

3 Configuration

This IP is used to monitor the sFlow samples sent by sFlow Agent(our switch).

By default, The IP is set to 0.0.0.0,and a new entry has to be added to it.

Port:

A port to listen to the sFlow Agent has to be configured for the Collector.

The value of the port number has to be typed into the text box.

The value accepted is within the range of 1-65535. But an appropriate port number not used by other protocols need to be configured. By default, the port's number is 6343

Time out:

It is the duration during which the collector receives samples, Once it is expired the sampler stops sending the samples. It is through the management the value is set before it expires. The value accepted is within the range of 0-2147483647. By default it is set to 0.

Datagram Size:

It is the maximum UDP datagram size to send out the sFlow samples to the receiver. The value accepted is within the range of 200-1500 bytes. The default is 1400 bytes.

Buttons:

Save – Click to save changes.

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

3.16.2 Sampler

This section shows how to configure the sFlow sampler to suit specific requirements. An average of 1 out of N packets/operations is randomly sampled, which results not in a 100% accurate result, but in a rather accurate approximation with quantifiable accuracy.

Web Interface

To configure the sFlow Agent in the web interface:














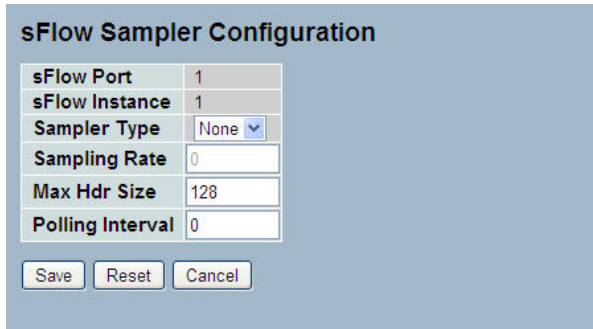
1. Click Configuration, sFlow Agent, sampler
2. Click the  to edit the sFlow sampler parameters
3. Scroll to Sample Type to choice with None, Tx, Rx or All.
4. Click Apply to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

Figure 3-16.2: The sFlow Sampler Configuration (GS-2310P)

sFlow Sampler Configuration						
sFlow Ports	sFlow Instance	Flow Sampling			Counter Sampling	
		Sampler Type	Sampling Rate	Max Hdr Size	Polling Interval	
1	1	None	0	128	0	
2	1	None	0	128	0	
3	1	None	0	128	0	
4	1	None	0	128	0	
5	1	None	0	128	0	
6	1	None	0	128	0	
7	1	None	0	128	0	
8	1	None	0	128	0	
9A	1	None	0	128	0	
10A	1	None	0	128	0	
9B	1	None	0	128	0	
10B	1	None	0	128	0	



The image shows a configuration window titled "sFlow Sampler Configuration". It contains a table of settings and three buttons at the bottom.

sFlow Port	1
sFlow Instance	1
Sampler Type	None
Sampling Rate	0
Max Hdr Size	128
Polling Interval	0

Buttons: Save, Reset, Cancel

Parameter description:

sFlow Ports:

List of the port numbers on which sFlow is configured.

sFlow Instance:

Configured sFlow instance for the port number.

Sampler Type:

Configured sampler type on the port and could be any of the types: None, Rx, Tx or All. You can scroll to choice one for your sampler type.

By default, The value is "None".

Sampling Rate:

Configured sampling rate on the ports.

Max Hdr Size:

Configured size of the header of the sampled frame.

Polling Interval:

Configured polling interval for the counter sampling.

Buttons:

• - Edits the Data source sampler configuration.

Save – Click to save changes.

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

Cancel - Click to cancel your changes.

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh:

Refresh the sFlow Sampler information manually.

3.17 Loop Protection

The loop Protection is used to detect the presence of traffic. When the switch receives packets (looping detection frame) with a MAC address equal to its own, the Loop Protection will take action. The port will be locked when it receives the looping Protection frames.

3.17.1 Configuration

The section describes how to configure Loop Protection.

Web Interface

To configure the Loop Protection parameters in the web interface:

1. Click Configuration, Loop Protection, Configuration
2. Activate to select enable or disable the port loop Protection.
3. Click Apply to save the setting
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

Figure 3-17.1: The Loop Protection Configuration (GS-2310P)

Global Configuration			
Enable Loop Protection	Disable ▾		
Transmission Time	5	seconds	
Shutdown Time	180	seconds	

Port Configuration			
Port	Enable	Action	Tx Mode
*	<input type="checkbox"/>	<> ▾	<> ▾
1	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
2	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
3	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
4	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
5	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
6	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
7	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
8	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
9A	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
10A	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
9B	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
10B	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾

Apply Reset

Parameter description:

General Settings:

Enable Loop Protection:

Controls whether loop protections is enabled (as a whole).

Transmission Time:

The interval between each loop protection PDU sent on each port. valid values are 1 to 10 seconds.

Shutdown Time:

The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).

Port Configuration:

Port:

The switch port number of the port

Enable:

Controls whether loop protection is enabled on this switch port.

Action:

Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log or Log Only.

TX Mode:

Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

Buttons:

Save – Click to save changes.

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

3.17.2 Status

This page displays the loop protection port status of the ports of the currently selected switch

Web Interface

To configure the Loop Protection parameters in the web interface:

1. Click Configuration, Loop Protection, Status
2. Activate the Auto-refresh or click to refresh the Loop protection Port status manually.

Figure 3-17.2: The Loop Protection Status (GS-2310P)

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Up	-	-
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9A	Shutdown	Enabled	0	Down	-	-
10A	Shutdown	Enabled	0	Down	-	-
9B	Shutdown	Enabled	0	Down	-	-
10B	Shutdown	Enabled	0	Down	-	-

Parameter description:

Port:

The switch port number of the logical port.

Action:

The currently configured port action.

Transmit:

The currently configured port transmit mode.

Loops:

The number of loops detected on this port.

Status:

The current loop protection status of the port.

3 Configuration

Loop:

Whether a loop is currently detected on the port.

Time of Last Loop:

The time of the last loop event detected.

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh:

Refresh the Loop Protection information manually.

3.18 Single IP

Single IP Management (SIM) is a simple and useful method to optimize network utilities and management. It is designed to manage a group of switches as a single entity by employing a virtual stacking structure. With SIM you have the following advantages:

- Simplify management of small workgroups or wiring closets while scaling networks to handle increased bandwidth demand.
- Reduce the number of IP addresses needed on the network.
- Eliminate any specialized cables for stacking and remove the distance barriers that typically limit topology options when using other stacking technology.

Each single IP group consists of one master switch and up to 32 slave switches. The master switch is used as an agent to manage all switches in the group. The slave switch joins a group and can be accessed from the master switch.

3.18.1 Configuration

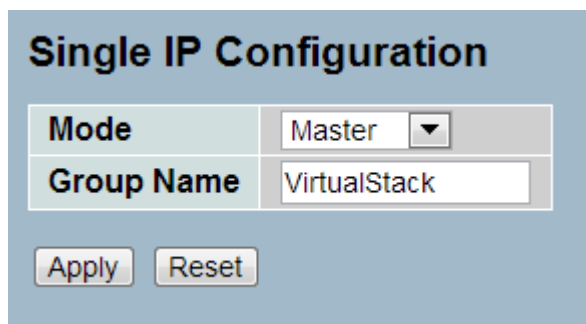
Web Interface

To configure the single IP in the web interface:

1. Click Configuration, Single IP, Configuration
2. Choose the mode of the switch
3. Set a group name
4. Click Apply to save the settings

If you want to cancel the setting you need to click the reset button. It will revert to previously saved values.

Figure 3-18.1: The Single IP Configuration



Single IP Configuration	
Mode	Master ▼
Group Name	VirtualStack
Apply Reset	

Parameter description:

Mode: The role of the switch in the group (Disabled/Master/Slave).

Group Name: The name of the group. The maximum length is 64 characters.

Buttons:

Apply – Apply changes.

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

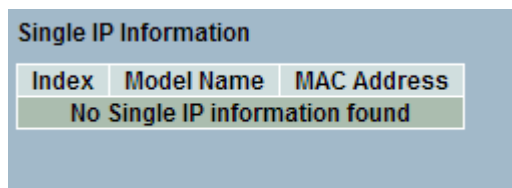
3.18.2 Information

Web Interface

To display the active slave information in the web interface:

1. Click Configuration, Single IP, Information
2. Click Refresh to update the single IP information manually or enable auto-refresh

Figure 3-18.2: The Single IP Information



Index	Model Name	MAC Address
No Single IP information found		

Parameter description:

Index: The ID of the active slave switch.

Model Name: The Model name of the slave switch.

MAC Address: The MAC address of the slave switch.

Buttons:

Refresh – Refresh the single IP information.

Auto-refresh – Automatically refresh the single IP information at regular intervals.

3.19 Easy Port

Easy Port provides a convenient way to save and share common configurations. You can use it to enable features and settings based on the location of a switch in the network and for mass configuration deployments across the network. You could easily implement included Voice IP phone, Wireless Access Point and IP Camera...etc. Others you can leverage configuration to run a converged voice, video, and data network considering quality of service (QoS), bandwidth, latency, and high performance.

Web Interface

To configure the Easy Port in the web interface:

1. Click Configuration, Easy Port.
2. Set the parameters
3. Scroll to Role for what kind device you want to set on the Easy Port and connect to.
4. Click Apply to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

Figure 3-19.1: The Easy Port Configuration

3 Configuration

Port Members													
1	2	3	4	5	6	7	8	9	10	11	12	13	14
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Role: IP-Phone

Access VLAN	1
VLAN Mode	Hybrid
Voice VLAN	1000
Traffic Class	7(High)
Port Security	Enable
Port Security Action	Trap
Port Security Limit	1
Spanning Tree Admin Edge	Enable
Spanning Tree BPDU Guard	Enable

Apply Reset

Parameter description:

Port Members:

To activate which Port wants to enable the Easy Port function.

Role:

To scroll to select what kind device you want to connect and implement with the Easy Port setting.

Access VLAN:

To set the Access VLAN ID, it means the switch port access VLAN ID (AVID).

VLAN Mode:

To scroll to select the VLAN mode with Access, Trunk or Hybrid.

Voice VLAN:

If you connect the IP Phone you need to assign the Voice VLAN ID.

The value of the port number has to be typed into the text box.

Traffic Class:

To scroll to select the traffic class for the data stream priority. The available value from 0 (Low) to 7 (High). If you want the voice has high priority then you can set the value with 7.

Port Security:

To scroll to enable or disable the Port Security function on the Port. If you turn on the function then you need to set Port Security limit to allow how many device can access the port (via MAC address).

Port Security Action:

To scroll to select when the device wasn't allow to access then switch action as trap, shutdown or trap & shutdown.

Port Security limit:

To set the Port security limit, the default is 1.

Port Security limit:

To set the Port security limit (It means you can set how many device MAC address will allow to access the port), the default is 1.

Spanning Tree Admin Edge:

To scroll to enable or disable the Spanning Tree Admin Edge function on the Easy Port.

Spanning Tree BPDU Guard:

To scroll to enable or disable the Spanning Tree BPDU Guard function on the Easy Port.

Buttons:

Save – Click to save changes.

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

3.20 Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Mirror Configuration is used to monitor the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring.

Web Interface

To configure the Mirror in the web interface:

1. Click Configuration, Mirroring
2. Select Port to mirror on which port
3. Scroll to disabled, enable, TX Only and RX Only to set the Port mirror mode
4. Click Apply to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

Figure 3-20.1: The Mirror Configuration (GS-2310P)

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

Parameter description:

Port to mirror on:

Port to mirror also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. Disabled disables mirroring.

Mirror Port Configuration

The following table is used for Rx and Tx enabling.

Port:

3 Configuration

The logical port for the settings contained in the same row.

Mode:


Select mirror mode.

Rx only Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.

Tx only Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.

Disabled Neither frames transmitted nor frames received are mirrored.

Enabled Frames received and frames transmitted are mirrored on the mirror port.

 For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames on the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

Buttons:

Save – Click to save changes.

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

3.21 Trap Event Severity

The function is used to send an Alarm trap and get the Event log. The Trap Events Configuration function is used to enable the switch to send out the trap information when pre-defined trap events occur.

Web Interface

To configure the Trap Event Severity in the web interface:

1. Click Configuration, Trap Event Severity Configuration
2. Select the Group name and Severity Level
3. Click Apply to save the setting
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

Figure 3-21.1: The Trap Event Severity Configuration

Group Name	Severity Level
ACL	Info
ACL Log	Debug
Access Mgmt	Info
Auth Failed	Warning
Cold Start	Warning
Config Info	Info
Firmware Upgrade	Info
Import Export	Info
LACP	Info
Link Status	Warning
Login	Info
Logout	Info
Mgmt IP Change	Info
Module Change	Notice
NAS	Info
Passwd Change	Info
Port Security	Info
Thermal Protect	Info
VLAN	Info
Warm Start	Warning

Save Reset

Parameter description:

Group Name:

The field describe the Trap Event definition.

Severity Level:

To scroll to select the event type with “Emerg, Alert, Crit, Error, Warning, Notice, Info and Debug”.

Buttons:

Save – Click to save changes.

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

3.22 SMTP Configuration

The function, is used to set a Alarm trap when the switch alarm then you could set the SMTP server to send you the alarm mail.

Web Interface

To configure the SMTP in the web interface:

1. Click Configuration, SMTP Configuration
2. Select the Severity Level
3. Specify the parameters in each blank field.
4. Click Apply to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

Figure 3-22.1: The SMTP Configuration

SMTP Configuration	
Mail Server	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Serverity Level	Info <input type="button" value="v"/>
Sender	<input type="text"/>
Return Path	<input type="text"/>
Email Address 1	<input type="text"/>
Email Address 2	<input type="text"/>
Email Address 3	<input type="text"/>
Email Address 4	<input type="text"/>
Email Address 5	<input type="text"/>
Email Address 6	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

Parameter description:

These parameters are displayed on the SMTP Configuration page:

Mail Server:

Specify the IP Address of the server transferring your email.

Username:

Specify the username on the mail server.

Password:

Specify the password on the mail server.

Sender:

To set the mail sender name.

Return-Path:

To set the mail return-path as sender mail address.

Email Address 1-6:

Email address that would like to receive the alarm message.

Buttons:

Save – Click to save changes.

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

3.23 UPnP

UPnP is an acronym for Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components

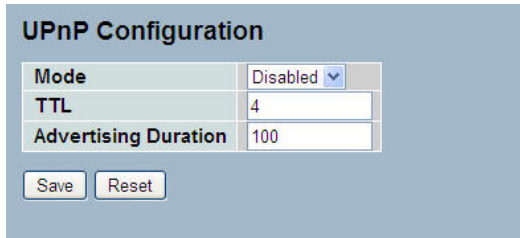
Web Interface

To configure the UPnP in the web interface:

1. Click Configuration, UPnP

2. Select the mode to enable or disable
3. Specify the parameters in each blank field.
4. Click Apply to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

Figure 3-23.1: The UPnP Configuration



UPnP Configuration	
Mode	Disabled ▾
TTL	4
Advertising Duration	100

Save Reset

Parameter description:

These parameters are displayed on the UPnP Configuration page:

Mode:

Indicates the UPnP operation mode. Possible modes are:

Enabled: Enable UPnP mode operation.

Disabled: Disable UPnP mode operation.

When the mode is enabled, two ACEs are added automatically to trap UPnP related packets to CPU. The ACEs are automatically removed when the mode is disabled.

TTL:

The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255.

Advertising Duration:

The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.

Buttons:

Save – Click to save changes.

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

4 System Configuration

This chapter describes the entire basic configuration tasks which includes the System Information and any managing of the switch (e.g. time, account, IP, syslog and SNMP).

4.1 System Information

After you login, the switch shows you the system information. This page tells you the basic information of the system, including "Model Name", "System Description", "Contact", "Device Name", "System Up Time", "BIOS Version", "Firmware Version", "Hardware-Mechanical Version", "Serial Number", "Host IP Address", "Host Mac Address", "Device Port", "RAM Size", and "Flash Size".

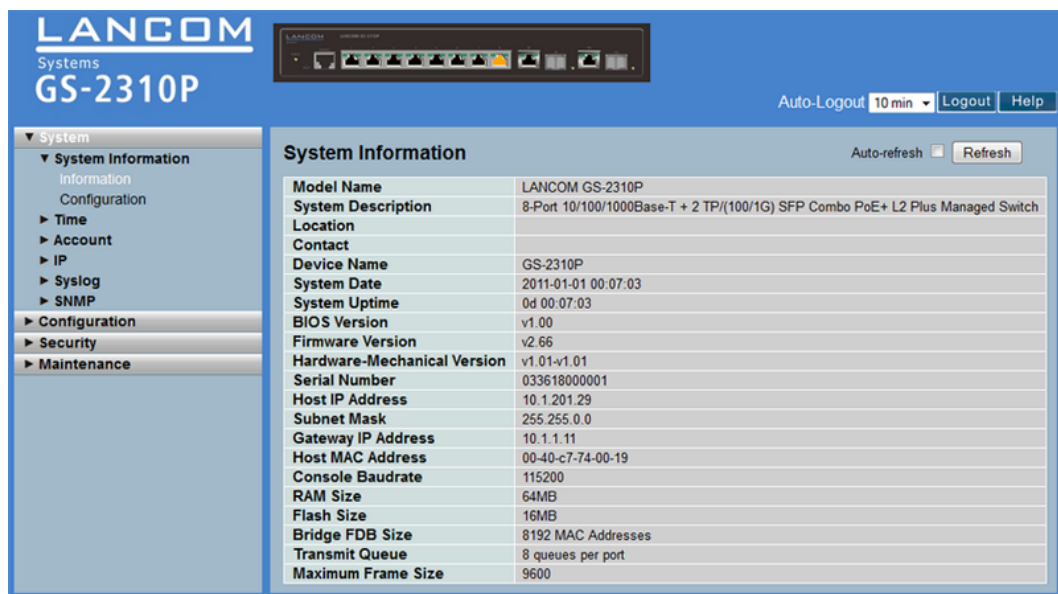
4.1.1 Information

The switch system information is provided here.

To access the System Information in the web interface:

1. Click SYSTEM, System, and Information.
2. Specify the contact information for the system administrator as well as the name and location of the switch. Also indicate the local time zone by configuring the appropriate offset.
3. Click Refresh

Figure 4-1.1: System Information (GS-2310P)



The screenshot shows the LANCOM GS-2310P web interface. The top navigation bar includes the LANCOM logo, the model name 'GS-2310P', and an 'Auto-Logout' timer set to 10 minutes. A sidebar on the left contains a menu with options like System Information, Time, Account, IP, Syslog, SNMP, Configuration, Security, and Maintenance. The main content area is titled 'System Information' and contains a table of system parameters.

Parameter	Value
Model Name	LANCOM GS-2310P
System Description	8-Port 10/100/1000Base-T + 2 TP/(100/1G) SFP Combo PoE+ L2 Plus Managed Switch
Location	
Contact	
Device Name	GS-2310P
System Date	2011-01-01 00:07:03
System Uptime	0d 00:07:03
BIOS Version	v1.00
Firmware Version	v2.66
Hardware-Mechanical Version	v1.01-v1.01
Serial Number	033618000001
Host IP Address	10.1.201.29
Subnet Mask	255.255.0.0
Gateway IP Address	10.1.1.11
Host MAC Address	00-40-c7-74-00-19
Console Baudrate	115200
RAM Size	64MB
Flash Size	16MB
Bridge FDB Size	8192 MAC Addresses
Transmit Queue	8 queues per port
Maximum Frame Size	9600

Parameter description:

Model name:

The model name of this device.

System description:

The description of the device. In this case: "44-Port 10/100/1000Base-T + 4 (100/1G) SFP Combo + 4 (1G/10G) SFP+ PoE+ L2 Plus Managed Switch".

Location:

The physical location of the switch. User-defined.

Contact:

For easy managing and maintenance of the device, you may enter the name of a contact person and a phone number here. You can configure this parameter through the device's user interface or SNMP.

Device name:

The name of the switch. User-defined.

System Date:

Shows the system time of the switch. Its format: day of week, month, day, hours: minutes: seconds, year.

System up time:

The time accumulated since this switch has been powered up. Its format is day, hour, minute, second.

BIOS version:

The version of the BIOS in the switch.

Firmware version:

The firmware version in the switch.

Hardware-Mechanical version:

The version of the electronic and the mechanical hardware. The figure before the hyphen shows the version of electronic hardware; the one after the hyphen show the version of mechanical hardware.

Serial number:

The serial number of the switch.

Host IP address:

The IP address of the switch.

Host MAC address:

The ethernet MAC address of the management agent in the switch.

Device Port:

Shows all types and numbers of the port in the switch.

RAM size:

The size of the RAM in the switch.

Flash size:

The size of the flash memory in the switch.

Bridge FDB size:

Displays the bridge FDB size information.

Transmit Queue:

Displays the transmit hardware priority queue information.

Maximum Frame size:

Displays the maximum frame size information.

4.1.2 Configuration

You can identify the system by configuring the contact information, name, and location of the switch.

Web interface

To configure the System Information in the web interface:

1. Click System, System Information, Configuration.
2. Enter System Contact, System Name, System Location.
3. Click Apply

Figure 4-1.2: System Information configuration



System Information Configuration	
System Contact	<input type="text"/>
System Name	GEP0EL2-ESW52KX
System Location	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

Parameter description:

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 the allowed content is the ASCII characters from 32 to 126.

System Name:

An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a 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 Location:

The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

4.1.3 CPU Load (GS-2326(P) only)

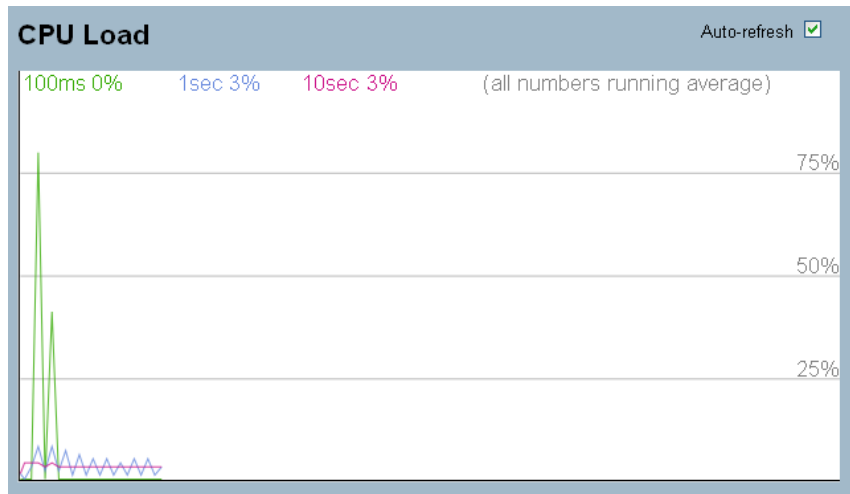
This page displays the CPU load, using an SVG graph. The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well. In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.

Web interface

To configure System Information in the web interface:

1. Click System, System Information, CPU Load.
2. Display the CPU Load on the screen
3. Click Auto-refresh.

Figure 4-1.3: CPU Load



Parameter description:

Auto-refresh

Activate the auto-refresh to refresh the log automatically.

4.2 Time

This page configures the switch's time. Local Time Configuration and NTP Configuration is supported.

4.2.1 Manual

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple and you just enter "Year", "Month", "Day", "Hour", "Minute" and "Second" within the valid value range indicated in each item.

Web Interface

To configure Time in the web interface:

1. Click Time, Manual.
2. Specify the time parameters.
3. Click Apply.

Figure 4-2.1: The time configuration

4 System Configuration

Time Configuration	
Clock Source:	<input checked="" type="radio"/> Use Local Settings <input type="radio"/> Use NTP Server
Local Time:	2011-01-01 00:10:20 YYYY-MM-DD HH:MM:SS
Time Zone Offset:	0 min
Daylight Savings	<input type="checkbox"/> Enable
Time Set Offset:	60 min. (Range: 1 - 1440, Default: 60)
Daylight Savings Type:	<input type="radio"/> By dates <input type="radio"/> Recurring
From:	YYYY-MM-DD HH:MM
To:	YYYY-MM-DD HH:MM
From:	Day: Sun Week: First Month: Jan Time: 00:00 HH:MM
To:	Day: Sun Week: First Month: Jan Time: 00:00 HH:MM
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

Parameter description:

Clock Source:

Select which clock source is used for the GS-2300 series. You can select "Use local Settings" or "Use NTP Server" as the switches' time clock source.

Local Time:

Shows the current time of the system.

Time Zone Offset:

Provides the time zone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes

Daylight Saving:

Daylight saving is adopted in some countries. If set, it will adjust the time according to the starting date and the ending date by the given amount. For example, you set the day light saving to be 1 hour. When the time passes over the starting time, the system time will be increased by one hour after one minute. When the time passes over the ending time, the system time will be decreased one hour after one minute.

The switch supports a configurable day light saving time offset of up to 24 hours. The zero for this parameter means it need not have to adjust current time, equivalent to in-act daylight saving. If you set daylight saving to be non-zero, you have to set the starting/ending date as well; otherwise, the daylight saving function will not be activated.

Time Set Offset:

Provide the Daylight saving time set offset. The offset is given in minutes east of GMT. The valid range is from 1 to 1440 minutes. default is 60 min

Daylight Savings Type:

Provide the Daylight savings type selection. You can select " By Dates" or "Recurring" two type for Daylight saving type.

From:

To configure Daylight saving start date and time, the format is "YYYY-MM-DD HH:MM".

To:

To configure Daylight saving end date and time, the format is "YYYY-MM-DD HH:MM".

4.2.2 NTP

NTP, the Network Time Protocol is used to sync the network time based on Greenwich Mean Time (GMT). You can use the built-in NTP time server or manually specify a user-defined NTP server as well as a Time Zone, the switch will sync the time shortly after pressing the <Apply> button. Though it synchronizes the time automatically, NTP does not update the time periodically without user's processing.

The Time Zone is an offset time off GMT. You have to select the time zone first and then perform time sync via NTP because the switch will combine the time zone offset and updated NTP time to provide the local time, otherwise, you will not able to get the correct time. The switch supports configurable time zone from -12 to +13 hours in steps of 1 hour.

Default Time zone: +8 Hrs.

Web Interface

To configure NTP in the web interface:

1. Click SYSTEM, NTP.
2. Specify the NTP parameters.
3. Click Apply.

Figure 4-2.2: The NTP configuration

NTP Configuration	
Server 1	<input type="text"/>
Server 2	<input type="text"/>
Server 3	<input type="text"/>
Server 4	<input type="text"/>
Server 5	<input type="text"/>

Save Reset

Parameter description:

Server 1 to 5:

The NTP's IPv4 or IPv6 address. The IPv6 address in 128-bit records is 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'.

Buttons

Save – Click to save changes.

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

4.3 Account

Only administrators can create, modify or delete usernames and passwords. Administrators can modify other guest identities' password without confirming the password except it is necessary to modify an administrator-equivalent identity. Guest-equivalent identities can modify their passwords only. Please note that you must select administrator/guest identity in the field of Authorization in advance before configuring the username and password. The number of administrator and guest accounts that you can create is not limited.

4.3.1 Users

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.

Web Interface

To configure accounts in the web interface:

Click SYSTEM, Account, Users.

Click Add new user

Specify the User Name parameter.

Click Apply.

Figure 4-3.1: The Users Account configuration

The screenshot shows two parts of the web interface. The top part is titled 'Users Configuration' and contains a table with two columns: 'User Name' and 'Privilege Level'. The table has one row with 'admin' in the 'User Name' column and '15' in the 'Privilege Level' column. Below the table is a button labeled 'Add new user'. The bottom part is titled 'Add User' and contains a form with the following fields: 'User Name' (text input), 'Password' (text input), 'Password (again)' (text input), and 'Privilege Level' (dropdown menu with '1' selected). At the bottom of the form are three buttons: 'Save', 'Reset', and 'Cancel'.

Parameter description:

User Name:

The name identifying the user. The allowed string length is 1 to 32. A valid user name consists of letters, numbers and underscores. This parameter is also a link to Add/Edit User.

Password

The password associated with the account. The allowed string length is 0 to 32, and the allowed content is the ASCII characters from 32 to 126.

Password (again)

You must type the same password again in this field.

Privilege Level:

The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, he can access all groups, i.e. he is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default settings, most groups with privilege level 5 have the read-only access and with privilege level 10 have the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.