IES/IGS/IGPS 3000-LA Series

Industrial Managed Ethernet Switch

Function Manual

V1.1A

www.oringnet.com

ORing Industrial Networking Corp.

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 231, Taiwan, R.O.C.
Tel: + 886 2 2218 1066 // Fax: + 886 2 2218 1014
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.

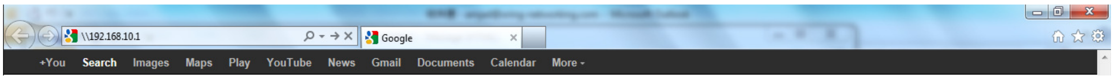
Note: By default, IE5.0 or later version do not allow Java applets to open sockets. You need to modify the browser setting separately in order to enable Java applets for network ports.

Management via Web Browser

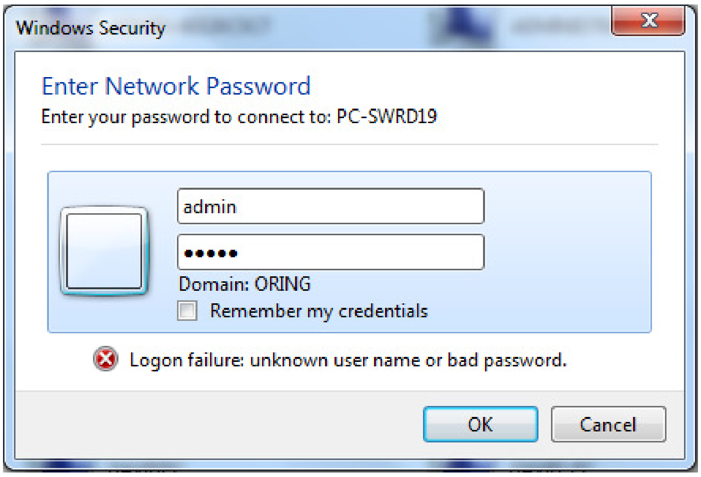
Follow the steps below to manage your switch via a Web browser

System Login

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



3. The login screen appears.
4. Type in the username and password. The default username and password is **admin**.
5. Click **Enter** or **OK** button and the main interface of the management page appears.


Windows Security

Enter Network Password

Enter your password to connect to: PC-SWRD19

admin

●●●●●

Domain: ORING

□ Remember my credentials

Logon failure: unknown user name or bad password.

Note: you can use the following default values:

IP Address: **192.168.10.1**

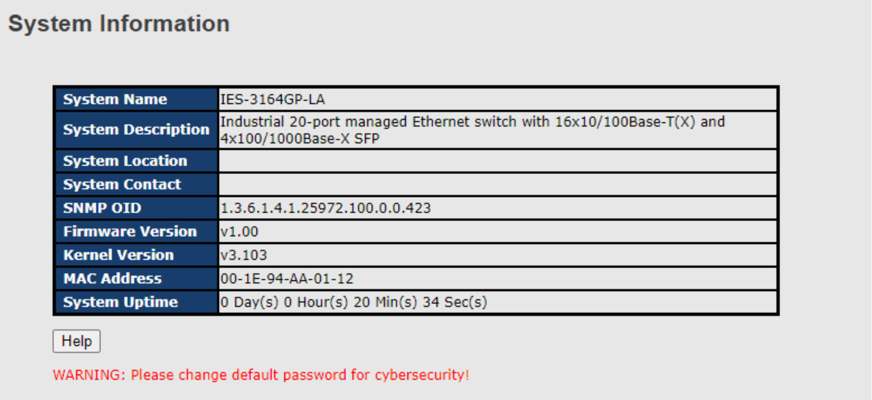
Subnet Mask: **255.255.255.0**

Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

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



System Information

System Name	IES-3164GP-LA
System Description	Industrial 20-port managed Ethernet switch with 16x10/100Base-T(X) and 4x100/1000Base-X SFP
System Location	
System Contact	
SNMP OID	1.3.6.1.4.1.25972.100.0.0.423
Firmware Version	v1.00
Kernel Version	v3.103
MAC Address	00-1E-94-AA-01-12
System Uptime	0 Day(s) 0 Hour(s) 20 Min(s) 34 Sec(s)

WARNING: Please change default password for cybersecurity!

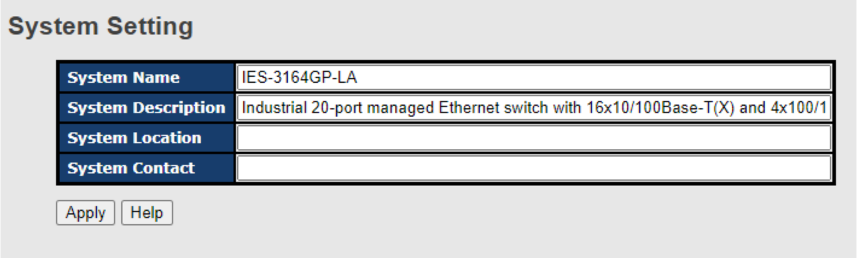
On the left hand side of the management interface shows links to various settings. Clicking on the links will bring you to individual configuration pages.

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.



System Setting

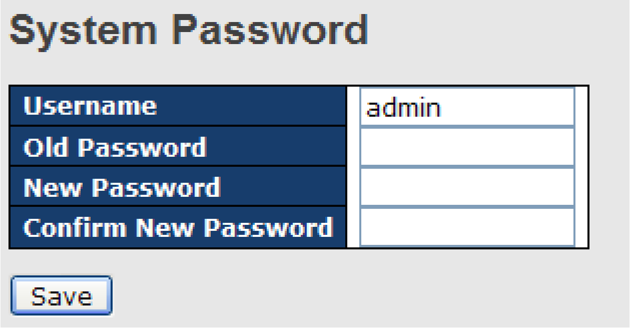
System Name	IES-3164GP-LA
System Description	Industrial 20-port managed Ethernet switch with 16x10/100Base-T(X) and 4x100/1
System Location	
System Contact	

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.
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.



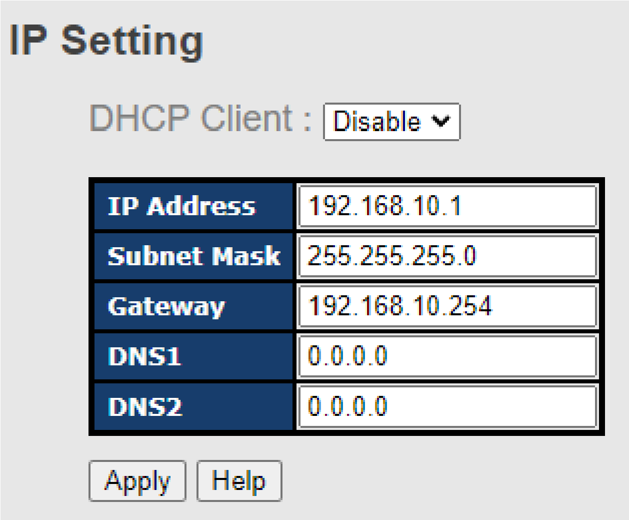
System Password

Username	admin
Old Password	
New Password	
Confirm New Password	

Label	Description
Old Password	The existing password. If this is incorrect, you cannot set the new password.
New Password	The new system password. The allowed string length is 0 to 31, and only ASCII characters from 32 to 126 are allowed.
Confirm New Password	Re-type the new password.
Save	Click to save changes.

1.1.3 IP Settings

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



IP Setting

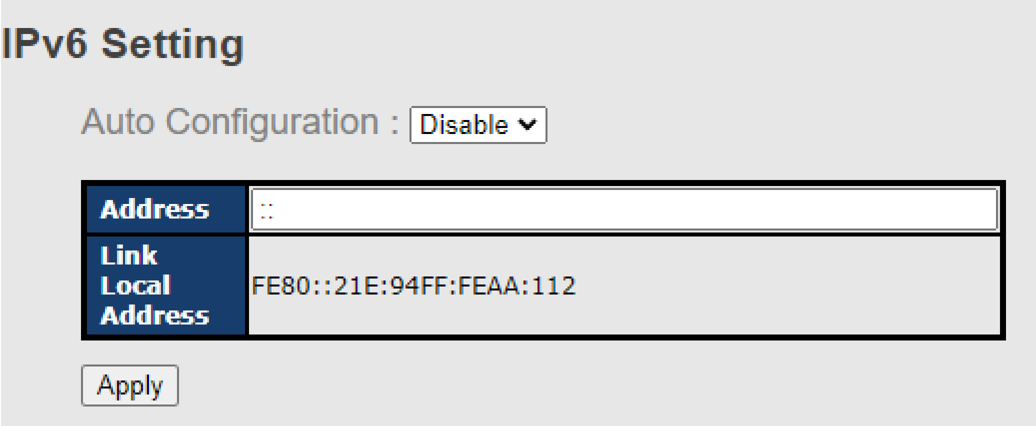
DHCP Client : Disable

IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway	192.168.10.254
DNS1	0.0.0.0
DNS2	0.0.0.0

Label	Description
DHCP Client	Enable the DHCP client by checking this box. 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	Assigns the network gateway for the switch. The default gateway is **192.168.10.254**.
DNS 1 / DNS 2	Enter the IP address of the DNS server in dotted decimal notation.
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously saved values

1.1.4 IPv6 Settings

IPv6 is the next-generation IP that uses a 128-bit address standard. It is developed to supplement, and eventually replace the IPv4 protocol. You can configure IPv6 information of the switch on the following page.



IPv6 Setting

Auto Configuration : Disable

Address	::
Link Local Address	FE80::21E:94FF:FEAA:112

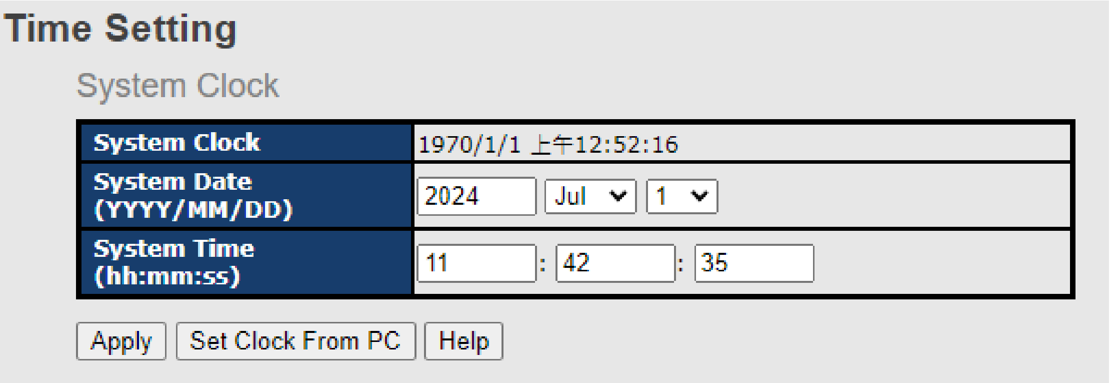
Label	Description
Auto Configuration	Check to enable IPv6 auto-configuration. If the system cannot obtain the stateless address in time, the configured IPv6 settings will be used. The router may delay responding to a router solicitation for a few seconds; therefore, the total time needed to complete auto-configuration may be much longer.
Address	Specify an IPv6 address for the switch. IPv6 address consists of 128 bits represented as eight groups of four hexadecimal digits with a colon separating each field (:). For example, in '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'.

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



Time Setting

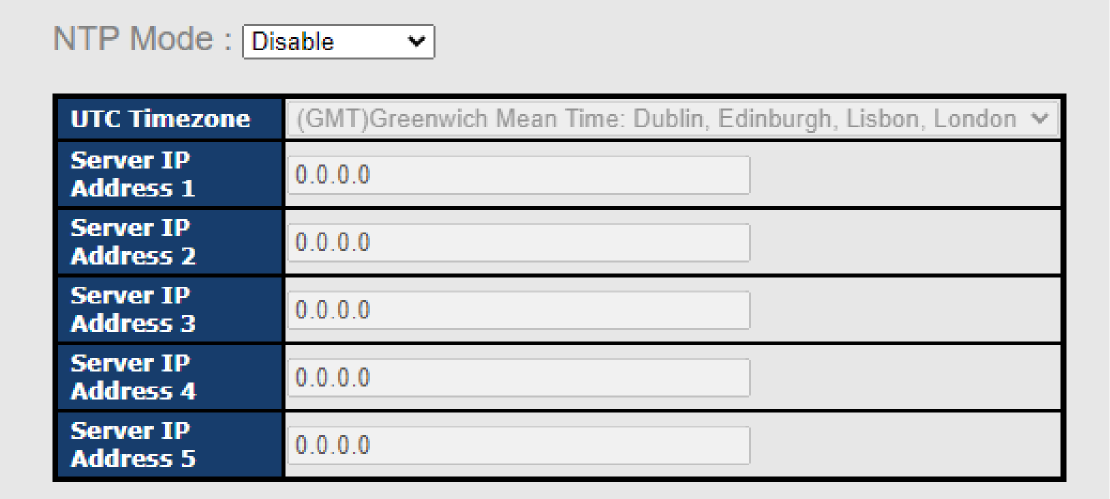
System Clock

System Clock	1970/1/1 上午12:52:16
System Date (YYYY/MM/DD)	2024 Jul 1
System Time (hh:mm:ss)	11 : 42 : 35

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

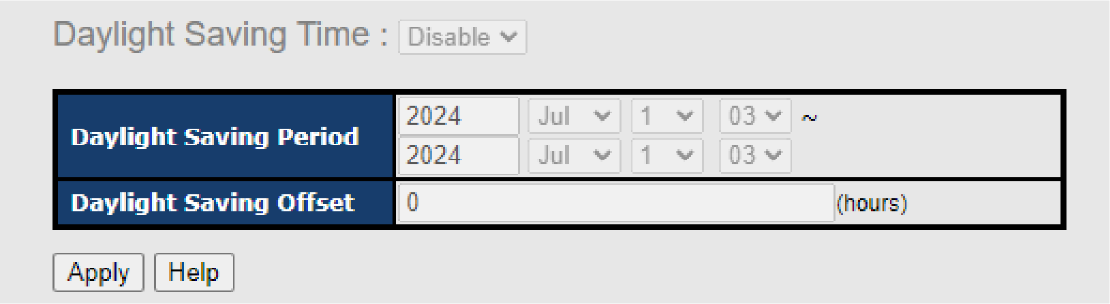
NTP

NTP (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.



NTP Mode : Disable

UTC Timezone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
Server IP Address 1	0.0.0.0
Server IP Address 2	0.0.0.0
Server IP Address 3	0.0.0.0
Server IP Address 4	0.0.0.0
Server IP Address 5	0.0.0.0



Daylight Saving Time : Disable

Daylight Saving Period	2024 Jul 1 03 ~ 2024 Jul 1 03
Daylight Saving Offset	0 (hours)

Label	Description
NTP Client	Enables or disables NTP function to retrieve the time from a NTP Server / Client.
UTC Time zone	Selects the time zone for the switch according to its location
NTP Sever Address (1 ~ 5)	Enters the NTP 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.

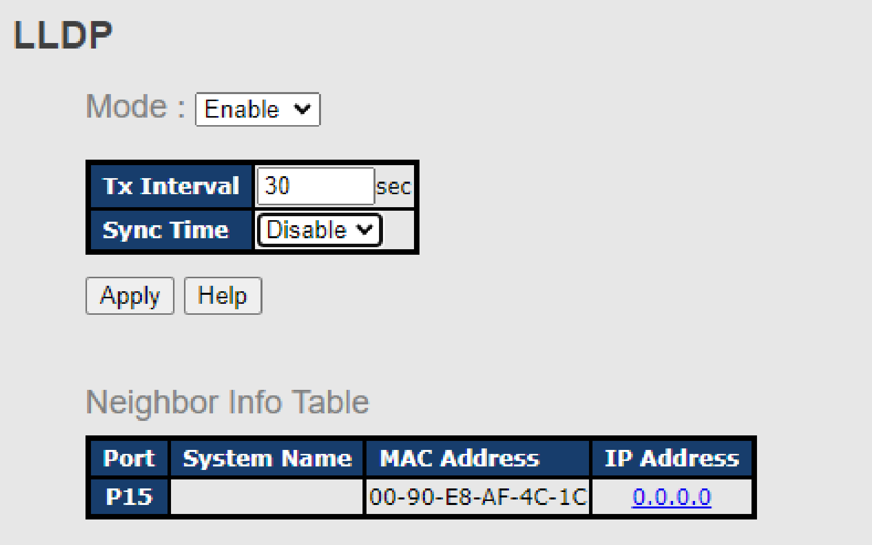
Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11 am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard 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

1.1.6 LLDP

LLDP Configurations

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.



LLDP

Mode : Enable

Tx Interval	30	sec
Sync Time	Disable	

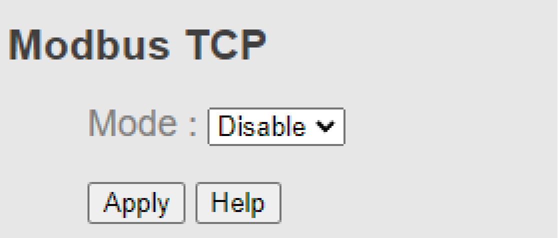
Neighbor Info Table

Port	System Name	MAC Address	IP Address
P15		00-90-E8-AF-4C-1C	0.0.0.0

Label	Description
Mode	Enable / Disable LLDP Function
Tx Interval	LLDP Packet reflash interval
Sync Time	Sync Time info in LLDP ,

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.



Modbus TCP

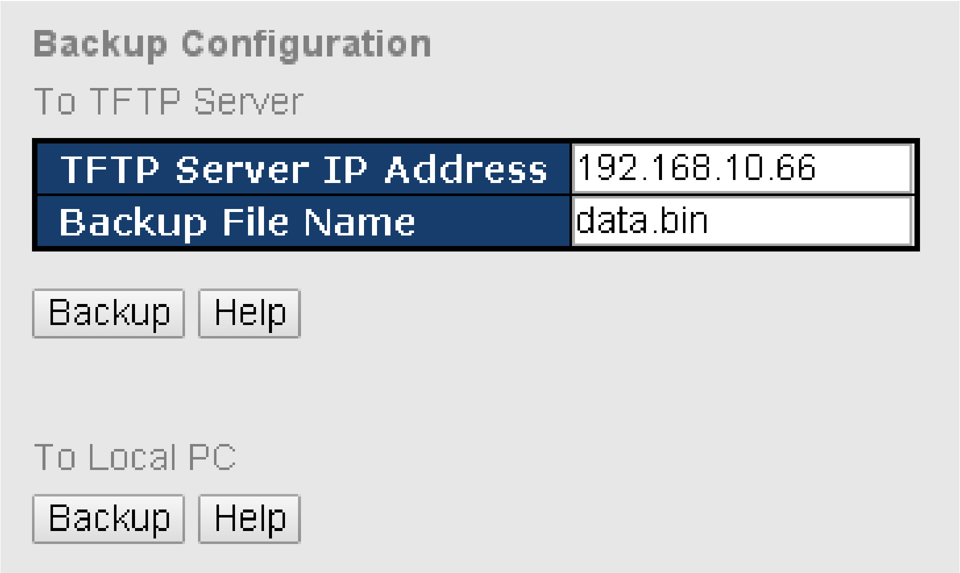
Mode : Disable

Label	Description
Mode	Shows the existing status of the Modbus TCP function

1.1.8 Backup/Restore Configurations

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.



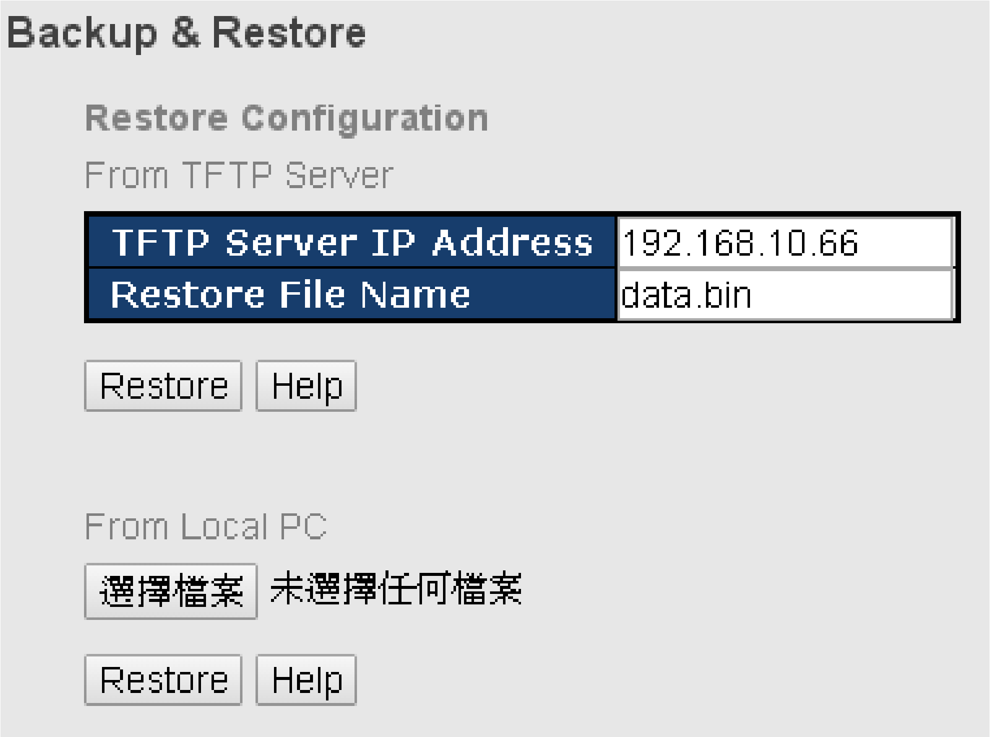
Backup Configuration

To TFTP Server

TFTP Server IP Address	192.168.10.66
Backup File Name	data.bin

To Local PC

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



Backup & Restore

Restore Configuration

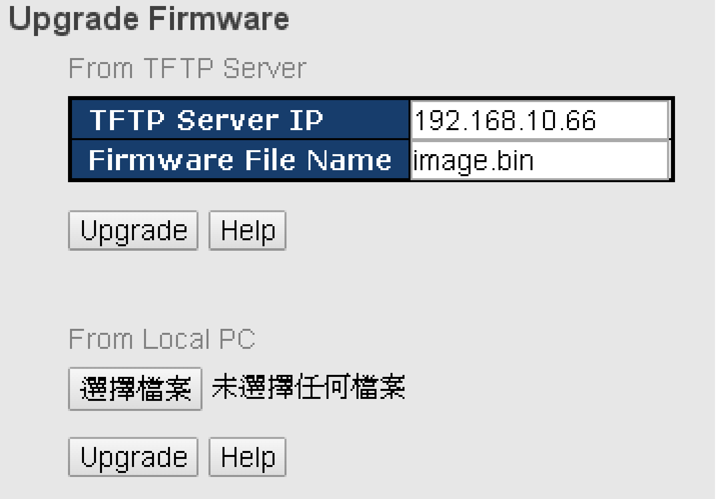
From TFTP Server

TFTP Server IP Address	192.168.10.66
Restore File Name	data.bin

From Local PC

1.1.9 Firmware Update

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.



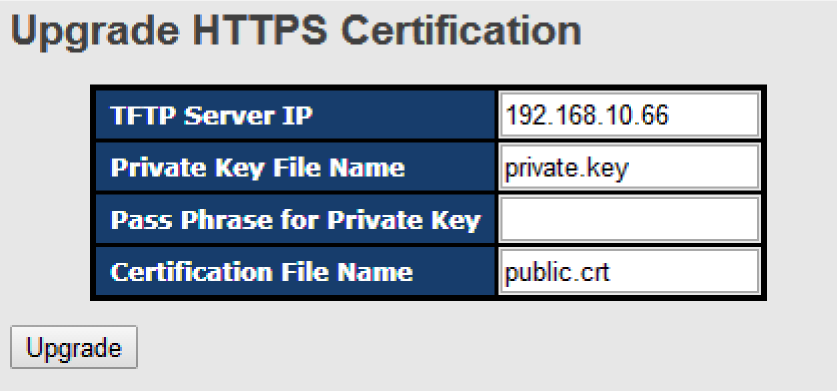
Upgrade Firmware

From TFTP Server

TFTP Server IP	192.168.10.66
Firmware File Name	image.bin

1.1.10 Upgrade HTTPS Certificate

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.



Upgrade HTTPS Certification

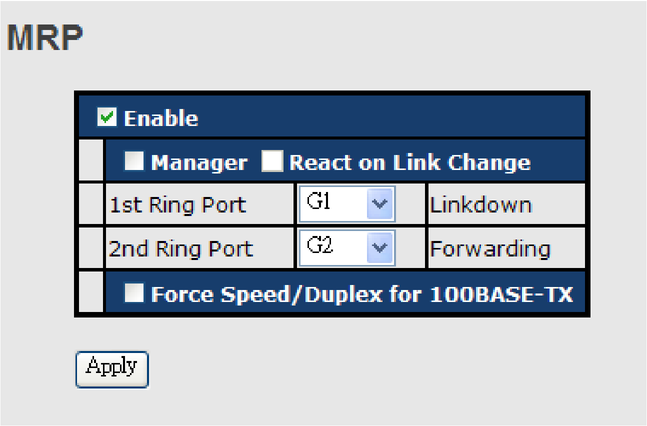
TFTP Server IP	192.168.10.66
Private Key File Name	private.key
Pass Phrase for Private Key	
Certification File Name	public.crt

1.2 Redundancy

1.2.1 MRP

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).

Configurations



MRP

☑ Enable

□ Manager □ React on Link Change

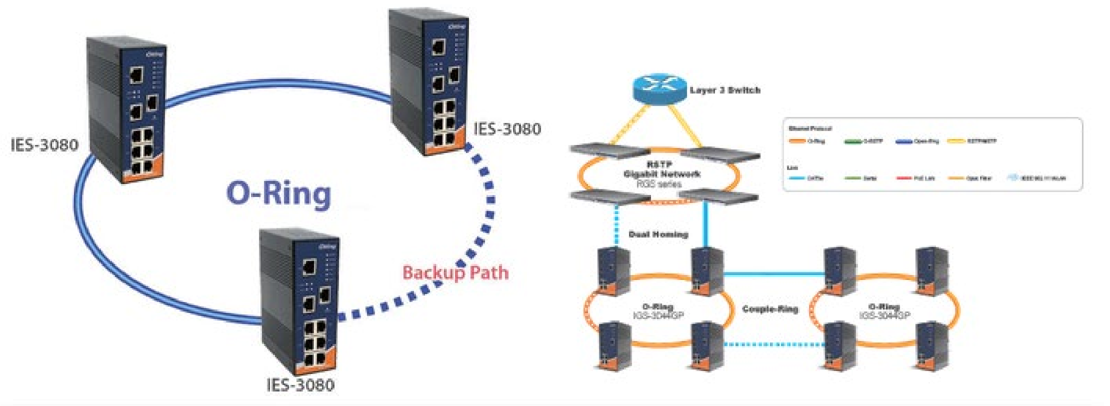
1st Ring Port	G1	Linkdown
2nd Ring Port	G2	Forwarding

□ Force Speed/Duplex for 100BASE-TX

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)

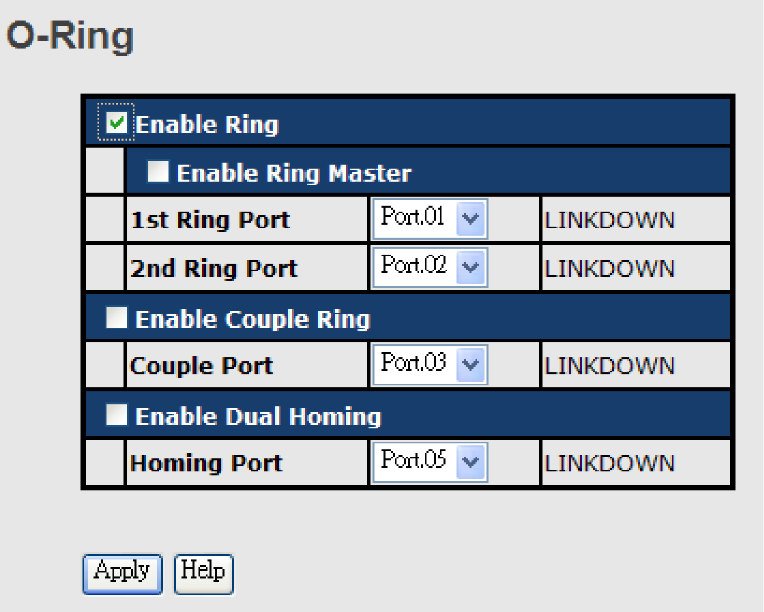
1.2.2 O-Ring

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.



Configurations

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



O-Ring

☑ Enable Ring			
	☐ Enable Ring Master		
	1st Ring Port	Port.01	LINKDOWN
	2nd Ring Port	Port.02	LINKDOWN
☐ Enable Couple Ring			
	Couple Port	Port.03	LINKDOWN
☐ Enable Dual Homing			
	Homing Port	Port.05	LINKDOWN

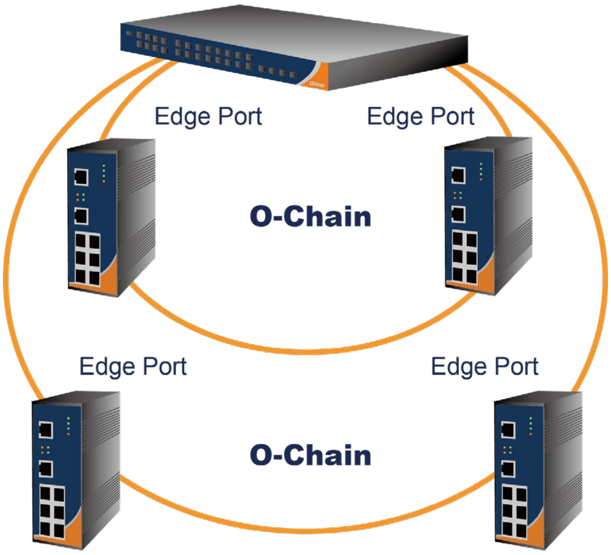
Label	Description
Enable Ring	Check to enable O-Ring topology.
Enable Ring Master	Only one ring master is allowed in a ring. However, if more than one switches are set to enable **Ring Master**, the switch with the lowest MAC address will be the active ring master and the others will be backup masters.
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.

1.2.3 O-Chain

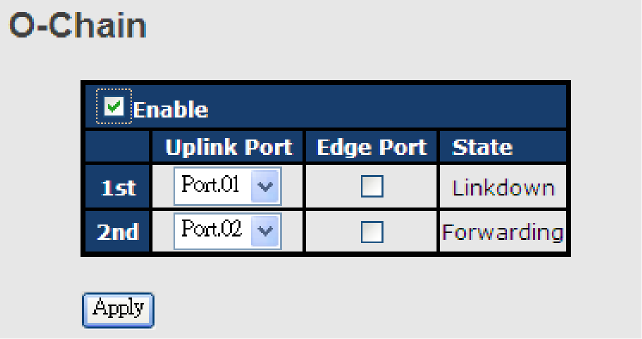
O-Chain is ORing's revolutionary network redundancy technology which enhances network redundancy for any backbone networks, providing ease-of-use and maximum fault-recovery swiftness, flexibility, compatibility, and cost-effectiveness in a set of network redundancy topologies. The self-healing Ethernet 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.



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.


O-Chain

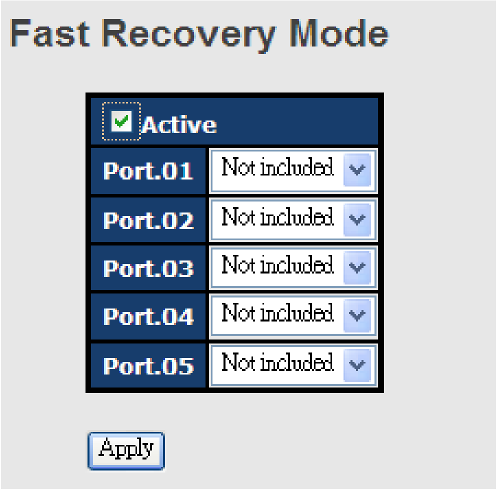
☑ Enable

	Uplink Port	Edge Port	State
1st	Port.01	□	Linkdown
2nd	Port.02	□	Forwarding

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.

1.2.4 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.



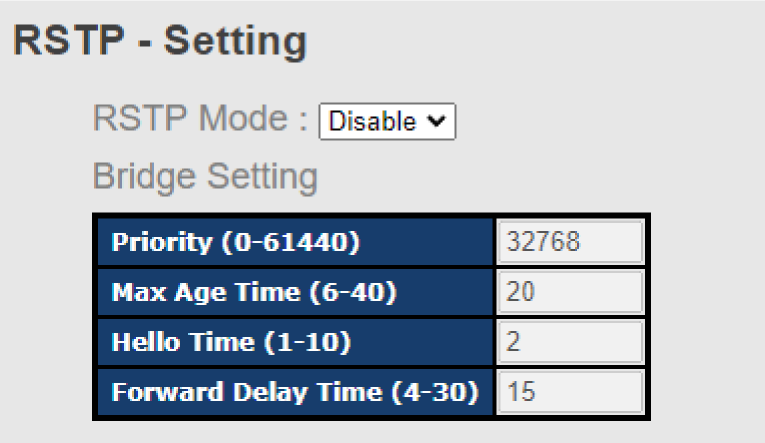
Fast Recovery Mode

☑ Active

Port.01	Not included
Port.02	Not included
Port.03	Not included
Port.04	Not included
Port.05	Not included

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.

1.2.5 RSTP



RSTP - Setting

RSTP Mode : Disable

Bridge Setting

Priority (0-61440)	32768
Max Age Time (6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15

Label	**Description**
RSTP mode	You must enable or disable RSTP function before configuring the

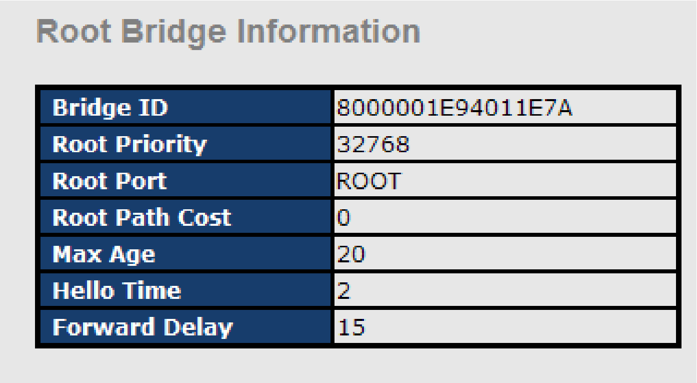
	related parameters.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, you must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule
Max Age 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)

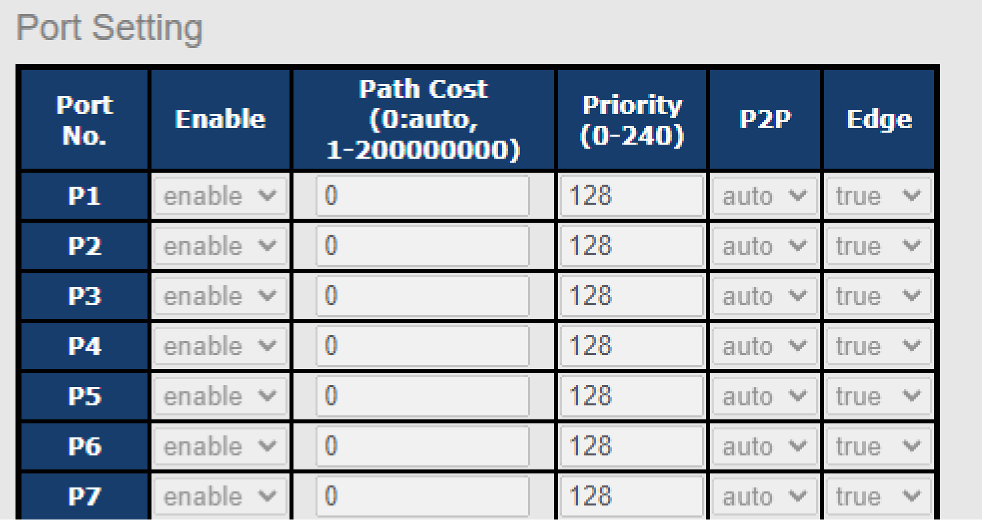
The following pages show the information of the root bridge, including its port status.

Information



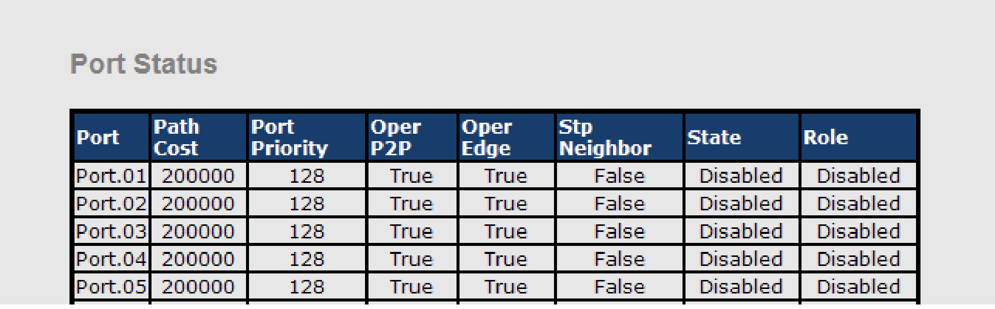
Root Bridge Information

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



Port Setting

Port No.	Enable	Path Cost (0:auto, 1-200000000)	Priority (0-240)	P2P	Edge
P1	enable	0	128	auto	true
P2	enable	0	128	auto	true
P3	enable	0	128	auto	true
P4	enable	0	128	auto	true
P5	enable	0	128	auto	true
P6	enable	0	128	auto	true
P7	enable	0	128	auto	true



Port Status

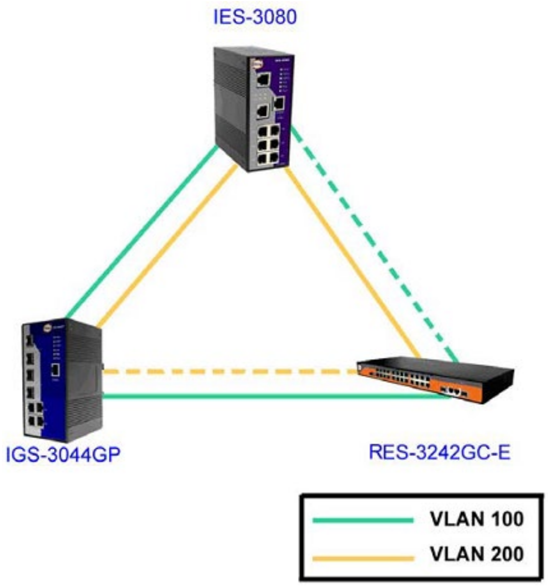
Port	Path Cost	Port Priority	Oper P2P	Oper Edge	Stp Neighbor	State	Role
Port.01	200000	128	True	True	False	Disabled	Disabled
Port.02	200000	128	True	True	False	Disabled	Disabled
Port.03	200000	128	True	True	False	Disabled	Disabled
Port.04	200000	128	True	True	False	Disabled	Disabled
Port.05	200000	128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

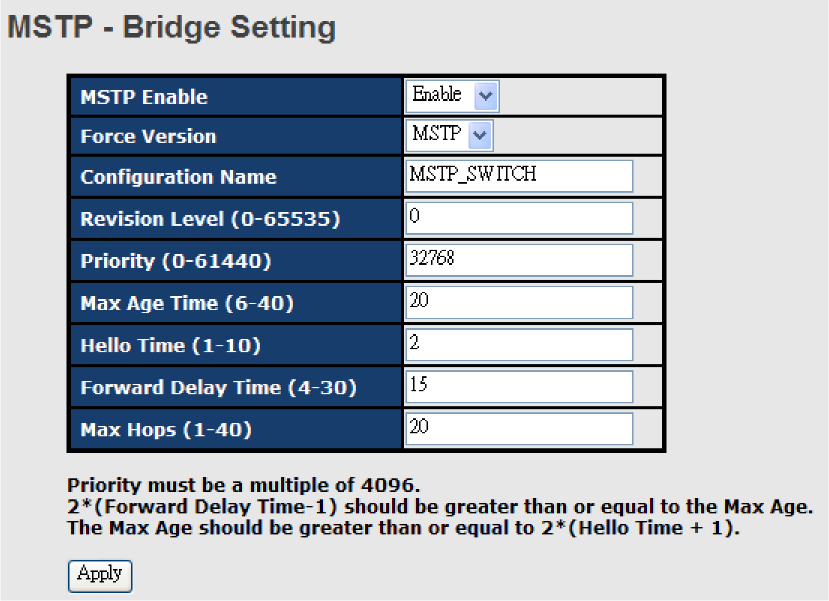
1.2.6 MSTP

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.



MSTP - Bridge Setting

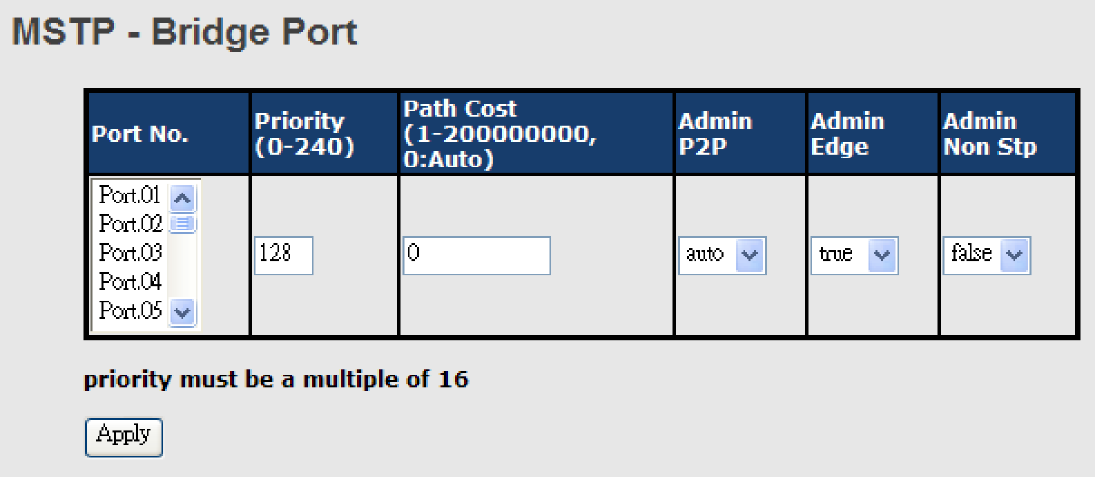
MSTP Enable	Enable
Force Version	MSTP
Configuration Name	MSTP_SWITCH
Revision Level (0-65535)	0
Priority (0-61440)	32768
Max Age Time (6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15
Max Hops (1-40)	20

Priority must be a multiple of 4096.
2*(Forward Delay Time-1) should be greater than or equal to the Max Age.
The Max Age should be greater than or equal to 2*(Hello Time + 1).

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



MSTP - Bridge Port

Port No.	Priority (0-240)	Path Cost (1-200000000, 0:Auto)	Admin P2P	Admin Edge	Admin Non Stp
Port.01 Port.02 Port.03 Port.04 Port.05	128	0	auto	true	false

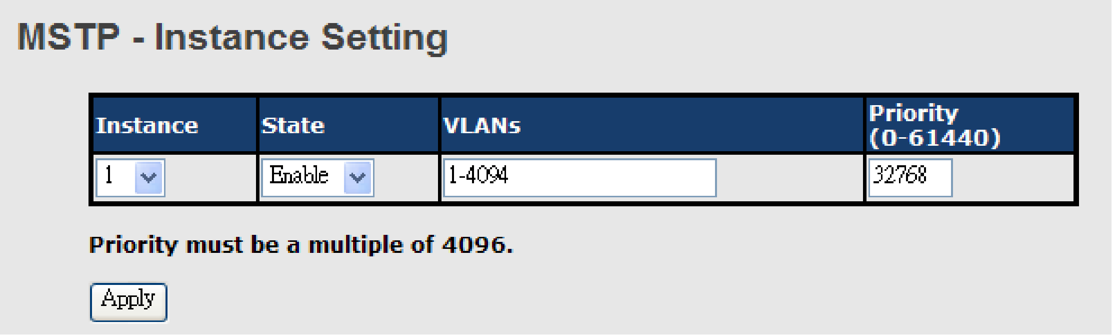
priority must be a multiple of 16

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.



MSTP - Instance Setting

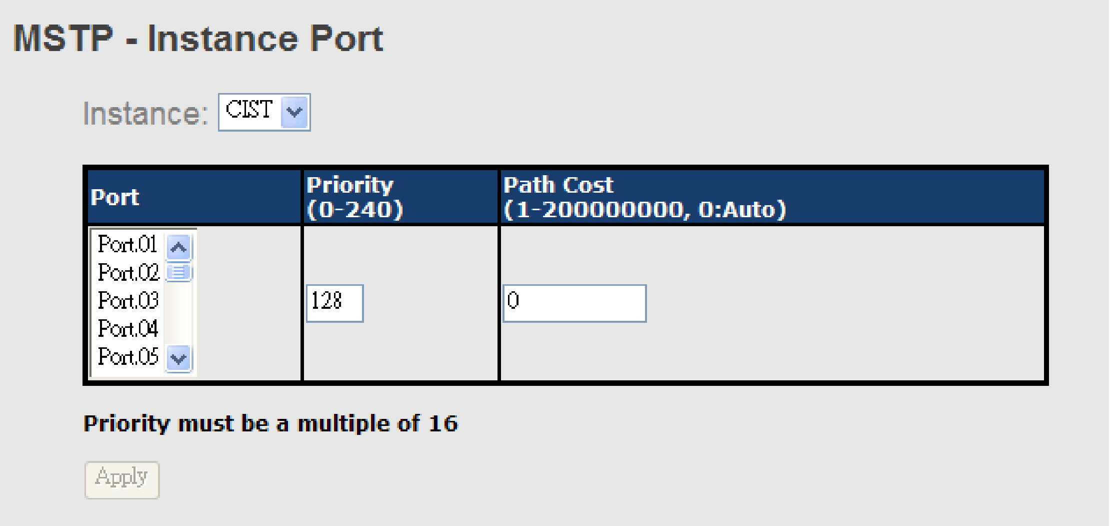
Instance	State	VLANs	Priority (0-61440)
1	Enable	1-4094	32768

Priority must be a multiple of 4096.

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.



MSTP - Instance Port

Instance: CIST

Port	Priority (0-240)	Path Cost (1-200000000, 0:Auto)
Port.01 Port.02 Port.03 Port.04 Port.05	128	0

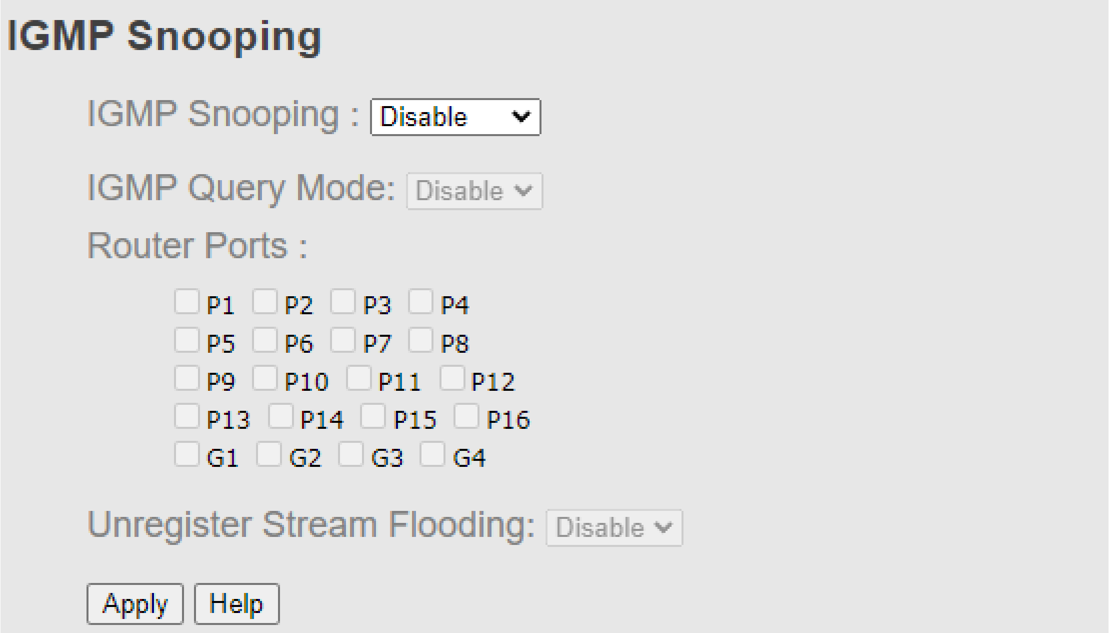
Priority must be a multiple of 16

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.

1.3 Multicast

1.3.1 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.



IGMP Snooping

IGMP Snooping : Disable

IGMP Query Mode: Disable

Router Ports :

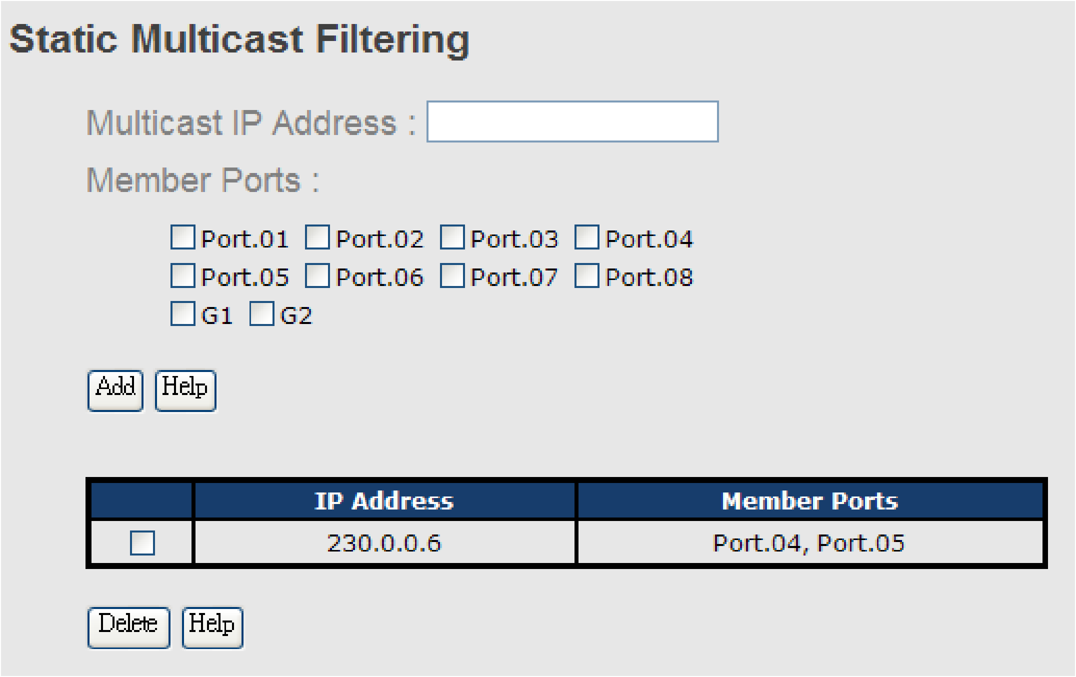
□ P1 □ P2 □ P3 □ P4
□ P5 □ P6 □ P7 □ P8
□ P9 □ P10 □ P11 □ P12
□ P13 □ P14 □ P15 □ P16
□ G1 □ G2 □ G3 □ G4

Unregister Stream Flooding: Disable

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.
Router Port	Router port will always forwarding multicast packet .
Apply	Click to apply the configurations.
Help	Shows help file.

1.3.2 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.


Static Multicast Filtering

Multicast IP Address :

Member Ports :

□ Port.01 □ Port.02 □ Port.03 □ Port.04
□ Port.05 □ Port.06 □ Port.07 □ Port.08
□ G1 □ G2

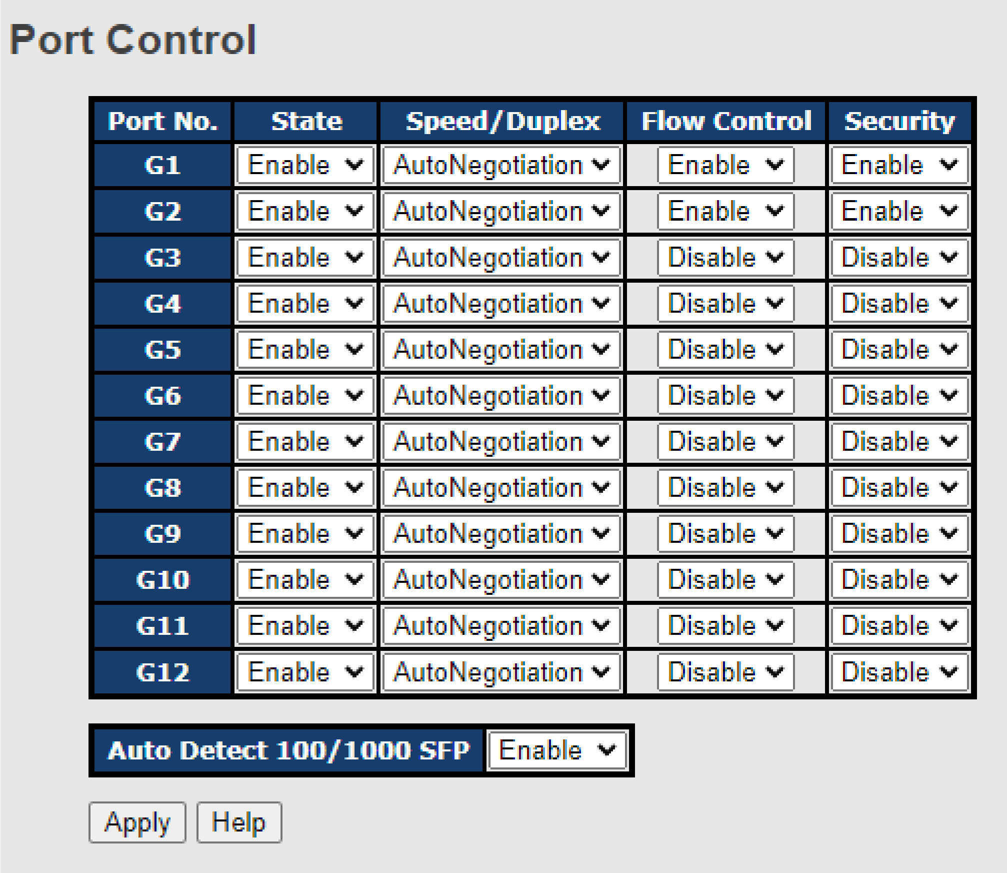
	IP Address	Member Ports
□	230.0.0.6	Port.04, Port.05

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.

1.4 Port Setting

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

Port Control



Port Control

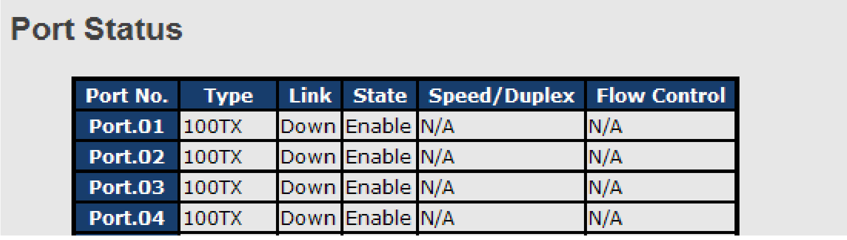
Port No.	State	Speed/Duplex	Flow Control	Security
G1	Enable	AutoNegotiation	Enable	Enable
G2	Enable	AutoNegotiation	Enable	Enable
G3	Enable	AutoNegotiation	Disable	Disable
G4	Enable	AutoNegotiation	Disable	Disable
G5	Enable	AutoNegotiation	Disable	Disable
G6	Enable	AutoNegotiation	Disable	Disable
G7	Enable	AutoNegotiation	Disable	Disable
G8	Enable	AutoNegotiation	Disable	Disable
G9	Enable	AutoNegotiation	Disable	Disable
G10	Enable	AutoNegotiation	Disable	Disable
G11	Enable	AutoNegotiation	Disable	Disable
G12	Enable	AutoNegotiation	Disable	Disable

Auto Detect 100/1000 SFP: Enable

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	Enable or Disable FLOW Control function
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

1.4.1 Port Status

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

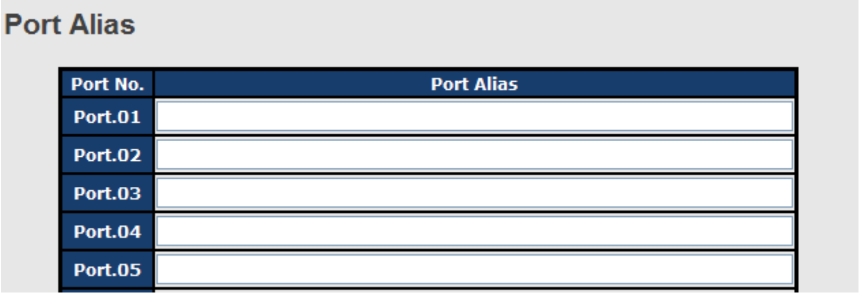


Port Status

Port No.	Type	Link	State	Speed/Duplex	Flow Control
Port.01	100TX	Down	Enable	N/A	N/A
Port.02	100TX	Down	Enable	N/A	N/A
Port.03	100TX	Down	Enable	N/A	N/A
Port.04	100TX	Down	Enable	N/A	N/A

1.4.2 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.

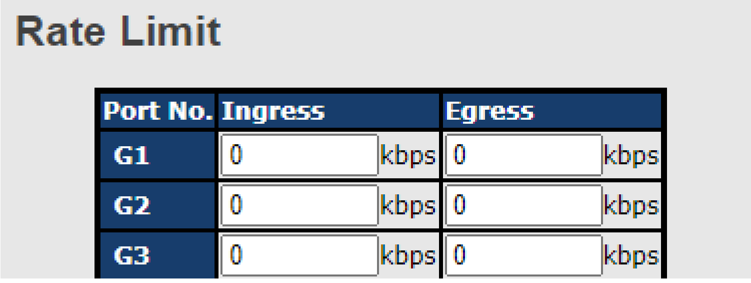


Port Alias

Port No.	Port Alias
Port.01	
Port.02	
Port.03	
Port.04	
Port.05	

1.4.3 Rate Limit

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



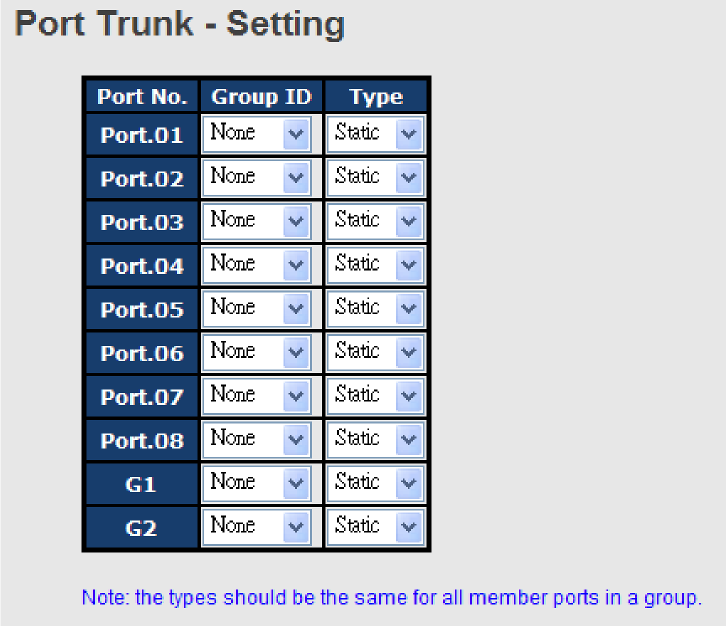
Rate Limit

Port No.	Ingress	Egress
G1	0 kbps	0 kbps
G2	0 kbps	0 kbps
G3	0 kbps	0 kbps

Label	Description
Ingress	The transmission rate for incoming traffic
Egress	The transmission rate for outgoing traffic
Apply	Click to activate the configurations.

1.4.4 Port Trunk

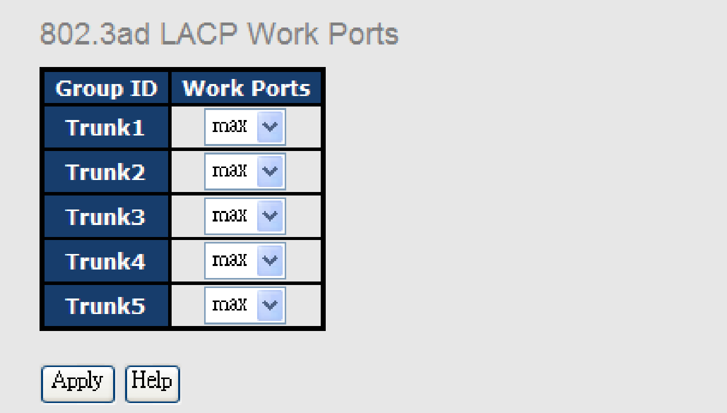
A port trunk is a group of ports that have been grouped together to function as one logical path. This method provides an economical way for you to increase the bandwidth between the switch and another networking device. In addition, it is useful when a single physical link between the devices is insufficient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



Port Trunk - Setting

Port No.	Group ID	Type
Port.01	None	Static
Port.02	None	Static
Port.03	None	Static
Port.04	None	Static
Port.05	None	Static
Port.06	None	Static
Port.07	None	Static
Port.08	None	Static
G1	None	Static
G2	None	Static

Note: the types should be the same for all member ports in a group.

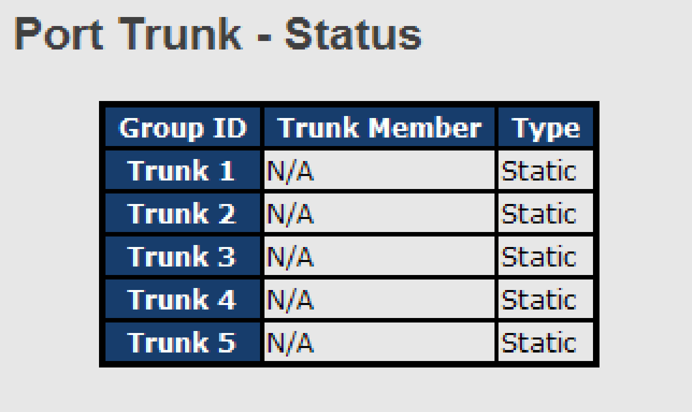


802.3ad LACP Work Ports

Group ID	Work Ports
Trunk1	max
Trunk2	max
Trunk3	max
Trunk4	max
Trunk5	max

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.



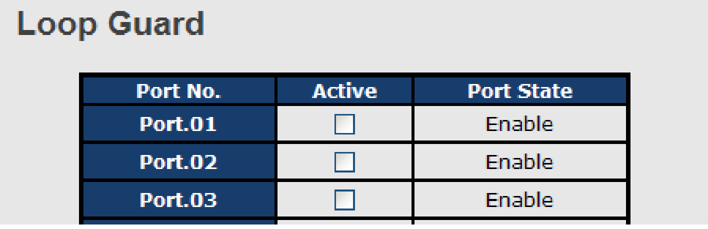
Port Trunk - Status

Group ID	Trunk Member	Type
Trunk 1	N/A	Static
Trunk 2	N/A	Static
Trunk 3	N/A	Static
Trunk 4	N/A	Static
Trunk 5	N/A	Static

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

1.4.5 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.



Loop Guard

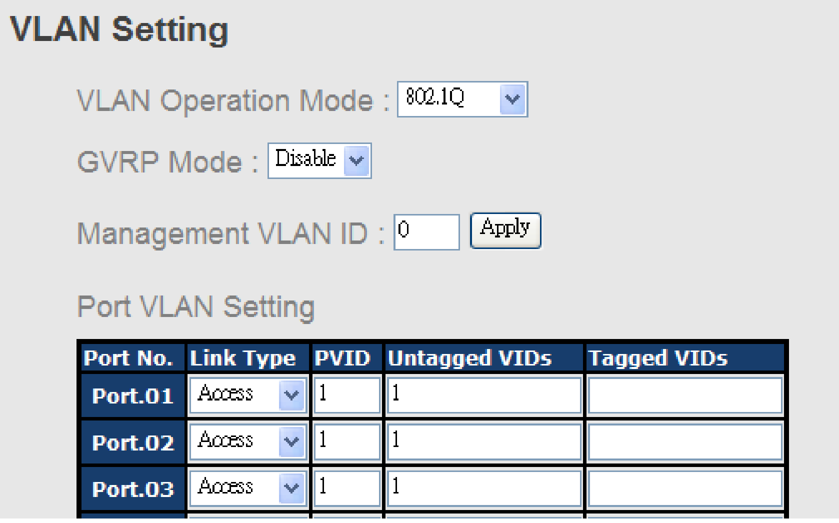
Port No.	Active	Port State
Port.01	□	Enable
Port.02	□	Enable
Port.03	□	Enable

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

1.5 VLAN

1.5.1 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.



VLAN Setting

VLAN Operation Mode : 802.1Q

GVRP Mode : Disable

Management VLAN ID : 0

Port VLAN Setting

Port No.	Link Type	PVID	Untagged VIDs	Tagged VIDs
Port.01	Access	1	1	
Port.02	Access	1	1	
Port.03	Access	1	1	

Label	Description
VLAN Operation Mode	Available options include **Disable a**nd **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.

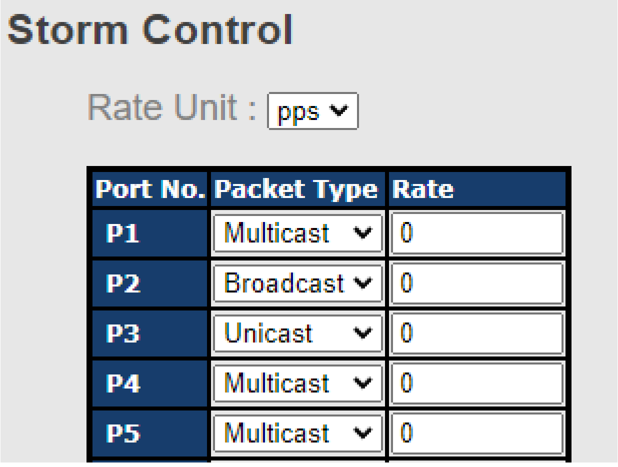
1.6 Traffic Prioritization

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.

1.6.1 Storm Control

A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configuration, or users issuing a denial-of-service attack can cause a storm. Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port. In this page, you can specify the rate at which packets are received for unicast, multicast, and broadcast traffic. The unit of the rate can be either pps (packets per second) or bps



Storm Control

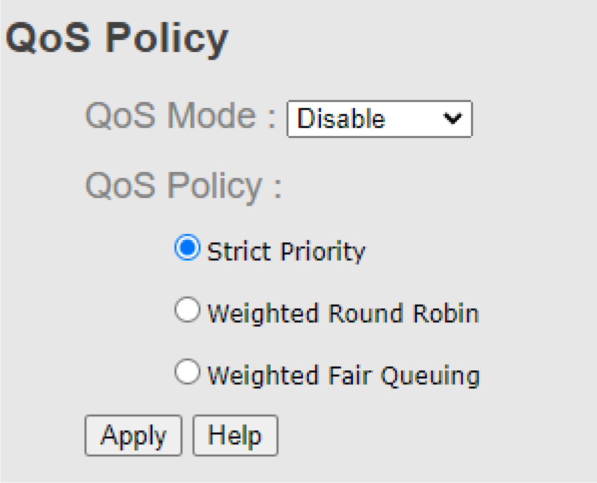
Rate Unit : pps

Port No.	Packet Type	Rate
P1	Multicast	0
P2	Broadcast	0
P3	Unicast	0
P4	Multicast	0
P5	Multicast	0

Label	Description
Rate Unit	Select Rate Unit , (pps or bps)
Packet type	Select packet type (Unicast / multicast / broadcast)
Rate	Define ratee value

1.6.2 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.



QoS Policy

QoS Mode : Disable

QoS Policy :

● Strict Priority

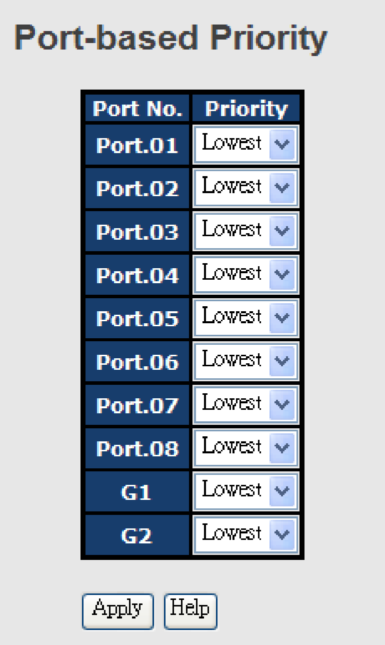
○ Weighted Round Robin

○ Weighted Fair Queuing

Label	Description
QOS Mode	Available modes include: **Disable**: disables the mode **Port-base**: the output priority is determined by ingress port.

	802.1p only: the output priority is determined by 802.1p only. **DSCP only**: the output priority is determined by DSCP only. **802.1p first**: the output priority is determined by 802.1p and DSCP, but 802.1p first. **DSCP first**: the output priority is determined by 802.1p and DSCP, but DSCP first.
QOS policy	**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.

1.6.3 Port-base Priority



Port-based Priority

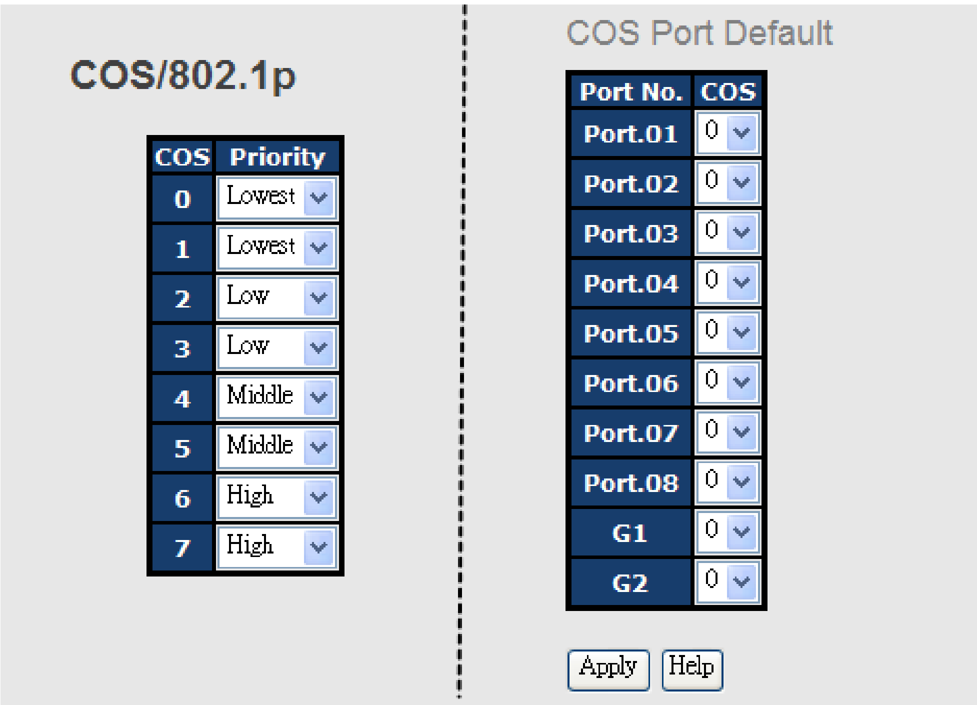
Port No.	Priority
Port.01	Lowest
Port.02	Lowest
Port.03	Lowest
Port.04	Lowest
Port.05	Lowest
Port.06	Lowest
Port.07	Lowest
Port.08	Lowest
G1	Lowest
G2	Lowest

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.

1.6.4 802.1p

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.



COS/802.1p

COS	Priority
0	Lowest
1	Lowest
2	Low
3	Low
4	Middle
5	Middle
6	High
7	High

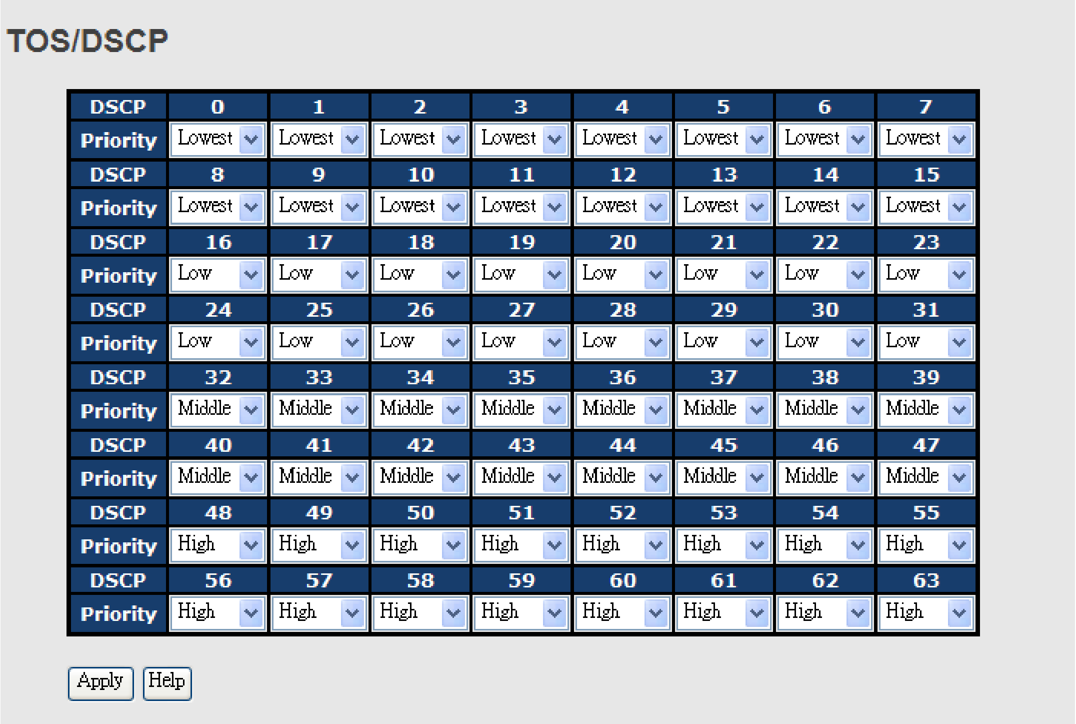
COS Port Default

Port No.	COS
Port.01	0
Port.02	0
Port.03	0
Port.04	0
Port.05	0
Port.06	0
Port.07	0
Port.08	0
G1	0
G2	0

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.

1.6.5 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.



TOS/DSCP

DSCP	0	1	2	3	4	5	6	7
Priority	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
DSCP	8	9	10	11	12	13	14	15
Priority	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
DSCP	16	17	18	19	20	21	22	23
Priority	Low	Low	Low	Low	Low	Low	Low	Low
DSCP	24	25	26	27	28	29	30	31
Priority	Low	Low	Low	Low	Low	Low	Low	Low
DSCP	32	33	34	35	36	37	38	39
Priority	Middle	Middle	Middle	Middle	Middle	Middle	Middle	Middle
DSCP	40	41	42	43	44	45	46	47
Priority	Middle	Middle	Middle	Middle	Middle	Middle	Middle	Middle
DSCP	48	49	50	51	52	53	54	55
Priority	High	High	High	High	High	High	High	High
DSCP	56	57	58	59	60	61	62	63
Priority	High	High	High	High	High	High	High	High

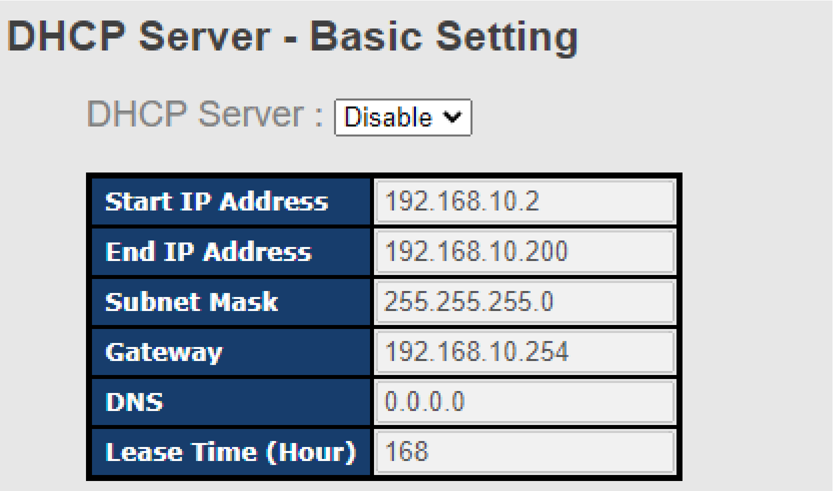
Label	Description
Priority	Assigns a port to a priority queue. Four priority queues are available: **High**, **Middle**, **Low**, and **Lowest**.
Apply	Click to apply the configurations
Help	Shows help file.

1.7 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.

1.7.1 Basic Settings

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.



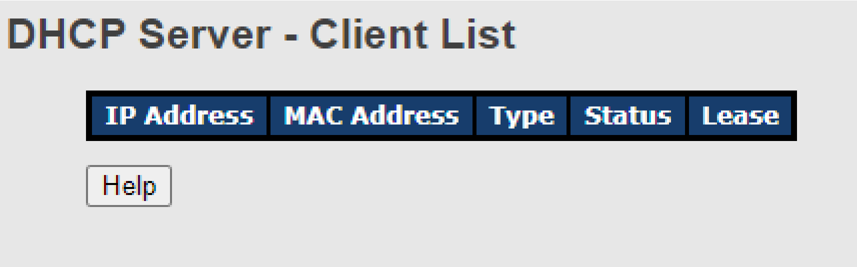
DHCP Server - Basic Setting

DHCP Server : Disable

Start IP Address	192.168.10.2
End IP Address	192.168.10.200
Subnet Mask	255.255.255.0
Gateway	192.168.10.254
DNS	0.0.0.0
Lease Time (Hour)	168

1.7.2 Client List

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.

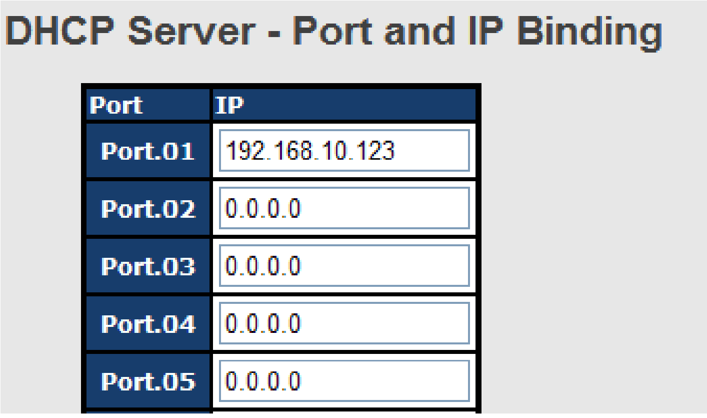


DHCP Server - Client List

IP Address	MAC Address	Type	Status	Lease

1.7.3 Port and IP Binding

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.

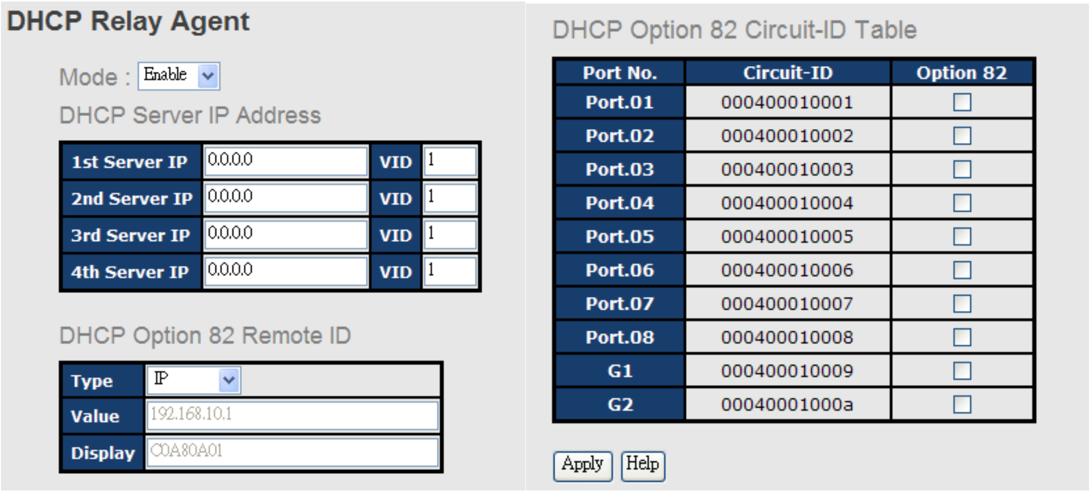


DHCP Server - Port and IP Binding

Port	IP
Port.01	192.168.10.123
Port.02	0.0.0.0
Port.03	0.0.0.0
Port.04	0.0.0.0
Port.05	0.0.0.0

1.7.4 DHCP 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.



DHCP Relay Agent

Mode : Enable

DHCP Server IP Address

1st Server IP	0.0.0.0	VID	1
2nd Server IP	0.0.0.0	VID	1
3rd Server IP	0.0.0.0	VID	1
4th Server IP	0.0.0.0	VID	1

DHCP Option 82 Remote ID

Type	IP
Value	192.168.10.1
Display	C0A80A01

DHCP Option 82 Circuit-ID Table

Port No.	Circuit-ID	Option 82
Port.01	000400010001	□
Port.02	000400010002	□
Port.03	000400010003	□
Port.04	000400010004	□
Port.05	000400010005	□
Port.06	000400010006	□
Port.07	000400010007	□
Port.08	000400010008	□
G1	000400010009	□
G2	00040001000a	□

2

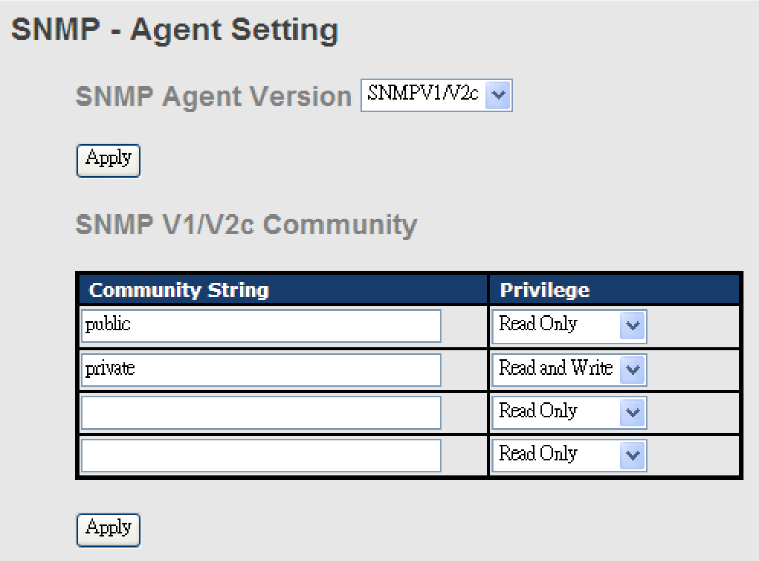
Label	Description
DHCP Relay	Enables or disables DHCP relay agent
DHCP Server IP Address and VID	Specify the IP address and VID of the DHCP server. **0.0.0.0** means the server is inactive.
DHCP Option 82 Remote ID	Provides an identifier for the remote server. Four types of IDs are supported: **IP**, **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

1.9 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.

1.9.1 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.



SNMP - Agent Setting

SNMP Agent Version: SNMPV1/V2c

SNMP V1/V2c Community

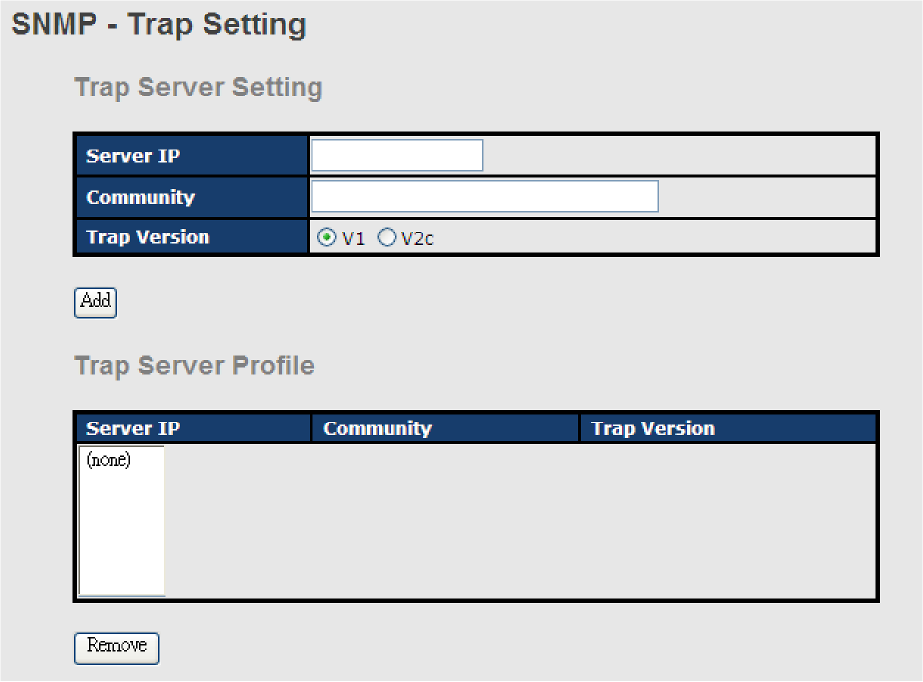
Community String	Privilege
public	Read Only
private	Read and Write
	Read Only
	Read Only

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

1.9.2 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.



SNMP - Trap Setting

Trap Server Setting

Server IP	
Community	
Trap Version	● V1 ○ V2c

Trap Server Profile

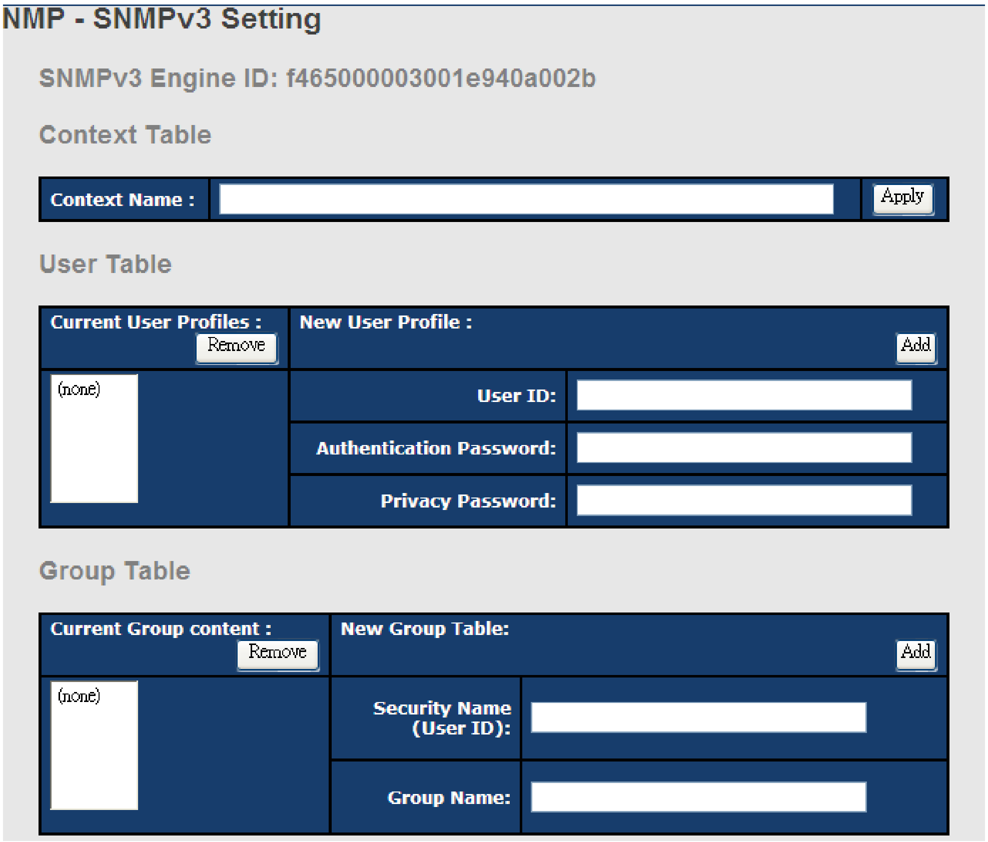
Server IP	Community	Trap Version
(none)		

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

1.9.3 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 :

User Table

Current User Profiles : (none)

New User Profile :

User ID:

Authentication Password:

Privacy Password:

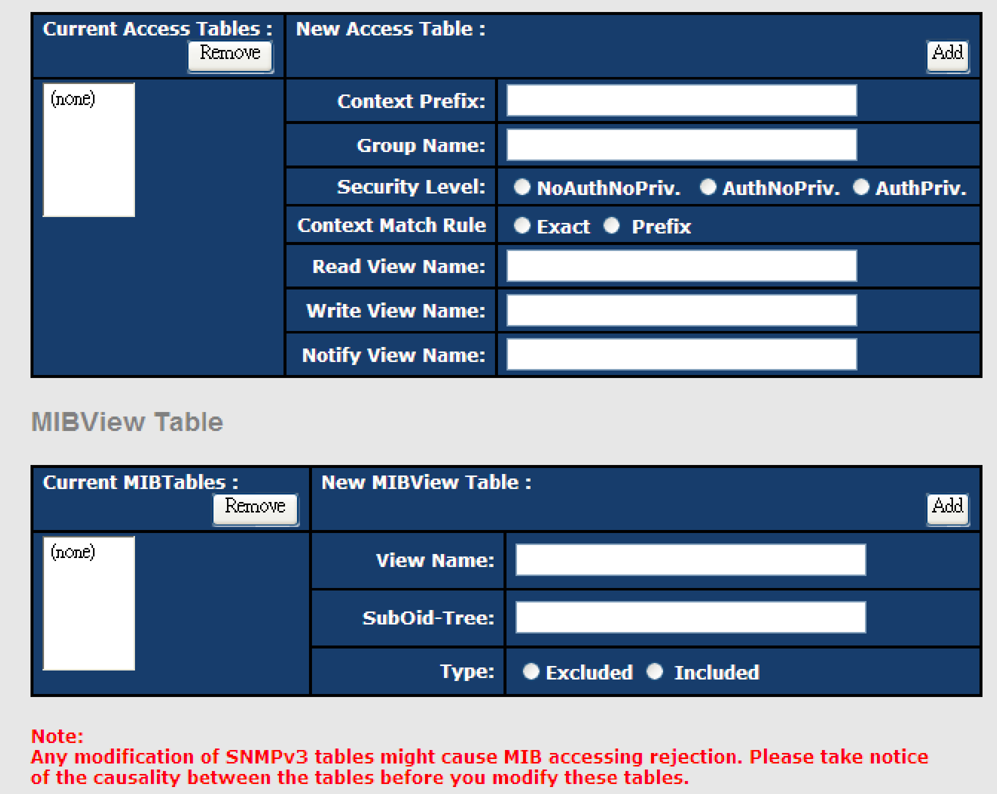
Group Table

Current Group content : (none)

New Group Table:

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

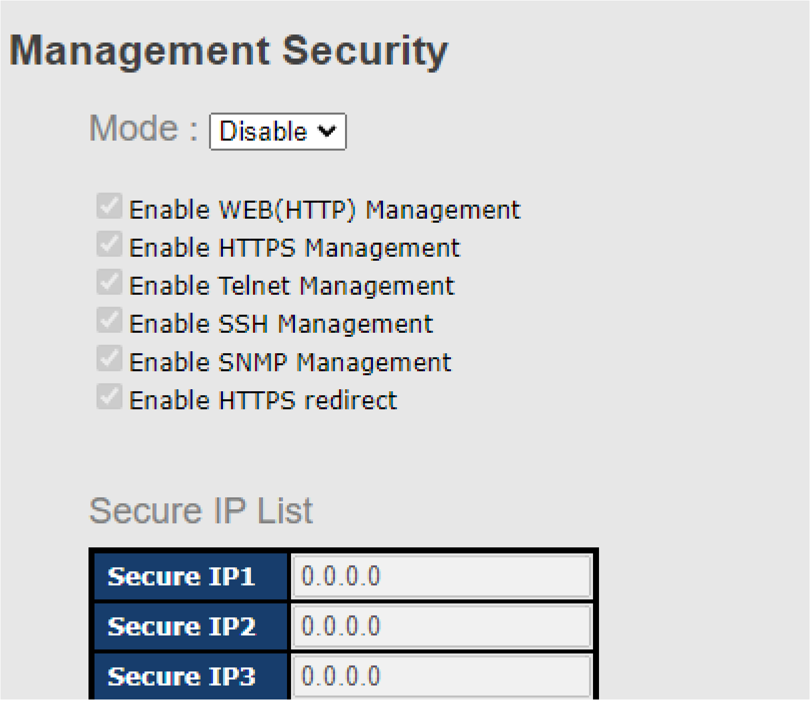
Note:
Any modification of SNMPv3 tables might cause MIB accessing rejection. Please take notice of the causality between the tables before you modify these tables.

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.

1.10 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.).



Management Security

Mode : Disable

☑ Enable WEB(HTTP) Management
☑ Enable HTTPS Management
☑ Enable Telnet Management
☑ Enable SSH Management
☑ Enable SNMP Management
☑ Enable HTTPS redirect

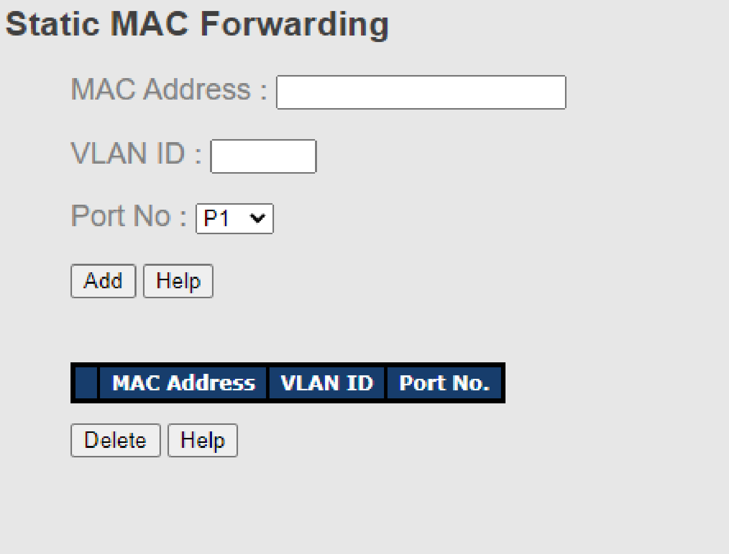
Secure IP List

Secure IP1	0.0.0.0
Secure IP2	0.0.0.0
Secure IP3	0.0.0.0

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.
Enable HTTP Management	Mark the blank to enable WEB (HTTP) Management.
Apply	Click o set the configurations.
Help	Show help file.

Static MAC Forwarding

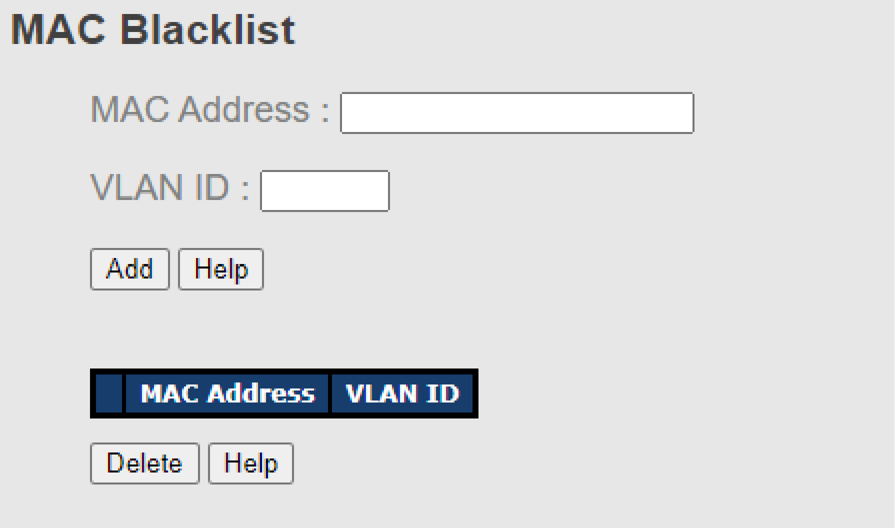
You can use static MAC addresses to provide port security for the switch. With this method, only the frames with the MAC addresses in this list will be forwarded, otherwise will be discarded.



Label	Description
MAC Address	Enter a MAC address for a specific port.
VLAN ID	Select VLAN Number
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.



MAC Blacklist

MAC Address :

VLAN ID :

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

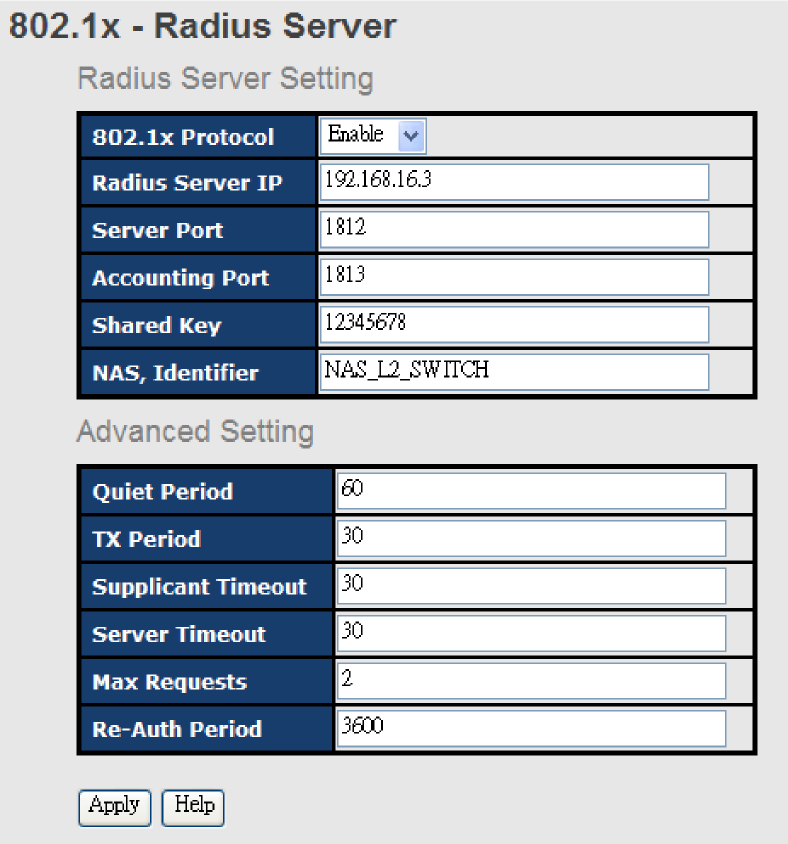
1.10.1 802.1x

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.



802.1x - Radius Server

Radius Server Setting

802.1x Protocol	Enable
Radius Server IP	192.168.16.3
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

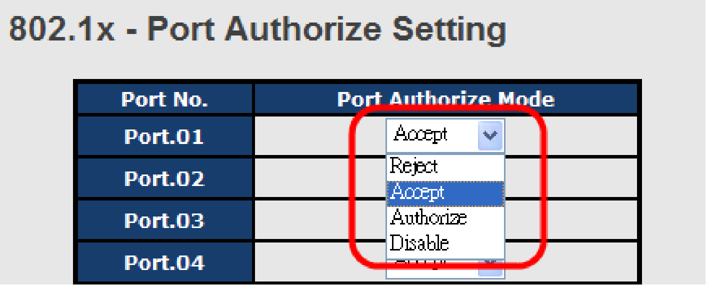
Advanced Setting

Quiet Period	60
TX Period	30
Supplicant Timeout	30
Server Timeout	30
Max Requests	2
Re-Auth Period	3600

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

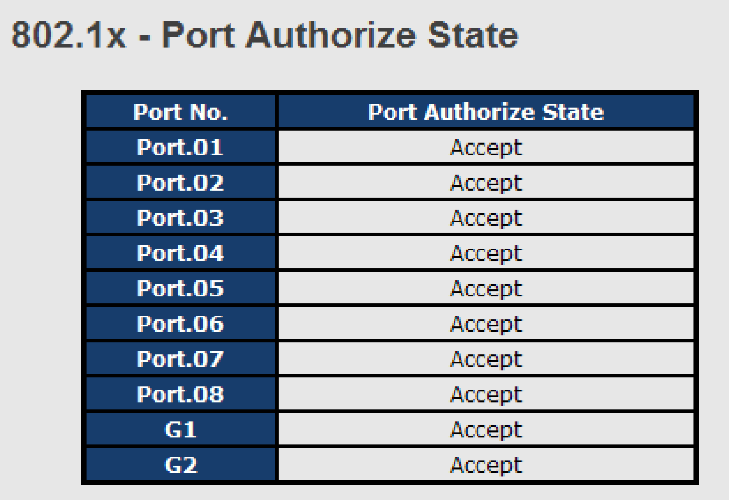
Accounting Port	The number of the UDP port that the RADIUS server uses for accounting requests.
Shared Key	A key shared between the switch and authentication server
NAS, Identifier	A string used to identify the switch.
Quiet Period	The time interval between authentication failure and the start of a new 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:



802.1x - Port Authorize Setting

Port No.	Port Authorize Mode
Port.01	Accept
Port.02	
Port.03	
Port.04	



802.1x - Port Authorize State

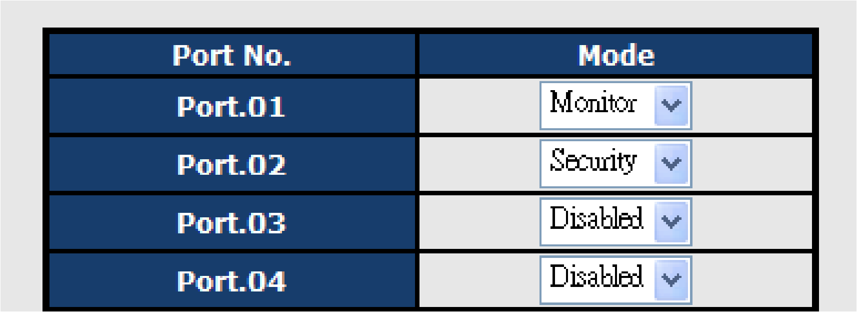
Port No.	Port Authorize State
Port.01	Accept
Port.02	Accept
Port.03	Accept
Port.04	Accept
Port.05	Accept
Port.06	Accept
Port.07	Accept
Port.08	Accept
G1	Accept
G2	Accept

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

1.10.2 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.



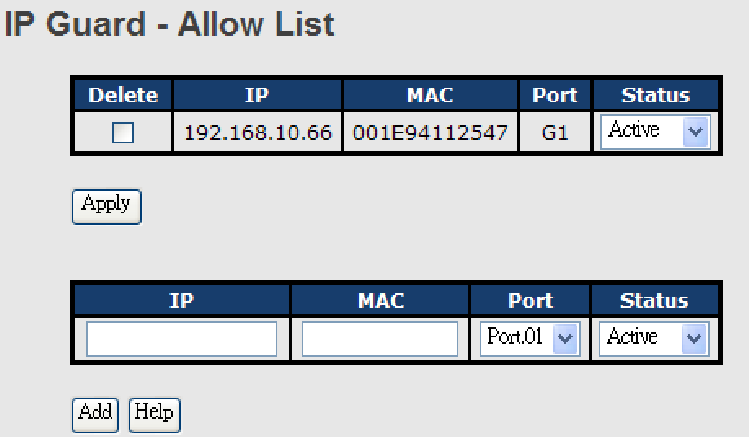
Port No.	Mode
Port.01	Monitor
Port.02	Security
Port.03	Disabled
Port.04	Disabled

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.



IP Guard - Allow List

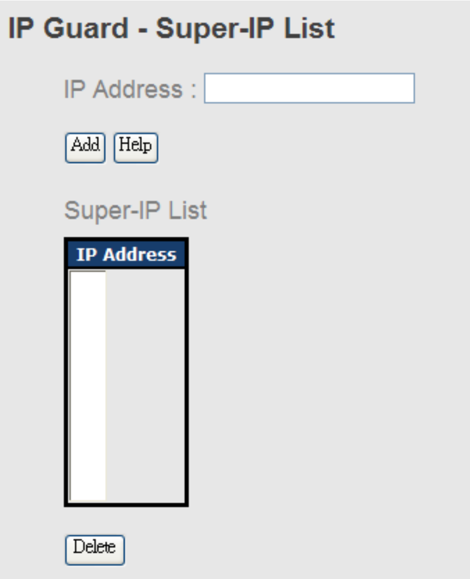
Delete	IP	MAC	Port	Status
□	192.168.10.66	001E94112547	G1	Active

IP	MAC	Port	Status
		Port.01	Active

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.



IP Guard - Super-IP List

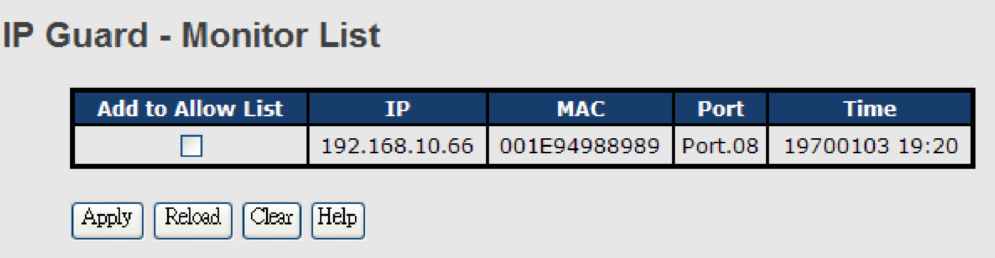
IP Address :

Super-IP List

IP Address

Monitor List

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



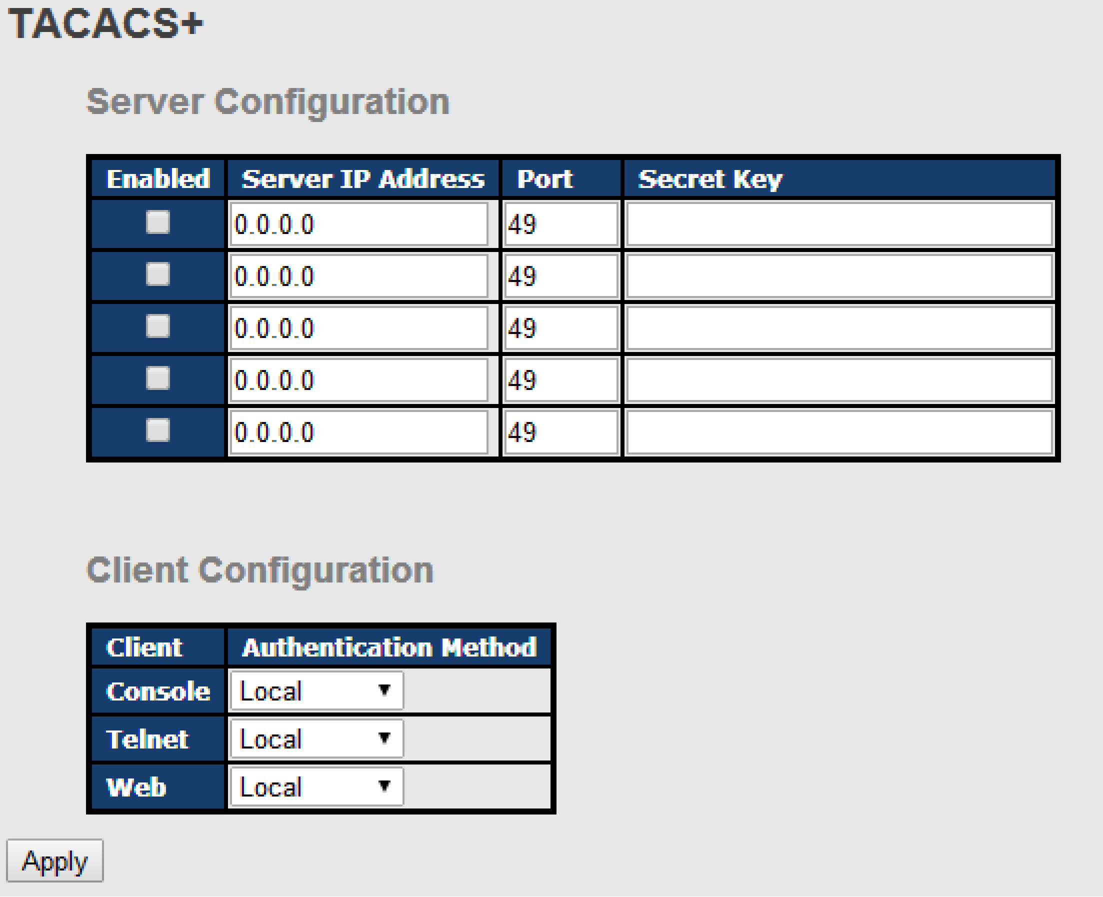
IP Guard - Monitor List

Add to Allow List	IP	MAC	Port	Time
□	192.168.10.66	001E94988989	Port.08	19700103 19:20

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

1.10.3 TACACS+

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



TACACS+

Server Configuration

Enabled	Server IP Address	Port	Secret Key
□	0.0.0.0	49	
□	0.0.0.0	49	
□	0.0.0.0	49	
□	0.0.0.0	49	
□	0.0.0.0	49	

Client Configuration

Client	Authentication Method
Console	Local ▾
Telnet	Local ▾
Web	Local ▾

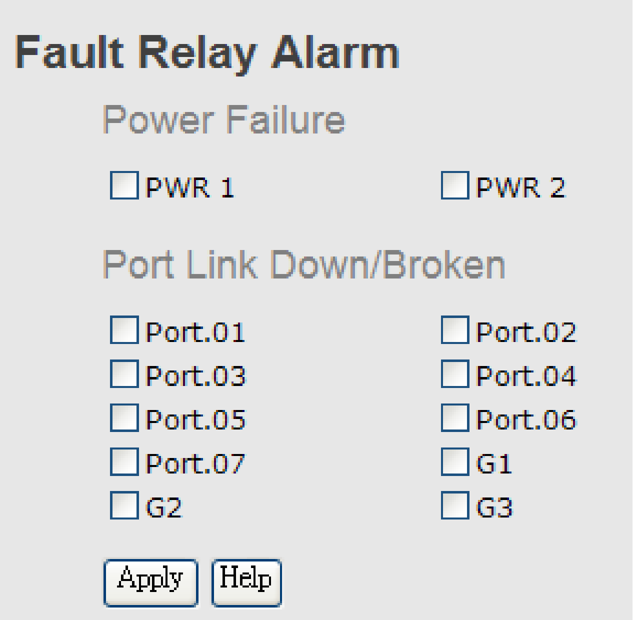
Label	Description
Enable check box	Enable / disable server connect
Server IP Address	Input TACACS+ Server IP Address .
Port	Input TACACS+ use Port number
Secret key	Input TACACS+ use key value(need same TACACS+ Server)
Authentication Method	User can select Authentication Method , support local / TACACS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

1.11 Warning

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.

1.11.1 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.



Fault Relay Alarm

Power Failure

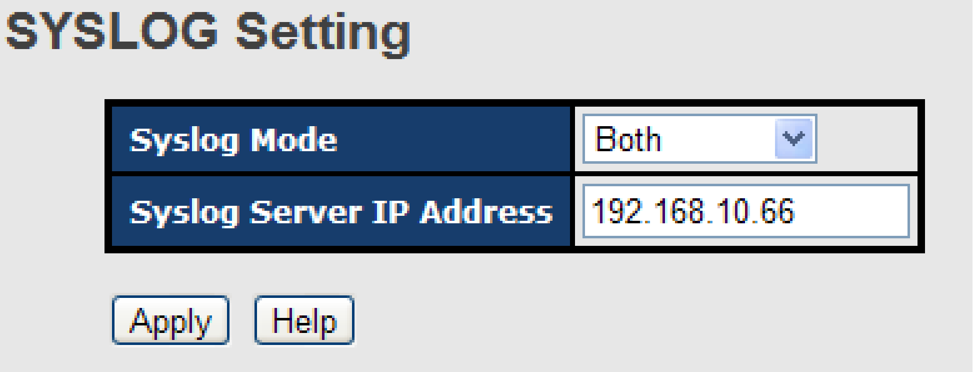
☐ PWR 1 ☐ PWR 2

Port Link Down/Broken

☐ Port.01 ☐ Port.02
☐ Port.03 ☐ Port.04
☐ Port.05 ☐ Port.06
☐ Port.07 ☐ G1
☐ G2 ☐ G3

1.11.2 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.



SYSLOG Setting

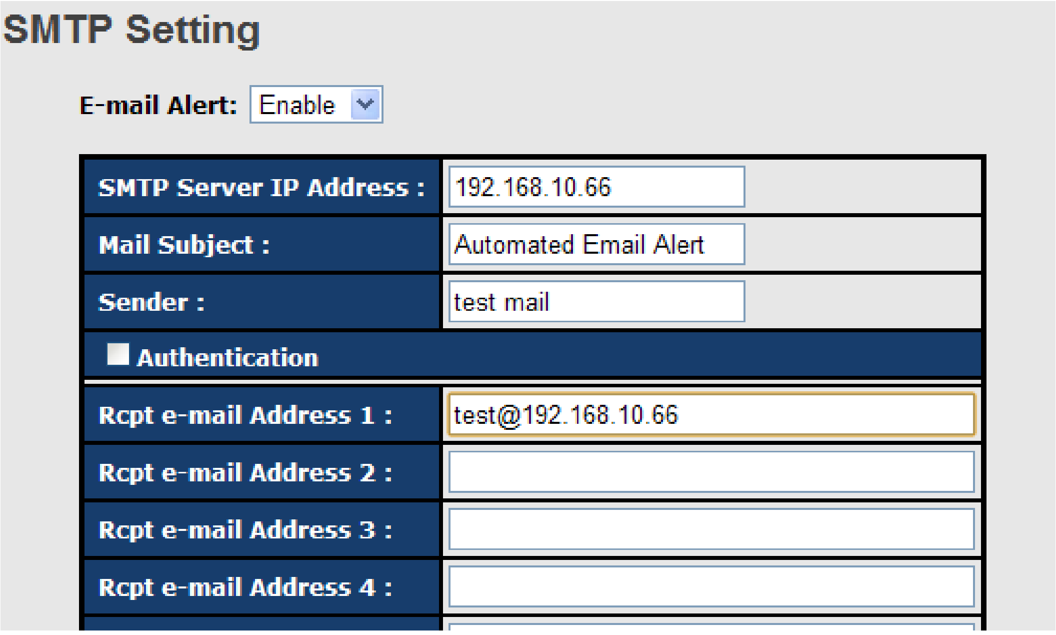
Syslog Mode	Both
Syslog Server IP Address	192.168.10.66

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

1.11.3 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.



SMTP Setting

E-mail Alert: Enable

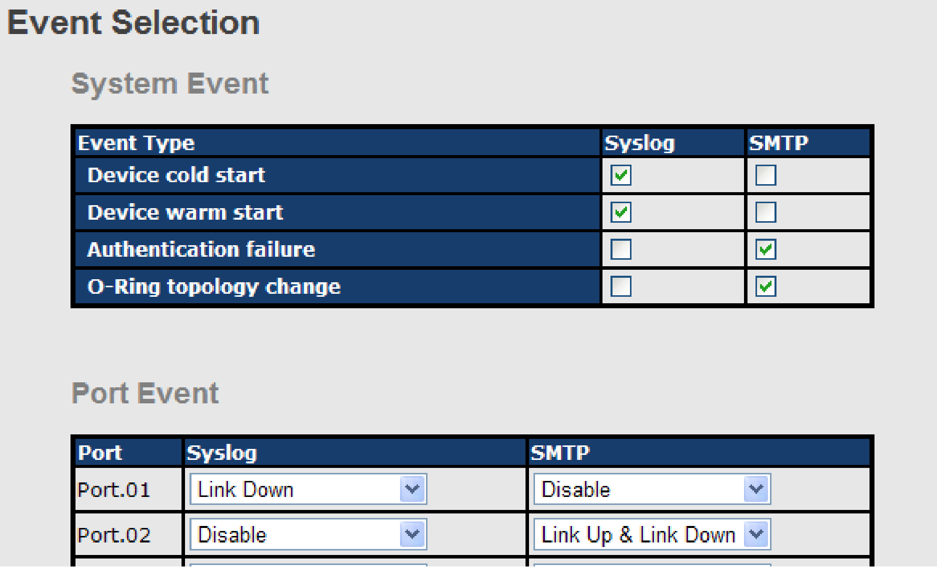
SMTP Server IP Address :	192.168.10.66
Mail Subject :	Automated Email Alert
Sender :	test mail
□ Authentication	
Rcpt e-mail Address 1 :	test@192.168.10.66
Rcpt e-mail Address 2 :	
Rcpt e-mail Address 3 :	
Rcpt e-mail Address 4 :	

Label	Description
E-mail Alert	Enables or disables transmission of system warnings by e-mail
SMTP Server IP Address	The IP address of the SMTP server to receive the notification 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	The recipient's e-mail address. A mail allows for 6 recipients.

Address	
Apply	Click to activate the configurations
Help	Shows help file

1.11.4 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.



Event Selection

System Event

Event Type	Syslog	SMTP
Device cold start	☑	□
Device warm start	☑	□
Authentication failure	□	☑
O-Ring topology change	□	☑

Port Event

Port	Syslog	SMTP
Port.01	Link Down	Disable
Port.02	Disable	Link Up & Link Down

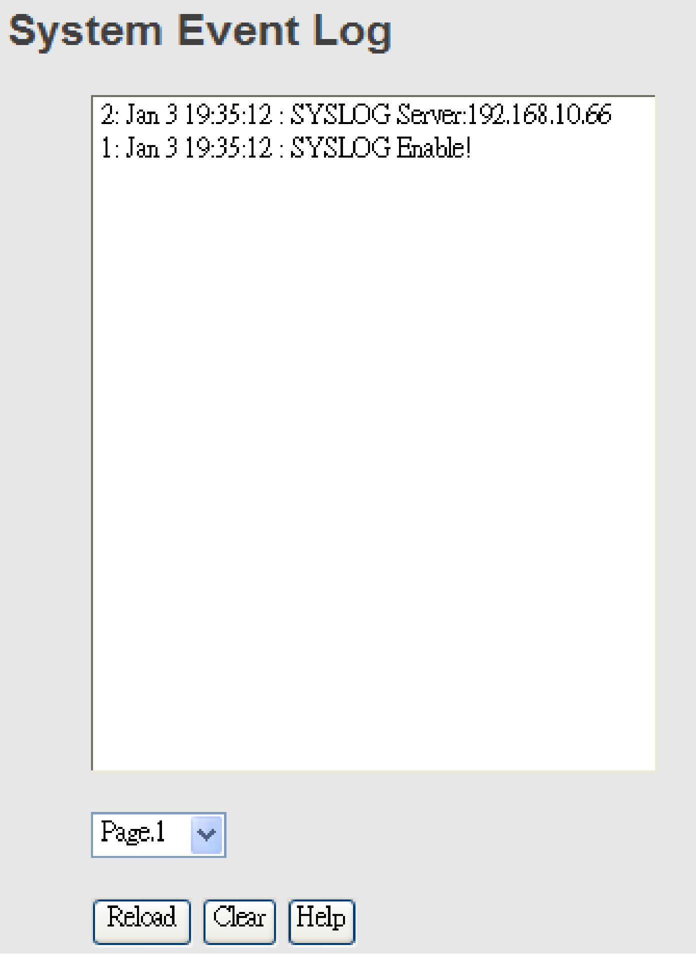
Label	Description
Device cold start	Sends alerts when you restart the device using the power button on your PC.
Device warm start	Sends alerts when you restart the device using the Reset button or software.
Authentication Failure	Sends alerts when SNMP authentication fails
O-Ring topology change	Sends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

1.12Monitor and Diag

1.12.1 System Event Log

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



System Event Log

```
2: Jan 3 19:35:12 : SYSLOG Server:192.168.10.66
1: Jan 3 19:35:12 : SYSLOG Enable!
```

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

1.12.2 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.

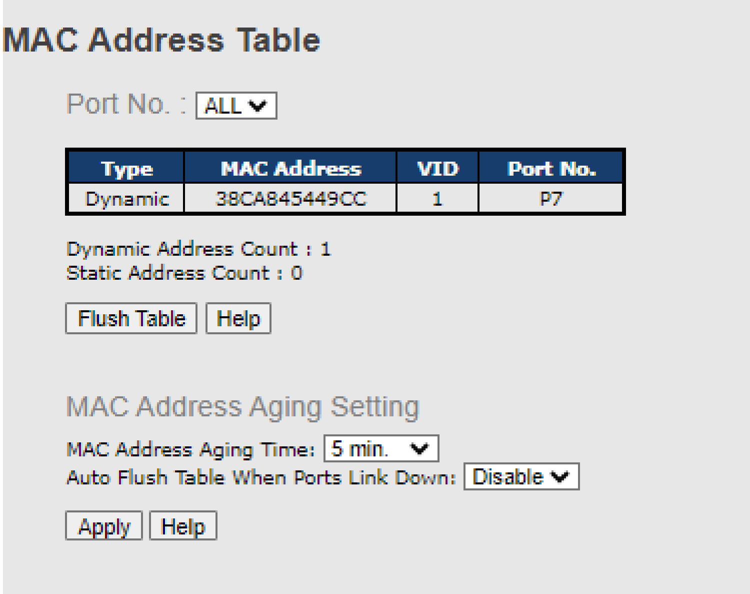
Entries in a MAC address table fall into two types: dynamic and static entries. Entries in a static MAC table are added or removed manually and cannot age out by themselves. Entries in a dynamic MAC tablet will age out after a configured aging time. Such entries can be added by learning or manual configuration.

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.



MAC Address Table

Port No. : ALL

Type	MAC Address	VID	Port No.
Dynamic	38CA845449CC	1	P7

Dynamic Address Count : 1
Static Address Count : 0

MAC Address Aging Setting

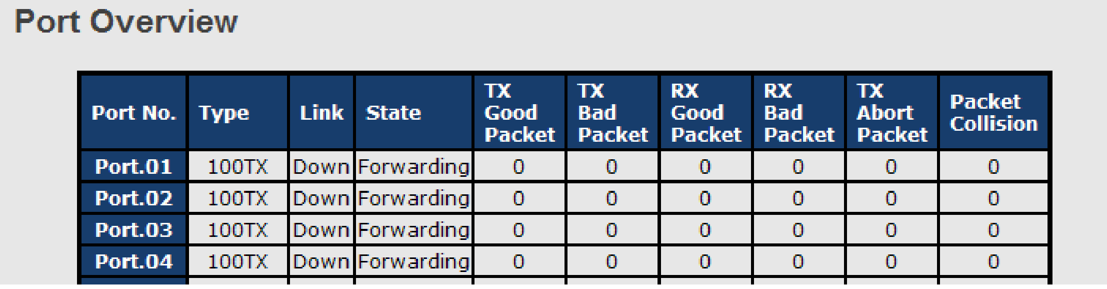
MAC Address Aging Time: 5 min.
Auto Flush Table When Ports Link Down: Disable

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
Apply	Click to apply the configurations.

1.12.3 Port Overview

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



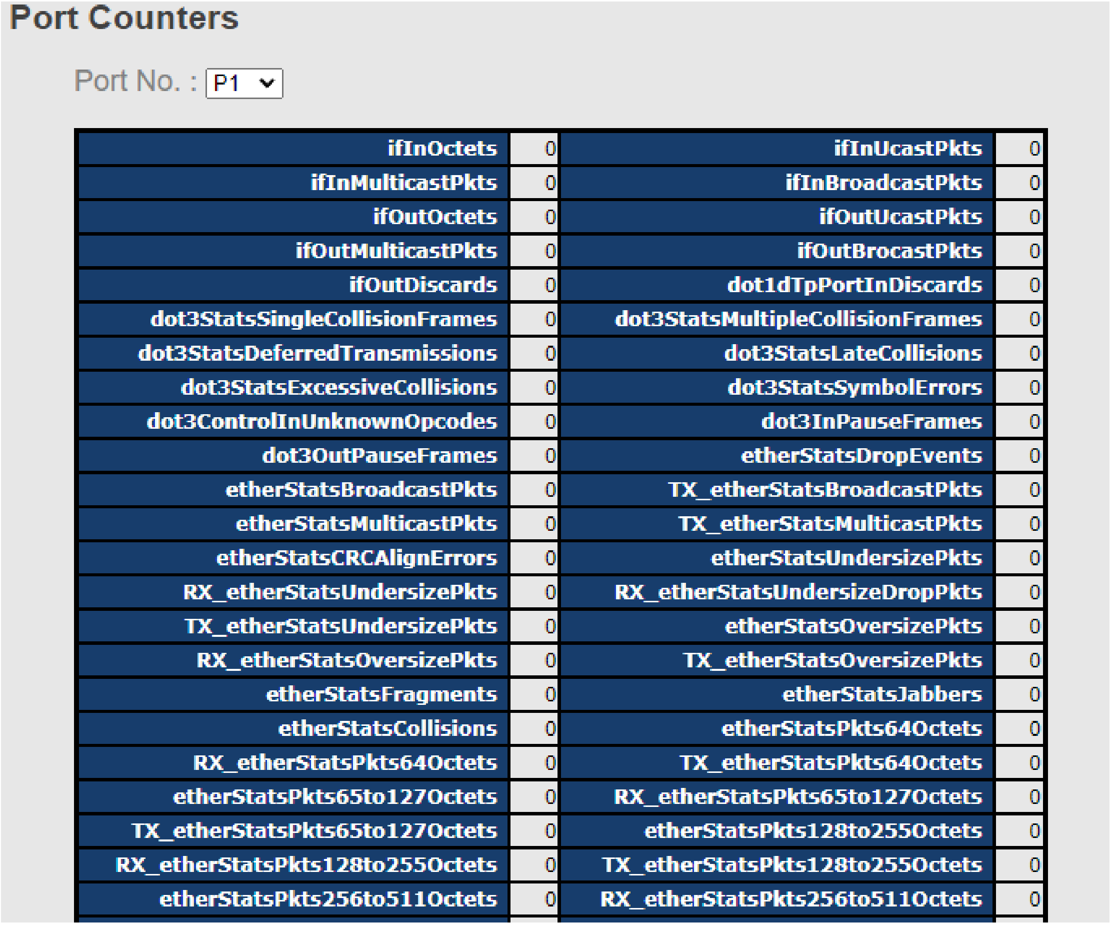
Port Overview

Port No.	Type	Link	State	TX Good Packet	TX Bad Packet	RX Good Packet	RX Bad Packet	TX Abort Packet	Packet Collision
Port.01	100TX	Down	Forwarding	0	0	0	0	0	0
Port.02	100TX	Down	Forwarding	0	0	0	0	0	0
Port.03	100TX	Down	Forwarding	0	0	0	0	0	0
Port.04	100TX	Down	Forwarding	0	0	0	0	0	0

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

1.12.4 Port Counters

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



Port Counters

Port No. : P1

ifInOctets	0	ifInUcastPkts	0
ifInMulticastPkts	0	ifInBroadcastPkts	0
ifOutOctets	0	ifOutUcastPkts	0
ifOutMulticastPkts	0	ifOutBrocastPkts	0
ifOutDiscards	0	dot1dTpPortInDiscards	0
dot3StatsSingleCollisionFrames	0	dot3StatsMultipleCollisionFrames	0
dot3StatsDeferredTransmissions	0	dot3StatsLateCollisions	0
dot3StatsExcessiveCollisions	0	dot3StatsSymbolErrors	0
dot3ControlInUnknownOpcodes	0	dot3InPauseFrames	0
dot3OutPauseFrames	0	etherStatsDropEvents	0
etherStatsBroadcastPkts	0	TX_etherStatsBroadcastPkts	0
etherStatsMulticastPkts	0	TX_etherStatsMulticastPkts	0
etherStatsCRCAlignErrors	0	etherStatsUndersizePkts	0
RX_etherStatsUndersizePkts	0	RX_etherStatsUndersizeDropPkts	0
TX_etherStatsUndersizePkts	0	etherStatsOversizePkts	0
RX_etherStatsOversizePkts	0	TX_etherStatsOversizePkts	0
etherStatsFragments	0	etherStatsJabbers	0
etherStatsCollisions	0	etherStatsPkts64Octets	0
RX_etherStatsPkts64Octets	0	TX_etherStatsPkts64Octets	0
etherStatsPkts65to127Octets	0	RX_etherStatsPkts65to127Octets	0
TX_etherStatsPkts65to127Octets	0	etherStatsPkts128to255Octets	0
RX_etherStatsPkts128to255Octets	0	TX_etherStatsPkts128to255Octets	0
etherStatsPkts256to511Octets	0	RX_etherStatsPkts256to511Octets	0

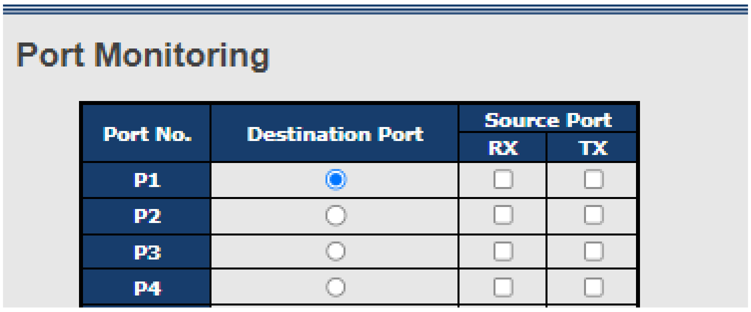
Label	Description
InGoodOctetsLo	The lower 32-bits of the 64-bit InGoodOctets counter. This field indicates the total length of all good Ethernet frames received.
InGoodOctetsHi	The upper 32-bits of the 64-bit InGoodOctets counter. This field indicates the total length of all good Ethernet frames received.
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.

1.12.5 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.



Port Monitoring

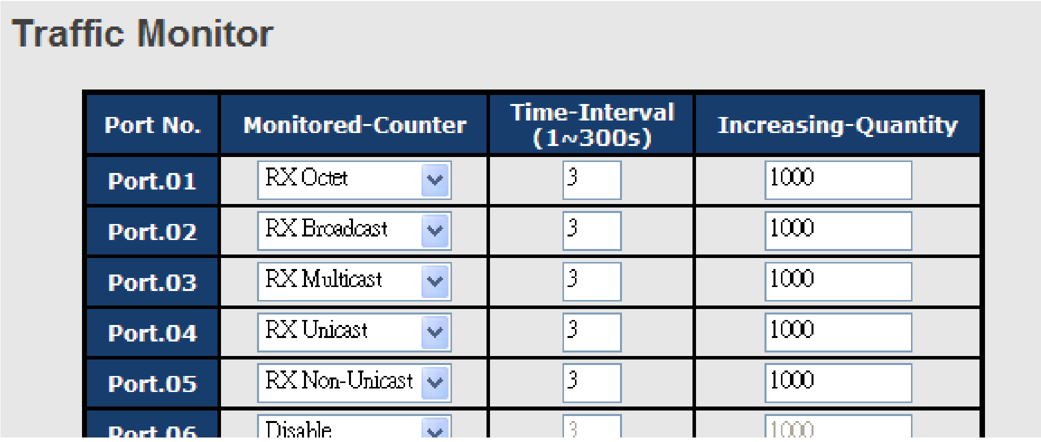
Port No.	Destination Port	Source Port	
		RX	TX
P1	●	□	□
P2	○	□	□
P3	○	□	□
P4	○	□	□

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

1.12.6 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.



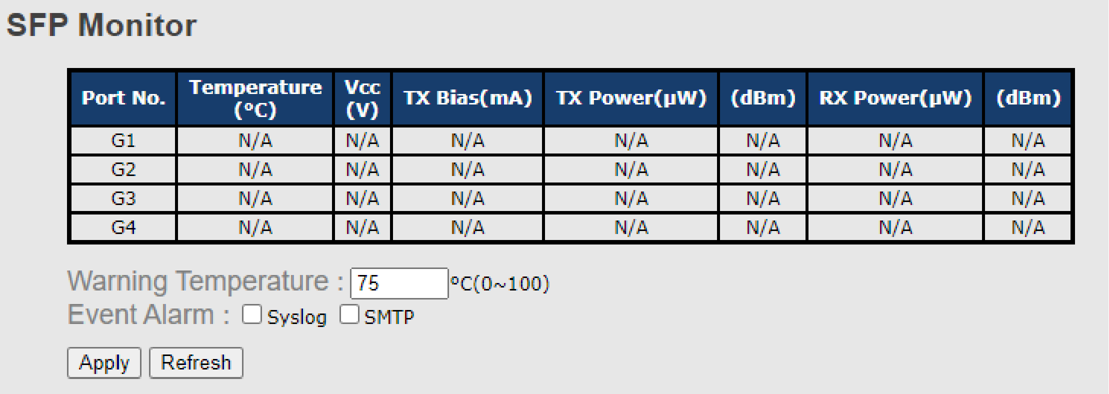
Traffic Monitor

Port No.	Monitored-Counter	Time-Interval (1~300s)	Increasing-Quantity
Port.01	RX Octet	3	1000
Port.02	RX Broadcast	3	1000
Port.03	RX Multicast	3	1000
Port.04	RX Unicast	3	1000
Port.05	RX Non-Unicast	3	1000
Port.06	Disable	3	1000

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)

1.12.7 SFP Monitor

DDM function, can pass SFP module which supports DDM function, measure the temperature of the apparatus .And manage and set up event alarm module through DDM WEB



SFP Monitor

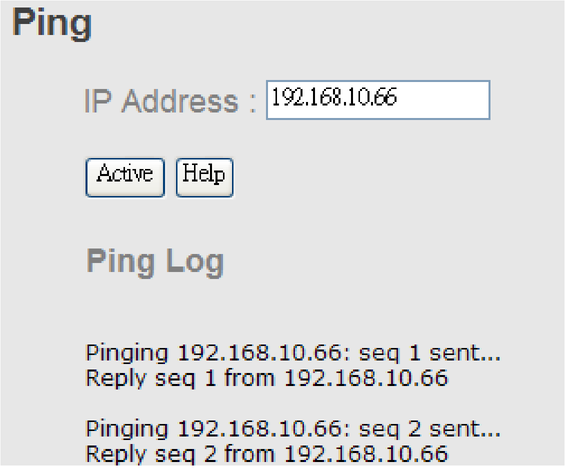
Port No.	Temperature (°C)	Vcc (V)	TX Bias(mA)	TX Power(μW)	(dBm)	RX Power(μW)	(dBm)
G1	N/A	N/A	N/A	N/A	N/A	N/A	N/A
G2	N/A	N/A	N/A	N/A	N/A	N/A	N/A
G3	N/A	N/A	N/A	N/A	N/A	N/A	N/A
G4	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Warning Temperature : 75 °C(0~100)

Event Alarm : □ Syslog □ SMTP

1.12.8 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.



Ping

IP Address : 192.168.10.66

Ping Log

```
Pinging 192.168.10.66: seq 1 sent...
Reply seq 1 from 192.168.10.66

Pinging 192.168.10.66: seq 2 sent...
Reply seq 2 from 192.168.10.66
```

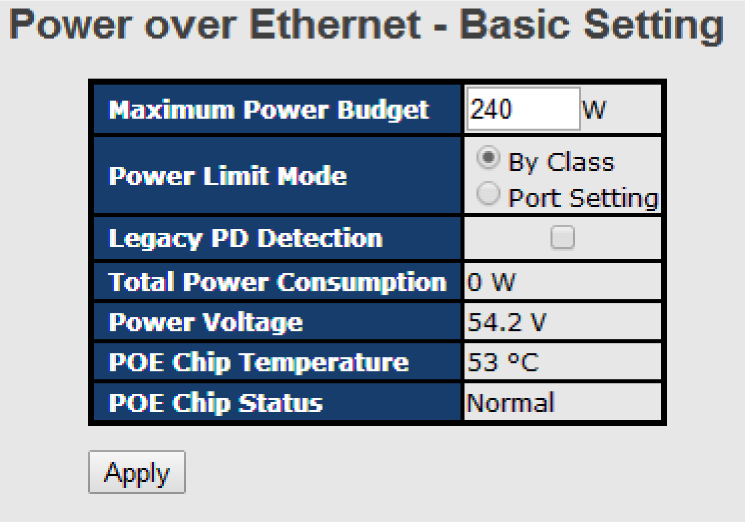
After you press **Active**, four ICMP packets will be transmitted, and the sequence number and roundtrip time will be displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

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

1.13 Power Over Ethernet (only for IGPS Series)

1.13.1 Basic Setting

PoE (Power over Ethernet) is a technology that transmits electrical power to devices such as IP telephones, wireless LAN access points, and IP cameras over standard Ethernet cables. The ability is very useful in places where power supply is difficult or expensive deploy.



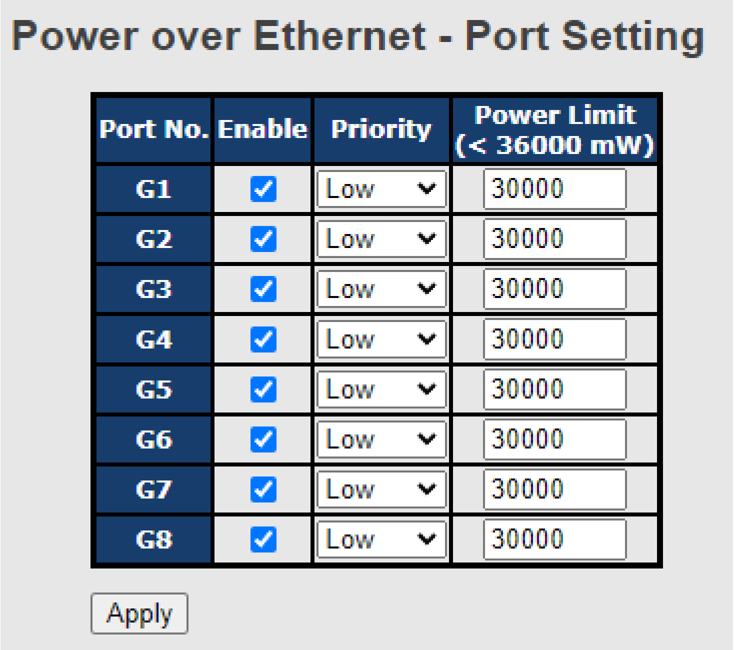
Power over Ethernet - Basic Setting

Maximum Power Budget	240 W
Power Limit Mode	● By Class ○ Port Setting
Legacy PD Detection	□
Total Power Consumption	0 W
Power Voltage	54.2 V
POE Chip Temperature	53 °C
POE Chip Status	Normal

Label	Description
maximum power budget	**setting maximum power available.**
Power Limit Mode	**By Class : In this mode each port automatic determines how much power to reserve according to the "class" the connected PD** **Port Setting : In this mode each port power output follow "port setting--->power limit" value.(maximum = 36W)**
Legacy PD Detection	**Enable Legacy PD Mode**
Total Power Consumption	**switch total power consumption (W)**
Power voltage	**POE Power Voltage(V)**
PoE Chip Temperature	**Switch POE Chip Temperature (˚C)**
POE Chip Status	**POE Chip work status .**

1.13.2 Port Setting

You can configure settings for each port in this section.



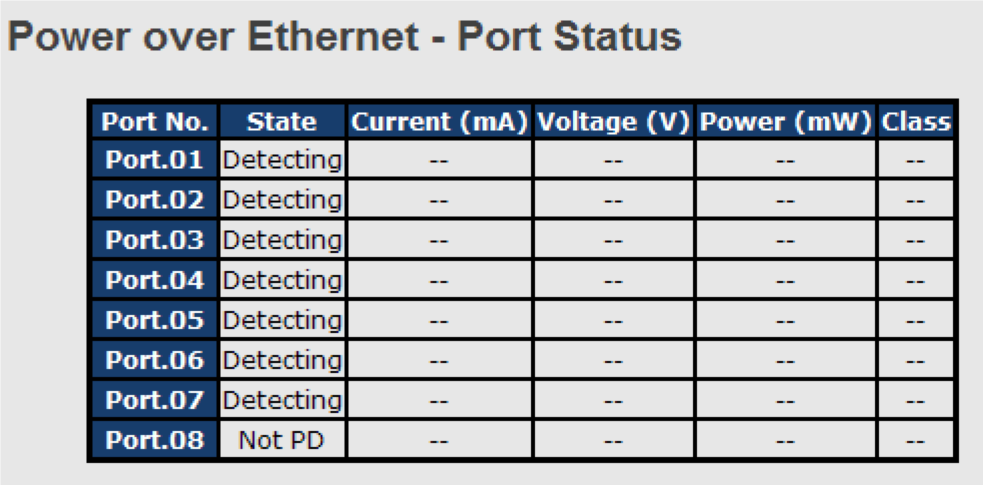
Power over Ethernet - Port Setting

Port No.	Enable	Priority	Power Limit (< 36000 mW)
G1	☑	Low	30000
G2	☑	Low	30000
G3	☑	Low	30000
G4	☑	Low	30000
G5	☑	Low	30000
G6	☑	Low	30000
G7	☑	Low	30000
G8	☑	Low	30000

Label	Description
Port	Port number.
Enable	Check to enable PoE function for specific ports.
Power Limit From Classification	Check to decide the power limit method; when this check box is ticked, the system will limit the power supply to the powered device in accordance with the related class.
Legacy	The legacy detection is to identify the PD devices not compliant with the IEEE 802.3af standard. Check it to support the legacy power devices.
Priority	Choose the priority of power supplying from the drop-down list. Set port priority for P.O.E. power management. 1 = C (critical), 2 = H (High), 3 = L (Low).
Power Limit	Input a value to set the power limit value. The maximum value 15400.

1.13.3 Port Status

This page allows you to examine the current status for all PoE ports.



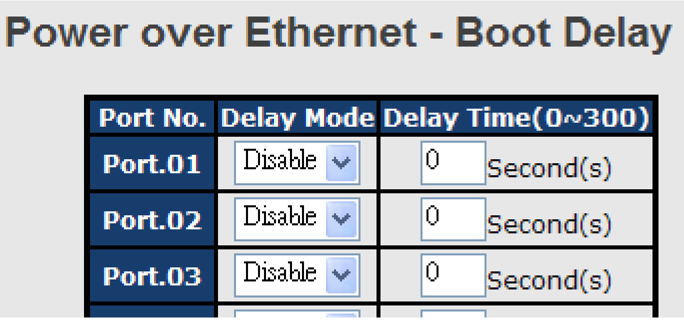
Power over Ethernet - Port Status

Port No.	State	Current (mA)	Voltage (V)	Power (mW)	Class
Port.01	Detecting	--	--	--	--
Port.02	Detecting	--	--	--	--
Port.03	Detecting	--	--	--	--
Port.04	Detecting	--	--	--	--
Port.05	Detecting	--	--	--	--
Port.06	Detecting	--	--	--	--
Port.07	Detecting	--	--	--	--
Port.08	Not PD	--	--	--	--

Label	Description
Port	Port number.
State	Shows P.S.E. Status.
Current(mA)	Displays current value.
Voltage(V)	Displays voltage value.
Power(mW)	Displays watt value.
Class	Displays power class. When Bypass classification is enable, the class value will not show in here.

1.13.4 Boot Delay

You can specify how much time for the switch to wait for a key stroke while booting.



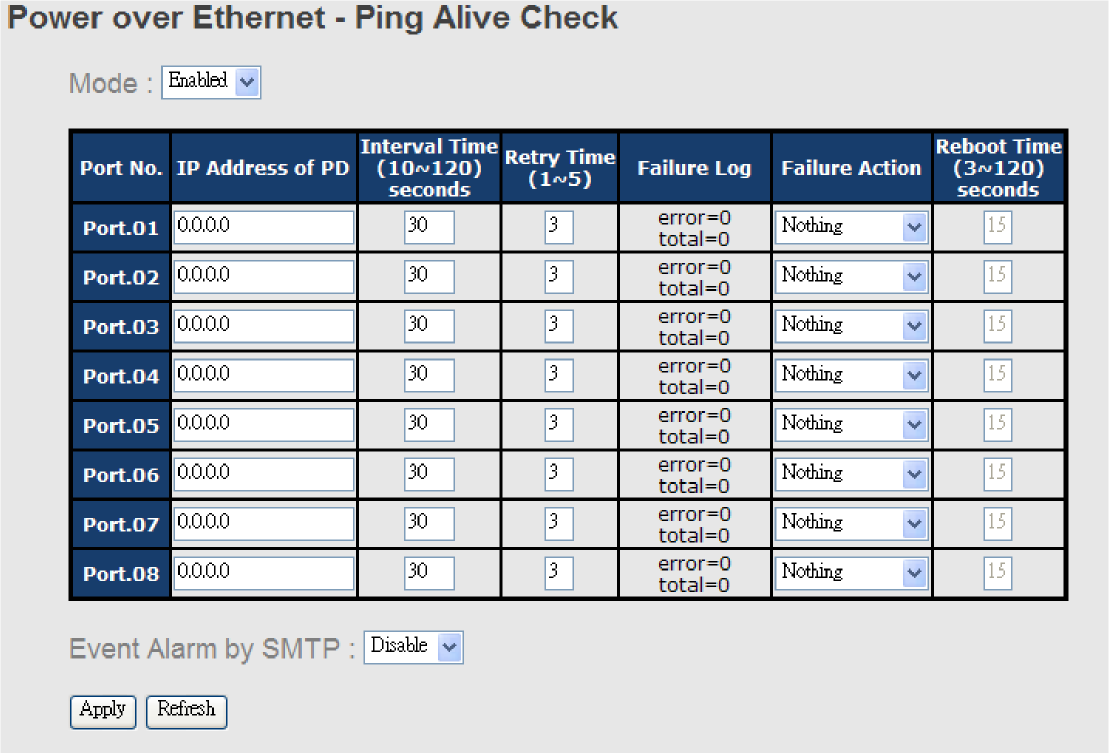
Power over Ethernet - Boot Delay

Port No.	Delay Mode	Delay Time(0~300)
Port.01	Disable	0 Second(s)
Port.02	Disable	0 Second(s)
Port.03	Disable	0 Second(s)

Label	Description
Port	Port number.
Delay Mode	Enables or disables Delay Mode.
Delay Time(0-300)	Time interval for providing power.

1.13.5 Ping Alive Check

You can control PoE functions via ping commands which will enable or disable other PoE devices connected to the configured ports.



Power over Ethernet - Ping Alive Check

Mode : Enabled

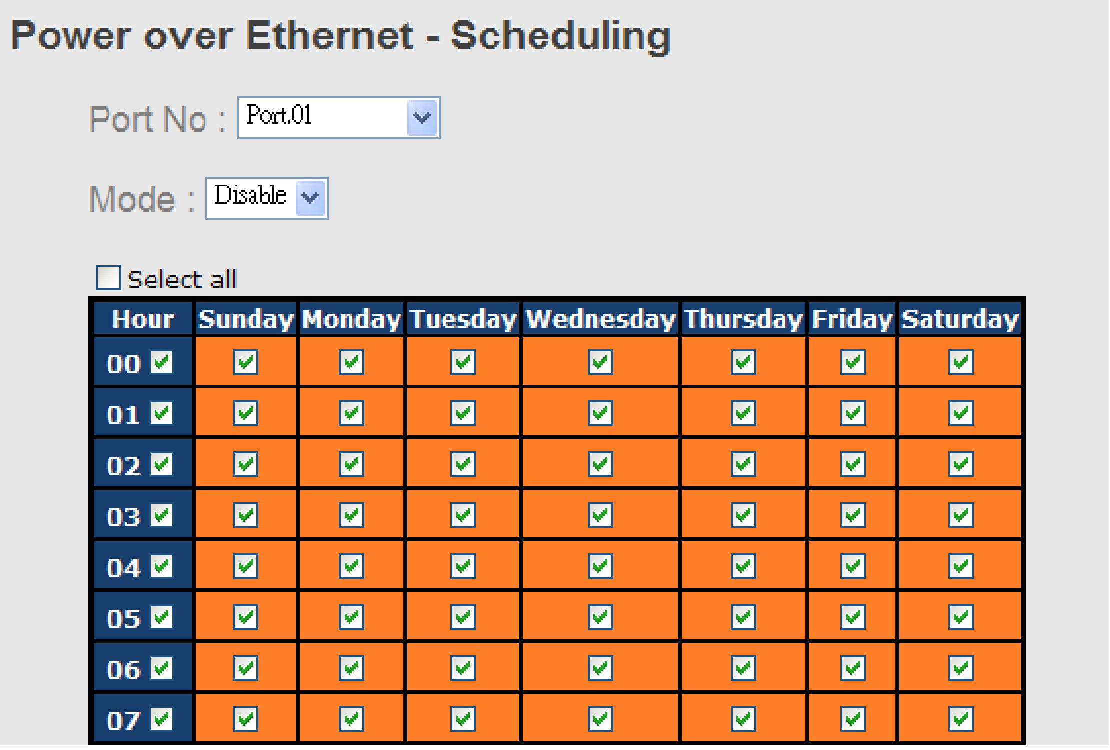
Port No.	IP Address of PD	Interval Time (10~120) seconds	Retry Time (1~5)	Failure Log	Failure Action	Reboot Time (3~120) seconds
Port.01	0.0.0.0	30	3	error=0 total=0	Nothing	15
Port.02	0.0.0.0	30	3	error=0 total=0	Nothing	15
Port.03	0.0.0.0	30	3	error=0 total=0	Nothing	15
Port.04	0.0.0.0	30	3	error=0 total=0	Nothing	15
Port.05	0.0.0.0	30	3	error=0 total=0	Nothing	15
Port.06	0.0.0.0	30	3	error=0 total=0	Nothing	15
Port.07	0.0.0.0	30	3	error=0 total=0	Nothing	15
Port.08	0.0.0.0	30	3	error=0 total=0	Nothing	15

Event Alarm by SMTP : Disable

Label	Description
Ping Check	Enables or disables ping check function.
Send Mail	When ping fails, an email notification will be sent.
Port	Ports which you want to perform auto-ping check function.
Ping IP Address	Enter an IP address
Interval Time	Assigns a time interval for the check (10 - 120 seconds)
Retry Time	Set up the number of times for which the function will perform repeatedly
Failure Log	Note down failed results
Failure Action	Assign the action you want to perform
Reboot Time	Assigns the time for rebooting the switch after check fails
Event Alarm by SMTP	Send alarm message form SMTP mail

1.13.6 Schedule

You can appoint a date and time as well as enable or disable PoE functions. The switch will perform PoE functions based on your configurations (SNTP function must be enabled).



Power over Ethernet - Scheduling

Port No : Port.01

Mode : Disable

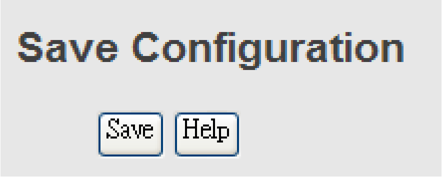
□ Select all

Hour	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00 ☑	☑	☑	☑	☑	☑	☑	☑
01 ☑	☑	☑	☑	☑	☑	☑	☑
02 ☑	☑	☑	☑	☑	☑	☑	☑
03 ☑	☑	☑	☑	☑	☑	☑	☑
04 ☑	☑	☑	☑	☑	☑	☑	☑
05 ☑	☑	☑	☑	☑	☑	☑	☑
06 ☑	☑	☑	☑	☑	☑	☑	☑
07 ☑	☑	☑	☑	☑	☑	☑	☑

Label	Description
Port No.	Select a port for the schedule.
Mode	Enables or disables the schedule mode.
Select all	Check to have the schedule enabled at all time.
Hour	Check to choose the hour for the schedule.
Sunday ~ Saturday	Check to choose the day for the schedule.

1.14 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.

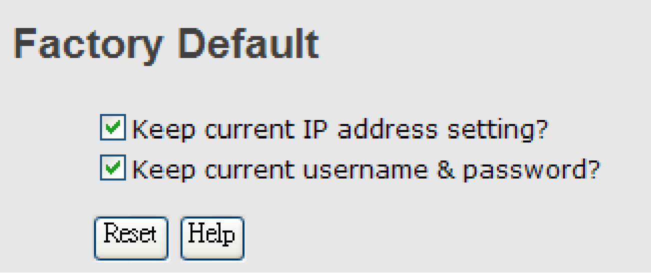


Save Configuration

Label	Description
Save	Saves all configurations
Help	Shows help file

1.15 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.



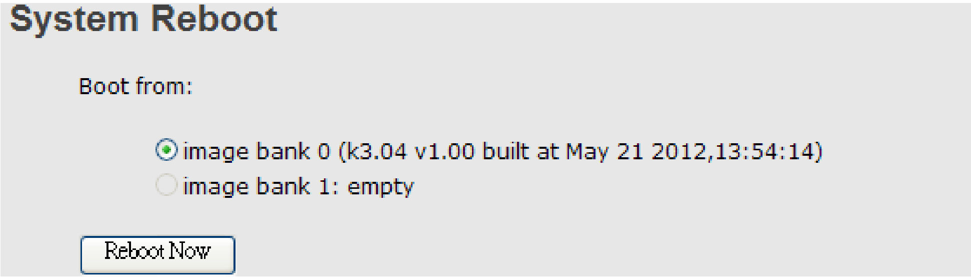
Factory Default

☑ Keep current IP address setting?

☑ Keep current username & password?

1.16 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.



System Reboot

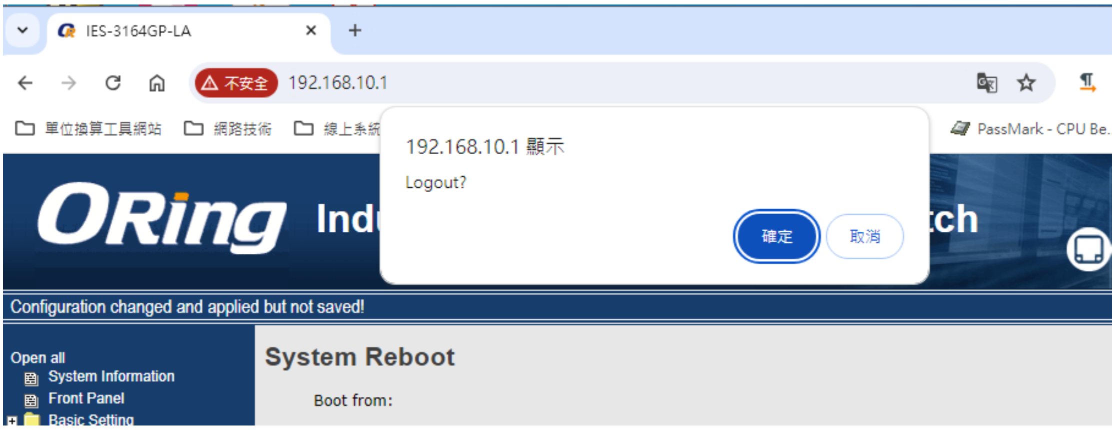
Boot from:

● image bank 0 (k3.04 v1.00 built at May 21 2012,13:54:14)

○ image bank 1: empty

1.17Logout

Logout your device .



192.168.10.1 顯示

Logout?

確定 取消

Configuration changed and applied but not saved!

System Reboot

Boot from: