Clear all entries.

5.6 AAA

This section shows you to use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a TACACS+ or RADIUS server to create and manage objects that contain settings for using AAA servers.

5.6.1 Configuration

This section describes how to configure AAA for TACACS+ or RADIUS server.

To configure AAA in the web interface:

1. Set Timeout (Default is 15 seconds).

2. Set Dead Time (Default is 300 seconds).

To configure a TACACS+ Authorization and Accounting Configuration of AAA in the web interface:

1. Select "Enabled" in the Authorization.

2. Select "Enabled" in the Failback to Local Authorization.

3. Select "Enabled" in the Account.

To configure a RADIUS Authentication Server Configuration of AAA in the web interface:

1. Check "Enabled".

2. Specify IP address or Hostname for Radius Server.

3. Specify Authentication Port for Radius Server (Default is 1812).

4. Specify the Secret with Radius Server.

To configure a RADIUS Accounting Server Configuration of AAA in the web interface:

1. Check "Enabled".

2. Specify IP address or Hostname for Radius Server.

3. Specify Accounting Port for Radius Server (Default is 1813).

4. Specify the Secret with Radius Server.

To configure a TACACS+ Authentication Server Configuration of AAA in the web interface:

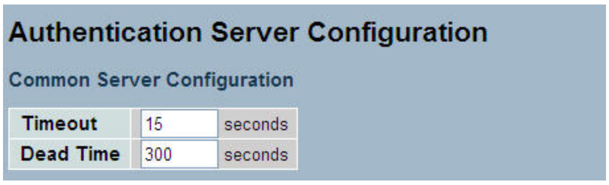
1. Check "Enabled".

2. Specify IP address or Hostname for TACACS+ Server.

3. Specify Authentication Port for TACACS+ Server (Default is 49).

4. Specify the Secret with TACACS+ Server.

Figure 5-5.3.1: The Common Server Configuration

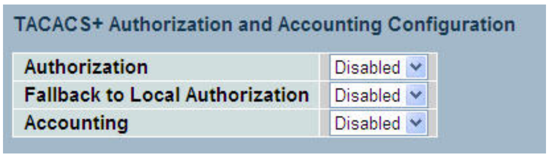


Authentication Server Configuration

Common Server Configuration

Timeout	15	seconds
Dead Time	300	seconds

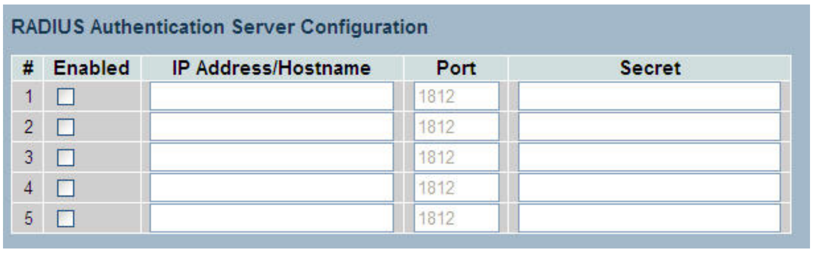
Figure 5-5.3.2: The TACACS+ Accounting Configuration



TACACS+ Authorization and Accounting Configuration

Authorization	Disabled
Fallback to Local Authorization	Disabled
Accounting	Disabled

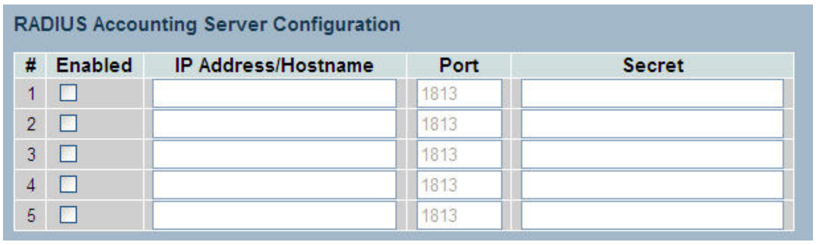
Figure 5-5.3.3: The RADIUS Configuration



RADIUS Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	□		1812	
2	□		1812	
3	□		1812	
4	□		1812	
5	□		1812	

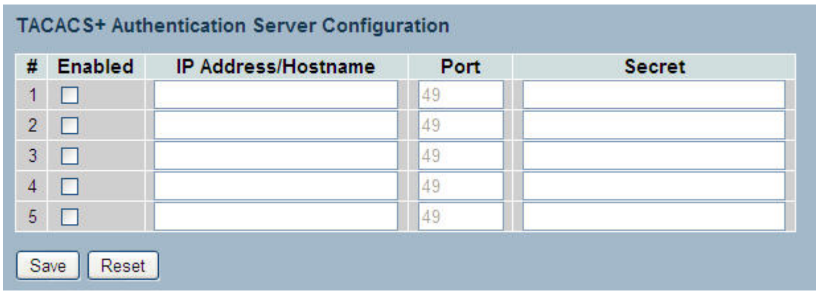
Figure 5-5.3.4: The RADIUS Accounting Configuration



RADIUS Accounting Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	□		1813	
2	□		1813	
3	□		1813	
4	□		1813	
5	□		1813	

Figure 5-5.3.4: The TACACS+ Authentication Configuration



TACACS+ Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	□		49	
2	□		49	
3	□		49	
4	□		49	
5	□		49	

Parameter description:

Timeout:

The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server.

If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any).

RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.

Dead Time:

The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

RADIUS Authentication Server Configuration

The table has one row for each RADIUS Authentication Server and a number of columns, which are:

#:

The RADIUS Authentication Server number for which the configuration below applies.

Enabled:

Enable the RADIUS Authentication Server by checking this box.

IP Address/Hostname:

The IP address or hostname of the RADIUS Authentication Server. IP address is expressed in dotted decimal notation.

Port:

The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.

Secret:

The secret - up to 29 characters long - shared between the RADIUS Authentication Server and the switch.

RADIUS Accounting Server Configuration

The table has one row for each RADIUS Accounting Server and a number of columns, which are:

#:

The RADIUS Accounting Server number for which the configuration below applies.

Enabled:

Enable the RADIUS Accounting Server by checking this box.

IP Address/Hostname:

The IP address or hostname of the RADIUS Accounting Server. IP address is expressed in dotted decimal notation.

Port:

The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.

Secret:

The secret - up to 29 characters long - shared between the RADIUS Accounting Server and the switch.

TACACS+ Authentication Server Configuration

The table has one row for each TACACS+ Authentication Server and a number of columns, which are:

#:

The TACACS+ Authentication Server number for which the configuration below applies.

Enabled:

Enable the TACACS+ Authentication Server by checking this box.

IP Address/Hostname:

The IP address or hostname of the TACACS+ Authentication Server. IP address is expressed in dotted decimal notation.

Port:

The TCP port to use on the TACACS+ Authentication Server. If the port is set to 0 (zero), the default port (49) is used on the TACACS+ Authentication Server.

Secret:

The secret - up to 29 characters long - shared between the TACACS+ Authentication Server and the switch.

Buttons:

Save – Click to save changes.

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

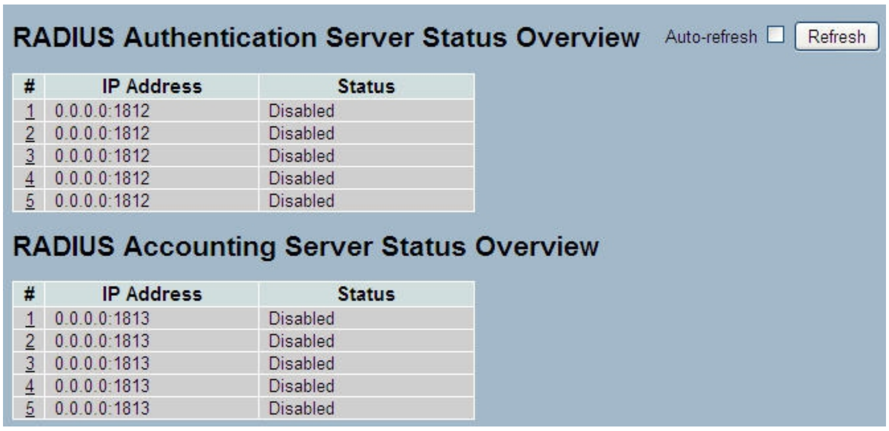
5.6.2 Radius Overview

This section provides an overview of the RADIUS Authentication and Accounting servers status to ensure the function is working.

To show the RADIUS Overview in the web interface:

1. Check "Auto-refresh".

Figure 5-6.2: The RADIUS Authentication Server Status Overview



RADIUS Authentication Server Status Overview

#	IP Address	Status
1	0.0.0.0:1812	Disabled
2	0.0.0.0:1812	Disabled
3	0.0.0.0:1812	Disabled
4	0.0.0.0:1812	Disabled
5	0.0.0.0:1812	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:1813	Disabled
2	0.0.0.0:1813	Disabled
3	0.0.0.0:1813	Disabled
4	0.0.0.0:1813	Disabled
5	0.0.0.0:1813	Disabled

Parameter description:

#:

The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address:

The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

State:

The current state of the server. This field takes one of the following values:

Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Accounting Servers

#:

The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address:

The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

State:

The current state of the server. This field takes one of the following values:

Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.

Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh:

Refresh the RADIUS Status manually.

5.6.3 Radius Details

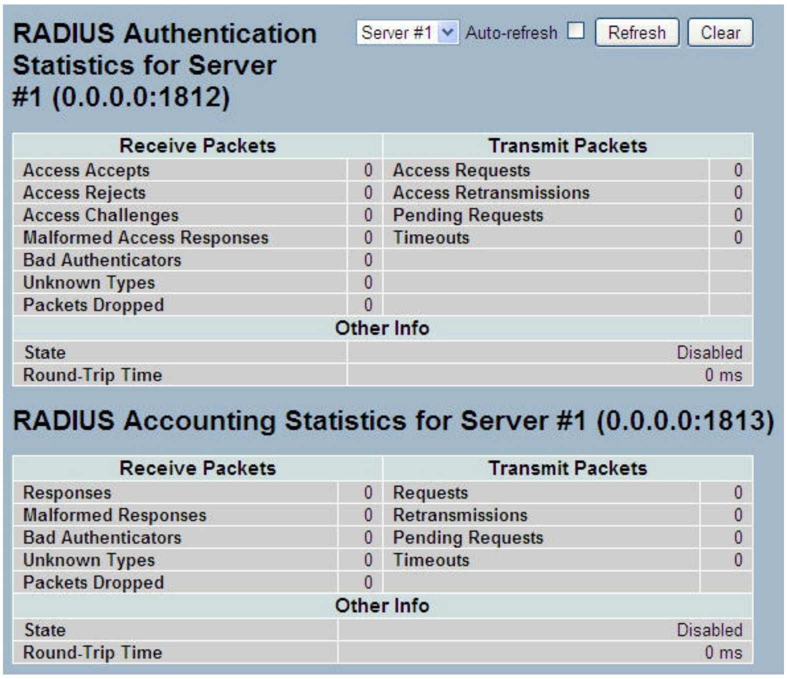
This section provides detailed statistics of the RADIUS Authentication and Accounting servers. The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

To configure RADIUS Details in the web interface:

1. Specify Port which want to check.

2. Checked "Auto-refresh".

Figure 5-6.3: The RADIUS Authentication Statistics Server



RADIUS Authentication Statistics for Server #1 (0.0.0.0:1812)

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		

Other Info	
State	Disabled
Round-Trip Time	0 ms

RADIUS Accounting Statistics for Server #1 (0.0.0.0:1813)

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		

Other Info	
State	Disabled
Round-Trip Time	0 ms

Parameter description:

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh:

Refresh the RADIUS Statistics information manually.

Clear:

Clear all entries.

5.7 Port Security

This section shows how to configure the Port Security settings of the Switch. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

5.7.1 Limit Control

This section shows how to configure the Port Security settings of the Switch. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

Web Interface

To configure Limit Control in the web interface:

1. Select “Enabled” in the Mode of System Configuration.

2. Check Aging Enabled.

3. Set Aging Period (Default is 3600 seconds).

To configure a Port Configuration of Limit Control in the web interface:

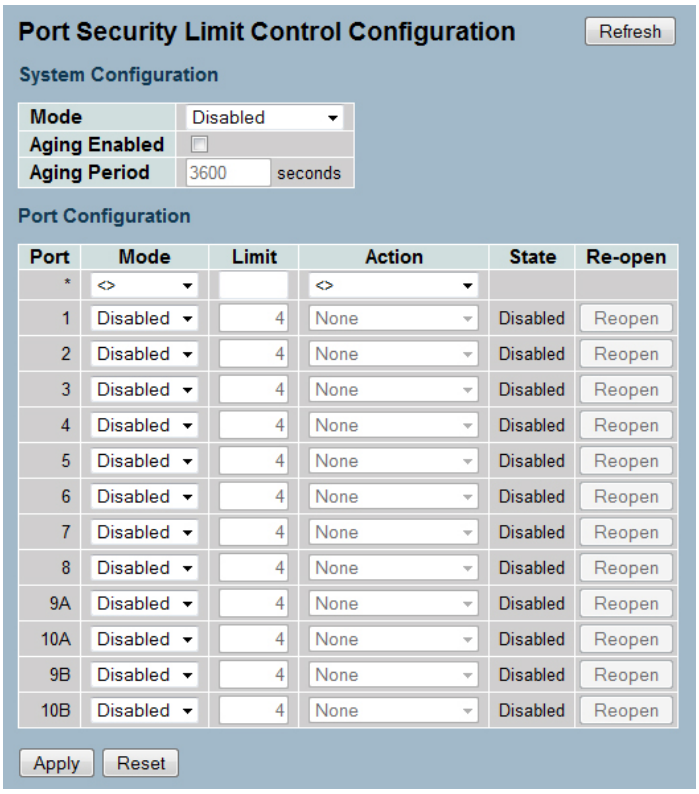
1. Select “Enabled” in the Mode of Port Configuration.

2. Specify the limit of MAC addresses.

3. Set Action (Trap, Shutdown, Trap & Shutdown)

4. Click Apply.

Figure 5-7.1: The Port Security Limit Control Configuration (GS-2310P)



Port Security Limit Control Configuration

System Configuration

Mode	Disabled
Aging Enabled	□
Aging Period	3600 seconds

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	<>		<>		
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen
9A	Disabled	4	None	Disabled	Reopen
10A	Disabled	4	None	Disabled	Reopen
9B	Disabled	4	None	Disabled	Reopen
10B	Disabled	4	None	Disabled	Reopen

Parameter description:

System Configuration

Mode:

Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

Aging Enabled:

If checked, secured MAC addresses are subject to aging as discussed under Aging Period.

Aging Period:

If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

The Aging Period can be set to a number between 10 and 10,000,000 seconds.

To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Port Configuration

The table has one row for each port on the selected switch and a number of columns, which are:

Port:

The port number to which the configuration below applies.

Mode:

Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

Limit:

The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

Action:

If Limit is reached, the switch can take one of the following actions:

None: Do not allow more than Limit MAC addresses on the port, but take no further action.

Trap: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.

Shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:

Boot the switch,

Disable and re-enable Limit Control on the port or the switch,

Click the Reopen button.

Trap & Shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

State:

This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:

Disabled: Limit Control is either globally disabled or disabled on the port.

Ready: The limit is not yet reached. This can be shown for all actions.

Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap.

Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.

Re-open Button:

If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shutdown in the Action section.

❗ Clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost

Upper right icon (Refresh):

Refresh the Port Security information manually.

Buttons:

Save – Click to save changes.

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

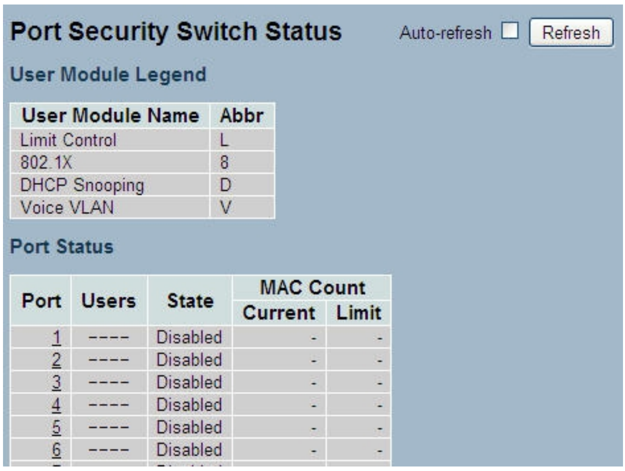
5.7.2 Switch Status

This section shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

To configure Port Security Switch Status in the web interface:

1. Check “Auto-refresh”

Figure 5-7.2: The Port Security Switch Status



Port Security Switch Status

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
DHCP Snooping	D
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	----	Disabled	-	-
2	----	Disabled	-	-
3	----	Disabled	-	-
4	----	Disabled	-	-
5	----	Disabled	-	-
6	----	Disabled	-	-

.

Parameter description:

User Module Legend:

The legend shows all user modules that may request Port Security services.

User Module Name:

The full name of a module that may request Port Security services.

Abbr:

A one-letter abbreviation of the user module. This is used in the Users column in the port status table.

Port Status:

The table has one row for each port on the selected switch and a number of columns, which are:

Port:

The port number for which the status applies. Click the port number to see the status for this particular port.

Users:

Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.

State:

Shows the current state of the port. It can take one of four values:

Disabled: No user modules are currently using the Port Security service.

Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.

Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.

Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

MAC Count (Current, Limit):

The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

If no user modules are enabled on the port, the Current column will show a dash (-).

If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Indicates the number of currently learned MAC addresses (forwarding as well as blocked) on the port. If no user modules are enabled on the port, a dash (-) will be shown.

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh

Refresh the Port Security Switch Status information manually.

5.7.3 Port Status

This section shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

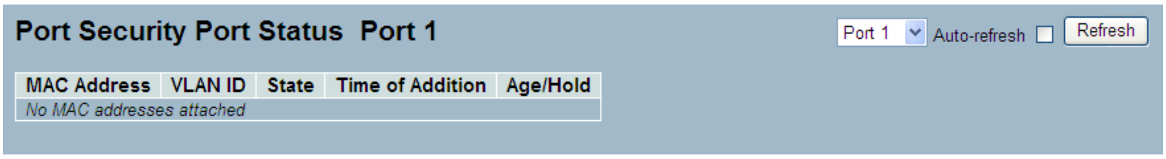
Web Interface

To show the Port Security Switch Status in the web interface:

1. Specify the Port you want to monitor.

2. Check “Auto-refresh”.

Figure 5-7.3: The Port Security Port Status



Port Security Port Status Port 1

Port 1 Auto-refresh □ Refresh

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
No MAC addresses attached				

Parameter description:

MAC Address & VLAN ID:

The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.

State:

Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition:

Shows the date and time when this MAC address was first seen on the port.

Age/Hold:

If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh

Refresh the Port Security Port Status information manually.

5.8 Access Management

This section explains how to configure access management of the switch including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the Switch over an Ethernet LAN, or over the Internet.

5.8.1 Configuration

This section shows you how to configure access management table of the Switch. The maximum entry number is 16. If the application's type match any one of the access management entries, it will allow access to the switch.

Web Interface

To configure Access Management in the web interface:

1. Select “Enabled” in the Mode of Access Management Configuration.

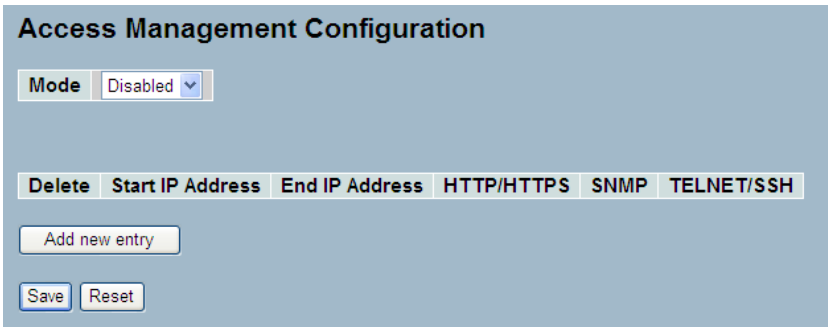
2. Click “Add new entry”.

3. Specify the Start IP Address, End IP Address.

4. Checked Access Management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.

5. Click Apply.

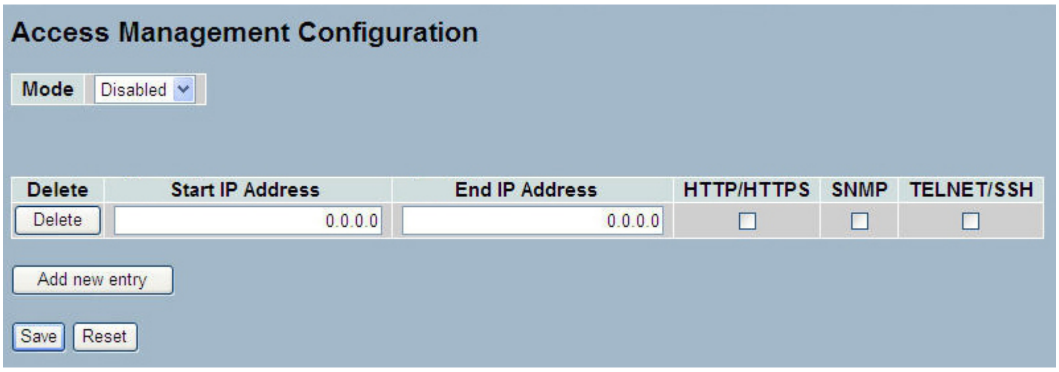
Figure 5-8.1: The Access Management Configuration



Access Management Configuration

Mode: Disabled

Delete	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH



Access Management Configuration

Mode	Disabled

Delete	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	0.0.0.0	0.0.0.0	□	□	□

Parameter description:

Mode:

Indicates the access management mode operation. Possible modes are:

Enabled: Enable access management mode operation.

Disabled: Disable access management mode operation.

Delete:

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

Start IP address:

Indicates the start IP address for the access management entry.

End IP address:

Indicates the end IP address for the access management entry.

HTTP/HTTPS:

Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

SNMP:

Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

TELNET/SSH:

Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

Buttons:

Save – Click to save changes.

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

5.8.2 Statistics

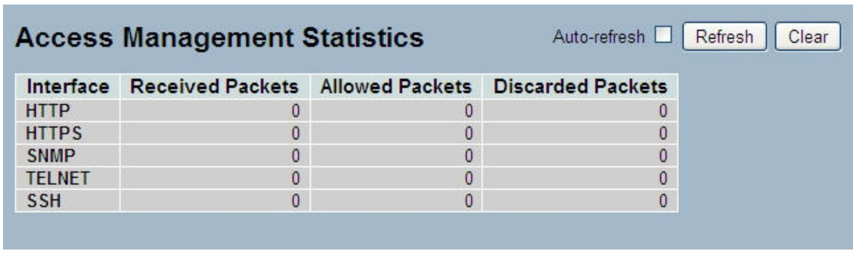
This section shows you detailed statistics of the Access Management including HTTP, HTTPS, SSH. TELNET, and SSH.

Web Interface

To configure Assess Management Statistics in the web interface:

1. Check “Auto-refresh”.

Figure 5-8.2: The Access Management Statistics



Access Management Statistics

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Parameter description:

Interface:

The interface type through which the remote host can access the switch.

Received Packets:

Number of received packets from the interface when access management mode is enabled.

Allowed Packets:

Number of allowed packets from the interface when access management mode is enabled

Discarded Packets.:

Number of discarded packets from the interface when access management mode is enabled.

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh

Refresh the Access Management Statistics information manually.

Clear

Clear the statistics.

5.9 SSH

This section shows you to use SSH (Secure Shell) to securely access the Switch. SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication.

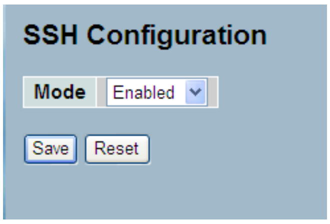
Web Interface

To configure SSH in the web interface:

1. Select “Enabled” in the Mode of SSH Configuration.

2. Click "Save".

Figure 5-9.1: The SSH Configuration



SSH Configuration

Mode: Enabled

Parameter description:

Mode:

Indicates the SSH mode operation. Possible modes are:

Enabled: Enable SSH mode operation.

Disabled: Disable SSH mode operation.

Buttons:

Save – Click to save changes.

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

5.10 HTTPs

This section shows how to use HTTPS to securely access the Switch. HTTPS is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication via the browser.

Web Interface

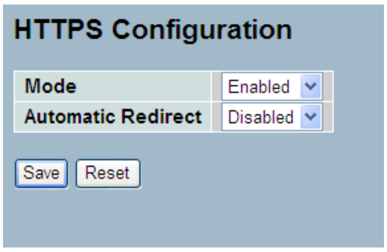
To configure a HTTPS in the web interface:

1. Select "Enabled" in the Mode of HTTPS Configuration.

2. Select "Enabled" in the Automatic Redirect of HTTPS Configuration.

3. Click Apply.

Figure 5-10.1: The HTTPS Configuration



HTTPS Configuration

Mode	Enabled
Automatic Redirect	Disabled

Parameter description:

Mode:

Indicates the HTTPS mode operation. Possible modes are:

Enabled: Enable HTTPS mode operation.

Disabled: Disable HTTPS mode operation.

Automatic Redirect:

Indicates the HTTPS redirect mode operation. Automatically redirect web browser to HTTPS when HTTPS mode is enabled. Possible modes are:

Enabled: Enable HTTPS redirect mode operation.

Disabled: Disable HTTPS redirect mode operation.

5.11 Auth Method

This page shows how to configure the user authentication method of the switch.

Web Interface

To configure a Authentication Method in the web interface:

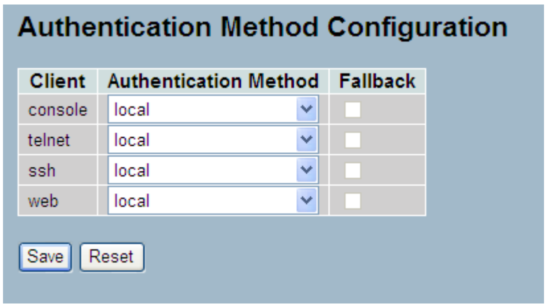
1. Specify the Client (console, telnet, ssh, web) which you want to monitor.

2. Specify the Authentication Method (none, local, radius, tacacs+)

3. Check Fallback.

4. Click Apply.

Figure 5-11.1: The HTTPS Configuration



Authentication Method Configuration

Client	Authentication Method	Fallback
console	local	□
telnet	local	□
ssh	local	□
web	local	□

Parameter description:

Client:

The management client for which the configuration below applies.

Authentication Method:

Authentication Method can be set to one of the following values:

none: authentication is disabled and login is not possible.

local: use the local user database on the switch for authentication.

radius: use a remote RADIUS server for authentication.

tacacs+: use a remote TACACS+ server for authentication.

Fallback:

Enable fallback to local authentication by checking this box.

If none of the configured authentication servers are alive, the local user database is used for authentication.

This is only possible if the Authentication Method is set to a value other than 'none' or 'local'.

Buttons:

Save – Click to save changes.

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

6 Maintenance

This chapter describes all of the switch Maintenance configuration tasks to enhance the performance of local network including Restart Device, Firmware upgrade, Save/Restore, Import/Export, and Diagnostics.

6.1 Restart Device

This section describes how to restart switch for any maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

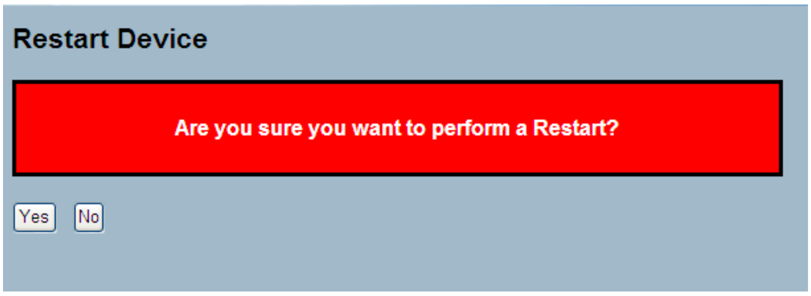
Web Interface

To restart the device:

1. Click Restart Device.

2. Click Yes.

Figure 6-1.1: Restart Device



Restart Device

Are you sure you want to perform a Restart?

Parameter description:

Restart Device:

You can restart the switch on this page. After restart, the switch will boot normally.

Buttons:

Yes – Click to restart the device.

No- Click to undo any restart action.

6.2 Firmware

This section describes how to upgrade the Firmware. The Switch can be enhanced with more value-added functions by installing firmware upgrades.

6.2.1 Firmware Upgrade

This page facilitates an update of the firmware of the switch.

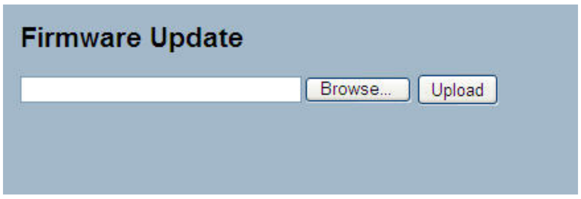
Web Interface

To upgrade the firmware via the web interface:

1. Click "Browse..." to select the firmware for your device.

2. Click "Upload".

Figure 6-2.1: The Firmware update



Parameter description:

Browse:

Click the “Browse...” button to search the Firmware URL or filename.

Upload:

Click the “Upload” button start the upload of the firmware from the specified location.

This page facilitates an update of the firmware controlling the switch. Uploading software will update all managed switches according to the software image. After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and all managed switches restart.

WARNING: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

6.2.2 Firmware Selection

The switch supports dual images for firmware redundancy purposes. You can select the firmware image for your devices' start firmware or operating firmware. This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

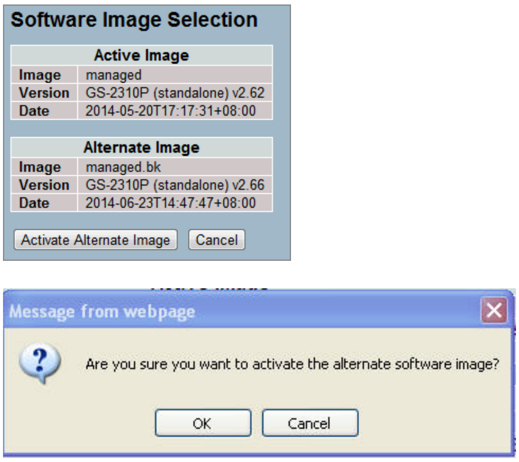
Web Interface

To select the firmware in the web interface:

1. Click "Activate" Alternate Image.

2. Click "Yes" to complete firmware selection.

Figure 6-2.2: The Firmware Selection



Software Image Selection

Active Image	
Image	managed
Version	GS-2310P (standalone) v2.62
Date	2014-05-20T17:17:31+08:00

Alternate Image	
Image	managed.bk
Version	GS-2310P (standalone) v2.66
Date	2014-06-23T14:47:47+08:00

Are you sure you want to activate the alternate software image?

Parameter description:

Activate Alternate Image:

Click to use the alternate image. This button may be disabled depending on system state.

Cancel:

Cancel activating the backup image. Navigates away from this page.

Image:

The flash index name of the firmware image. The name of the primary (preferred) image is image, the alternate image is named image.bk.

Version:

The version of the firmware image.

Date:

The date where the firmware was produced.

In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.

If the alternate image is active (due to a corruption of the primary image or manually intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate it.

The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

6.3 Save / Restore

This section describes how to save and restore the Switch configuration including reset to Factory Defaults, Save Start, Save Users, Restore Users for any maintenance needs.

6.3.1 Factory Defaults

This section describes how to reset the switch configuration to factory defaults. Any configuration files or scripts will be set to factory default values.

Restoring factory defaults can also be performed by pushing the reset button for more than 10 seconds.

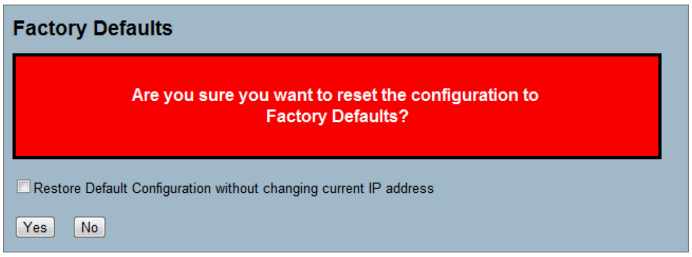
Web Interface

To reset to Factory Defaults in the web interface:

1. Click "Factory Defaults".

2. Click "Yes".

Figure 6-3.1: The Factory Defaults



Factory Defaults

Are you sure you want to reset the configuration to Factory Defaults?

□ Restore Default Configuration without changing current IP address

Parameter description:

Buttons:

Yes – Click to reset the configuration to Factory Defaults.

No – Click to return to the Port State page without resetting the configuration.

6.3.2 Save Start

This section describes how to save the Switch Start configuration.

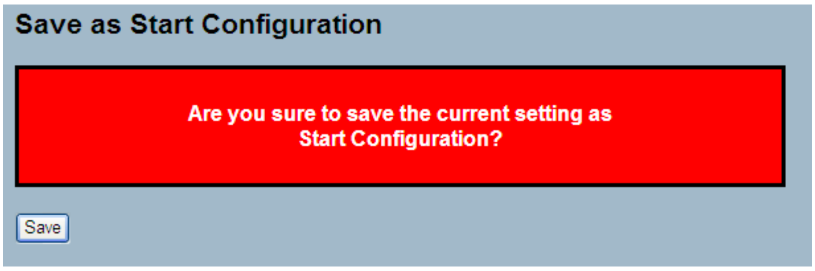
Web Interface

To save a Start Configuration via the web interface:

1. Click "Save Start".

2. Click "Yes".

Figure 6-3.2: The Save as Start configuration



Save as Start Configuration

Are you sure to save the current setting as Start Configuration?

Parameter description:

Buttons:

Save – Click to save current configuration as Start Configuration.

6.3.3 Save User

This section describes how to save users information.

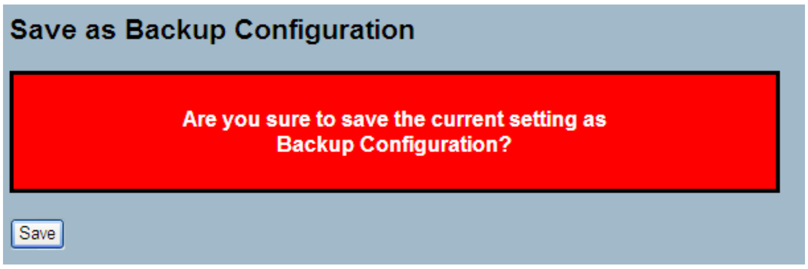
Web Interface

To save a User configuration in the web interface:

1. Click "Save User".

2. Click "Yes".

Figure 6-3.3: The Save as Backup Configuration



Save as Backup Configuration

Are you sure to save the current setting as Backup Configuration?

Parameter description:

Buttons:

Save – Click to save current settings as Backup Configuration.

6.3.4 Restore User

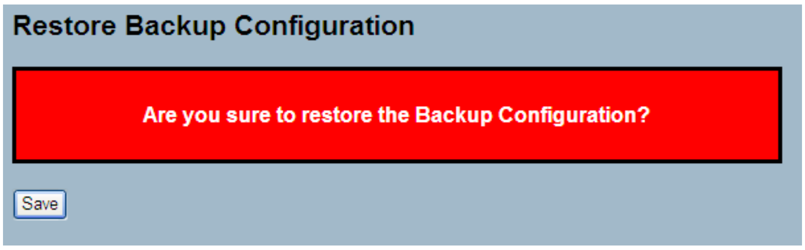
This section describes how to restore users information back to the switch.

Web Interface

To restore a User configuration in the web interface:

1. Click "Restore User".
2. Click "Yes".

Figure 6-3.4: Restore the Backup Configuration



Restore Backup Configuration

Are you sure to restore the Backup Configuration?

Parameter description:

Buttons:

Save – Click to restore the Backup Configuration to the switch.

6.4 Export / Import

This section describes how to export and import the Switch configuration. Any current configuration file will be exported in XML format.

6.4.1 Export Config

This section describes how to export the Switch Configuration for maintenance needs. Any current configuration file will be exported in XML format.

Web Interface

To export a configuration through the web interface:

1. Click "Save configuration".
2. Save the file to your device.