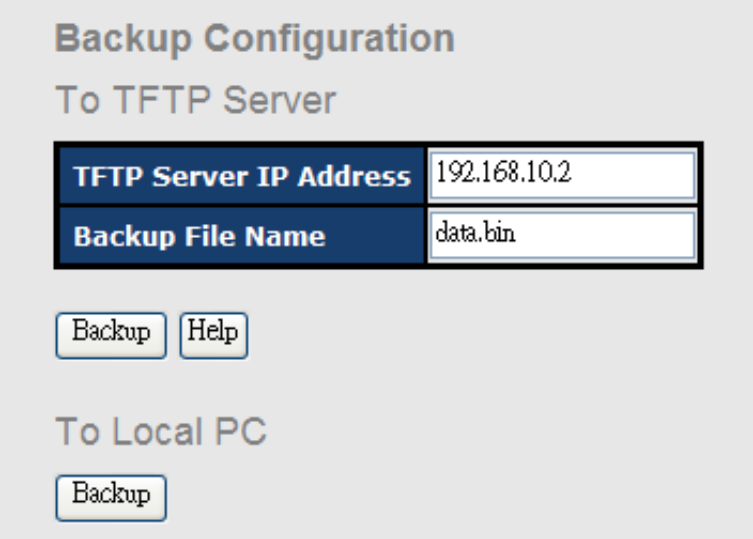
1.1.9 Backup & Restore

You can save current values from the switch to a TFTP server, and restore the switch to the settings by going to the TFTP restore configuration page.

The following page allows you to save the existing configurations as a backup file to a TFTP server.



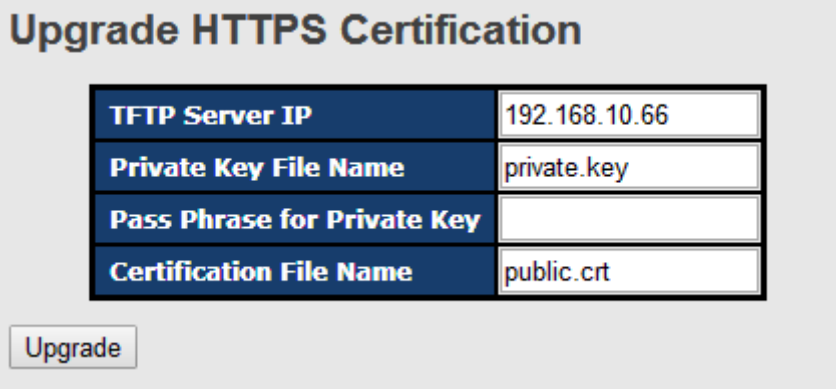
The following page allows you to restore the system to previous configurations from a TFTP server.



Label	Description
TFTP Server IP Address	The IP address of the FTFP where you put the configuration file or where you want to restore the switch to previous settings.
Backup File Name	The name of the configuration file you want to save as.
Restore File Name	The name of the configuration file you want to use for the switch.
Backup	Click to back up the configurations.
To Local PC	You can save the configuration file to your your PC instead of a TFTP server.
Restore	Click to restore the configurations.
Form Local PC	You can use the file stored on a local PC instead of from the TFTP server. Click **Browse** to locate the file you want to use for update, and then click **Restore**.

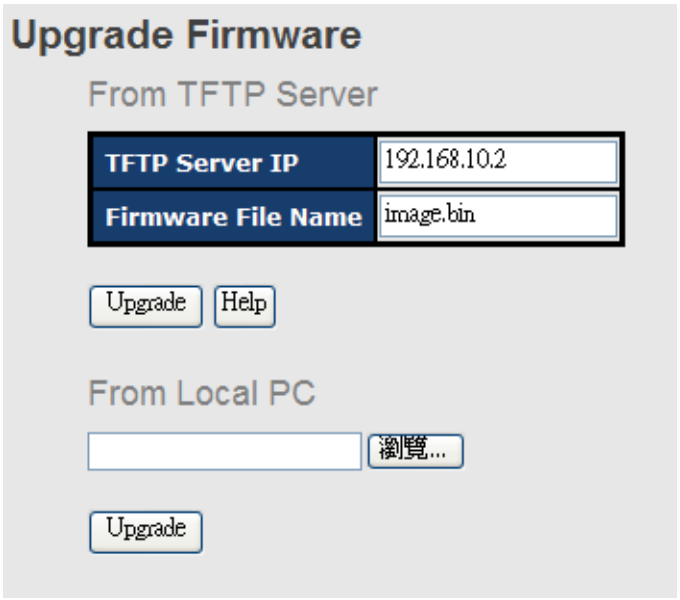
1.1.10 Upgrade HTTPS Certification

Upgrade HTTPS Certification allows user to update the switch HTTPS Certification file. Before updating, make sure you have your TFTP server ready and the Certification key file is on the TFTP server.



1.1.11 Upgrade Firmware

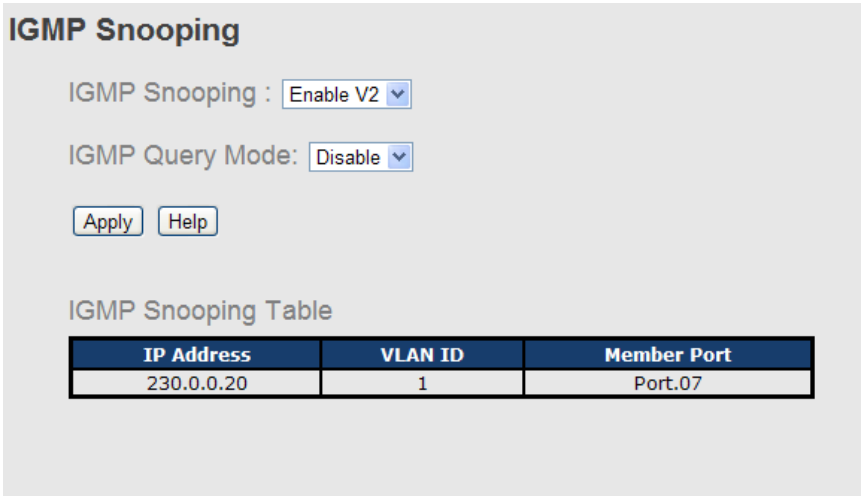
This page allows you to update the firmware of the switch. Before updating, make sure you have your TFTP server ready and the firmware file is on the TFTP server. Enter the IP address of the TFTP server you want to connect to and the firmware file name, and then click upgrade to start upgrading. You can also choose the firmware file form your PC.



2.1 Multicast

2.1.1 IGMP Snooping

IGMP (Internet Group Management Protocol) snooping monitors the IGMP traffic between hosts and multicast routers. The switch uses what IGMP snooping learns to forward multicast traffic only to interfaces that are connected to interested receivers. This conserves bandwidth by allowing the switch to send multicast traffic to only those interfaces that are connected to hosts that want to receive the traffic, instead of flooding the traffic to all interfaces in the VLAN. This page allows you to set up IGMP snooping configurations.

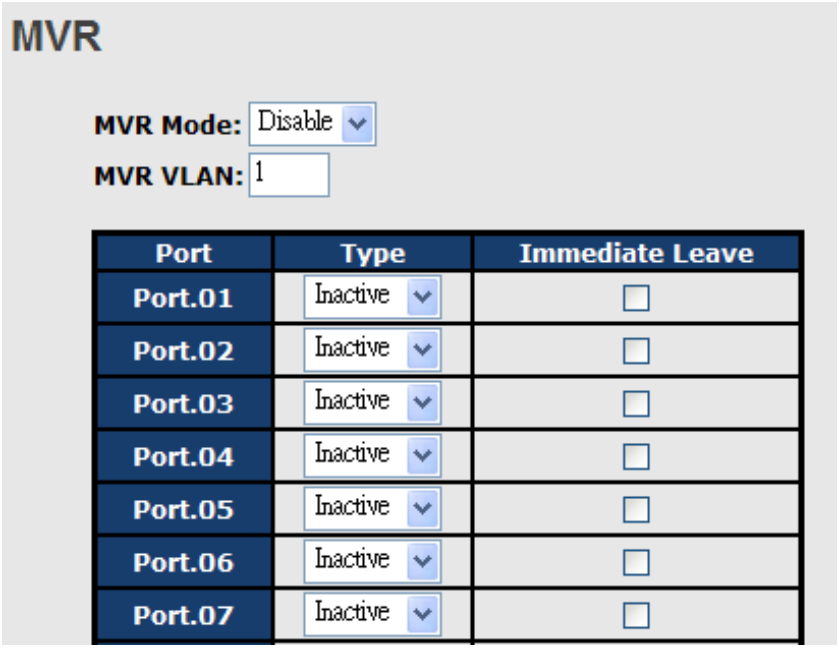


Label	Description
IGMP Snooping	Check to enable global IGMP snooping

IGMP Query Mode	Configures the switch to be the IGMP querier. Only one IGMP querier is allowed in an IGMP application. **Auto** will select the switch with the lowest IP address as the querier.
Apply	Click to apply the configurations.
Help	Shows help file.

2.1.2 MVR

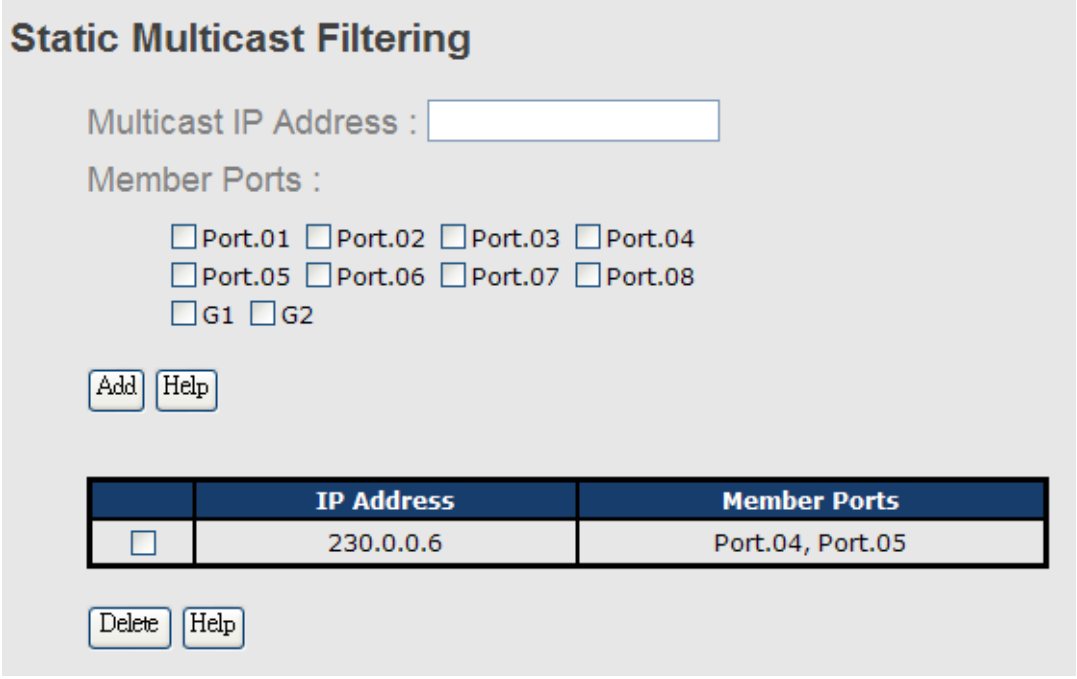
MVR (Multicast VLAN registration) enables hosts that are not part of a multicast VLAN to receive multicast streams from the multicast VLAN. As a result, the multicast VLAN can be shared across the network and there is no need to send duplicate multicast streams to each requesting VLAN in the network.



Label	Description
MVR Mode	Enables or disables MVR
MVR VLAN	The number of MVR VLANs
Type	Indicates the MVR type of the port. **Inactive** means the port is not participating in any MVR groups.
Immediate Leave	Check to enables immediate leave function. Immediate leave reduces the length of time it takes the switch to stop forwarding multicast traffic when the last member host on the interface leaves the group.

2.1.3 Static Multicast Filtering

Static multicast filtering provides a method for users to configure multicast group memberships manually. The function enables end devices to receive multicast traffic only if they register to join specific multicast groups. With static multicast filtering, network devices only forward multicast traffic to the ports connected to registered end devices. The function allows you to control the multicast traffic precisely.

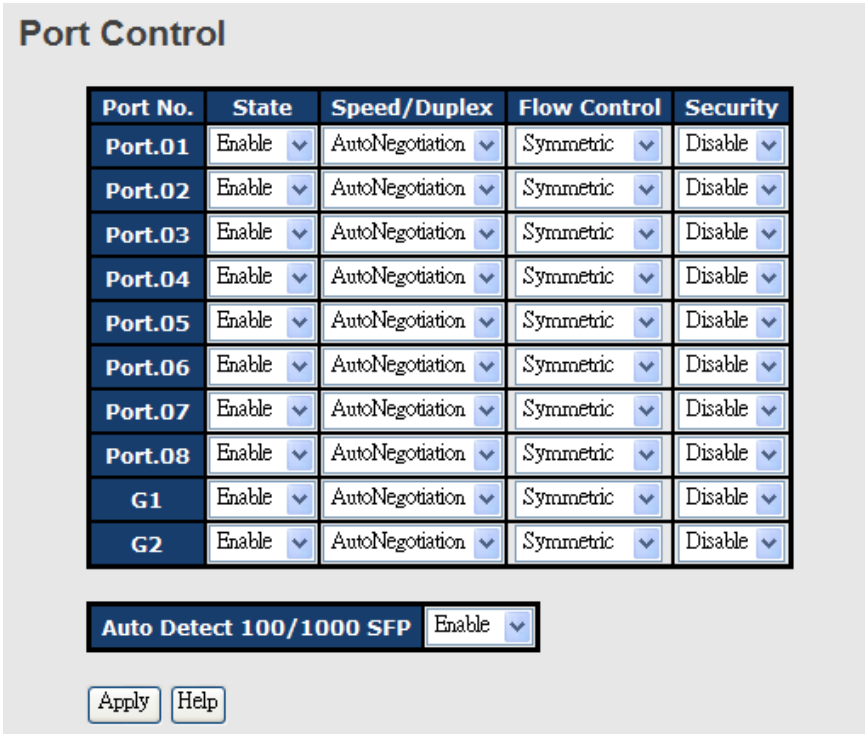


Label	Description
Multicast IP Address	Assigns a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255
Member Ports	Check the box next to the port number to include them as member ports in the specific multicast group.
Add	Click to add the ports to the IP multicast list
Delete	Deletes an entry from the table
Help	Shows help file.

2.1.4 Port Setting

Port Setting allows you to manage individual ports of the switch, including speed/duplex, flow control, and security.

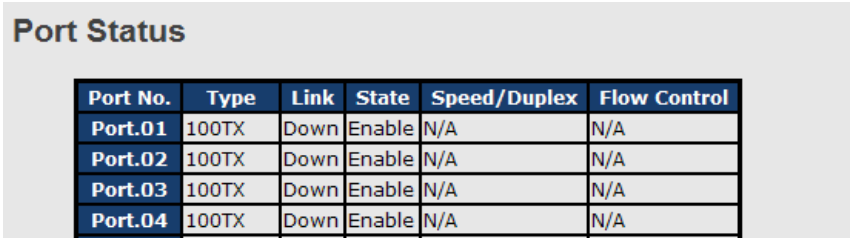
Port Control



Label	Description
Port NO.	The number of the port to be configured.
State	Enables or disables the port.
Speed/Duplex	Available values include **auto-negotiation**, **100-full**, **100-half**, **10-full**, or **10-half**
Flow Control	Supports symmetric and asymmetric modes to avoid packet loss when congestion occurs
Security	Enabling port security will disable MAC address learning in this port. Thus only the frames with MAC addresses in the port security list will be forwarded, otherwise will be discarded.
Auto Detect 100/1000	Automatically detects SFP port speed (100M / 1000M)
Apply	Click to apply the configurations

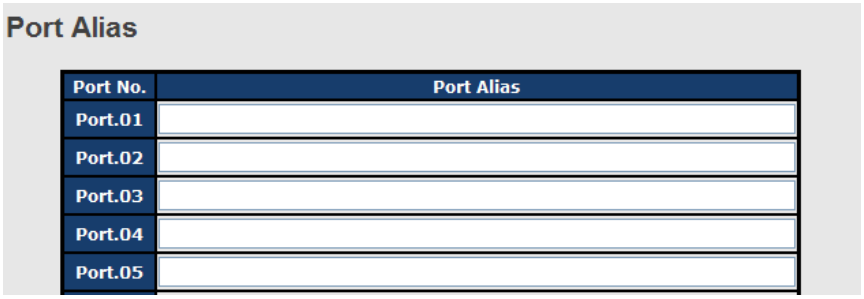
2.1.5 Port Status

This page shows the status of the each port in terms of its state, speed/duplex, and flow control.



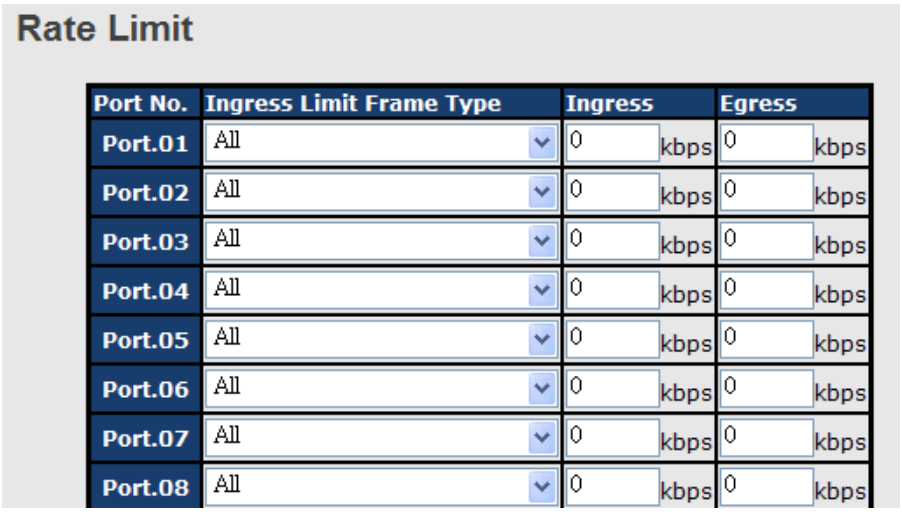
2.1.6 Port Alias

This page provides alias IP address configuration. Some devices might have more than one IP addresses. You could specify other IP addresses here.



2.1.7 Rate Limit

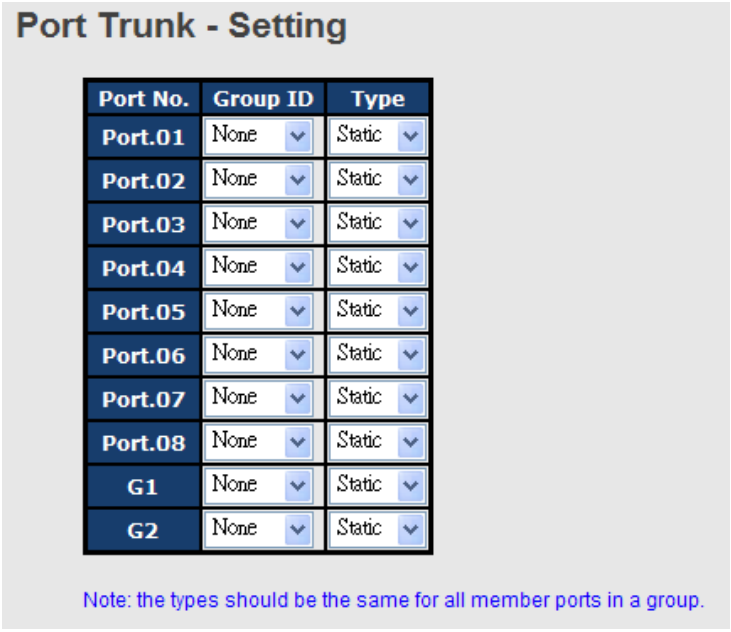
This page allows you to define the rate limits applied to a port, including incoming and outgoing traffic.

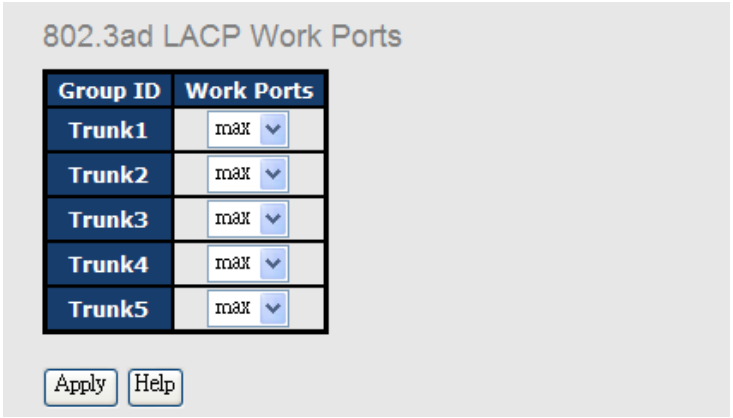


Label	Description
Ingress Limit Frame Type	Valid values include **All**, **Broadcast only**, **Broadcast/Multicast** and **Broadcast/Multicast/Flooded Unicast**.
Ingress	The transmission rate for incoming traffic
Egress	The transmission rate for outgoing traffic
Apply	Click to activate the configurations.

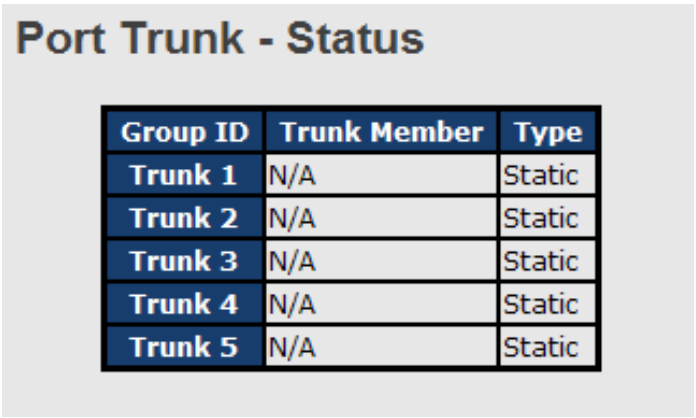
2.1.8 Port Trunking

A port trunk is a group of ports that have been grouped together to function as one logical path. This method provides an economical way for you to increase the bandwidth between the switch and another networking device. In addition, it is useful when a single physical link between the devices is insufficient to handle the traffic load. This page allows you to configure the aggregation hash mode and the aggregation group.





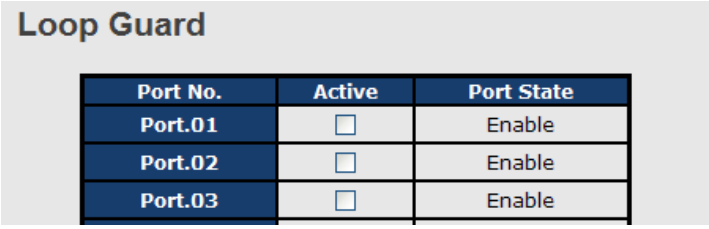
Label	Description
Group ID	Indicates the ID of each aggregation group. **None** means no aggregation. Only one group ID is valid per port.
Type	The switch supports two types of link aggregation; static and 802.3ad LACP. Static trunks are manually configured, while. LACP-configured ports will automatically negotiate a trunk with LACP-configured ports on another device.
Work Ports	The total number of active ports in a dynamic trunk group. The default value of works ports is **Max**. In a dynamic trunk group, if the number of work ports is lower than the number of members of the trunk group, the exceed ports are standby/redundant ports and can be aggregated if working ports fail. If it is a static trunk group, the number of work ports must equal the total number of group member ports.
Apply	Click to activate the configurations.



Label	Description
Group ID	Indicates the ID of each aggregation group. **None** means no aggregation. Only one group ID is valid per port.
Trunk Member	Lists members of a specific trunk group.
Type	Indicates the type of the port trunk

2.1.9 Loop Guard

This feature prevents loop attack. When receiving loop packets, the port will be disabled automatically, preventing the loop attack from affecting other network devices.



Label	Description
Active	Check to enable Loop Guard
Port Status	Indicates the enabled/disabled status of the port.

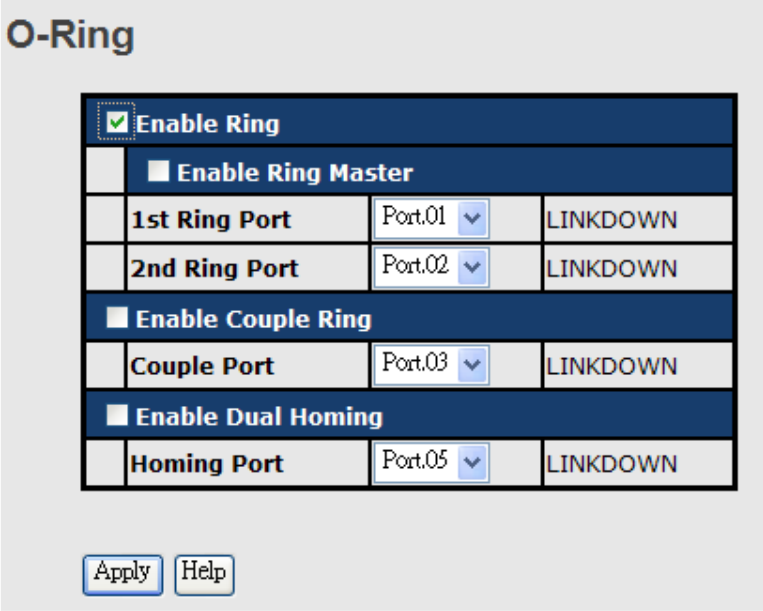
3.1 O-Ring

3.1.1 Introduction

O-Ring is ORing's proprietary redundant ring technology, with recovery time of less than 30 milliseconds (in full-duplex Gigabit operation) or 10 milliseconds (in full-duplex Fast Ethernet operation) and up to 250 nodes. The ring protocols identify one switch as the master of the network, and then automatically block packets from traveling through any of the network's redundant loops. In the event that one branch of the ring gets disconnected from the rest of the network, the protocol automatically readjusts the ring so that the part of the network that was disconnected can reestablish contact with the rest of the network. The O-Ring redundant ring technology can protect mission-critical applications from network interruptions or temporary malfunction with its fast recover technology.

3.1.2 Configurations

O-Ring supports three ring topologies: **Ring Master**, **Coupling Ring**, and **Dual Homing**. You can configure the settings in the interface below.



Label	Description
Enable Ring	Check to enable O-Ring topology.
Enable Ring Master	Only one ring master is allowed in a ring. However, if more than one switches are set to enable **Ring Master**, the switch with the lowest MAC address will be the active ring master and the others will be backup masters.
1st Ring Port	The primary port when the switch is ring master
2nd Ring Port	The backup port when the switch is ring master
Enable Coupling Ring	Check to enable **Coupling Ring**. **Coupling Ring** can divide a big ring into two smaller rings to avoid network topology changes affecting all switches. It is a good method for connecting two rings.
Couple Port	Ports for connecting multiple rings. A coupling ring needs four switches to build an active and a backup link. Links formed by the coupling ports will run in active/backup mode.
Enable Dual Homing	Check to enable **Dual Homing**. When **Dual Homing** is enabled, the ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work in active/backup mode, and connect each ring to the normal switches in RSTP mode.
Apply	Click to activate the configurations.

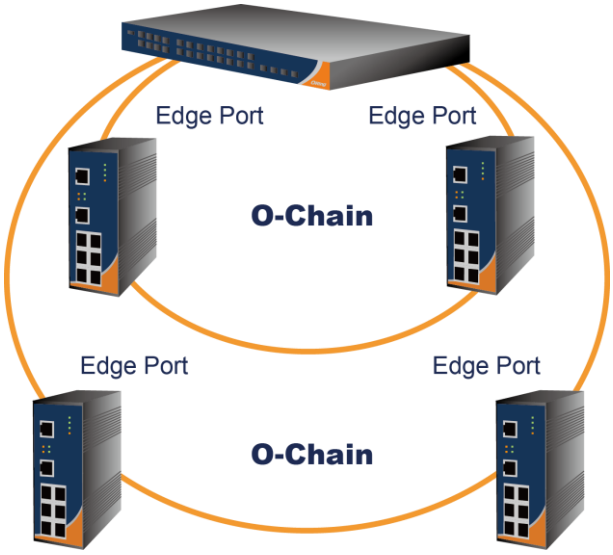
Note: due to heavy loading, setting one switch as ring master and coupling ring at the same time is not recommended.

3.2 O-Chain

3.2.1 Introduction

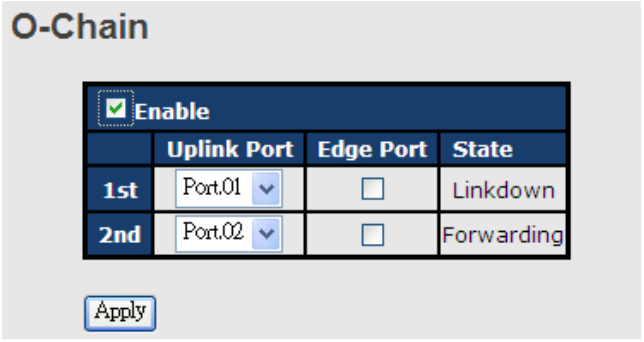
O-Chain is ORing's revolutionary network redundancy technology which enhances network redundancy for any backbone networks, providing ease-of-use and maximum fault-recovery swiftness, flexibility, compatibility, and cost-effectiveness in a set of network redundancy topologies. The self-healing Ethernet technology designed for distributed and complex industrial networks enables the network to recover in less than 30 milliseconds (in full-duplex Gigabit operation) or 10 milliseconds (in full-duplex Fast Ethernet operation) for up to 250 switches if at any time a segment of the chain fails.

O-Chain allows multiple redundant rings of different redundancy protocols to join and function together as a large and the most robust network topologies. It can create multiple redundant networks beyond the limitations of current redundant ring technologies.



3.2.2 Configurations

O-Chain is very easy to configure and manage. Only one edge port of the edge switch needs to be defined. Other switches beside them just need to have O-Chain enabled.



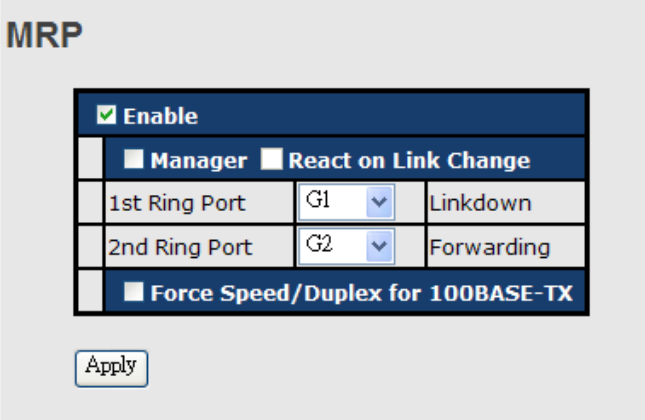
Label	Description
Enable	Check to enable O-Chain function
1st Ring Port	The first port connecting to the ring
2nd Ring Port	The second port connecting to the ring
Edge Port	An O-Chain topology must begin with edge ports. The ports with a smaller switch MAC address will serve as the backup link and RM LED will light up.

3.3 MRP

3.3.1 Introduction

MRP (Media Redundancy Protocol) is an industry standard for high-availability Ethernet networks. MRP allowing Ethernet switches in ring configuration to recover from failure rapidly to ensure seamless data transmission. A MRP ring (IEC 62439) can support up to 50 devices and will enable a back-up link in 80ms (adjustable to max. 200ms/500ms).

3.3.2 Configurations



Label	Description
Enable	Enables the MRP function
Manager	Every MRP topology needs a MRP manager. One MRP topology can only have a Manager. If two or more switches are set to be Manager, the MRP topology will fail.
React on Link Change (Advanced mode)	Faster mode. Enabling this function will cause MRP topology to converge more rapidly. This function only can be set in MRP manager switch.
1st Ring Port	Chooses the port which connects to the MRP ring
2nd Ring Port	Chooses the port which connects to the MRP ring

Force Speed / Duplex for 100BASE-TX	By default, this is in auto-negotiation mode. Enabling this function will automatically change the default to **Full** mode.(this function is used in combination with Hirschmann's switch as the MRP ring port speed/duplex of Hirschmann's switches are always in **Full** mode)

***NOTE: This function is by request and only available on "-MRP" model(s).**

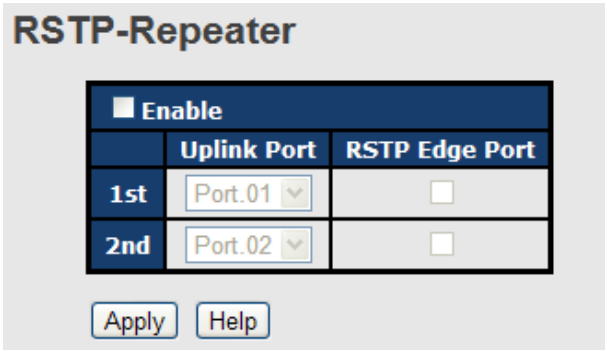
3.4 STP/RSTP/MSTP

3.4.1 STP/RSTP

STP (Spanning Tree Protocol), and its advanced versions RSTP (Rapid Spanning Tree Protocol) and MSTP (Multiple Spanning Tree Protocol), are designed to prevent network loops and provide network redundancy. Network loops occur frequently in large networks as when two or more paths run to the same destination, broadcast packets may get in to an infinite loop and hence causing congestion in the network. STP can identify the best path to the destination, and block all other paths. The blocked links will stay connected but inactive. When the best path fails, the blocked links will be activated. Compared to STP which recovers a link in 30 to 50 seconds, RSTP can shorten the time to 5 to 6 seconds. In other words, RSTP provides faster spanning tree convergence after a topology changes. The switch supports STP and will auto detect the connected device running on STP or RSTP protocols.

RSTP Repeater

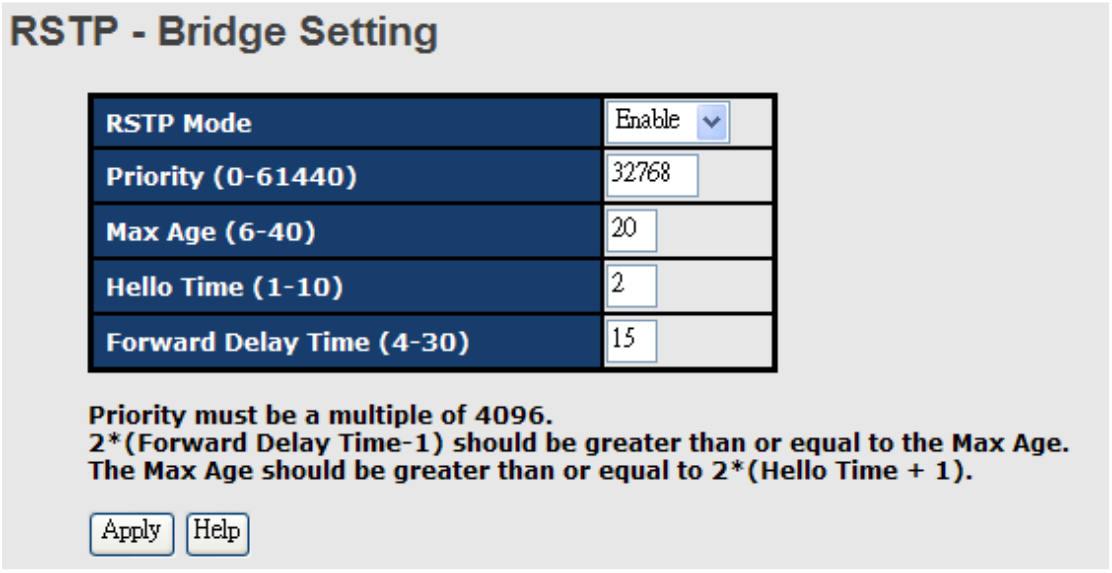
A repeater can pass a BPDU packet directly from one RSTP device to another as if the two devices are connected.



Label	Description
Enable	Check to enable RSTP Repeater
1st Ring Port	The first port connecting to the RSTP network
2nd Ring Port	The second port connecting to the RSTP network

Edge Port	Only the edge device (connected to RSTP device) needs to specify edge port. The user must specify the edge port according to topology of network.

RSTP Bridge Setting

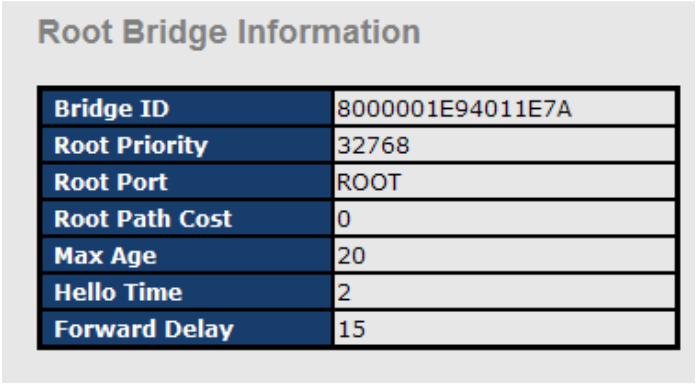


Label	Description
RSTP mode	You must enable or disable RSTP function before configuring the related parameters.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, you must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule
Max Age Time(6-40)	The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. The valid value is between 6 through 40.
Hello Time (1-10)	The time interval a switch sends out the BPDU packet to check RSTP current status. The time is measured in seconds and the valid value is between 1 through 10.
Forwarding Delay Time (4-30)	The time of a port waits before changing from RSTP learning and listening states to forwarding state. The valid value is between 4 through 30.
Apply	Click to apply the configurations.

NOTE: the calculation of the MAX Age, Hello Time, and Forward Delay Time is as follows:

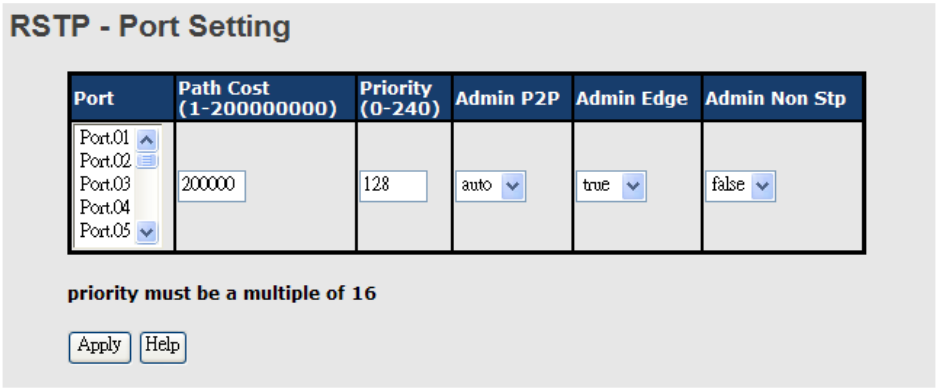
2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)

The following pages show the information of the root bridge, including its port status.



Root Bridge Information

Bridge ID	8000001E94011E7A
Root Priority	32768
Root Port	ROOT
Root Path Cost	0
Max Age	20
Hello Time	2
Forward Delay	15

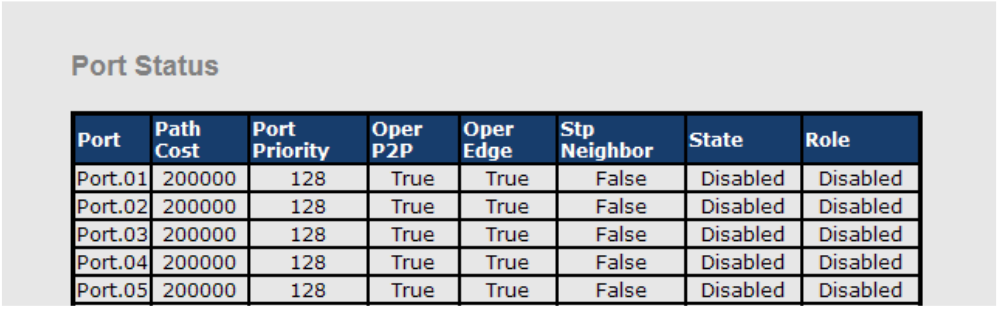


RSTP - Port Setting

Port	Path Cost (1-200000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non Stp
Port.01 Port.02 Port.03 Port.04 Port.05	200000	128	auto	true	false

priority must be a multiple of 16

Apply Help



Port Status

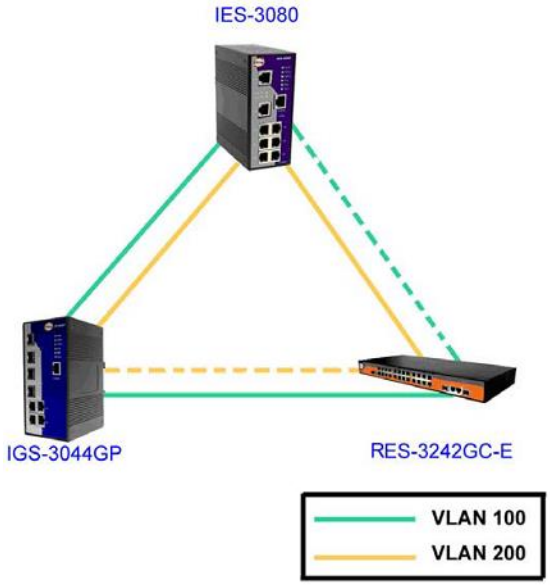
Port	Path Cost	Port Priority	Oper P2P	Oper Edge	Stp Neighbor	State	Role
Port.01	200000	128	True	True	False	Disabled	Disabled
Port.02	200000	128	True	True	False	Disabled	Disabled
Port.03	200000	128	True	True	False	Disabled	Disabled
Port.04	200000	128	True	True	False	Disabled	Disabled
Port.05	200000	128	True	True	False	Disabled	Disabled

Label	Description
Path Cost (1-200000000)	The path cost incurred by the port. The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. The range of valid values is 1 to 200000000.
Port Priority (0-240)	Decide which port should be blocked by priority in the LAN. The

	valid value is between 0 and 240, and must be a multiple of 16
Oper P2P	Configures the port connects to a point-to-point LAN rather than a shared medium. This can be configured automatically or set to true or false manually. True means P2P enabling. False means P2P disabling. Transiting to forwarding state is faster for point-to-point LANs than for shared media.
Oper Edge	A flag indicating whether the port is connected directly to edge devices or not (no bridges attached). Transiting to the forwarding state is faster for edge ports (operEdge set to true) than other ports.
STP Neighbor	The port uses mathematical calculations according to STP. **True** means not included in mathematical calculations, and **False** means contained in mathematical calculations according to STP.
State	Determines the STP state of the port
Role	When enabled, the port will not be selected as root port for CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an alternate port after the root port has been selected. If set, spanning trees will lose connectivity. It can be set by a network administrator to prevent bridges outside a core region of the network from influencing the active spanning tree topology because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
Apply	Click to apply the configurations.

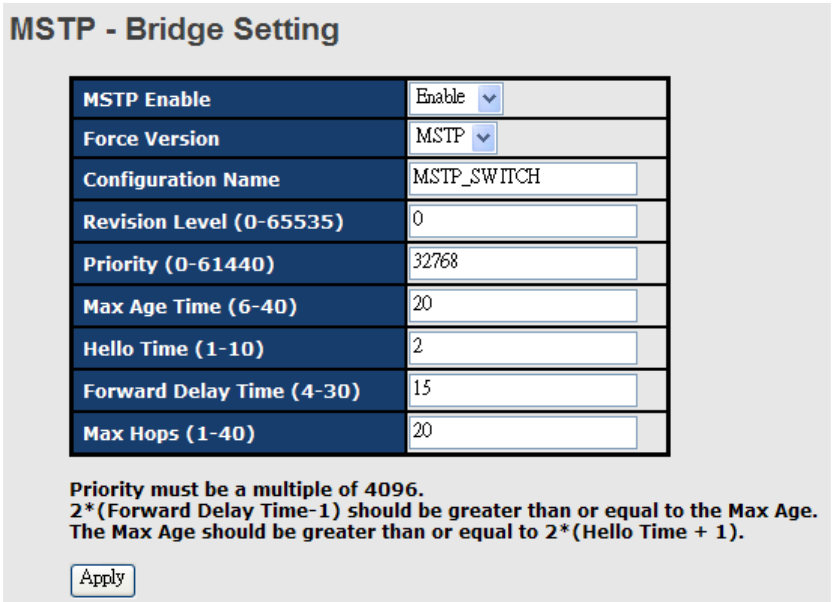
3.4.2 MSTP

Since the recovery time of STP and RSTP takes seconds, which is unacceptable in industrial applications, MSTP was developed. The technology supports multiple spanning trees within a network by grouping and mapping multiple VLANs into different spanning-tree instances, known as MSTIs, to form individual MST regions. Each switch is assigned to an MST region. Hence, each MST region consists of one or more MSTP switches with the same VLANs, at least one MST instance, and the same MST region name. Therefore, switches can use different paths in the network to effectively balance loads.



Bridge Settings

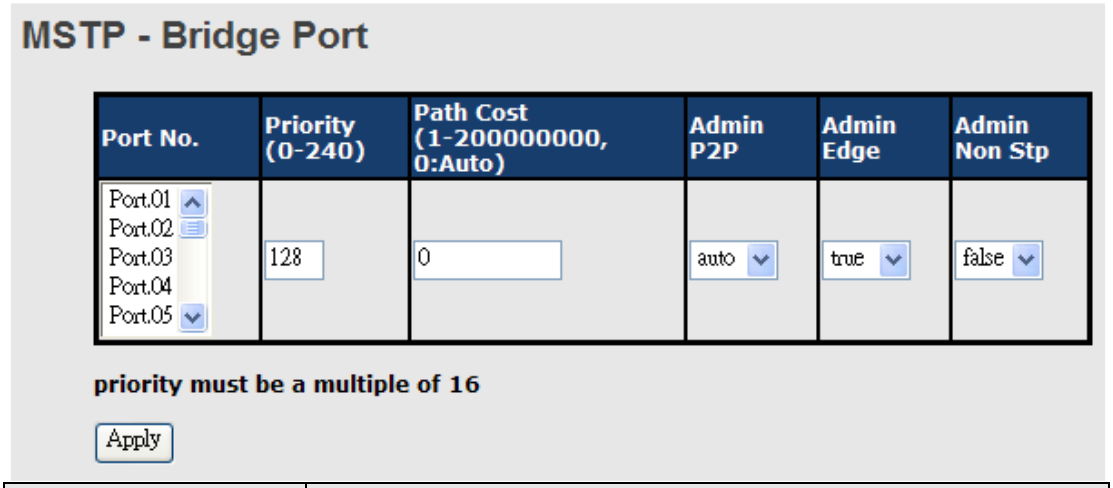
This page allows you to examine and change the configurations of current MSTI ports. A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must be selected before MSTI port configuration options are displayed.



Label	Description
MSTP Enable	Enables or disables MSTP function.
Force Version	Forces a VLAN bridge that supports RSTP to operate in an STP-compatible manner.

Configuration Name	The name which identifies the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configurations in order to share spanning trees for MSTIs (intra-region). The name should not exceed 32 characters.
Revision Level (0-65535)	Revision of the MSTI configuration named above. This must be an integer between 0 and 65535.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, you must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.
Max Age Time(6-40)	The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. The valid value is between 6 through 40.
Hello Time (1-10)	The time interval a switch sends out the BPDU packet to check RSTP current status. The time is measured in seconds and the valid value is between 1 through 10.
Forwarding Delay Time (4-30)	The time of a port waits before changing from RSTP learning and listening states to forwarding state. The valid value is between 4 through 30.
Max Hops (1-40)	An additional parameter for those specified for RSTP. A single value applies to all STP within an MST region (the CIST and all MSTIs) for which the bridge is the regional root.
Apply	Click to apply the configurations.

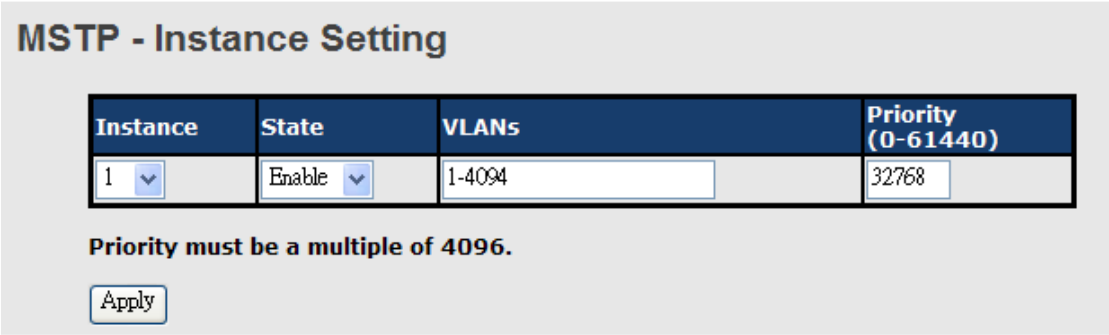
Bridge Port



Label	Description
Port No.	The number of port you want to configure
Priority (0-240)	Decide which port should be blocked by priority in the LAN. The valid value is between 0 and 240, and must be a multiple of 16.
Path Cost (1-200000000)	The path cost incurred by the port. The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. The range of valid values is 1 to 200000000.
Admin P2P	Configures whether the port connects to a point-to-point LAN rather than a shared medium. This can be configured automatically or set to true or false manually. True means P2P enabling. False means P2P disabling. Transiting to forwarding state is faster for point-to-point LANs than for shared media.
Admin Edge	Specify whether this port is an edge port or a nonedge port. An edge port is not connected to any other bridge. Only edge ports and point-to-point links can rapidly transition to forwarding state. To configure the port as an edge port, set the port to True.
Admin Non STP	The port includes the STP mathematic calculation. True is not including STP mathematic calculation, false is including the STP mathematic calculation.
Apply	Click to apply the configurations.

Instance Setting

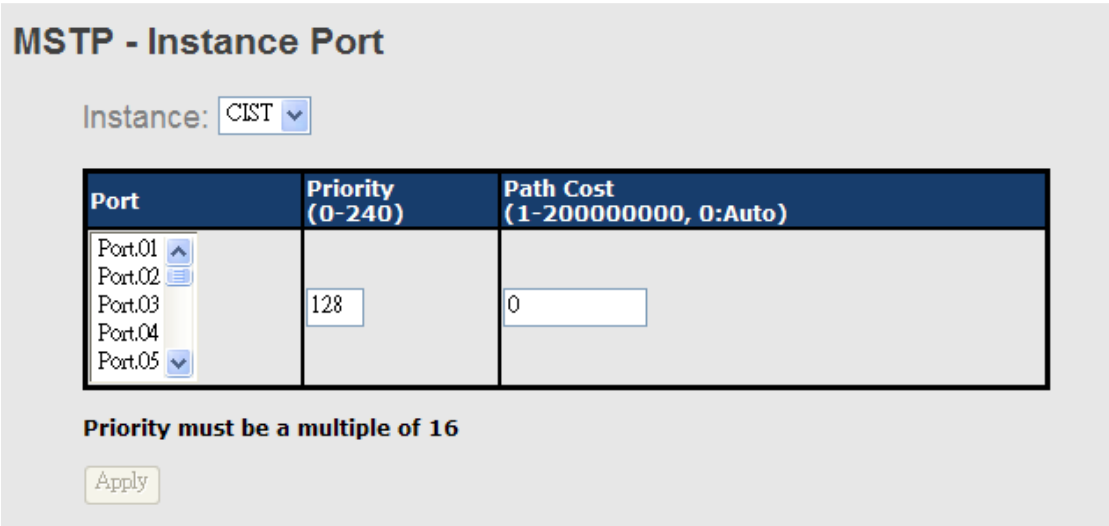
This page allows you to change the configurations of current MSTI bridge instance.



Label	Description
Instance	Set the instance from 1 to 15
State	Enables or disables the instance
VLANs	The VLAN which is mapped to the MSTI. A VLAN can only be mapped to one MSTI. An unused MSTI will be left empty (ex. without any mapped VLANs).
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, you must reboot the switch. The value must be a multiple of 4096 according to the protocol standard
Apply	Click to apply the configurations.

Port Priority

This page allows you to change the configurations of current MSTI bridge instance priority.

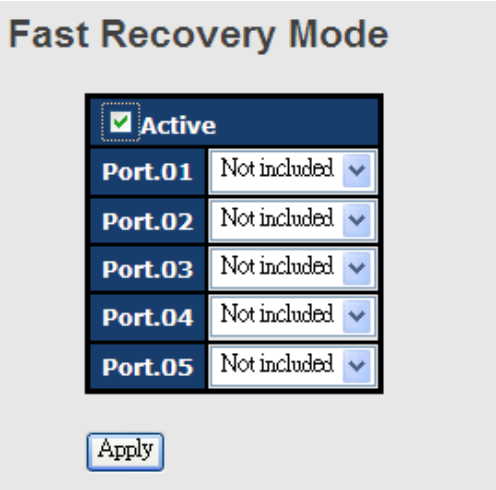


Label	Description
Instance	The bridge instance. CIST is the default instance, which is always

	active.
Port	The port number which you want to configure.
Priority (0-240)	Decides the priority of ports to be blocked in the LAN. The valid value is between 0 and 240, and must be a multiple of 16
Path Cost (1-200000000)	The path cost incurred by the port. The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. The range of valid values is 1 to 200000000.
Apply	Click to apply the configurations.

3.5 Fast Recovery

Fast recovery mode can be set to connect multiple ports to one or more switches, thereby providing redundant links. Fast recovery mode supports 5 priorities. Only the first priority will be the active port, and the other ports with different priorities will be backup ports.

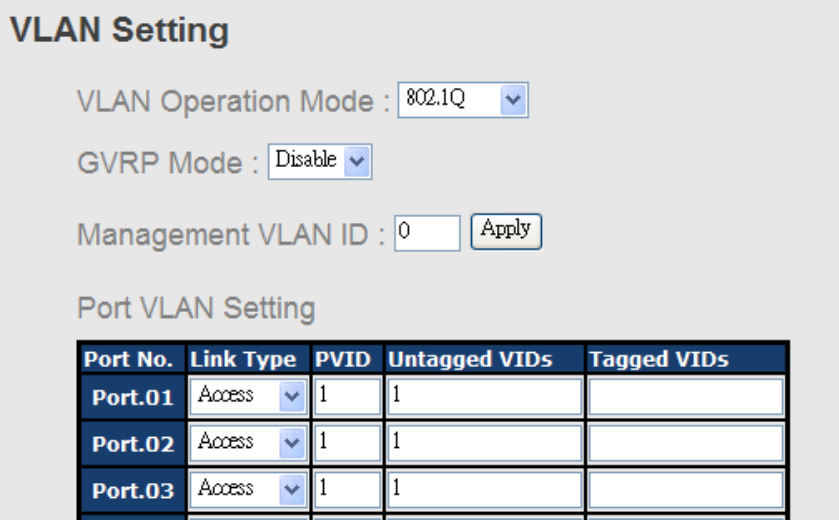


Label	Description
Active	Activate fast recovery mode
Port.01 - 05	Ports can be set to 5 priorities. Only the port with the highest priority will be the active port. 1st Priority is the highest.
Apply	Click to activate the configurations.

3.6 VLAN

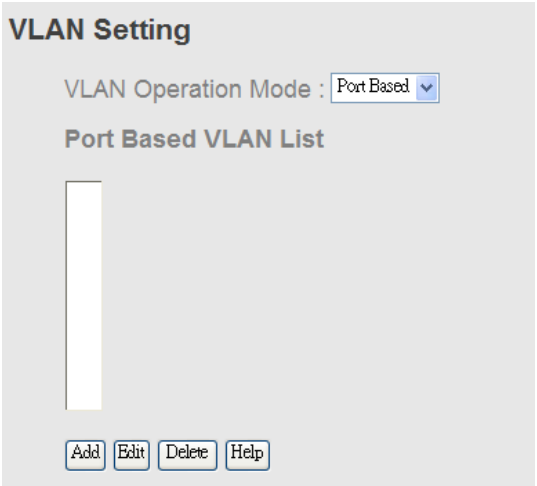
3.6.1 VLAN Setting - IEEE 802.1Q

A VLAN (Virtual LAN) is a logical LAN based on a physical LAN with links that does not consist of a physical (wired or wireless) connection between two computing devices but is implemented using methods of network virtualization. A VLAN can be created by partitioning a physical LAN into multiple logical LANs using a VLAN ID. You can assign switch ports to a VLAN and add new VLANs in this page.

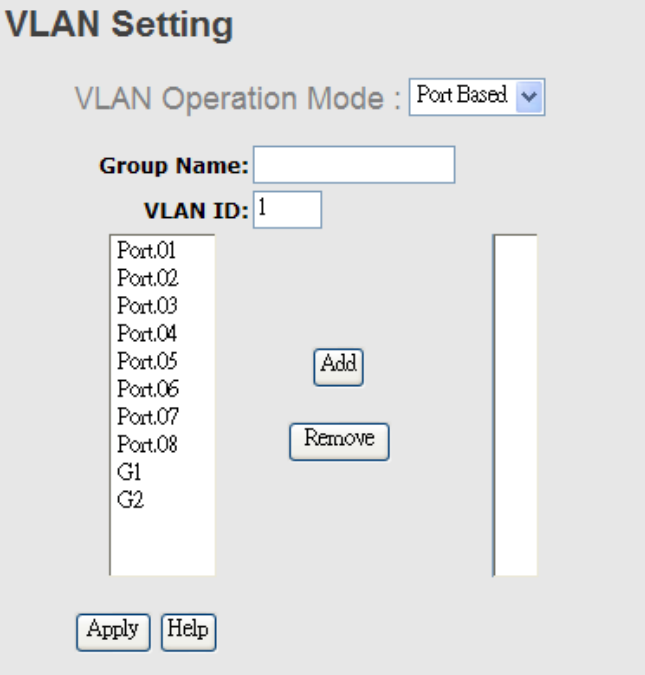


Label	Description
VLAN Operation Mode	Available options include **Disable**, **Port Base**, and **802.1Q**
GVRP Mode	GVRP is a GARP application that provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. With GVRP, the switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 802.1Q trunk ports.
Management VLAN ID	The VLAN ID for the entry.
Link type	Three link types are available: **Access Link**: An access link connects a VLAN-unaware device to the port of a VLAN-aware bridge. All frames on access links must e implicitly tagged (untagged).

	Trunk Link: All the devices connected to a trnk link, including workstations, must be VLAN-aware. All frames on a trunk linke must have a special header attached. **Hybrid Link**: The combination of Access Link and Trunk Link. This is a link where both VLAN-aware and VLAN-unaware devices are attached. It can have both tagged and untagged frames, but all the frames for a specific VLAN must be either tagged or untagged. **Hybrid(QinQ) Link**: Allows one more VLAN tag in an original VLAN frame.
Untagged VID	Set the port default VLAN ID for untagged devices that connect to the port. The range is 1 to 4094.
Tagged VIDs	Set the tagged VIDs to carry different VLAN frames to other switch.
Apply	Click to set the configurations.



Label	Description
VLAN Operation Mode	Available options include **Disable**, **Port Base**, and **802.1Q**
Add	Click to start adding a VLAN
Edit	Edits existing VLANs
Delete	Deletes existing VLANs
Help	Shows help file.



Label	Description
VLAN Operation Mode	Available options include **Disable**, **Port Base**, and **802.1Q**
Group Name	The name of the VLAN that you want to change settings.
VLAN ID	The number of the VLAN
Add	Select ports from the left column and clicks **Add** to include them to the VLAN group
Remove	Remove ports from the VLAN group
Apply	Click to apply the configurations
Help	Shows help file.

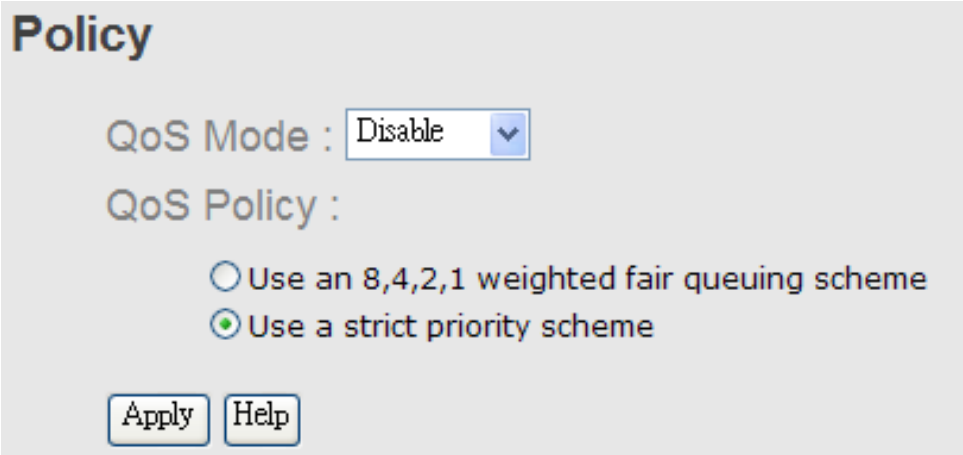
3.7 Traffic Prioritization

With traffic prioritization schemes, the switch can transmit data based on its importance, thereby ensuring mission-critical applications, such as VoIP and video teleconferencing, have sufficient bandwidth for transmission when the network is congested.

QoS (Quality of Service) is a method to achieve efficient bandwidth utilization between devices by prioritizing frames according to individual requirements and transmit the frames based on their importance. Frames in higher priority queues receive a bigger slice of bandwidth than those in a lower priority queue.

3.7.1 QoS Policy

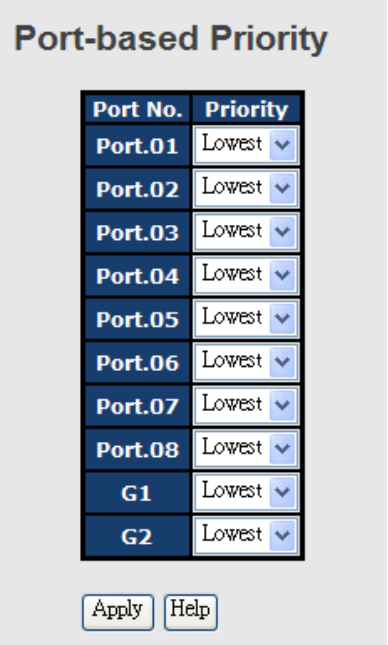
Policing is a traffic regulation mechanism for limiting the rate of traffic streams, thereby controlling the maximum rate of traffic sent or received on an interface. When the traffic rate exceeds the configured maximum rate, policing drops or remarks the excess traffic. This page allows you to configure QoS policies for the switch.



Label	Description
QOS Mode	Available modes include: **Disable**: disables the mode **Port-base**: the output priority is determined by ingress port. **COS only**: the output priority is determined by COS only. **TOS only**: the output priority is determined by TOS only. **COS first**: the output priority is determined by COS and TOS, but COS first. **TOS first**: the output priority is determined by COS and TOS, but TOS first.
QOS policy	**Using the 8,4,2,1 weight fair queue scheme**: the output queues will use an 8:4:2:1 ratio to transmit packets from the highest to lowest queue. For example: 8 high queue packets, 4 middle queue packets, 2 low queue packets, and the one lowest queue packets are transmitted in one turn. **Use the strict priority schem**e: when traffic arrives at the device, traffic on the highest priority queue will be transmitted first, followed by traffic on lower priorities. If there is always some content in the highest priority queue, then the other packets in the rest of queues will not be sent until the highest priority queue is

	empty.
Apply	Click to apply the configurations
Help	Shows help file.

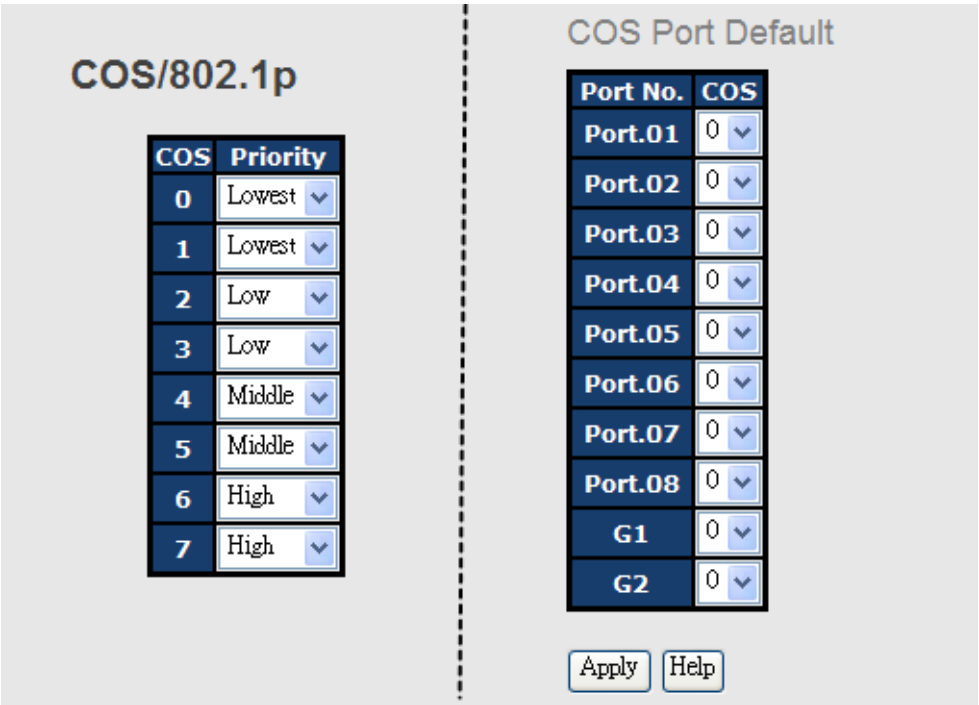
3.7.2 Port-base Priority



Label	Description
Priority	Assigns a port to a priority queue. Four priority queues are available: **High**, **Middle**, **Low**, and **Lowest**.
Apply	Click to apply the configurations
Help	Shows help file.

3.7.3 COS/802.1p

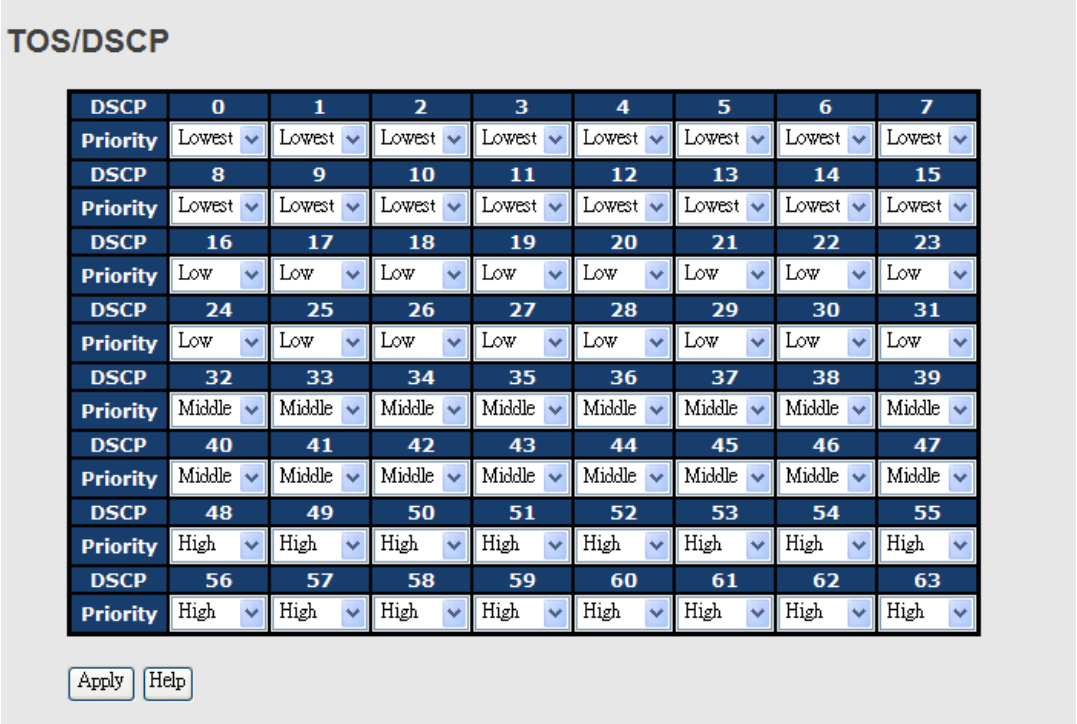
COS (Class of Service), also known as 802.1p, is a parameter for differentiating the types of payloads contained in the packet to be transmitted. CoS operates only on 802.1Q VLAN Ethernet at Layer 2, while other QoS mechanisms operate at the Layer 3or use a local QoS tagging system that does not modify the actual packet. COS supports up to 7 priorities and 4 priority queues: High, Middle, Low, and Lowest. When an ingress packet has no VLAN tag, the default priority value will be used.



Label	Description
Priority	Assigns a port to a priority queue. Four priority queues are available: **High**, **Middle**, **Low**, and **Lowest**.
Apply	Click to apply the configurations
Help	Shows help file.

3.7.4 TOS/DSCP

TOS (Type of Service) is a field in the IP header of a packet. It is used by Differentiated Services and is called the DSCP (Differentiated Services Code Point). The output priority of a packet can be determined by this field and the supported priority value ranges from 0 to 63. DSCP supports four priority queues: High, Middle, Low, and Lowest.



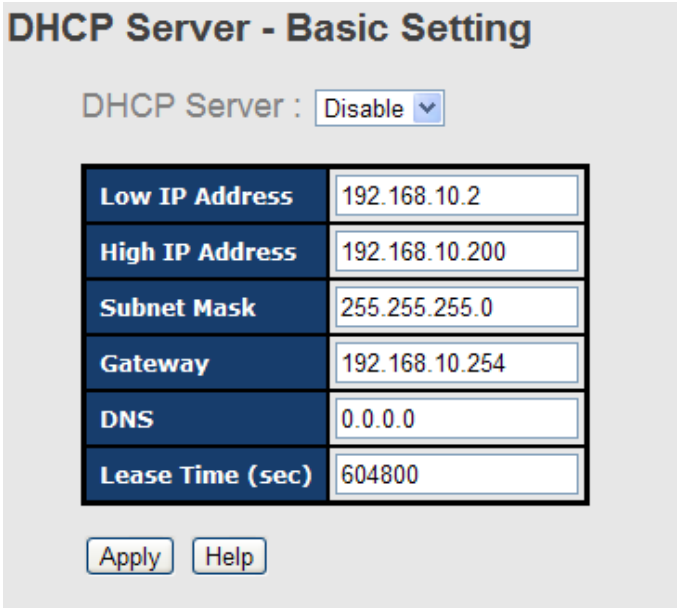
Label	Description
Priority	Assigns a port to a priority queue. Four priority queues are available: **High**, **Middle**, **Low**, and **Lowest**.
Apply	Click to apply the configurations
Help	Shows help file.

3.8 DHCP Server

The switch provides DHCP server functions. By enabling DHCP, the switch will become a DHCP server and dynamically assigns IP addresses and related IP information to network clients.

3.8.1 Basic Setting

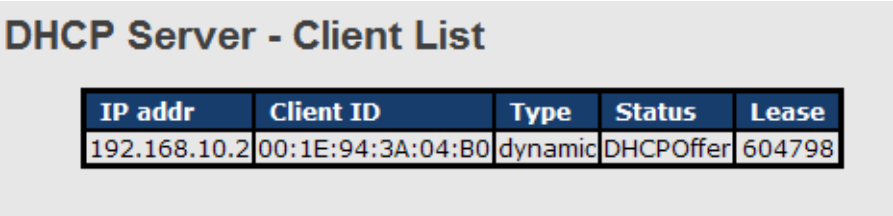
This page allows you to set up DHCP settings for the switch. You can check the **Enabled** checkbox to activate the function. Once the box is checked, you will be able to input information in each column.



Label	Description
DHCP Server	Enables or disables DHCP server function. When enabled, the switch will become the DHCP server on your local network.
Low IP Address	The beginning of the dynamic IP address range. The lowest IP address in the range is considered the start IP address. For example, if the range is from 192.168.1.100 to 192.168.1.200, 192.168.1.100 will be the start IP address.
High IP Address	The end of the dynamic IP address range. The highest IP address in the range is considered the end IP address. For example, if the range is from 192.168.1.100 to 192.168.1.200, 192.168.1.200 will be the end IP address
Subnet Mask	The subnet mask for the dynamic IP assign range
Gateway	The gateway of your network
DNS	The DNS IP of your network
Lease Time (sec)	The length of time that the client may use the IP address it has been assigned. The time is measured in seconds.
Apply	Click to apply the configurations

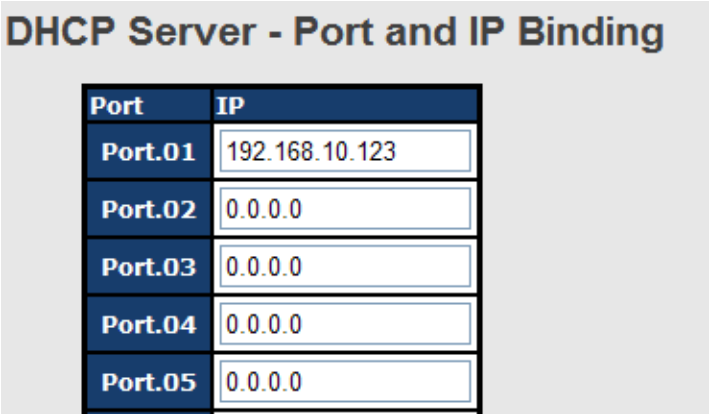
3.8.2 Client List

When DHCP server functions are activated, the switch will collect DHCP client information and display it in the following table.



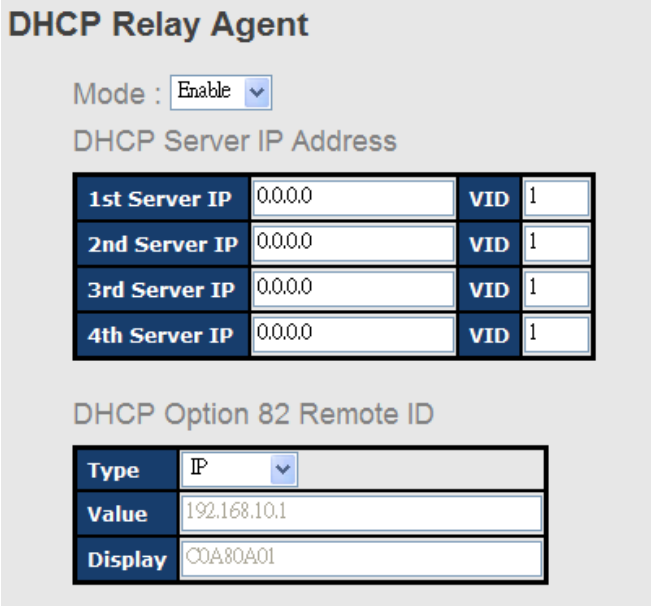
3.8.3 Port and IP Bindings

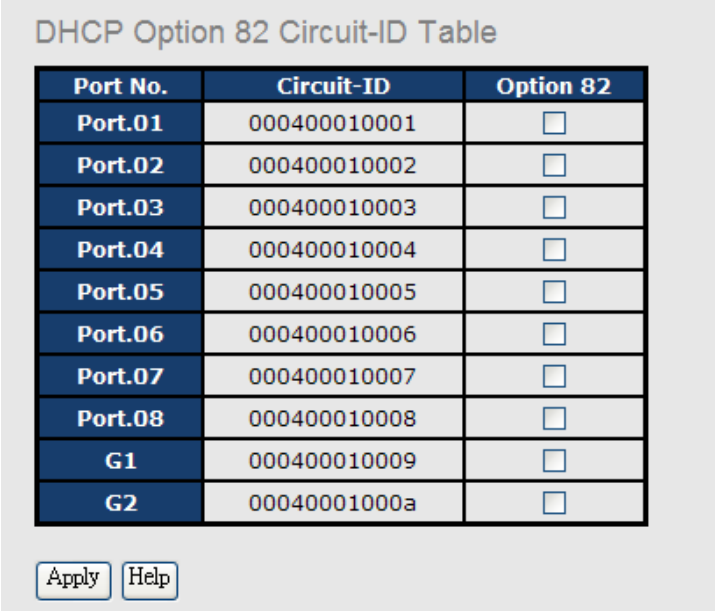
You can assign a specific IP address within the dynamic IP range to a specific port. When a device is connected to the port and requests for dynamic IP assigning, the switch will assign the IP address that has previously been assigned to the connected device.



3.8.4 Relay Agent

DHCP relay is used to forward and transfer DHCP messages between the clients and the server when they are not in the same subnet domain. You can configure the function in this page.





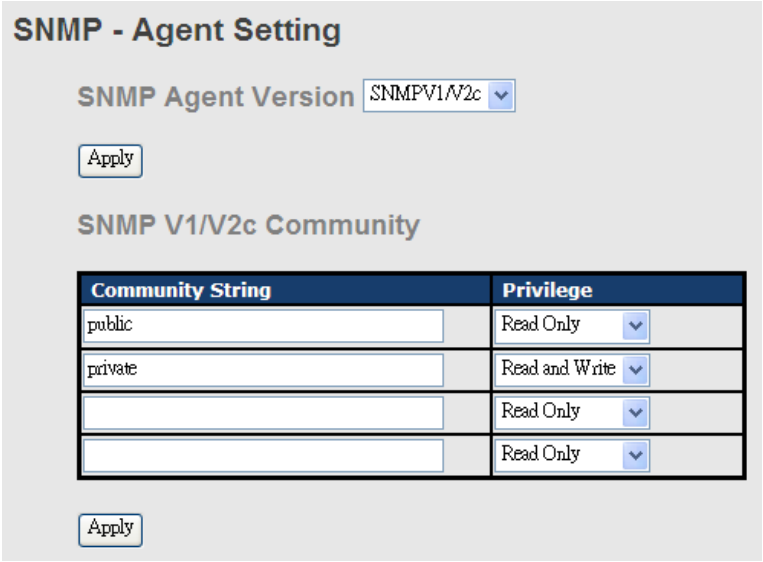
Label	Description
DHCP Relay	Enables or disables DHCP relay agent
DHCP Server IP Address and VID	Specify the IP address and VID of the DHCP server. **0.0.0.0** means the server is inactive.
DHCP Option 82 Remote ID	Provides an identifier for the remote server. Four types of IDs are supported: **IP**, **MAC**, **Client-ID**, and **Other**.
DHCP Option 82 Circuit-ID Table	Encodes an agent-local identifier of the circuit from which a DHCP client-to-server packet is received. It is intended for use by agents in relaying DHCP responses back to the proper circuit.
Apply	Click to apply the configurations

3.9 SNMP

SNMP (Simple Network Management Protocol) is a protocol for managing devices on IP networks. It is mainly used network management systems to monitor the operational status of networked devices. In an event-triggered situation, traps and notifications will be sent to administrators.

3.9.1 Agent Setting

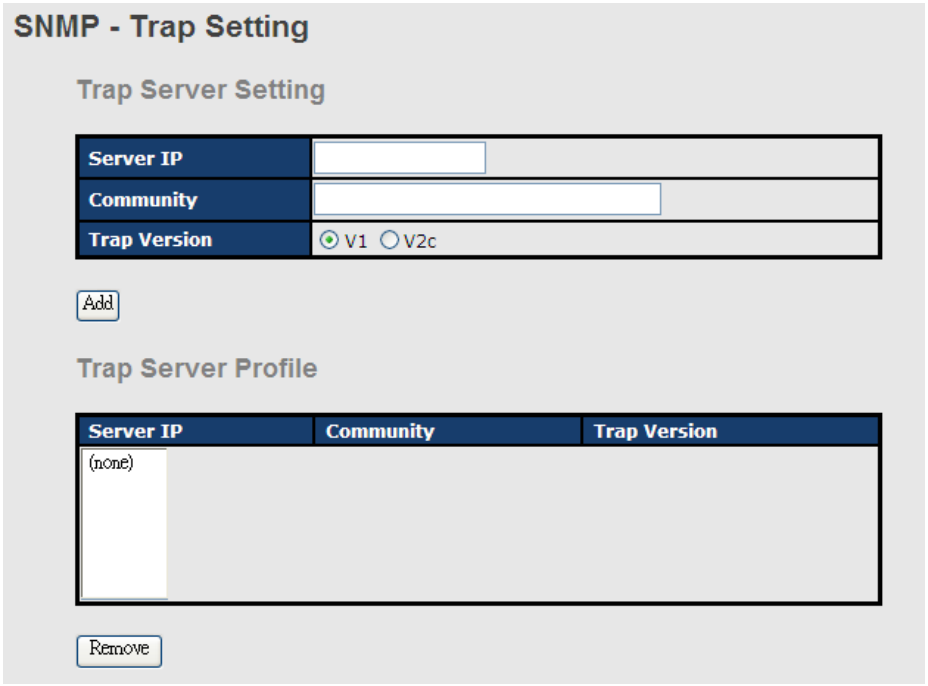
An SNMP agent will receive and process requests, send responses to the manager, and send traps when an event occurs. The following page allows you to configure the SNMP agent for the switch.



Label	Description
SNMP Agent Version	The column shows the version of the SNMP agent used by the switch. Three SNMP versions are supported, including **SNMP V1**, **SNMP V2c**, and **SNMP V3**. SNMP V1/SNMP V2c agents use a community string to authenticate the SNMP management station and SNMP agent. SNMP V3 requires MD5 or DES authentication which will encrypt data for higher data security.
Community String	The default community string that provides monitoring or read capability is often **public**. The default management or write community string is often **private**. Do not leave the community string to public on any of your SNMP agents. Since anyone with SNMP manager software installed on his/her PC can make changes to your SNMP agents, this will expose your SNMP agent to any SNMP management station.
Privilege	Choose the appropriate access level from the dropdown list. **Read Only**: The community string can only read the values of MIB objects. **Write Only**: The community string can read and write the values of MIB objects. **Read and Write**: The community string can read and write the values of MIB objects and send MIB object values for a trap and inform messages.
Apply	Click to apply the configurations

3.9.2 Trap Setting

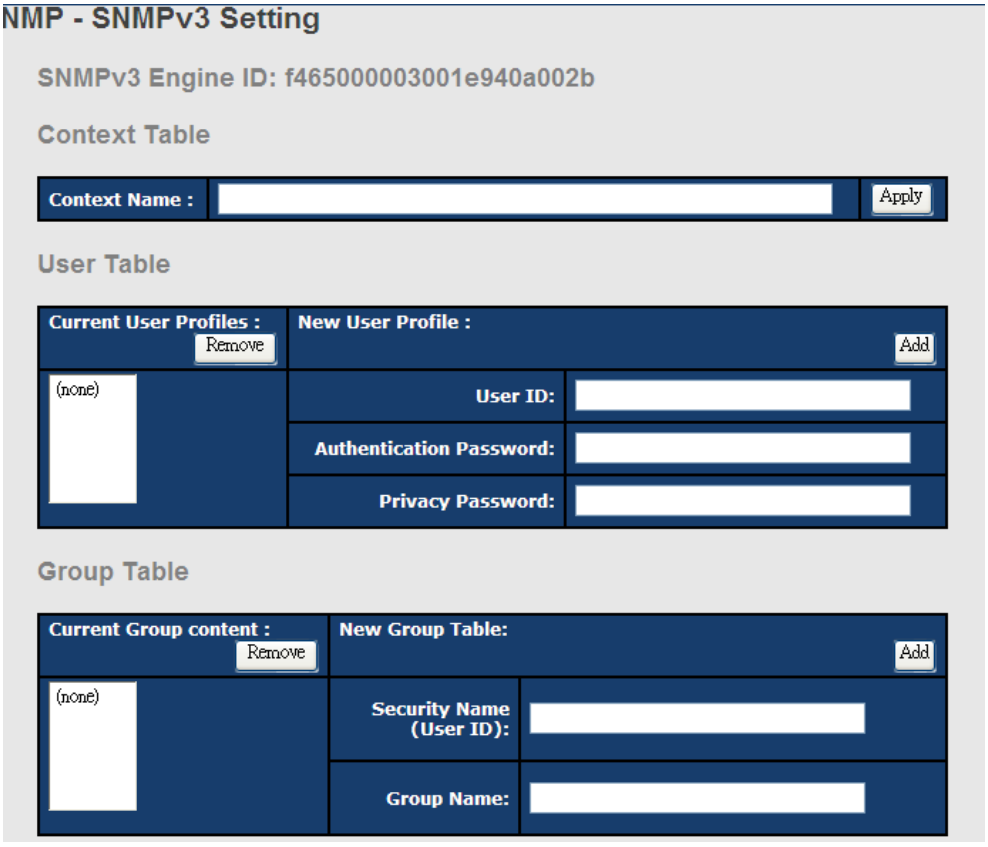
SNMP traps are event reports sent to a list of managers configured to receive event notifications when an error occurs. SNMP traps provide the value of one or more instances of management information. A trap manager is a management station that receives traps. If no trap manager is defined, no traps will be issued. You can create a trap manager by entering the IP address of the station and a community string.

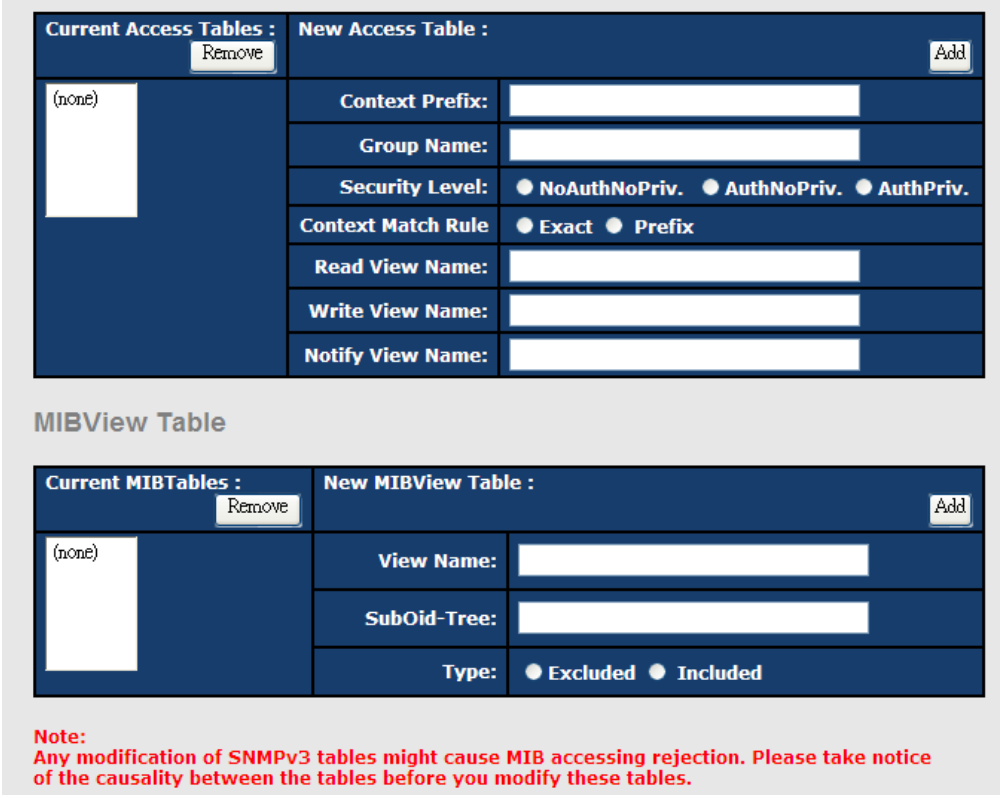


Label	Description
Server IP	The IP address of the server to receive traps
Community	The community string for authentication
Trap Version	The trap version. V1 and V2c are supported.
Add	Click to add the trap sever to the trap server profile.
Trap Server Profile	Shows a list of trap servers, including their community strings and trap versions.
Remove	Click to remove a trap server from the profile

3.9.3 SNMPV3

Unlike SNMP v1 and v2 which uses community strings for authentication, SNMP v3 uses username/password authentication, along with an encryption key. Therefore, SNMPv3 provides greater security features for authentication, privacy, and access control. The switch supports SNMP v3 which can be configured in the following page.


NMP - SNMPv3 Setting
SNMPv3 Engine ID: f465000003001e940a002b
Context Table
Context Name :
Apply
User Table
Current User Profiles :
Remove
(none)
New User Profile :
Add
User ID:
Authentication Password:
Privacy Password:
Group Table
Current Group content :
Remove
(none)
New Group Table:
Add
Security Name (User ID):
Group Name:


Current Access Tables :
Remove
(none)
New Access Table :
Add
Context Prefix:
Group Name:
Security Level:
NoAuthNoPriv.
AuthNoPriv.
AuthPriv.
Context Match Rule
Exact
Prefix
Read View Name:
Write View Name:
Notify View Name:
MIBView Table
Current MIBTables :
Remove
(none)
New MIBView Table :
Add
View Name:
SubOid-Tree:
Type:
Excluded
Included
Note:
Any modification of SNMPv3 tables might cause MIB accessing rejection. Please take notice of the causality between the tables before you modify these tables.

Label	Description
Context Table	Context is a collection of management information accessible by a SNMP entity and is stored in the context table. You can assign a context name to the context table and click **Apply** to change the name.
User Table	You can manage existing and add new user profiles in this section. In Current User Profiles, select an entry you want to remove and click Remove. In New User Profiles, specify the following information of a new entry: **User ID**: the username of the user **Authentication Password**: the authentication password for the user **Privacy Password**: the private password for the user Click **Add** after inputting the information.
Group Table	You can manage existing and add new group content in this section. In Current Group Content, select an entry you want to remove and click **Remove**. In New Group Table, specify the following information for a new entry: **Security Name (User ID)**: the name of the user to be added to the table. **Group Name**: the name of the group Click **Add** after inputting the information.
Access Table	The Access table lists the access rights and restrictions of the various groups. 1. You can manage existing and add new tables in this section. In Current Access Tables, select an entry you want to remove and click **Remove**. In New Access Table, specify the following information for a new entry: **Context Prefix**: the context name of the user as defined in the context table. **Group Name**: set up the group. **Security Level**: the security level of the user **Context Match Rule**: the rule for matching context **Read View Name**: the read view name provided for the v3 user **Write View Name**: the write view name provided for the v3 user. **Notify View Name**: the notify view name provided for the v3 user. Click **Add** after inputting the information.

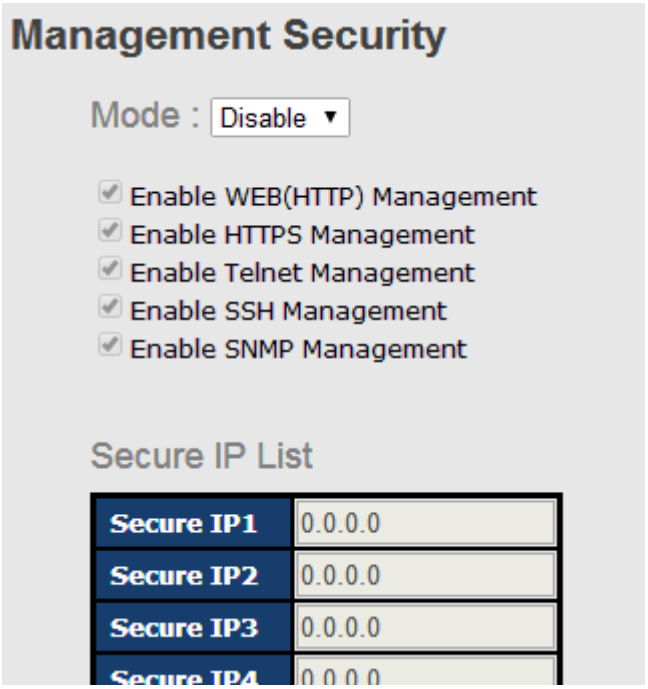
MIBview Table	You can configure MIB views for users and groups by entering the OID number of the MIB view. A MIB view consists of a family of view subtrees which may be individually included in or (occasionally) excluded from the view. Each view subtree is efined by a combination of an OID subtree together with a bit string mask. The view table is indexed by the view name and subtree OID values. In New MIBview Table, enter the following information: **ViewName**: the name of the view **Sub-Oid Tree**: fill in the Sub OID. **Type**: select the type as **excluded** or **included**. Click **Add** after inputting the information.

3.10 Security

The switch supports five security functions: IP security, port security, MAC blacklist, MAC address aging, and 802.1x protocol.

3.10.1 IP Security

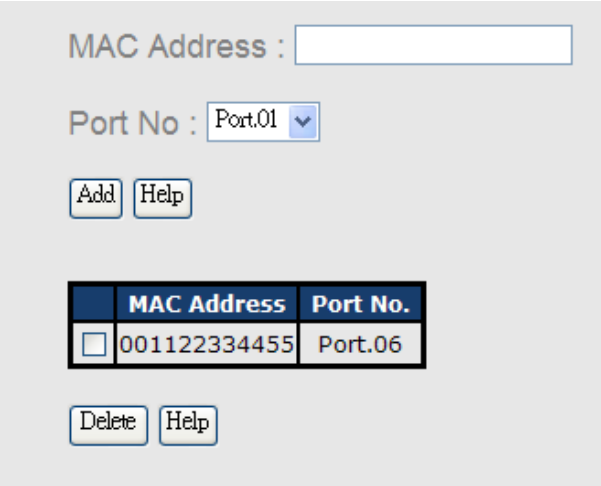
By setting up a secure IP list, only IP addresses in the list can manage the switch according to the management mode you have specified (WEB, Telnet, SNMP, etc.).



Label	Description
MODE	Enable/Disable the IP security function.
Enable WEB (HTTP) Management	Mark the blank to enable WEB (HTTP) Management.
Enable HTTPS Management	Mark the blank to enable WEB (HTTPS) Management.
Enable Telnet Management	Mark the blank to enable Telnet Management.
Enable SSH Management	Mark the blank to enable WEB Management.
Enable SNMP Management	Mark the blank to enable SNMP Management.
Apply	Click o set the configurations.
Help	Show help file.

Port Security

You can use static MAC addresses to provide port security for the switch. With this method, only the frames with the MAC addresses in this list will be forwarded, otherwise will be discarded.

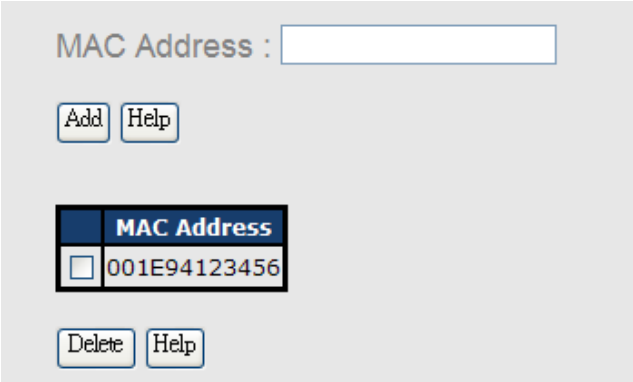


Label	Description
MAC Address	Enter a MAC address for a specific port.
Port NO.	Select a switch port
Add	Add the MAC address and port information.
Delete	Deletes an entry

Help	Shows help file

MAC Blacklist

You can block specific devices from network access by creating a MAC blacklist.MAC blacklists will prevent traffic from forwarding to specific MAC addresses in the list. Any frames forwarding to the MAC addresses in this list will be discarded. As a result, the target device will never receive any frame.



Label	Description
MAC Address	Enter a MAC address for a specific port.
Port NO.	Select a switch port
Add	Add the MAC address and port information.
Delete	Delete an entry
Help	Shows help file

802.1x

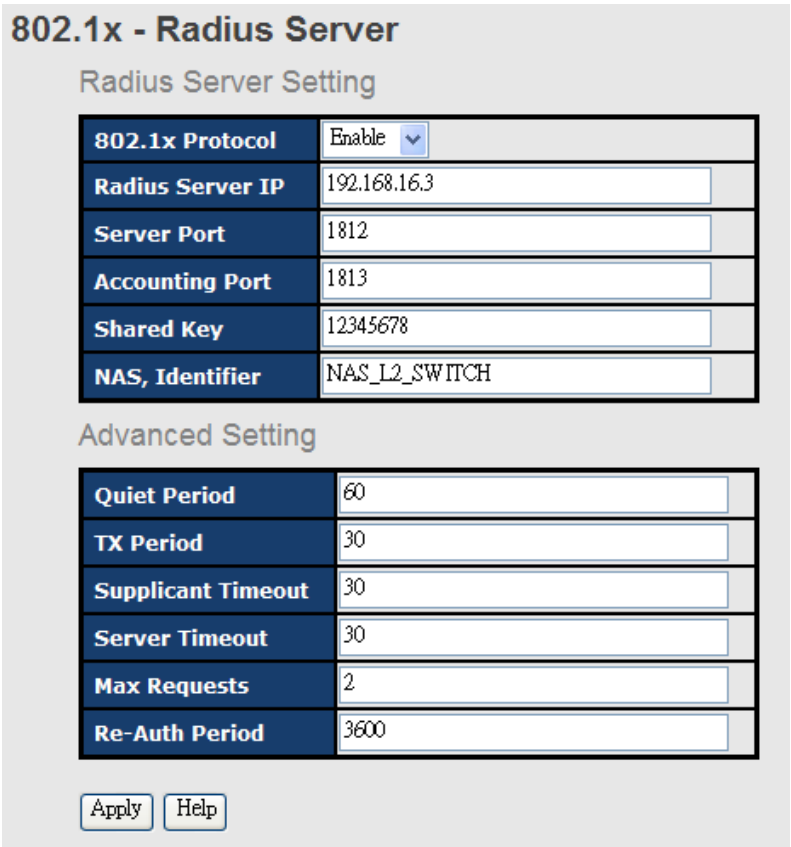
The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more backend servers (RADIUS) determine whether the user is allowed access to the network.

In an 802.1X network environment, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames which encapsulate EAP PDUs. Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible as it allows for different

authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) does not need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

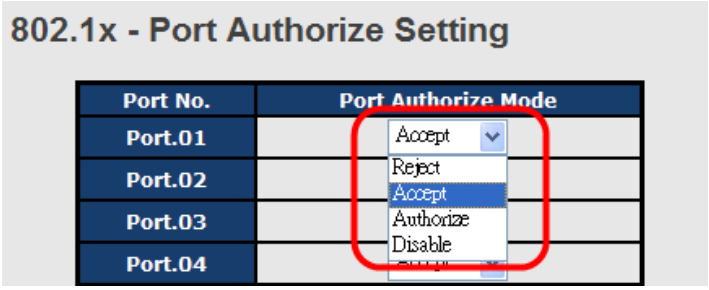
When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding the result to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

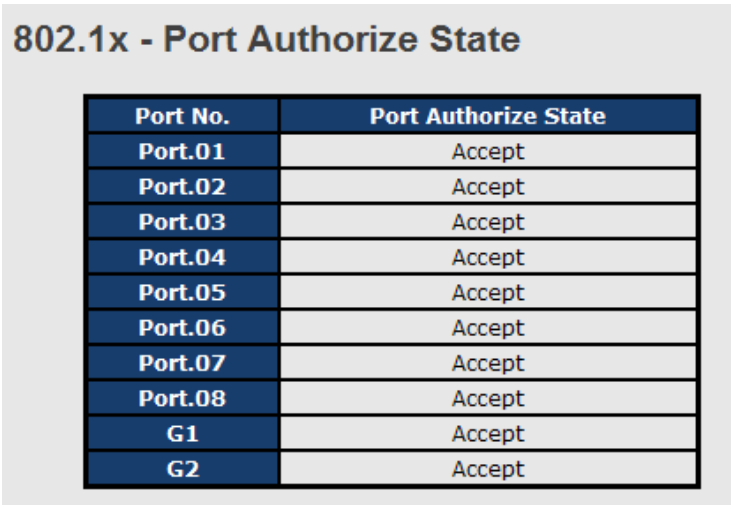
Note: in an environment where two backend servers are enabled, the server timeout is configured to X seconds (using the authentication configuration page), and the first server in the list is currently down (but not considered dead), if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, it will never be authenticated because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. Since the server has not failed (because the X seconds have not expired), the same server will be contacted when the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.



Label	Description
802.1x Protocol	Enables or disables 802.1X Radius server
Radius Server IP	IP address of the authentication server
Server Port	The UDP port number used by the authentication server to authenticate
Accounting Port	The number of the UDP port that the RADIUS server uses for accounting requests.
Shared Key	A key shared between the switch and authentication server
NAS, Identifier	A string used to identify the switch.
Quiet Period	The time interval between authentication failure and the start of a new authentication attempt.
Tx Period	The time that the switch waits for response to an EAP request/identity frame from the client before resending the request.
Supplicant Timeout	The period of time the switch waits for a supplicant respond to an EAP request.
Server Timeout	The period of time the switch waits for a Radius server respond to an authentication request.
Max Requests	The maximum number of times to retry sending packets to the supplicant.
Re-Auth Period	The period of time after which clients connected must be re-authenticated
Apply	Click to apply the configurations
Help	Shows help file

The 802.1x authorized mode of each port can be set in the following dialog:



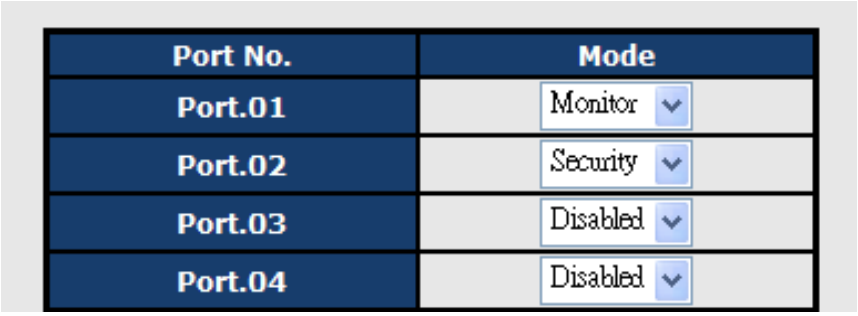


Label	Description
Port Authorize Mode	**Reject**: force the port to be unauthorized **Accept**: force the port to be authorized **Authorize**: the state of the port is determined by the outcome of the 802.1x authentication **Disable**: the port will not participate in the 802.1x portocol
Apply	Click to apply the configurations
Help	Shows help file

3.10.2 IP Guard

Port Setting

This page allows you to configure IP guard functions for each port, an intelligent and user-friendly IP security method. It protects the network from unknown IP (IPs not in the allowed list) attack. Unauthorized IP traffic will be blocked.

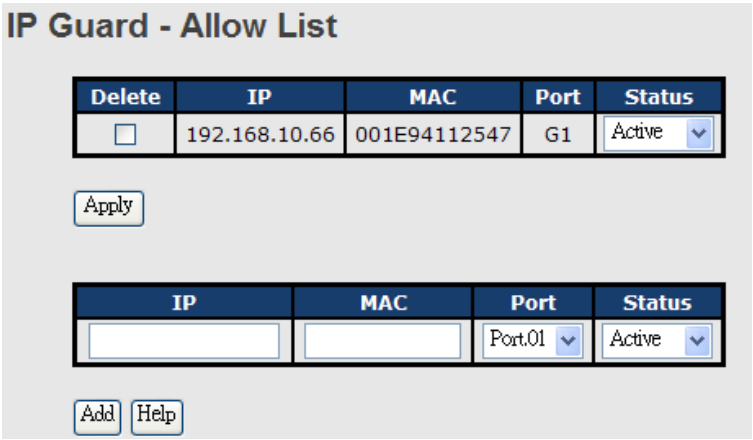


Label	Description
Mode	**Disabled**: disables the function

	Monitor: scans the IP information of the connected device before implementing further actions **Security**: performs security actions without scanning the information of the connected device
Apply	Click to apply the configurations
Help	Shows help file

Allow List

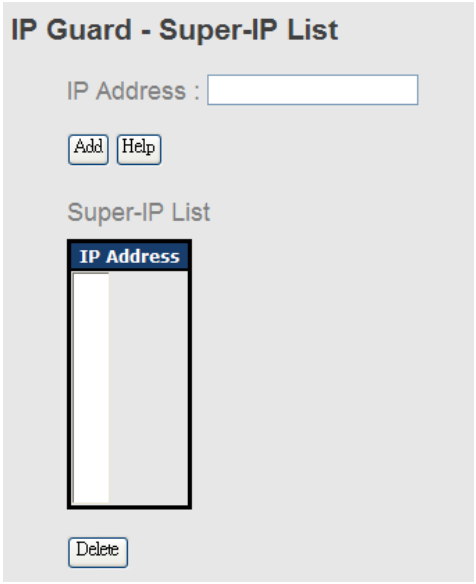
By creating an allow list, traffic from the IP addresses in the list will be allowed.



Label	Description
IP	IP address of the allowed entry
MAC	MAC address of the allowed entry
Port	Port number of the allowed entry
Status	The option allows you to block suspicious IP traffic. **Active**: allows the IP traffic. **Suspend**: blocks the IP traffic.
Delete	Check to delete an entry

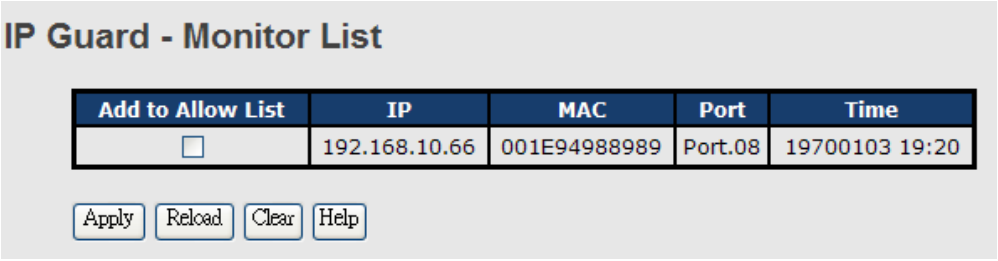
Super-IP List

A super-IP list enables you to give full access to the switch to the user you specify. Devices with the IP addresses listed in the table will be able to manage the switch disregarding the rule you have set.



Monitor List

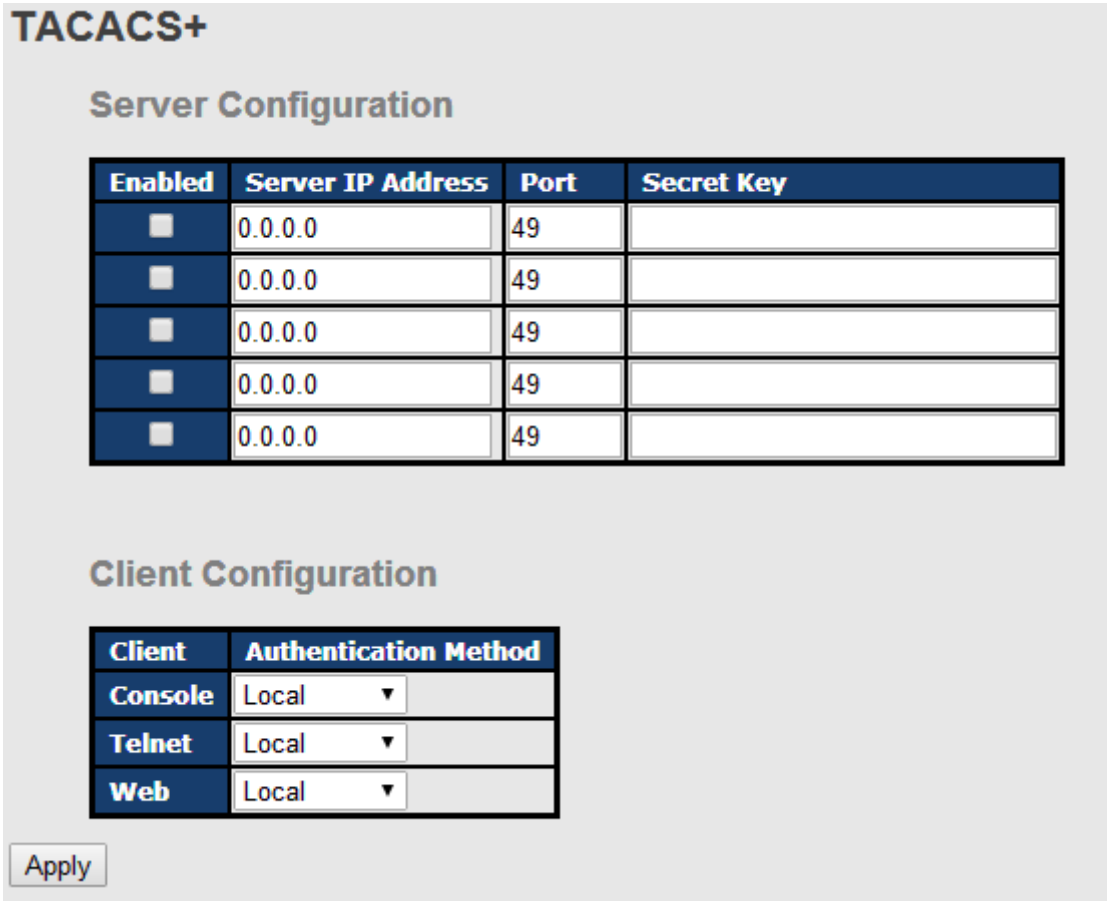
You can create a monitor list to monitor IP traffic of individual ports automatically.



Label	Description
IP	IP address of the port
MAC	MAC address of the port
Port	The port number you want to monitor
Time	The time when the entry is logged.
Add to Allow List	Check to add the entry to the allow list

3.10.3 TACACS+

In this page , use can setting TACACS+ Server info and Client Authentication Method , if want use this function first need ready TACACS+ Server .



Label	Description
Enable check box	Enable / disable server connect
Server IP Address	Input TACACS+ Server IP Address .
Port	Input TACACS+ use Port number
Secret key	Input TACACS+ use key value(need same TACACS+ Server)
Authentication Method	User can select Authentication Method , support local / TACACS +

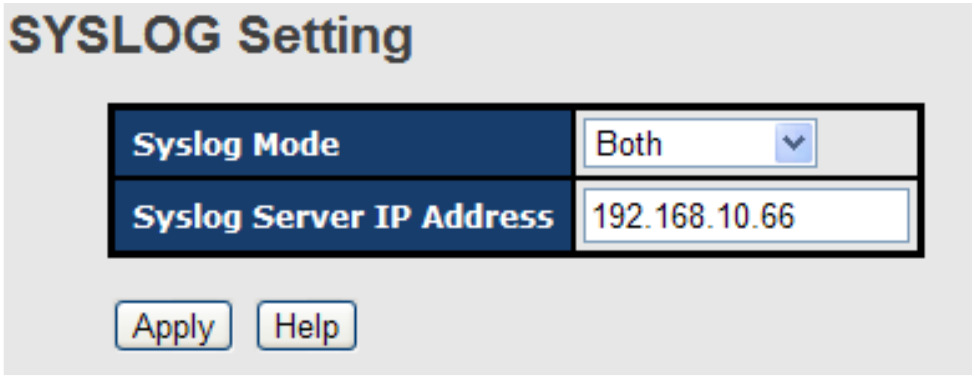
3.11Warning

The switch supports several alerting methods, including SYSLOG, e-mail, and fault relay. These methods enable you to monitor switch status remotely. When an event occurs, the system will send an alert to your appointed servers.

3.11.1 SYSLOG Setting

SYSLOG is a protocol that allows a device to send event notification messages across IP networks to event message collectors. It permits separation of the software that generates

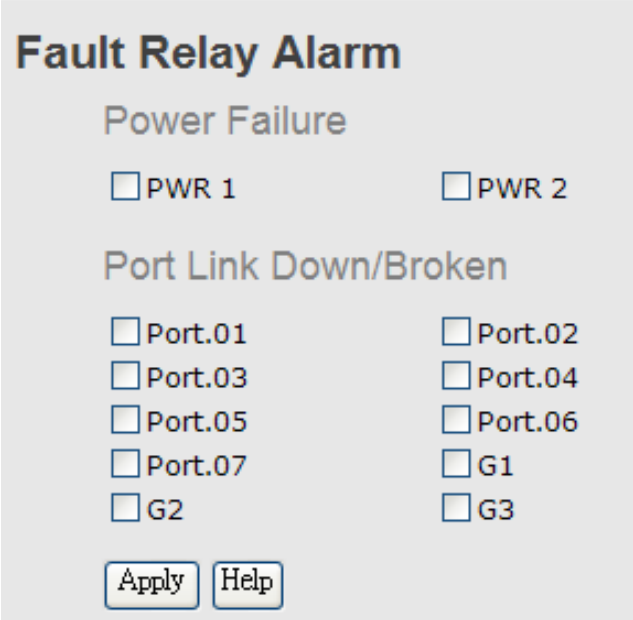
messages from the system that stores them and the software that reports and analyzes them. As Syslog messages are UDP-based, the sender and receiver will not be aware of it if the packet is lost due to network disconnection and no UDP packet will be resent.



Label	Description
Syslog Mode	**Disable**: disables SYSLOG **Client Only**: logs in to a local system **Server Only**: logs in to a remote SYSLOG server **Both**: logs in to a local and remote server.
SYSLOG Server IP Address	The IP address of the remote SYSLOG server
Apply	Click to apply the configurations
Help	Shows help file

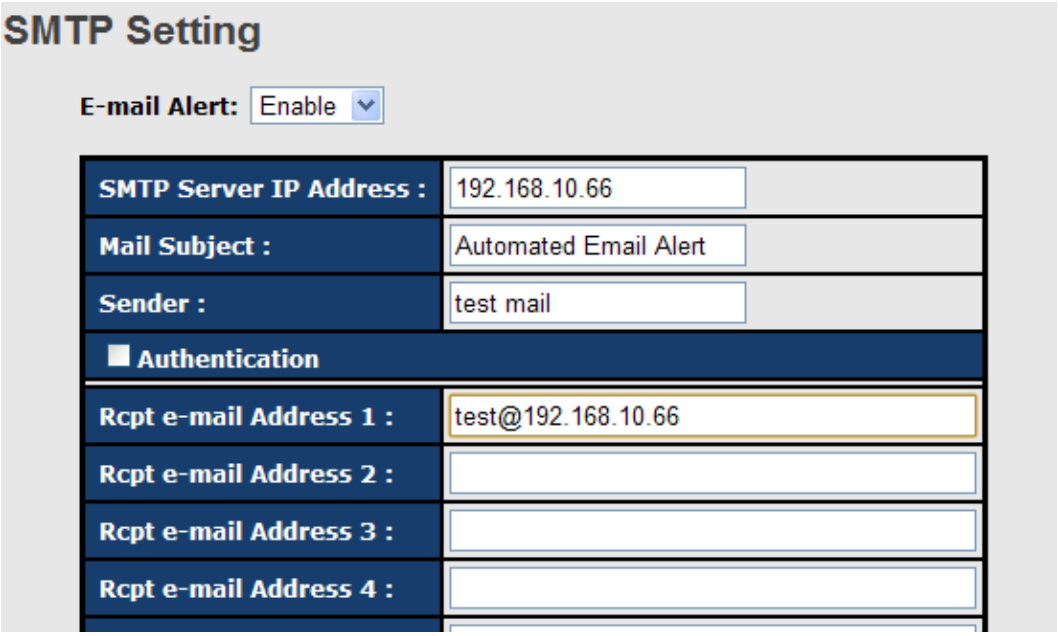
3.11.2 Fault Relay

When any selected fault event happens, the Fault LED on the switch panel will light up and the electric relay will signal at the same time. You can set the switch to trigger alarms when power fails or ports are disconnected.



3.11.3 SMTP Setting

SMTP (Simple Mail Transfer Protocol) is a protocol for transmitting e-mails across the Internet. By setting up SMTP alert, the device will send a notification e-mail when a user-defined event occurs.

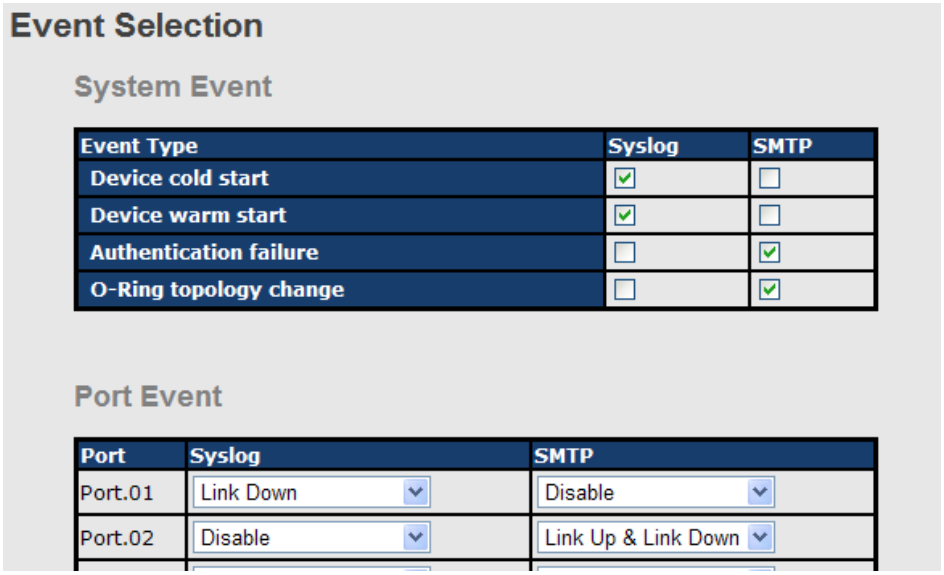


Label	Description
E-mail Alert	Enables or disables transmission of system warnings by e-mail
SMTP Server IP	The IP address of the SMTP server to receive the notification

Address	e-mail
Mail Subject	Subject of the mail
Sender	The email account to send the alert
Authentication	■ **Username:** the authentication username ■ **Password:** the authentication password ■ **Confirm Password:** re-enter password
Recipient E-mail Address	The recipient's e-mail address. A mail allows for 6 recipients.
Apply	Click to activate the configurations
Help	Shows help file

3.11.4 Event Selection

The device supports both SYSLOG and SMTP alerts. Check the corresponding box to enable the system event warning method you want. Please note that the checkboxes will gray out if SYSLOG or SMTP is disabled.



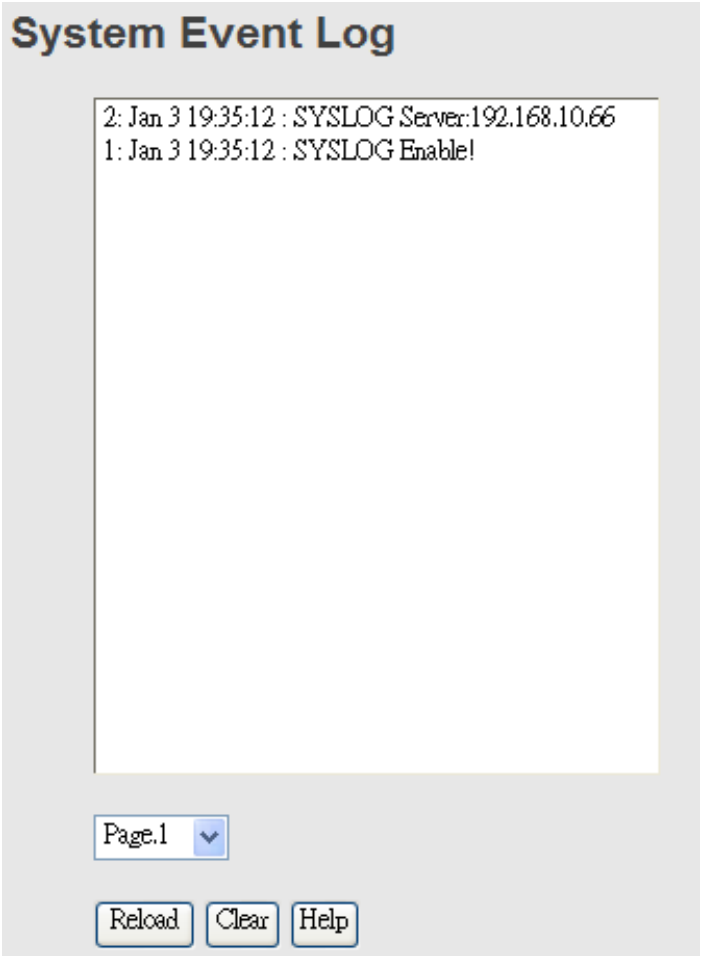
Label	Description
Device cold start	Sends alerts when you restart the device using the power button on your PC.
Device warm start	Sends alerts when you restart the device using the Reset button or software.
Authentication Failure	Sends alerts when SNMP authentication fails
O-Ring topology	Sends alerts when O-Ring topology changes

change	
Port Event	Sends alerts when the port meets a specified condition. Available options include: ■ **Disable**: disables alert function ■ **Link Up**: sends alerts when port is connected ■ **Link Down**: sends alerts when port is not connected ■ **Link Up & Link Down**: sends alerts when port is connected and disconnected
Apply	Click to apply the configurations
Help	Shows help file

3.12 Monitor and Diag

3.12.1 System Event Log

If a system log client is enabled, the system event log will be shown in this table.



Label	Description
Page	The page number of the selected LOG
Reload	Click to refresh the information in this page
Clear	Clear log
Help	Shows help file

3.12.2 MAC Address Table

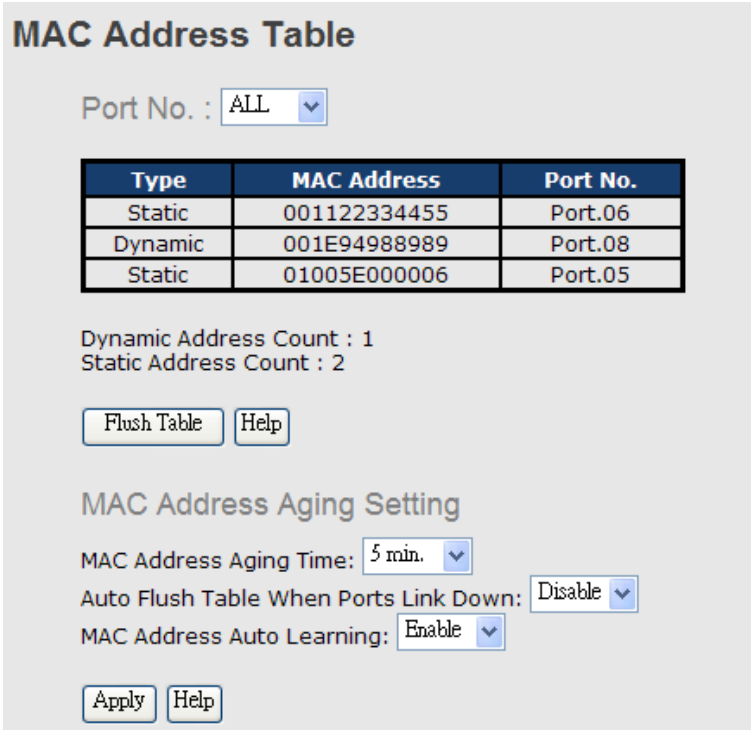
A MAC address tablet is a table in a network switch that maps MAC addresses to ports. The switch uses the table to determine which port the incoming packet should be forwarded to. Entries in a MAC address table fall into two types: dynamic and static entries. Entries in a static MAC table are added or removed manually and cannot age out by themselves. Entries in a dynamic MAC tablet will age out after a configured aging time. Such entries can be added by learning or manual configuration.

Aging Configuration

Aging enables the switch to track only active MAC addresses on the network and flush out MAC addresses that are no longer used, thereby keeping the table current. You can configure aging time by entering a value in the **MAC Address Aging Time** box. Note that aging time must be a multiple of 15.

MAC Table Learning

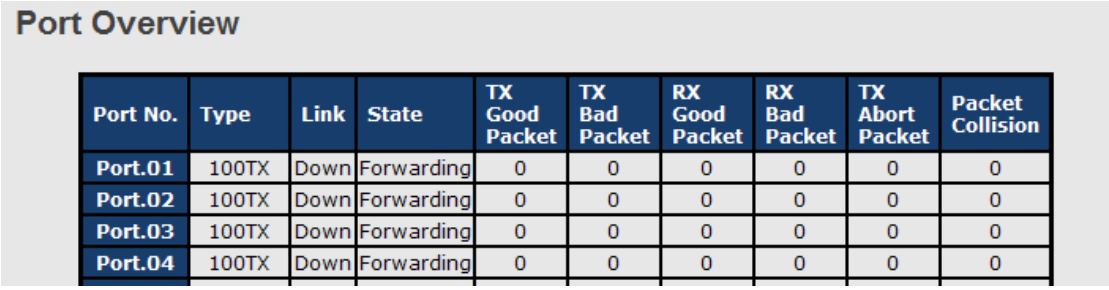
The switch can add the address and port on which the packet was received to the MAC table if the address does not exist in the table by examining the source address of each packet received on a port. This is called learning. It allows the MAC table to expand dynamically. If the learning mode for a given port is grayed out, it means another module is in control of the mode, and thus the user cannot change the configurations. An example of such a module is MAC-Based authentication under 802.1X.



Label	Description
Port NO. :	Shows all MAC addresses mapped to a selected port in the table
Flush Table	Clears all MAC addresses in the table
Help	Shows help file.
MAC Address Aging Time	The time of an entry stays valid in the table
Auto Flush Table When Ports Link Down	Clears the MAC table automatically when ports are disconnected
MAC Address Auto Learning	Enables or disables MAC learning function
Apply	Click to apply the configurations.

Port Overview

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



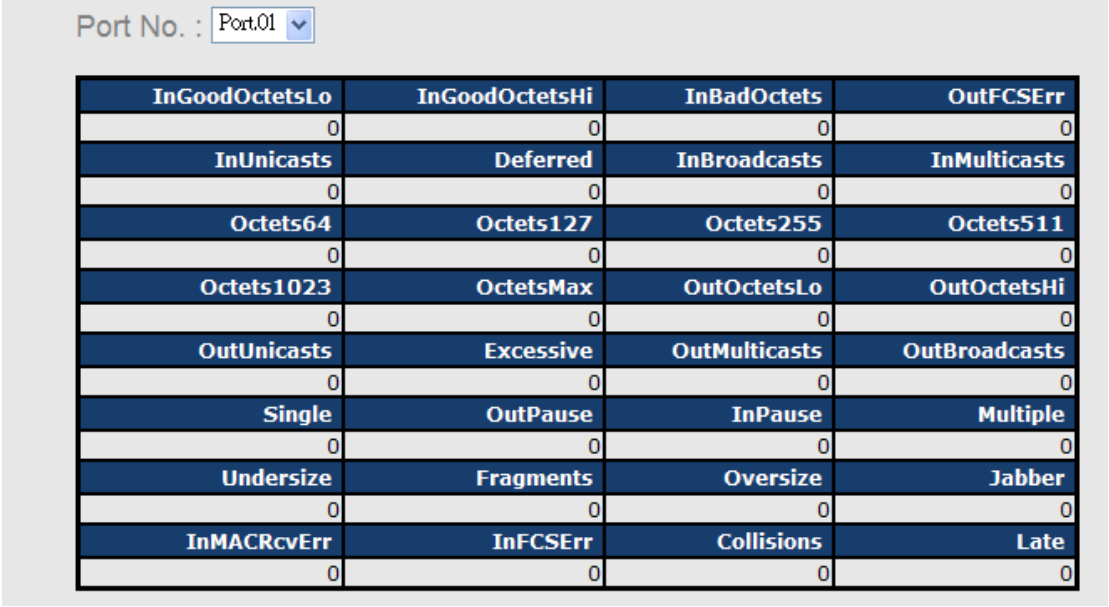
Label	Description
Type	Shows port speed and media type.
Link	Shows port link status
State	Shows port status
TX GOOD Packet	The number of good packets sent by this port
TX Bad Packet	The number of bad packets sent by this port
RX GOOD Packet	The number of good packets received by this port
RX Bad Packet	The number of bad packets received by this port
TX Abort Packet	The number of packets aborted by this port
Packet Collision	The number of times a collision is detected by this port
Clear	Clears all counters
Help	Shows help file

Port Counter

The displayed counters include the total number for receive and transmit, the size for receive and transmit, and the errors for receive and transmit.

3.12.3 Port Counters

This page shows statistic counters for the port. The **Clear** button will reset all counters to zero.



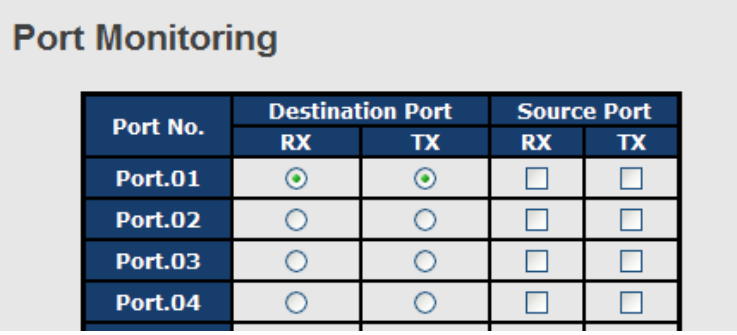
Label	Description
InGoodOctetsLo	The lower 32-bits of the 64-bit InGoodOctets counter. This field indicates the total length of all good Ethernet frames received.
InGoodOctetsHi	The upper 32-bits of the 64-bit InGoodOctets counter. This field indicates the total length of all good Ethernet frames received.
InBadOctets	The total length of all bad Ethernet frames received.
OutFCSErr	The number of frames transmitted with an invalid FCS. Whenever a frame is modified during transmission (e.g., to add or remove a tag), the frame's original FCS is inspected before a new FCS is added to a modified frame. If the original FCS is invalid, the new FCS is made invalid too and this counter is incremented.
InUnicasts	The number of good frames received that have a Unicast destination MAC address.
Deferred	The total number of successfully transmitted frames without collision but are delayed because the medium is busy during the first attempt. This counter is applicable in half-duplex only.
InBroadcasts	The number of good frames received that have a Broadcast destination MAC address.
InMulticasts	The number of good frames received that have a Multicast destination MAC address.
Octets64	Total frames received (and/or transmitted) with a length of exactly 64 octes, including those with errors.

Octets127	Total frames received (and/or transmitted) with a length of between 65 and 127 octes, including those with errors.
Octets255	Total frames received (and/or transmitted) with a length of between 128 and 255 octes, including those with errors.
Octets511	Total frames received (and/or transmitted) with a length of between 256 and 511 octes, including those with errors.
Octets1023	Total frames received (and/or transmitted) with a length of between 512 and 1023 octes, including those with errors.
OctetsMax	Total frames received (and/or transmitted) with a length of between 1024 and MaxSize octes, including those with errors.
OutOctetsLo	The lower 32-bit of the 64-bit OutOctets counter. This field indicates the total length of all Ethernet frames sent from this MAC address.
OutOctetsHi	The upper 32-bit of the 64-bit OutOctets counter. This field indicates the total length of all Ethernet frames sent from this MAC address.
OutUnicasts	The number of frames sent with an Unicast destination MAC address.
Excessive	The number frames dropped in the transmitted MAC address because the frame experiences 16 consecutive collisions. This counter is applicable in half-duplex only and only when DiscardExcessive is one.
OutBroadcasts	The number of good frames sent with a Broadcast destination MAC address
Single	The total number of successfully transmitted frames that experiences exactly one collision. This counter is applicable in half-duplex only.
OutPause	The number of good Flow Control frames sent
InPause	The number of good Flow Control frames received
Multiple	The total number of successfully transmitted frames that experience more than one collision. This counter is applicable in half-duplex only.
Undersize	Total frames received with a length of less than 64 octets but with a valid FCS
Fragments	Total frames received with a length of more than 64 octets and with an invalid FCS

Oversize	Total frames received with a length of more than MaxSize octets but with a valid FCS
Jabber	Total frames received with a length of more than MaxSize octets but with an invalid FCS
InMACRcvErr	Total frames received with an RxErr signal from the PHY
InFCSErr	Total frames received with a CRC error not counted in Fragments, Jabber or RxErr.
Collisions	The number of frames for which one or more collisions occurred when the frames were sent, including single, multiple, excessive, or late collisions. This counter is applicable in half-duplex only.
Late	When a collision is detected by a station after it has sent the 512th bit of its frame, it is counted as a late collision. This counter is applicable in half-duplex only.

Port Monitoring

The switch supports several types of port monitoring including TX (egress) only, RX (ingress) only, and both TX/RX monitoring. TX monitoring sends any data that egress out checked TX source ports to a selected TX destination port as well. RX monitoring sends any data that ingress in checked RX source ports out to a selected RX destination port as well as sending the frame where it normally would have gone. Note that keep all source ports unchecked in order to disable port monitoring.

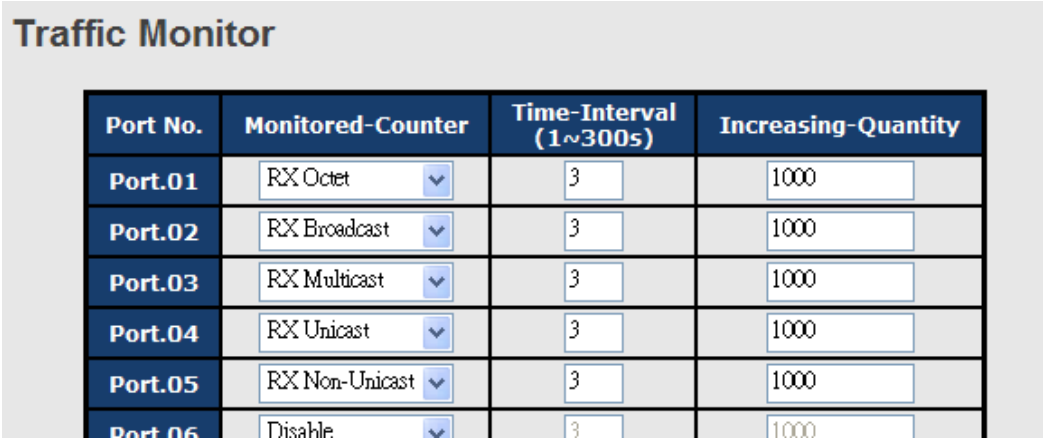


Label	Description
Destination Port	The port will receive a copied frame from source port for monitoring purpose.
Source Port	Check to monitor specific ports
TX	The frames transmitted by a port
RX	The frames received by a port
Apply	Click to activate the configurations.

Clear	Clears all checked boxes (disable the function)
Help	Shows help file

Traffic Monitoring

By enabling traffic monitoring function, the switch will send out an SYSLOG event notification or SMTP e-mail when the traffic becomes too large.



Label	Description
Monitored–Counter	Monitor the incoming traffic by bandwidth or number of packets. Available options include: RX Octet: calaculates the total bandwidth consumed by incoming traffic RX Broadcast: calaculates the number of broadcast packets RX Multicast: calaculates the number of multicast packets RX Unicast: calaculates the number of unicast packets RX Non-Unicast: calaculates the total number of multicast and broadcast packets Disable: disables the function
Time-Interval	Sets the time interval of counting
Increasing Quantity –	Specify a threahold for the counter. When the result of calucation exceeds the value, an alert will be issued.
Event Alarm	Specifies alarm type (SYSLOG or SMTP)

3.12.4 Ping

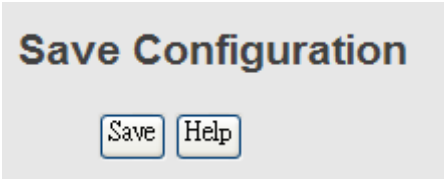
This command sends ICMP echo request packets to another node on the network. Using the ping command, you can see if another site on the network can be reached.

After you press **Active**, four ICMP packets will be transmitted, and the sequence number and roundtrip time will be displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

Label	Description
IP Address	Enter the IP address that you want to detect
Active	Click to send ICMP packets

3.13 Save Configuration

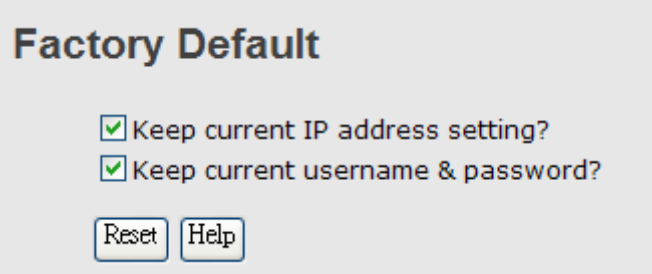
Click **Save Configuration** whenever you change a configuration to save current configurations; otherwise, the changes you make will be lost when the power is off or system is reset.



Label	Description
Save	Saves all configurations
Help	Shows help file

3.14 Factory Default

This function is to force the switch back to the original factory settings. You can decide to keep current IP address settings or username/password by checking in the boxes.



3.15 System Reboot

You can reset the stack switch on this page. After reset, the system will boot normally as if you have powered on the devices.

Command Line Interface Management

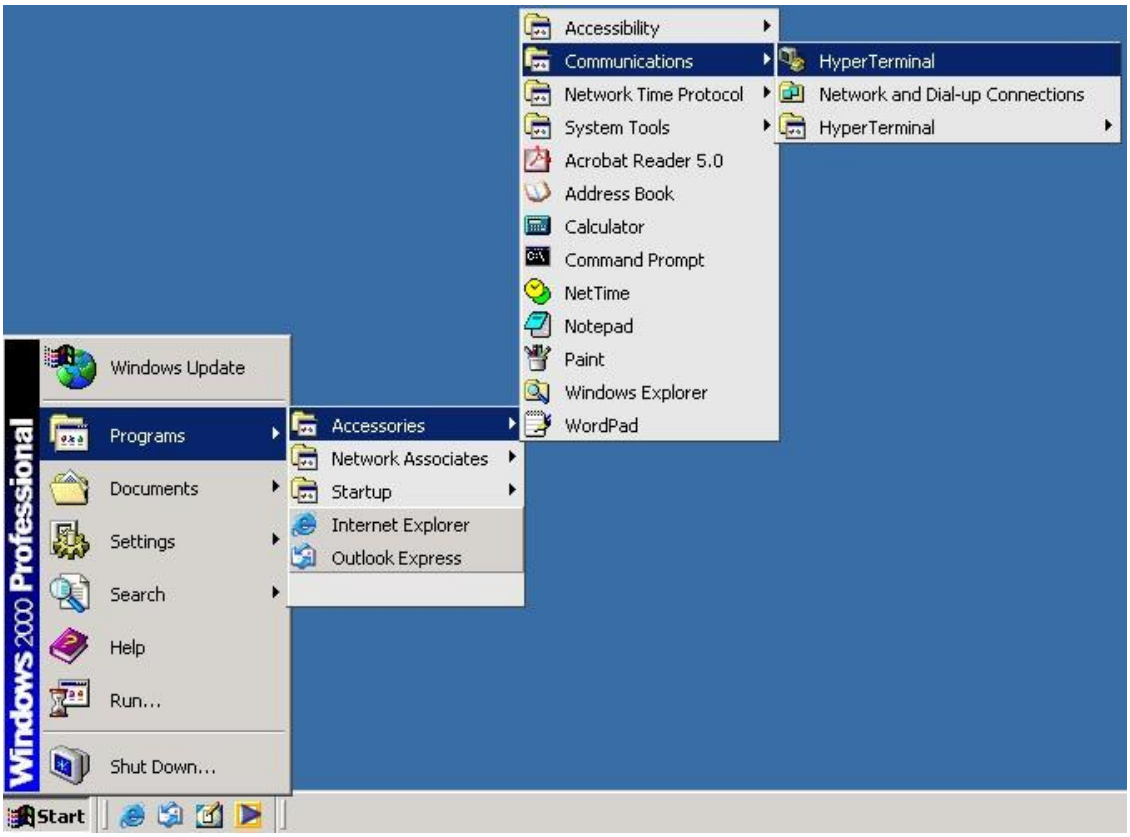
Besides Web-based management, the switch also supports CLI management. You can use console or telnet to manage the switch by CLI.

CLI Management by RS-232 Serial Console (9600, 8, none, 1, none)

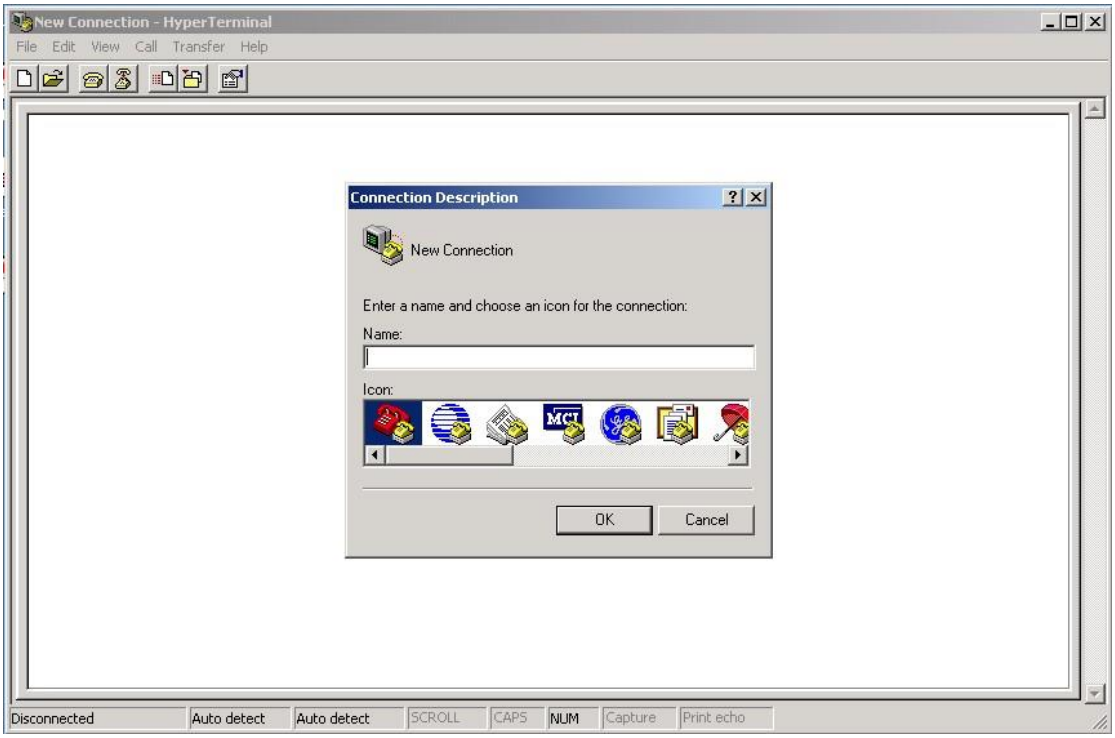
Before configuring RS-232 serial console, connect the RS-232 port of the switch to your PC Com port using a RJ45 to DB9-F cable.

Follow the steps below to access the console via RS-232 serial cable.

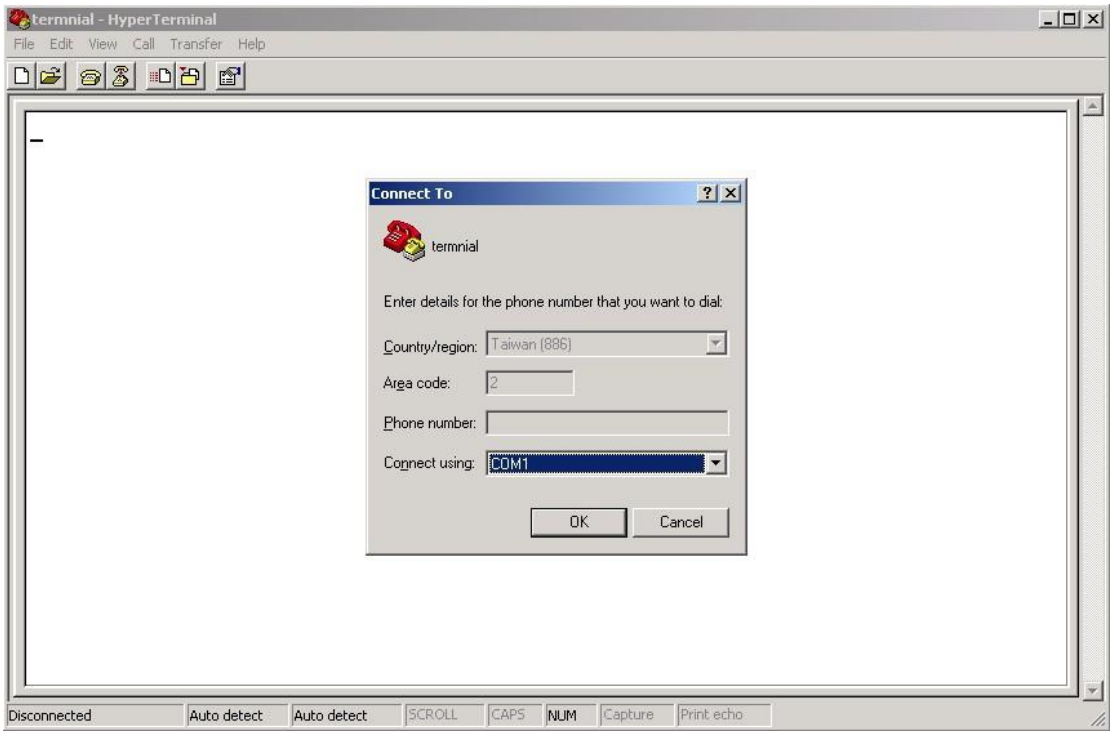
Step 1: On Windows desktop, click on **Start** -> **Programs** -> **Accessories** -> **Communications** -> **Hyper Terminal**



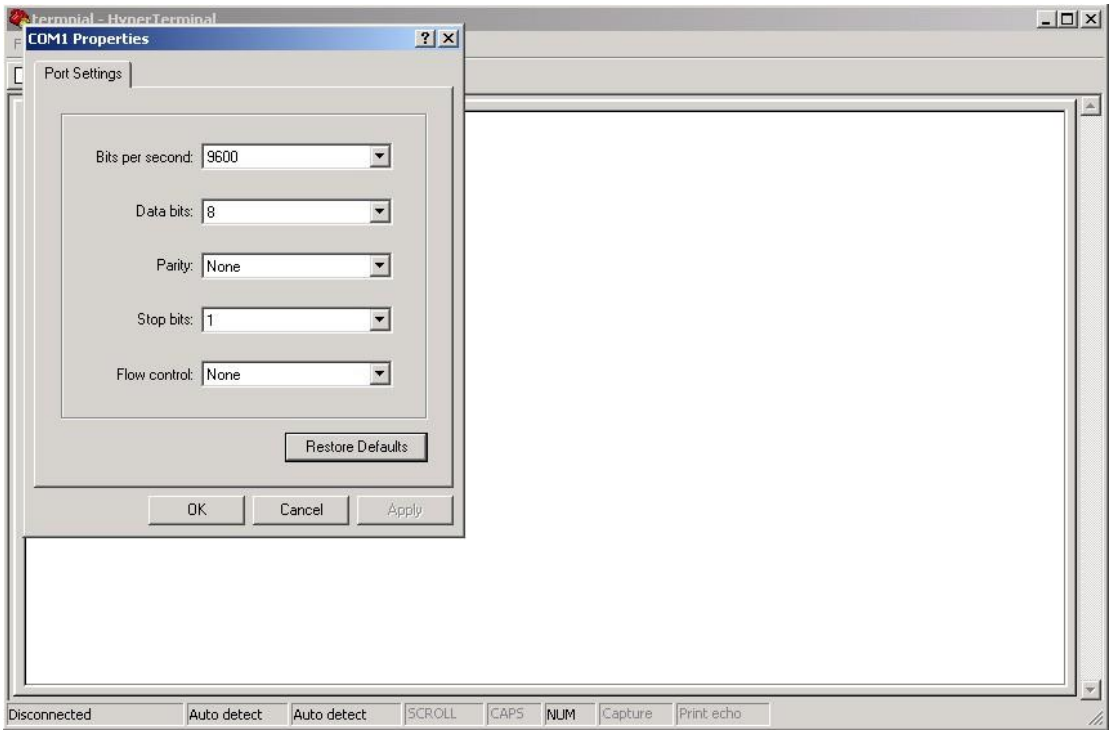
Step 2. Input a name for the new connection.



Step 3. Select a COM port in the drop-down list.



Step 4. A pop-up window that indicates COM port properties appears, including bits per second, data bits, parity, stop bits, and flow control.



Step 5. The console login screen will appear. Use the keyboard to enter the Username and Password (same as the password for Web browsers), then press **Enter**.

```
IES-3082GC
Command Line Interface

Username : _
Password :
```

CLI Management by Telnet

You can can use **TELNET**to configure the switch. The default values are:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

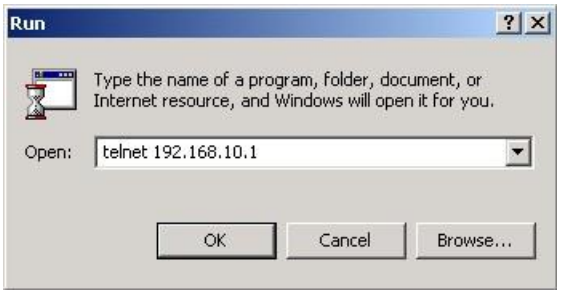
Default Gateway: **192.168.10.254**

User Name: **admin**

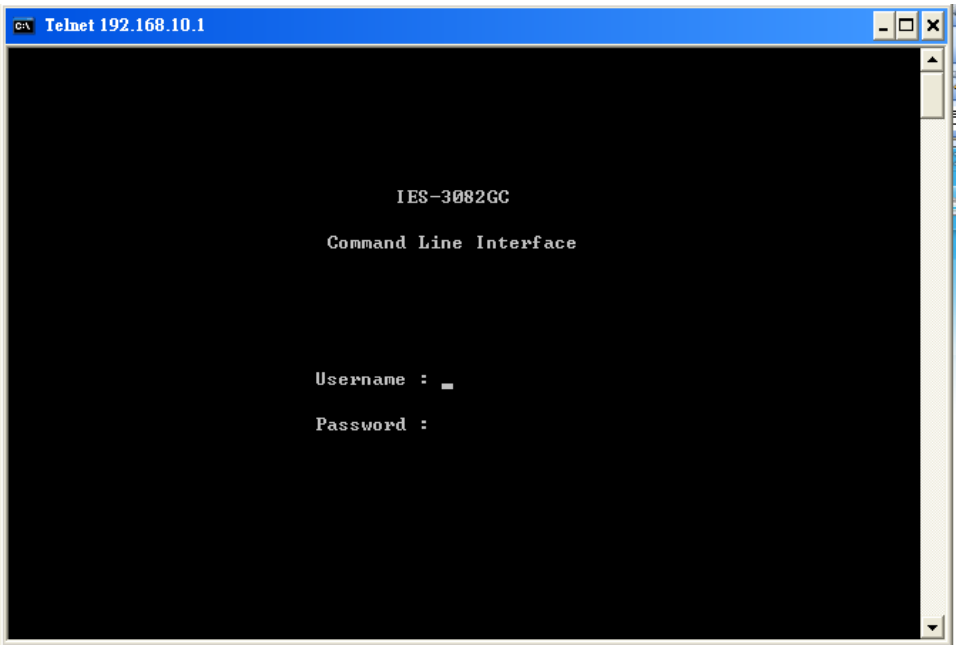
Password: **admin**

Follow the steps below to access console via Telnet.

Step 1. Telnet to the IP address of the switch from the **Run** window by inputingcommands (or from the MS-DOS prompt) as below.



Step 2. The Login screen will appear. Use the keyboard to enter the Username and Password (same as the password for Web browser), and then press **Enter.**



Commands Level

Modes	Access Method	Prompt	Exit Method	About This Model
User EXEC	Begin a session with your switch.	switch>	Enter **logout** or **quit**.	The user command available at the level of user is the subset of those available at the privileged level. Use this mode to • Enter menu mode. • Display system information.
Privileged EXEC	Enter the **enable** command while in user EXEC mode	switch#	Enter **disable** to exit.	The privileged command is advance mode Privileged this mode to • Display advance function status • Save configures
Global configuration	Enter the **configure** command while in privileged EXEC mode	switch(config)#	To exit to privileged EXEC mode, enter **exit** or **end**	Use this mode to configure parameters that apply to your switch as a whole
VLAN database	Enter the **vlan database** command while in privileged EXEC mode	switch(vlan)#	To exit to user EXEC mode, enter **exit**.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the **interface** command (with a specific interface) while in global configuration mode	switch(config-if)#	To exit to global configuration mode, enter **exit**. To exist privileged EXEC mode or **end.**	Use this mode to configure parameters for the switch and Ethernet ports

Symbol of Command Level

Mode	Symbol of Command Level
User EXEC	E
Privileged EXEC	P
Global configuration	G
VLAN database	V
Interface configuration	I

6.1 Command Set List—System Command Set

Commands	Level	Description	Example
show config	**E**	Show switch configuration	switch>show config
show terminal	**P**	Show console information	switch#show terminal
write memory	**P**	Save your configuration into permanent memory (flash rom)	switch#write memory
system name [System Name]	**G**	Configure system name	switch(config)#system name xxx
system location [System Location]	**G**	Set switch system location string	switch(config)#system location xxx
system description [System Description]	**G**	Set switch system description string	switch(config)#system description xxx
system contact [System Contact]	**G**	Set switch system contact window string	switch(config)#system contact xxx
show system-info	**E**	Show system information	switch>show system-info
ip address [Ip-address] [Subnet-mask] [Gateway]	**G**	Configure the IP address of switch	switch(config)#ip address 192.168.1.1 255.255.255.0 192.168.1.254
ip dhcp	**G**	Enable DHCP client function of switch	switch(config)#ip dhcp
show ip	**P**	Show IP information of switch	switch#show ip
no ip dhcp	**G**	Disable DHCP client function of switch	switch(config)#no ip dhcp
reload	**G**	Halt and perform a cold restart	switch(config)#reload
default	**G**	Restore to default	Switch(config)#default
admin username	**G**	Changes a login username.	switch(config)#admin

[Username]		(maximum 10 words)	username xxxxxx
admin password [Password]	**G**	Specifies a password (maximum 10 words)	switch(config)#admin password xxxxxx
show admin	**P**	Show administrator information	switch#show admin
dhcpserver enable	**G**	Enable DHCP Server	switch(config)#dhcpserver enable
dhcpserver lowip [Low IP]	**G**	Configure low IP address for IP pool	switch(config)# dhcpserver lowip 192.168.1.1
dhcpserver highip [High IP]	**G**	Configure high IP address for IP pool	switch(config)# dhcpserver highip 192.168.1.50
dhcpserver subnetmask [Subnet mask]	**G**	Configure subnet mask for DHCP clients	switch(config)#dhcpserver subnetmask 255.255.255.0
dhcpserver gateway [Gateway]	**G**	Configure gateway for DHCP clients	switch(config)#dhcpserver gateway 192.168.1.254
dhcpserver dnsip [DNS IP]	**G**	Configure DNS IP for DHCP clients	switch(config)# dhcpserver dnsip 192.168.1.1
dhcpserver leasetime [Hours]	**G**	Configure lease time (in hour)	switch(config)#dhcpserver leasetime 1
dhcpserver ipbinding [IP address]	**I**	Set static IP for DHCP clients by port	switch(config)#interface fastEthernet 2 switch(config-if)#dhcpserver ipbinding 192.168.1.1
show dhcpserver configuration	**P**	Show configuration of DHCP server	switch#show dhcpserver configuration
show dhcpserver clients	**P**	Show client entries of DHCP server	switch#show dhcpserver clinets
show dhcpserver ip-binding	**P**	Show IP-Binding information of DHCP server	switch#show dhcpserver ip-binding
no dhcpserver	**G**	Disable DHCP server function	switch(config)#no dhcpserver
security enable	**G**	Enable IP security function	switch(config)#security enable
security http	**G**	Enable IP security of HTTP server	switch(config)#security http
security telnet	**G**	Enable IP security of telnet server	switch(config)#security

			telnet
security ip [Index(1..10)] [IP Address]	**G**	Set the IP security list	switch(config)#security ip 1 192.168.1.55
show security	**P**	Show the information of IP security	switch#show security
no security	**G**	Disable IP security function	switch(config)#no security
no security http	**G**	Disable IP security of HTTP server	switch(config)#no security http
no security telnet	**G**	Disable IP security of telnet server	switch(config)#no security telnet

6.2 Command Set List—Port Command Set

Commands	Level	Description	Example
interface fastEthernet [Portid]	**G**	Choose the port for modification.	switch(config)#interface fastEthernet 2
duplex [full | half]	**I**	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#interface fastEthernet 2 switch(config-if)#duplex full
speed [10|100|1000|auto]	**I**	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
flowcontrol mode [Symmetric|Asymmetric]	**I**	Use the flowcontrol configuration command on Ethernet ports to control traffic rates during congestion.	switch(config)#interface fastEthernet 2 switch(config-if)#flowcontrol mode Asymmetric
no flowcontrol	**I**	Disable flow control of interface	switch(config-if)#no flowcontrol
security enable	**I**	Enable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#security enable

no security	I	Disable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no security
bandwidth type all	I	Set interface ingress limit frame type to “accept all frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all
bandwidth type broadcast-multicast -flooded-unicast	I	Set interface ingress limit frame type to “accept broadcast, multicast, and flooded unicast frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast-flooded -unicast
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to “accept broadcast and multicast frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast
bandwidth type broadcast-only	I	Set interface ingress limit frame type to “only accept broadcast frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-only
bandwidth in **[Value]**	I	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth in 100
bandwidth out **[Value]**	I	Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth out 100
show bandwidth	I	Show interfaces bandwidth control	switch(config)#interface fastEthernet 2 switch(config-if)#show bandwidth

state [Enable | Disable]	I	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)#interface fastEthernet 2 switch(config-if)#state Disable
show interface configuration	I	show interface configuration status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface configuration
show interface status	I	show interface actual status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface status
show interface accounting	I	show interface statistic counter	switch(config)#interface fastEthernet 2 switch(config-if)#show interface accounting
no accounting	I	Clear interface accounting information	switch(config)#interface fastEthernet 2 switch(config-if)#no accounting

6.3 Command Set List—Trunk Command Set

Commands	Level	Description	Example
aggregator priority [1to65535]	G	Set port group system priority	switch(config)#aggregator priority 22
aggregator activityport [Port Numbers]	G	Set activity port	switch(config)#aggregator activityport 2
aggregator group [GroupID] [Port-list] **lacp workp**	G	Assign a trunk group with LACP active. [GroupID] :1to3 [Port-list]:Member port list, This	switch(config)#aggregator group 1 1-4 lacp workp 2 or switch(config)#aggregator

[Workport]		parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	group 2 1,4,3 lacp workp 3
aggregator group [GroupID] [Port-list] **nolacp**	**G**	Assign a static trunk group. [GroupID] :1to3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#aggregator group 1 2-4 nolacp or switch(config)#aggreator group 1 3,1,2 nolacp
show aggregator	**P**	Show the information of trunk group	switch#show aggregator
no aggregator lacp [GroupID]	**G**	Disable the LACP function of trunk group	switch(config)#no aggreator lacp 1
no aggregator group [GroupID]	**G**	Remove a trunk group	switch(config)#no aggreator group 2

6.4 Command Set List—VLAN Command Set

Commands	Level	Description	Example
vlan database	**P**	Enter VLAN configure mode	switch#vlan database
vlan [8021q | gvrp]	**V**	To set switch VLAN mode.	switch(vlan)# vlanmode 802.1q or switch(vlan)# vlanmode gvrp
no vlan [VID]	**V**	Disable vlan group(by VID)	switch(vlan)#no vlan 2
no gvrp	**V**	Disable GVRP	switch(vlan)#no gvrp
IEEE 802.1Q VLAN			
vlan 8021q port [PortNumber] **access-link untag** [UntaggedVID]	**V**	Assign a access link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#vlan 802.1q port 3 access-link untag 33

vlan 8021q port [PortNumber] **trunk-link tag** [TaggedVID List]	V	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#vlan 8021q port 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q port 3 trunk-link tag 3-20
vlan 8021q port [PortNumber] **hybrid-link untag** [UntaggedVID] **tag** [TaggedVID List]	V	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)# vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q port 3 hybrid-link untag 5 tag 6-8
vlan 8021q aggreator [TrunkID] **access-link untag** [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(vlan)#vlan 8021q aggreator 3 access-link untag 33
vlan 8021q aggreator [TrunkID] **trunk-link tag** [TaggedVID List]	V	Assign a trunk link for VLAN by trunk group	switch(vlan)#vlan 8021q aggreator 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q aggreator 3 trunk-link tag 3-20
vlan 8021q aggreator [PortNumber] **hybrid-link untag** [UntaggedVID] **tag** [TaggedVID List]	V	Assign a hybrid link for VLAN by trunk group	switch(vlan)# vlan 8021q aggreator 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q aggreator 3 hybrid-link untag 5 tag 6-8
show vlan [VID] or **show vlan**	V	Show VLAN information	switch(vlan)#show vlan 23

6.5 Command Set List—Spanning Tree Command Set

Commands	Level	Description	Example
spanning-tree enable	G	Enable spanning tree	switch(config)#spanning-tree enable
spanning-tree priority [0to61440]	G	Configure spanning tree priority parameter	switch(config)#spanning-tree priority 32767
spanning-tree max-age [seconds]	G	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)# spanning-tree max-age 15
spanning-tree hello-time [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning-tree hello-time 3
spanning-tree forward-time [seconds]	G	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)# spanning-tree forward-time 20
stp-path-cost [1to200000000]	I	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-cost 20

		the forwarding state.	
stp-path-priority [Port Priority]	**I**	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-path-priority 127
stp-admin-p2p [Auto|True|False]	**I**	Admin P2P of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-p2p Auto
stp-admin-edge [True|False]	**I**	Admin Edge of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-edge True
stp-admin-non-stp [True|False]	**I**	Admin NonSTP of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-non-stp False
Show spanning-tree	**E**	Display a summary of the spanning-tree states.	switch>show spanning-tree
no spanning-tree	**G**	Disable spanning-tree.	switch(config)#no spanning-tree

6.6 Command Set List—QoS Command Set

Commands	Level	Description	Example
qos policy [weighted-fair|strict]	**G**	Select QOS policy scheduling	switch(config)#qos policy weighted-fair
qos prioritytype [port-based|cos-only|tos-only|cos-first|tos-first]	**G**	Setting of QOS priority type	switch(config)#qos prioritytype
qos priority portbased [Port] [lowest|low|middle|high]	**G**	Configure Port-based Priority	switch(config)#qos priority portbased 1 low

qos priority cos [Priority][lowest|low|middle|high]	**G**	Configure COS Priority	switch(config)#qos priority cos 22 middle
qos priority tos [Priority][lowest|low|middle|high]	**G**	Configure TOS Priority	switch(config)#qos priority tos 3 high
show qos	**P**	Display the information of QoS configuration	switch>show qos
no qos	**G**	Disable QoS function	switch(config)#no qos

6.7 Command Set List—IGMP Command Set

Commands	Level	Description	Example
igmp enable	**G**	Enable IGMP snooping function	switch(config)#igmp enable
Igmp-query auto	**G**	Set IGMP query to auto mode	switch(config)#Igmp-query auto
Igmp-query force	**G**	Set IGMP query to force mode	switch(config)#Igmp-query force
show igmp configuration	**P**	Displays the details of an IGMP configuration.	switch#show igmp configuration
show igmp multi	**P**	Displays the details of an IGMP snooping entries.	switch#show igmp multi
no igmp	**G**	Disable IGMP snooping function	switch(config)#no igmp
no igmp-query	**G**	Disable IGMP query	switch#no igmp-query

6.8 Command Set List—MAC/Filter Table Command Set

Commands	Level	Description	Example
mac-address-table static hwaddr [MAC]	**I**	Configure MAC address table of interface (static).	switch(config)#interface fastEthernet 2 switch(config-if)#mac-address-table static hwaddr 000012345678
mac-address-table filter hwaddr [MAC]	**G**	Configure MAC address table(filter)	switch(config)#mac-address-table filter hwaddr 000012348678
show	**P**	Show all MAC address table	switch#show

mac-address-table			mac-address-table
show mac-address-table static	**P**	Show static MAC address table	switch#show mac-address-table static
show mac-address-table filter	**P**	Show filter MAC address table.	switch#show mac-address-table filter
no mac-address-table static hwaddr [MAC]	**I**	Remove an entry of MAC address table of interface (static)	switch(config)#interface fastEthernet 2 switch(config-if)#no mac-address-table static hwaddr 000012345678
no mac-address-table filter hwaddr [MAC]	**G**	Remove an entry of MAC address table (filter)	switch(config)#no mac-address-table filter hwaddr 000012348678
no mac-address-table	**G**	Remove dynamic entry of MAC address table	switch(config)#no mac-address-table

6.9 Command Set List—SNMP Command Set

Commands	Level	Description	Example
snmp agent-mode [v1v2c | v3]	**G**	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2c
snmp-server host [IP address] **community** [Community-string] **trap-version** [v1|v2c]	**G**	Configure SNMP server host information and community string	switch(config)#snmp-server host 192.168.10.50 community public trap-version v1 (remove) Switch(config)# no snmp-server host 192.168.10.50
snmp community-strings [Community-string] **right** [RO|RW]	**G**	Configure the community string right	switch(config)#snmp community-strings public right RO or switch(config)#snmp

			community-strings public right RW
snmp snmpv3-user [User Name] **password** [Authentication Password] [Privacy Password]	**G**	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#snmp snmpv3-user test01 password AuthPW PrivPW
show snmp	**P**	Show SNMP configuration	switch#show snmp
show snmp-server	**P**	Show specified trap server information	switch#show snmp-server
no snmp community-strings [Community]	**G**	Remove the specified community.	switch(config)#no snmp community-strings public
no snmp snmpv3-user [User Name] **password** [Authentication Password] [Privacy Password]	**G**	Remove specified user of SNMPv3 agent. Privacy password could be empty.	switch(config)# no snmp snmpv3-user test01 password AuthPW PrivPW
no snmp-server host [Host-address]	**G**	Remove the SNMP server host.	switch(config)#no snmp-server 192.168.10.50

6.10 Command Set List—Port Mirroring Command Set

Commands	Level	Description	Example
monitor rx	**G**	Set RX destination port of monitor function	switch(config)#monitor rx
monitor tx	**G**	Set TX destination port of monitor function	switch(config)#monitor tx
show monitor	**P**	Show port monitor information	switch#show monitor
monitor [RX|TX|Both]	**I**	Configure source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#monitor RX
show monitor	**I**	Show port monitor information	switch(config)#interface

			fastEthernet 2 switch(config-if)#show monitor
no monitor	**I**	Disable source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#no monitor

6.11 Command Set List—802.1x Command Set

Commands	Level	Description	Example
8021x enable	**G**	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiousip [IP address]	**G**	Use the 802.1x system radious IP global configuration command to change the radious server IP.	switch(config)# 8021x system radiousip 192.168.1.1
8021x system serverport [port ID]	**G**	Use the 802.1x system server port global configuration command to change the radious server port	switch(config)# 8021x system serverport 1815
8021x system accountport [port ID]	**G**	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# 8021x system accountport 1816
8021x system sharekey [ID]	**G**	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# 8021x system sharekey 123456
8021x system nasid [words]	**G**	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# 8021x system nasid test1
8021x misc quietperiod [sec.]	**G**	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# 8021x misc quietperiod 10

8021x misc txperiod [sec.]	**G**	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# 8021x misc txperiod 5
8021x misc supportimeout [sec.]	**G**	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# 8021x misc supportimeout 20
8021x misc servertimeout [sec.]	**G**	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#8021x misc servertimeout 20
8021x misc maxrequest [number]	**G**	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# 8021x misc maxrequest 3
8021x misc reauthperiod [sec.]	**G**	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# 8021x misc reauthperiod 3000
8021x portstate [disable | reject | accept | authorize]	**I**	Use the 802.1x port state interface configuration command to set the state of the selected port.	switch(config)#interface fastethernet 3 switch(config-if)#8021x portstate accept
show 8021x	**E**	Display a summary of the 802.1x properties and also the port sates.	switch>show 8021x
no 8021x	**G**	Disable 802.1x function	switch(config)#no 8021x

6.12 Command Set List—TFTP Command Set

Commands	Level	Description	Defaults Example
backup flash:backup_cfg	**G**	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#backup flash:backup_cfg
restore flash:restore_cfg	**G**	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch(config)#restore flash:restore_cfg

upgrade flash:upgrade_fw	**G**	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#upgrade lash:upgrade_fw

6.13 Command Set List—SYSLOG, SMTP, EVENT Command Set

Commands	Level	Description	Example
systemlog ip [IP address]	**G**	Set System log server IP address.	switch(config)# systemlog ip 192.168.1.100
systemlog mode [client|server|both]	**G**	Specified the log mode	switch(config)# systemlog mode both
show systemlog	**E**	Display system log.	Switch>show systemlog
show systemlog	**P**	Show system log client & server information	switch#show systemlog
no systemlog	**G**	Disable systemlog functon	switch(config)#no systemlog
smtp enable	**G**	Enable SMTP function	switch(config)#smtp enable
smtp serverip [IP address]	**G**	Configure SMTP server IP	switch(config)#smtp serverip 192.168.1.5
smtp authentication	**G**	Enable SMTP authentication	switch(config)#smtp authentication
smtp account [account]	**G**	Configure authentication account	switch(config)#smtp account User
smtp password [password]	**G**	Configure authentication password	switch(config)#smtp password
smtp rcptemail [Index] [Email address]	**G**	Configure Rcpt e-mail Address	switch(config)#smtp rcptemail 1 Alert@test.com
show smtp	**P**	Show the information of SMTP	switch#show smtp
no smtp	**G**	Disable SMTP function	switch(config)#no smtp
event device-cold-start [Systemlog|SMTP|Both]	**G**	Set cold start event type	switch(config)#event device-cold-start both
event authentication-failure	**G**	Set Authentication failure event type	switch(config)#event authentication-failure both

[Systemlog|SMTP|Both]			
event O-Ring-topology-change [Systemlog|SMTP|Both]	**G**	Set s ring topology changed event type	switch(config)#event ring-topology-change both
event systemlog [Link-UP|Link-Down|Both]	**I**	Set port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#event systemlog both
event smtp [Link-UP|Link-Down|Both]	**I**	Set port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#event smtp both
show event	**P**	Show event selection	switch#show event
no event device-cold-start	**G**	Disable cold start event type	switch(config)#no event device-cold-start
no event authentication-failure	**G**	Disable Authentication failure event typ	switch(config)#no event authentication-failure
no event O-Ring-topology-change	**G**	Disable O-Ring topology changed event type	switch(config)#no event ring-topology-change
no event systemlog	**I**	Disable port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#no event systemlog
no event smpt	**I**	Disable port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#no event smtp
show systemlog	**P**	Show system log client & server information	switch#show systemlog

6.14 Command Set List—SNTP Command Set

Commands	Level	Description	Example
sntp enable	G	Enable SNTP function	switch(config)#sntp enable
sntp daylight	G	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight
sntp daylight-period [Start time] [End time]	G	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# sntp daylight-period 20060101-01:01 20060202-01-01
sntp daylight-offset [Minute]	G	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight-offset 3
sntp ip [IP]	G	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp ip 192.169.1.1
sntp timezone [Timezone]	G	Set timezone index, use "show sntp timzezone" command to get more information of index number	switch(config)#sntp timezone 22
show sntp	P	Show SNTP information	switch#show sntp
show sntp timezone	P	Show index number of time zone list	switch#show sntp timezone
no sntp	G	Disable SNTP function	switch(config)#no sntp
no sntp daylight	G	Disable daylight saving time	switch(config)#no sntp daylight

6.15 Command Set List—O-Ring Command Set

Commands	Level	Description	Example
Ring enable	G	Enable O-Ring	switch(config)# ring enable
Ring master	G	Enable ring master	switch(config)# ring master
Ring couplering	G	Enable couple ring	switch(config)# ring couplering
Ring dualhoming	G	Enable dual homing	switch(config)# ring dualhoming

Ring ringport [1st Ring Port] [2nd Ring Port]	**G**	Configure 1st/2nd Ring Port	switch(config)# ring ringport 7 8
Ring couplingport [Coupling Port]	**G**	Configure Coupling Port	switch(config)# ring couplingport 1
Ring controlport [Control Port]	**G**	Configure Control Port	switch(config)# ring controlport 2
Ring homingport [Dual Homing Port]	**G**	Configure Dual Homing Port	switch(config)# ring homingport 3
show Ring	**P**	Show the information of O-Ring	switch#show ring
no Ring	**G**	Disable O-Ring	switch(config)#no ring
no Ring master	**G**	Disable ring master	switch(config)# no ring master
no Ring couplering	**G**	Disable couple ring	switch(config)# no ring couplering
no Ring dualhoming	**G**	Disable dual homing	switch(config)# no ring dualhoming