

4.3.2 Privilege Level

This page provides an overview of the privilege levels. The switch provides user set privilege levels from 1 to 15 for Account, Aggregation, Diagnostics, EEE, GARP, GVRP, IP, ICMP Snooping, LACP, LLDP, LLDP, MED, MAC Table, MRP, MVR, MVRP, Maintenance Mirroring, POE Ports, Private VLANs, QoS, SMTP, SNMP, Security, Spanning Tree, System Trap Event, VCL, VLANs, Voice VLAN.

Web Interface

To configure Privilege Level in the web interface:

1. Click SYSTEM, Account, Privilege Level.
2. Specify the Privilege parameter.
3. Click Apply.

Figure 4-3.2: The Privilege Level configuration

Privilege Level Configuration

Group Name	Privilege Levels
Account	15 ▾
Aggregation	10 ▾
Diagnostics	10 ▾
EEE	10 ▾
Easyport	10 ▾
GARP	10 ▾
GVRP	10 ▾
IP	10 ▾
IPMC Snooping	10 ▾
LACP	10 ▾
LLDP	10 ▾
LLDP MED	10 ▾
Loop Detection	10 ▾
MAC Table	10 ▾
MRP	10 ▾
MVR	10 ▾
MVRP	10 ▾
Maintenance	15 ▾
Mirroring	10 ▾
POE	10 ▾
Ports	10 ▾
Private VLANs	10 ▾
QoS	10 ▾
SFlow	10 ▾
SMTP	10 ▾
SNMP	10 ▾
Security	10 ▾
Spanning Tree	10 ▾
System	10 ▾
Trap Event	10 ▾
VCL	10 ▾
VLANs	10 ▾
Voice VLAN	10 ▾

Parameter description:

Group Name

4 System Configuration

The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contain more than one. The following description defines the privilege level groups in details:

System: Contact, Name, Location, Time zone, Log.

Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and IP source guard.

IP: Everything except 'ping'.

Port: Everything except 'VeriPHY'.

Diagnostics: 'ping' and 'VeriPHY'.

Maintenance: System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.

Privilege Levels

Every group has an authorization privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. for clearing of statistics). User privilege should be equal or greater than the authorization Privilege level to have the access to that group.

4.4 IP

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. The new version of the Internet Protocol, IPv6, which has 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it.

4.4.1 IPv4

The IPv4 address for the switch could be obtained via DHCP Server for VLAN 1. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

Web Interface

To configure an IP address in the web interface:

1. Click System, IP Configuration.
2. Specify the IPv4 settings, and enable DNS proxy service if required.
3. Click Apply.

The Configured column is used to view or change the IP configuration.

The Current column is used to show the active IP configuration.

Figure 4-4.1: The IP configuration

IP Configuration

	Configured	Current
DHCP Client	<input type="checkbox"/>	Renew
IP Address	192.168.1.1	192.168.1.1
IP Mask	255.255.255.0	255.255.255.0
IP Router	0.0.0.0	0.0.0.0
VLAN ID	1	1
DNS Server	0.0.0.0	0.0.0.0

IP DNS Proxy Configuration

DNS Proxy

Save Reset

Parameter description:

DHCP Client:

Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

IP Address:

Provide the IP address of this switch in dotted decimal notation.

IP Mask:

Provide the IP mask of this switch dotted decimal notation.

IP Router:

Provide the IP address of the router in dotted decimal notation.

SNTP Server:

Provide the IP address of the SNTP Server in dotted decimal notation.

DNS Server:

Provide the IP address of the DNS Server in dotted decimal notation.

VLAN ID:

Provide the managed VLAN ID. The allowed range is 1 to 4094.

DNS Proxy:

When DNS proxy is enabled, DUT will relay DNS requests to the current configured DNS server on DUT, and reply as a DNS resolver to the client device on the network.

4.4.2 IPv6

This section describes how to configure the switches' IPv6 information.

Web Interface

To configure IPv6 on the switch in the web interface:

1. Click System, IPv6 Configuration.
2. Specify the IPv6 settings, and enable Auto Configuration service if required.
3. Click Apply.

The 'Configured' column is used to view or change the IPv6 configuration.

4 System Configuration

The 'Current' column is used to show the active IPv6 configuration.

Figure 4-4.2: The IPv6 configuration

IPv6 Configuration		
	Configured	Current
Auto Configuration	<input type="checkbox"/>	<input type="button" value="Renew"/>
Address	::192.168.1.1	::192.168.1.1 Link-Local Address: fe80::240:c7ff:fe74:d1
Prefix	96	96
Gateway	::	::

Parameter description:

Auto Configuration:

Enable IPv6 auto-configuration by checking this box. If it fails, the configured IPv6 address is zero. The router may delay responding to a router solicitation for a few seconds, the total time needed to complete auto-configuration can be significantly longer.

Address:

Provide the IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Prefix:

Provide the IPv6 Prefix of this switch. The allowed range is 1 to 128.

Router

Provide the IPv6 gateway address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

4.5 Syslog

The Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It can be used as generalized informational, analysis and debugging messages. It is supported by a wide variety of devices and receivers across multiple platforms.

4.5.1 Configuration

This section describes how to configure the system log and provide a wide variety of devices and receivers across multiple platforms.

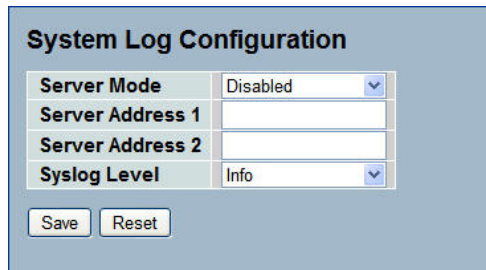
Web Interface

To configure Syslog in the web interface:

1. Click SYSTEM, Syslog.
2. Specify the syslog parameters includes IP Address of Syslog server and Port number.
3. Activate the Syslog to enable it.

4. Click Apply.

Figure 4-5.1: The System Log configuration



Parameter description:

Server Mode:

Indicates the server mode. When the mode operation is enabled, the syslog message will be sent out to a syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always be send out even if the syslog server does not exist. Possible modes are:

Enabled: Enable server mode operation.

Disabled: Disable server mode operation.

Server Address 1 and 2:

Indicates the IPv4 host address of the syslog server 1 and server 2 (For redundancy). If the switch provides DNS, it also can be a host name.

Syslog Level:

Indicates what kind of message will send to the syslog server. Possible modes are:

Info: Send information, warnings and errors.

Warning: Send warnings and errors.

Error: Send errors.

4.5.2 Log

This section describes the system log information of the switch

Web Interface

To display the log configuration in the web interface:

1. Click Syslog, Log.
2. Display the log information.

Figure 4-5.2: The System Log configuration

ID	Level	Time	Message
1	Info	-	Switch just made a cold boot.
2	Info	1970-01-01 00:00:05	Link up on port 1
3	Info	1970-01-01 00:26:08	Link down on port 1
4	Info	1970-01-01 00:55:53	Link up on port 1
5	Info	1970-01-01 01:47:14	Link down on port 1
6	Info	1970-01-01 01:48:36	Link up on port 1
7	Info	1970-01-01 02:20:04	Link down on port 1
8	Info	1970-01-01 18:55:49	Link up on port 1
9	Info	1970-01-01 19:58:11	Link down on port 1
10	Info	1970-01-01 19:58:45	Link up on port 1

Parameter description:

Auto-refresh

Activate the auto-refresh to refresh the log automatically.

Level

Level of the system log entry. The following level types are supported:

Information: Information level of the system log.

Warning: Warning level of the system log.

Error: Error level of the system log. All: All levels.

ID

ID (≥ 1) of the system log entry.

Time

The time of the system log entry.

Message

The message of the system log entry.

Refresh

Refresh the system log manually.

Clear

Clear the system log manually.

4.5.3 Detailed Log

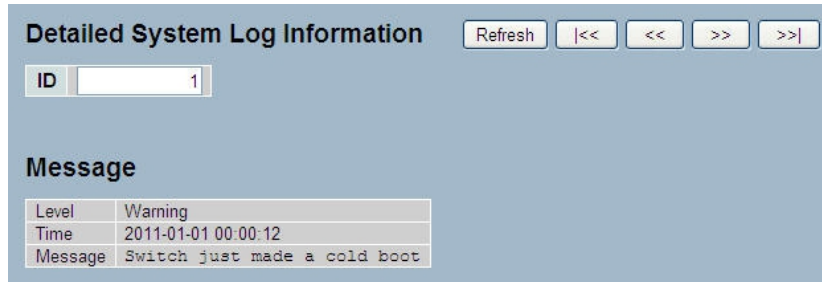
This section describes the detailed log information of the switch.

Web Interface

To display the detailed log configuration in the web interface:

1. Click Syslog, Detailed Log.
2. Display the log information.

Figure 4-5.3: The Detailed System Log Information



Parameter description:

ID

The ID (≥ 1) of the system log entry.

Message

The detailed message of the system log entry.

Refresh

Refresh the system log manually.

Clear

Clear the system log manually.

4.6 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP "Enable", the SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set "Disable", SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

4.6.1 System

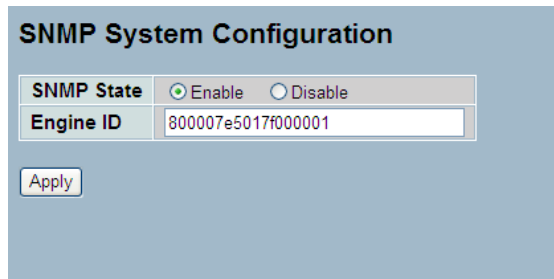
This section describes how to configure SNMP on the switch. This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. An SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click <Apply> button, for the setting to take effect.

Web Interface

To configure the SNMP System in the web interface:

1. Click SNMP, System.
2. Activate SNMP State to enable or disable the SNMP function.
3. Specify the Engine ID
4. Click Apply.

Figure 4-6.1: The SNMP System Configuration



SNMP System Configuration

SNMP State: Enable Disable

Engine ID:

Parameter description:

These parameters are displayed on the SNMP System Configuration page:

SNMP State:

Enable: Enable SNMP operation.

Disable: Disable SNMP operation.

Default: Enable.

Engine ID:

SNMPv3 engine ID. Syntax: 0-9,a-f,A-F, min 5 octet, max 32 octet, fifth octet must not be 00. If the Engine ID is changed it will clear all original users.

4.6.2 Communities

The function is used to configure SNMPv3 communities. The Community and UserName is unique. To create a new community account, please click on the <Add new community> button, and enter the account information and click on <Save>. Max Group Number: 4.

Web Interface

To configure SNMP Communities in the web interface:

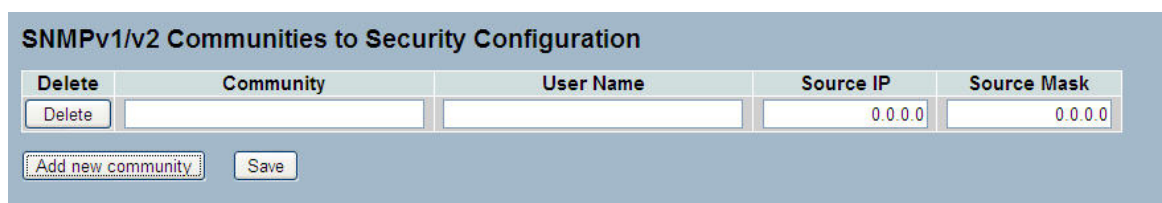
1. Click SNMP, Communities.
2. Click Add new community.
3. Specify the SNMP communities parameters.
4. Click Apply.
5. If you want to modify or clear the setting click Reset.

Figure 4-6.2: The SNMPv1/v2 Communities Security Configuration



SNMPv1/v2 Communities to Security Configuration

Delete	Community	UserName	Source IP	Source Mask
<input type="checkbox"/>	public	<input type="text"/>	0.0.0.0	0.0.0.0
<input type="checkbox"/>	private	<input type="text"/>	0.0.0.0	0.0.0.0



SNMPv1/v2 Communities to Security Configuration

Delete	Community	User Name	Source IP	Source Mask
<input type="button" value="Delete"/>	<input type="text"/>	<input type="text"/>	0.0.0.0	0.0.0.0

Parameter description:

Delete

Delete the entry. It will be deleted during the next save.

Community

Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.

UserName:

The UserName access string to permit access to the SNMPv3 agent. The length of the "UserName" string is restricted to 1-32 characters.

Source IP

Indicates the SNMP access source address. A particular range of source addresses can be used to restrict the source subnet when combined with source mask.

Source Mask

Indicates the SNMP access source address mask

4.6.3 Users

The function is used to configure SNMPv3 users. The Entry index key is UserName. To create a new UserName account, please click on the <Add new user> button, and enter the user information then click <Save>. Max Group Number: 10.

Web Interface

To configure SNMP Users in the web interface:

1. Click SNMP, Users.
2. Specify the Privilege parameter.
3. Click Apply.

Figure 4-6.3: The SNMP Users Configuration

SNMPv3 Users Configuration

Delete	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	default_user	NoAuth, NoPriv	None	None	None	None

SNMPv3 Users Configuration

Delete	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="button" value="Delete"/>	<input type="text"/>	Auth, Priv	MD5	<input type="text"/>	DES	<input type="text"/>

Parameter description:

Delete

Check to delete the entry. It will be deleted during the next save.

4 System Configuration

User Name

A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Level

Indicates the security model that this entry should belong to. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

The value of the security level cannot be modified if an entry already exists. That means it must first be ensured that the value is set correctly.

Authentication Protocol

Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

None: No authentication protocol.

MD5: An optional flag to indicate that this user uses MD5 authentication protocol.

SHA: An optional flag to indicate that this user uses SHA authentication protocol.

The value of the security level cannot be modified if an entry already exists. That means must first ensure that the value is set correctly.

Authentication Password

A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.

Privacy Protocol

Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

None: No privacy protocol.

DES: An optional flag to indicate that this user uses DES authentication protocol.

Privacy Password

A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

4.6.4 Groups

The function is used to configure SNMPv3 groups. The Entry index keys are Security Model and Security Name. To create a new group account, please check <Add new group> button, and enter the group information then check <Save>. Max Group Number: v1: 2, v2: 2, v3:10.

Web Interface

To configure SNMP Groups in the web interface:

1. Click SNMP, Groups.
2. Specify the Privilege parameter.
3. Click Apply.

Figure 4-6.4: The SNMP Groups Configuration

SNMPv3 Groups Configuration

Delete	Security Model	Security Name	Group Name
<input type="checkbox"/>	v1	public	default_ro_group
<input type="checkbox"/>	v1	private	default_rw_group
<input type="checkbox"/>	v2c	public	default_ro_group
<input type="checkbox"/>	v2c	private	default_rw_group
<input type="checkbox"/>	usm	default_user	default_rw_group

SNMPv3 Groups Configuration

Delete	Security Model	Security Name	Group Name
<input type="button" value="Delete"/>	v1	125323	

Parameter description:

Delete

Delete the entry. It will be deleted during the next save.

Security Model

Indicates the security model that this entry should belong to. Possible security models are:

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

Security Name

A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Group Name

A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

4.6.5 Views

The function is used to configure SNMPv3 view. The entries index keys are OID Subtree and View Name. To create a new view account, please click the <Add new view> button, and enter the view information then click <Save>. Max group number: 28.

Configure SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.

Web Interface

1. Click SNMP, Views.
2. Click Add new view.
3. Specify the SNMP View parameters.
4. Click Apply.
5. If you want to modify or clear the setting then click Reset.

Figure 4-6.5: The SNMP Views Configuration

The figure shows two screenshots of the 'SNMPv3 Views Configuration' web interface. The top screenshot displays a table with the following data:

Delete	View Name	View Type	OID Subtree
<input type="checkbox"/>	default_view	included	.1

Below the table are buttons for 'Add new view' and 'Save'. The bottom screenshot shows the same interface but with empty input fields for 'View Name', 'View Type', and 'OID Subtree', and a 'Delete' button in the 'Delete' column.

Parameter description:

Delete

Delete the entry. It will be deleted during the next save.

View Name

A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

View Type

Indicates the view type that this entry should belong to. Possible view types are:

included: An optional flag to indicate that this view subtree should be included.

excluded: An optional flag to indicate that this view subtree should be excluded.

In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and its OID subtree should overstep the 'excluded' view entry.

OID Subtree

The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Save

Save the configuration to the ROM.

4.6.6 Access

The function is used to configure SNMPv3 accesses. The entries index keys are Group Name, Security Model and Security level. To create a new access account, please click the <Add new access> button, and enter the access information. Then click <Save>. Max group number: 14

Web Interface

To configure SNMP access in the web interface:

1. Click SNMP, Accesses.
2. Click Add new Access.
3. Specify the SNMP Access parameters.
4. Click Apply.

5. If you want to modify or clear the setting then click Reset.

Figure 4-6.6: The SNMP Accesses Configuration

SNMPv3 Accesses Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="checkbox"/>	default_ro_group	any	NoAuth, NoPriv	default_view	None
<input type="checkbox"/>	default_rw_group	any	NoAuth, NoPriv	default_view	default_view

SNMPv3 Accesses Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="button" value="Delete"/>	3533	any	NoAuth, NoPriv	None	None

Parameter description:

Delete

Check to delete the entry. It will be deleted during the next save.

Group Name

A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Model

Indicates the security model that this entry should belong to. Possible security models are:

any: Any security model accepted(v1|v2c|usm).

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

Security Level

Indicates the security model that this entry should belong to. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

Read View Name

The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Write View Name

The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

4.6.7 Trap

The function is used to configure SNMP traps. To create a new trap account, please click on the <No number> button, and enter the trap information then click <Apply>. Max group number: 6.

Web Interface

To configure SNMP Traps:

1. Click SNMP, Trap.
2. Display the SNMP Trap Hosts information table.
3. Choose an entry to display and modify the detail parameters or click the delete button to delete the entry.

Figure 4-6.7: The SNMP Trap Host Configuration

Trap Hosts Configuration									
Delete	No	Version	Server IP	UDP Port	Community/Security Name	Severity Level	Security Level	Authentication Protocol	Privacy Protocol
	1								
	2								
	3								
	4								
	5								
	6								

Save

Trap Host Configuration	
Trap Version	v2c
Server IP	0.0.0.0
UDP Port	162
Community/Security Name	
Severity Level	Info
Security Level	NoAuth, NoPriv
Authentication Protocol	MD5
Authentication Password	
Privacy Protocol	DES
Privacy Password	

Save Reset

Parameters description:

Delete:

Check <Delete> entry then click the <Save> button, the entry will be deleted.

Trap Version:

You may choose v1, v2c or v3 trap.

Server IP:

Used SNMP Host IP address.

UDP Port:

Used Port number. Default: 162

Community / Security Name:

The length of "Community / Security Name" string is restricted to 1-32.

Security Level:

Indicates what kind of message will send to Security Level.

Possible modes are:

Info: Send information, warnings and errors.

Warning: Send warnings and errors.

Error: Send errors.

Security Level:

There are three kinds of choices.

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

Authentication Protocol:

You can choose MD5 or SHA for authentication.

Authentication Password:

The length of 'MD5 Authentication Password' is restricted to 8 – 32.

The length of 'SHA Authentication Password' is restricted to 8 – 40.

Privacy Protocol:

You can set DES encryption for UserName.

Privacy Password:

The length of 'Privacy Password' is restricted to 8 – 32.

5 Security

This chapter describes all of the switch security configuration tasks to enhance the security of local network including IP Source Guard, ARP Inspection, DHCP Snooping, AAA, etc.

5.1 IP Source Guard

The section describes how to configure the IP Source Guard detail parameters of the switch. The IP Source Guard configuration can be used to enable or disable ports of the switch.

5.1.1 Configuration

This section describes how to configure IP Source Guard setting including:

Mode (Enabled and Disabled)

Maximum Dynamic Clients (0, 1, 2, Unlimited)

To configure an IP Source Guard in the web interface:

1. Select "Enabled" in the Mode of IP Source Guard Configuration.
2. Select "Enabled" of the specific port in the Mode of Port Mode Configuration.
3. Select Maximum Dynamic Clients (0, 1, 2, Unlimited) of the specific port in the Mode of Port Mode Configuration.
4. Click Apply.

Figure 5-1.1: The IP Source Guard Configuration (GS-2310P)

IP Source Guard Configuration

Mode Disabled ▾

Translate dynamic to static

Port Mode Configuration

Port	Mode	Max Dynamic Clients
*	<> ▾	<> ▾
1	Disabled ▾	Unlimited ▾
2	Disabled ▾	Unlimited ▾
3	Disabled ▾	Unlimited ▾
4	Disabled ▾	Unlimited ▾
5	Disabled ▾	Unlimited ▾
6	Disabled ▾	Unlimited ▾
7	Disabled ▾	Unlimited ▾
8	Disabled ▾	Unlimited ▾
9A	Disabled ▾	Unlimited ▾
10A	Disabled ▾	Unlimited ▾
9B	Disabled ▾	Unlimited ▾
10B	Disabled ▾	Unlimited ▾

Apply
Reset

Parameter description:

Mode of IP Source Guard Configuration:

Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

Port Mode Configuration:

Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

Max Dynamic Clients:

Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Buttons:

Save – Click to save changes.

Reset – Click to undo any changes made locally and revert to previously saved values.

5.1.2 Static Table

The section describes how to configure the Static IP Source Guard Table parameters of the switch. You could use the Static IP Source Guard Table configure to manage the entries.

Web Interface

To configure a Static IP Source Guard Table in the web interface:

1. Click "Add new entry".
2. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
3. Click Apply.

Figure 5-1.2: The Static IP Source Guard Table

Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC address
Delete	1			

Buttons: Add new entry, Save, Reset

Parameter description:

Delete:

Delete the entry. It will be deleted during the next save.

5 Security

Port:

The logical port for the settings.

VLAN ID:

The vlan id for the settings.

IP Address:

Allowed source IP address.

IP Mask:

It can be used for calculating the allowed network with IP address.

MAC address:

Allowed source MAC address.

Add new entry:

Click to add a new entry to the Static IP Source Guard table. Specify the Port, VLAN ID, IP address, and IP Mask for the new entry. Click "Save".

Buttons:

Save – Click to save changes.

Reset – Click to undo any changes made locally and revert to previously saved values.

5.1.3 Dynamic Table

The section describes how to configure the Dynamic IP Source Guard Table parameters of the switch.

Web Interface

To configure a Dynamic IP Source Guard Table in the web interface:

1. Specify the Start from port, VLAN ID, IP Address, and entry per page.
2. Check "Auto-refresh".

Figure 5-1.3: The Dynamic Table

Dynamic IP Source Guard Table Auto-refresh Refresh |<< >>

Start from **Port 1**, VLAN ID **1** and IP address **0.0.0.0** with **20** entries per page.

Port	VLAN ID	IP Address	MAC Address
No more entries			

Parameter description:

Port:

Related switch port.

VLAN ID:

VLAN ID in which the IP traffic is permitted.

IP Address:

User IP address.

MAC Address:

Source MAC address.

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh:

Refresh the Dynamic IP Source Guard Table manually.

|<<, >>:

Go to previous/next page or entry.

5.2 ARP Inspection

The section describes how to configure the ARP Inspection parameters of the switch.

5.2.1 Configuration

This section describes how to configure ARP Inspection including:

Mode (Enabled and Disabled)

Port (Enabled and Disabled)

To configure ARP Inspection in the web interface:

1. Select "Enabled" in the Mode of ARP Inspection Configuration.
2. Select "Enabled" of the specific port in the Mode of Port Mode Configuration.
3. Click Apply.

Figure 5-2.1: The ARP Inspection Configuration (GS-2310P)

ARP Inspection Configuration

Mode: Disabled ▾

Translate dynamic to static

Port Mode Configuration

Port	Mode
*	<> ▾
1	Disabled ▾
2	Disabled ▾
3	Disabled ▾
4	Disabled ▾
5	Disabled ▾
6	Disabled ▾
7	Disabled ▾
8	Disabled ▾
9A	Disabled ▾
10A	Disabled ▾
9B	Disabled ▾
10B	Disabled ▾

Apply Reset

Parameter description:

5 Security

Mode of ARP Inspection Configuration:

Enable the Global ARP Inspection or disable the Global ARP Inspection.

Port Mode Configuration:

ARP Inspection is enabled on selected ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port.

Buttons:

Save – Click to save changes.

Reset – Click to undo any changes made locally and revert to previously saved values.

5.2.2 Static Table

The section describes how to configure the Static ARP Inspection Table parameters of the switch.

To configure a Static ARP Inspection Table in the web interface:

1. Click "Add new entry".
2. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
3. Click Apply.

Figure 5-2.2: The Static ARP Inspection Table

The figure displays two screenshots of the Static ARP Inspection Table configuration interface. The top screenshot shows the table with headers: Delete, Port, VLAN ID, MAC Address, IP Address. Below the headers are buttons for 'Add new entry', 'Save', and 'Reset'. The bottom screenshot shows the table with a single entry: Delete, Port (1), VLAN ID (empty), MAC Address (empty), IP Address (empty). Below the entry are buttons for 'Add new entry', 'Save', and 'Reset'.

Parameter description:

Delete:

Delete the entry. It will be deleted during the next save.

Port:

The logical port for the settings.

VLAN ID:

The vlan id for the settings.

MAC Address:

Allowed Source MAC address in ARP request packets.

IP Address:

Allowed Source IP address in ARP request packets.