D-Link®
Building Networks for People

Web UI Reference Guide

Product Model: DXS-3600-32S
Layer 2/3 Managed 10GbE Switch
Release 1.00

December, 2011. P/N 651XS3632010G

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operating in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his expense.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Warnung!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

VCCI Warning

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。VCCI-A

Intended Readers

The **DXS-3600-32S Web UI Reference Guide** contains detailed information about the Web User Interface of the switch in this series. This manual is intended for advanced level users that are familiar with network management concepts and terminology. For all practical reasons the **DXS-3600-32S** will simply be referred to as the **switch** throughout this manual.

Typographical Conventions

Convention	Description
[ ]	This convention is generally used in CLI commands. Square brackets indicate an optional entry. For example: [copy | paste] means that optionally you can type copy or you can type paste. Do not type the brackets.
Bold Font	This font is generally used to put emphasis on a key subject in a sentence throughout this manual. This font is also used to represent the physical CLI command used when explaining a topic.
`Boldface Typewriter Font`	This font is used to indicate CLI command examples used in this document.
Initial capital letter	The use of initial capital letters indicates that a referral to a specific name was made. This will be seen a lot when referring to protocols, standards, keyboard keys, and when we refer to the ‘Switch’ as a generic name for all switches with in the series. For example: Click Enter.
Menu Name > Menu Option	This convention indicates the referral to a menu structure found in the Web User Interface of this Switch. For example: Device > Port > Port Properties means the Port Properties menu option under the Port menu option that is located under the Device menu.

Notes, Notices, and Cautions

NOTE: A note indicates important information that helps you make better use of your device

NOTICE: A notice indicates either potential damage to hardware or loss of data and tells you how to avoid the problem

CAUTION: A caution indicates a potential for property damage, personal injury, or death.

Safety Instructions

Please pay careful attention to the following safety guidelines to ensure your own personal safety and to help protect your system from potential damage.

Safety Cautions

To greatly reduce the risk of physical injury, electrical shock, fire, and damage to equipment, observe the following precautions.

Observe and follow service markings.

- Do not attempt to service any product, except when it is explained in the system’s documentation.
- Opening or removing covers that are marked with this (⚠) symbol may expose the user to electrical shock.
- Only a trained service technician should service components inside these compartments.

If any of the following conditions occur, unplug the product from the electrical outlet immediately and replace the part or contact your trained service provider:

- Damage to the power cable, extension cable, or plug.
- An object has fallen into the product.
- The product has been exposed to water.
- The product has been dropped or damaged.
- The product does not operate correctly when the operating instructions are correctly followed.

General safety cautions:

- Keep the system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on system components, and never operate the product in a wet environment. If the system gets wet contact your trained service provider.
- Do not push any objects into the openings of the system. Doing so can cause fire or electric shock by shorting out interior components.
- Only use this product with approved equipment.
- Allow the product to cool before removing the cover or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If unsure of the type of power source required, consult your service provider or local power company.
- Be sure that attached devices are electrically rated to operate with the power available in your location.
- Use only approved power cable(s). If you have not been provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.
- To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If using an extension cable is necessary, use a 3-wire cable with properly grounded plugs.
- Observe the extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
- To help protect the system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully. Route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local or national wiring rules.

When connecting or disconnecting power to and from hot-pluggable power supplies, observe the following guidelines:

- Install the power supply before connecting the power cable to the power supply.
- Unplug the power cable before removing the power supply.
- If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
- Move products with care and ensure that all casters and stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.

To help avoid damage to the system, be sure that the voltage selection switch, on the power supply, is set to match the power available at the switch’s location:

- 115V/60Hz is used mostly in North and South America as well as Far Eastern countries like as South Korea and Taiwan
- 100V/50Hz is used mostly in Eastern Japan and 100V/60Hz in Western Japan
- 230V/50Hz is used mostly in Europe, the Middle East, Africa and the Far East

General Precautions for Rack-Mountable Products

Please pay careful attention to the following precautions concerning rack stability and safety. Systems are considered to be components in a rack. Thus, a component refers to any system, as well as to various peripherals or supporting hardware.

CAUTION: Installing systems in a rack without the front and side stabilizers installed could cause the rack to tip over, potentially resulting in serious injury. After installing system/components in a rack, never pull more than one component out of the rack on its slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and may result in serious injury.

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.
- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a component from the rack.
- Use caution when pressing the component rail release latches and sliding a component into or out of a rack; the slide rails can pinch your fingers.
- After a component is inserted into the rack, carefully extend the rail into a locking position, and then slide the component into the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Ensure that proper airflow is provided to components in the rack.
- Do not step on or stand on any component when servicing other components in a rack.

CAUTION: Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if uncertain that suitable grounding is available.

CAUTION: The system chassis must be positively grounded to the rack cabinet frame. Do not attempt to connect power to the system until grounding cables are connected. Completed power and safety ground wiring must be inspected by a qualified electrical inspector. An energy hazard will exist if the safety ground cable is omitted or disconnected.

Protecting Against Electrostatic Discharge

Static electricity can harm delicate components inside the system. To prevent static damage, discharge static electricity from your body before touching any of the electronic components, such as the microprocessor. This can be done by periodically touching an unpainted metal surface on the chassis.

The following steps can also be taken prevent damage from electrostatic discharge (ESD):

- When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until ready to install the component in the system. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
- When transporting a sensitive component, first place it in an antistatic container or packaging.
- Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads, workbench pads and an antistatic grounding strap.

Table of Contents

Web-based Switch Configuration

Management Options

This switch provides multiple access platforms that can be used to configure, manage and monitor networking features available on this switch. Currently there are three management platforms available and they are described below.

The Command Line Interface (CLI) through the Serial Port or remote Telnet

This switch can be managed, out-of-band, by using the console port on the front panel of the switch. Alternatively, the switch can also be managed, in-band, by using a Telnet connection to any of the LAN ports on this switch. The command line interface provides complete access to all switch management features.

SNMP-based Management

The switch can be managed with an SNMP-compatible console program. The switch supports SNMP version 1.0, version 2.0 and version 3.0. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

Web-based Management Interface

After successfully installing the switch, the user can configure the switch, monitor the LED panel, and display statistics graphically using a Web browser, such as Microsoft® Internet Explorer (version 5.5 and later), Mozilla Firefox (version 2.0 and later), Safari (version 4.0 and later), and Google Chrome (version 6.0 and later).

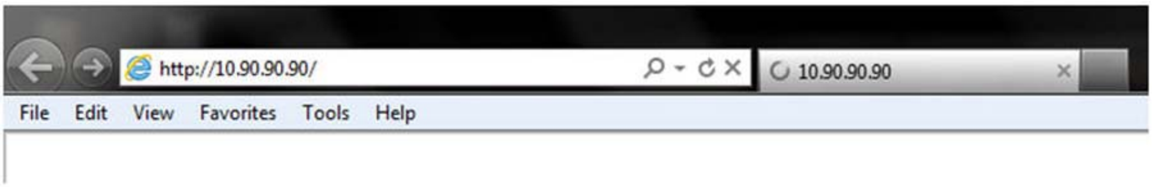
Connecting using the Web User Interface

All software functions of the switch can be managed, configured, and monitored via the embedded Web-based (HTML) interface. This can be done from any remote station on the network through a standard web browser, such as Internet Explorer (version 5.5 and later), Mozilla Firefox (version 2.0 and later), Safari (version 4.0 and later), or Google Chrome (version 6.0 and later). The browser acts as a universal access tool and can communicate directly with the switch using the HTTP protocol.

All the software features that can be configured using the Command Line Interface can also be configured using the Web User Interface. The Web User Interface is thus an alternative configuration method for the lesser analytical users.

Logging onto the Web Manager

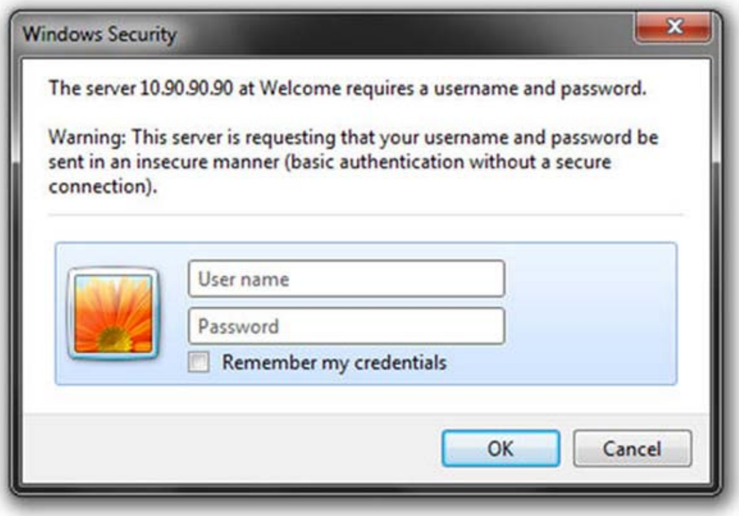
To access the Web User Interface the user simply runs the standard web browser and enter the Switch’s IP address into the address bar of the browser and press the ‘**Enter**’ key.



http://10.90.90.90/

Figure 2-1 Displays entering the IP address in Internet Explorer

This will open the user authentication window, as seen below.



Windows Security

The server 10.90.90.90 at Welcome requires a username and password.

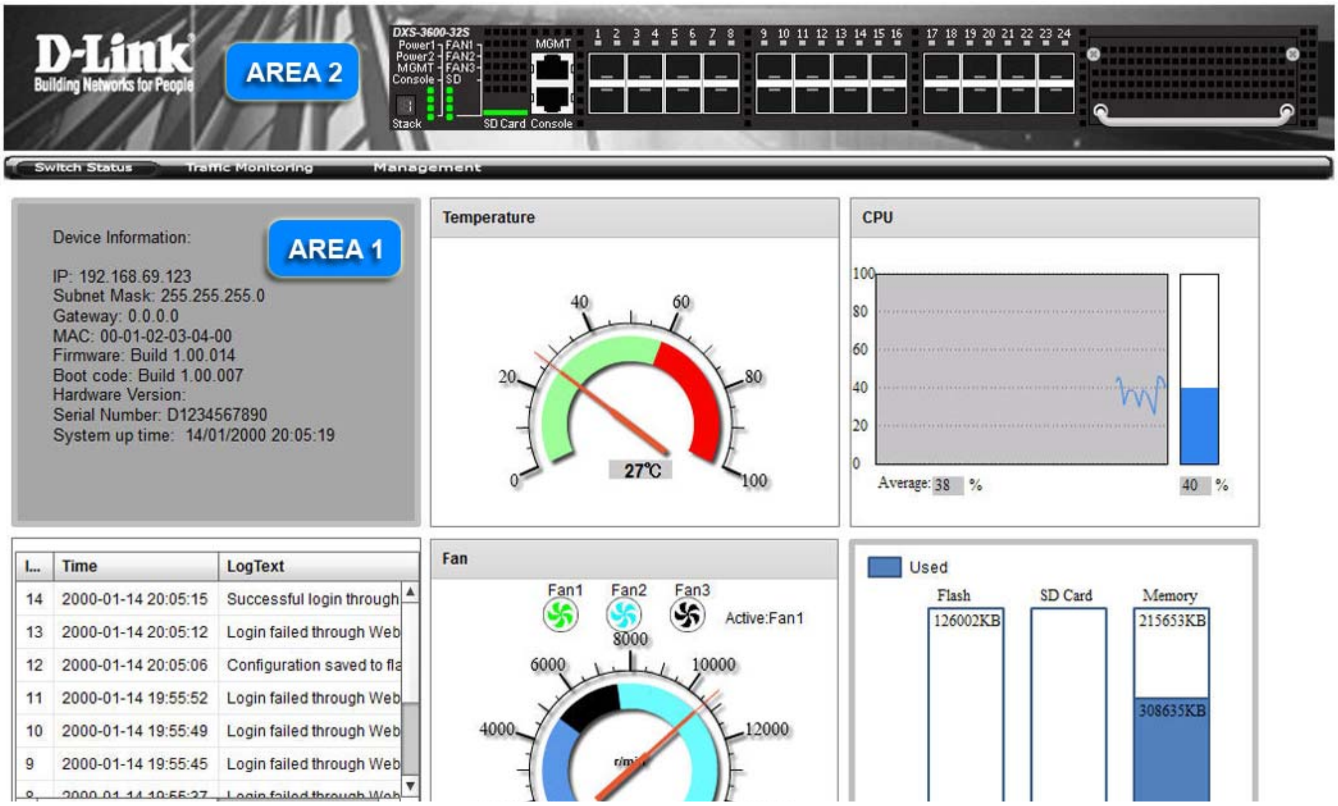
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

Figure 2-2 Enter Network Password window

As there is no default **User name** or **Password**, click **OK** to proceed. This will open the Web-based User Interface. The switch management features available in the Web-based manager are explained below.

Areas of the User Interface

After a successful connection to the Web User Interface has been made, the following page should be displayed.



Device Information:

IP: 192.168.69.123
Subnet Mask: 255.255.255.0
Gateway: 0.0.0.0
MAC: 00-01-02-03-04-00
Firmware: Build 1.00.014
Boot code: Build 1.00.007
Hardware Version:
Serial Number: D1234567890
System up time: 14/01/2000 20:05:19

I...	Time	LogText
14	2000-01-14 20:05:15	Successful login through
13	2000-01-14 20:05:12	Login failed through Web
12	2000-01-14 20:05:06	Configuration saved to fla
11	2000-01-14 19:55:52	Login failed through Web
10	2000-01-14 19:55:49	Login failed through Web
9	2000-01-14 19:55:45	Login failed through Web
8	2000-01-14 19:55:37	Login failed through Web

Figure 2-3 Main Web Manager window

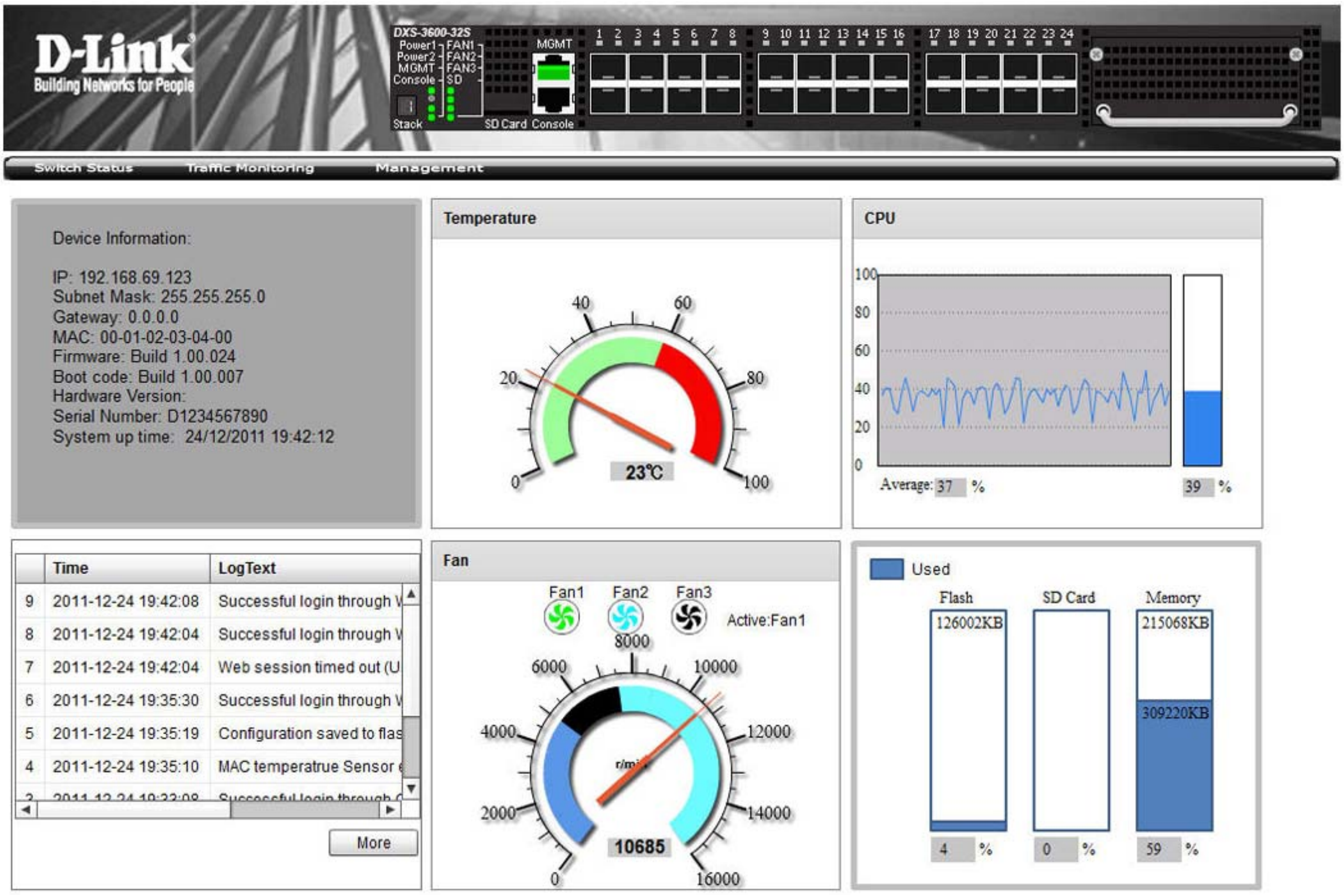
On this page we will find three main areas to observe.

Area Number	Function
AREA 1	This area displays graphical, real-time images of some of the hardware features running on this switch. Some of the features that can be monitored here are the **Device Information**, **Temperature**, **CPU Usage**, **System Log**, **Fan Status**, **Memory Usage**, and **Network Traffic Utilization**. In the **Management** window, the user can also **Download/Upload Firmware/Configuration** files to and from this switch.
AREA 2	This area displays a graphical, real-time image of the front panel of the Switch.

Switch Status

Device Information
Temperature Status
CPU Status
System Log Entries
Fan Status
Flash, SD Card, and Memory Status

After clicking on the **Switch Status** link, found in the menu, the following page will be displayed:



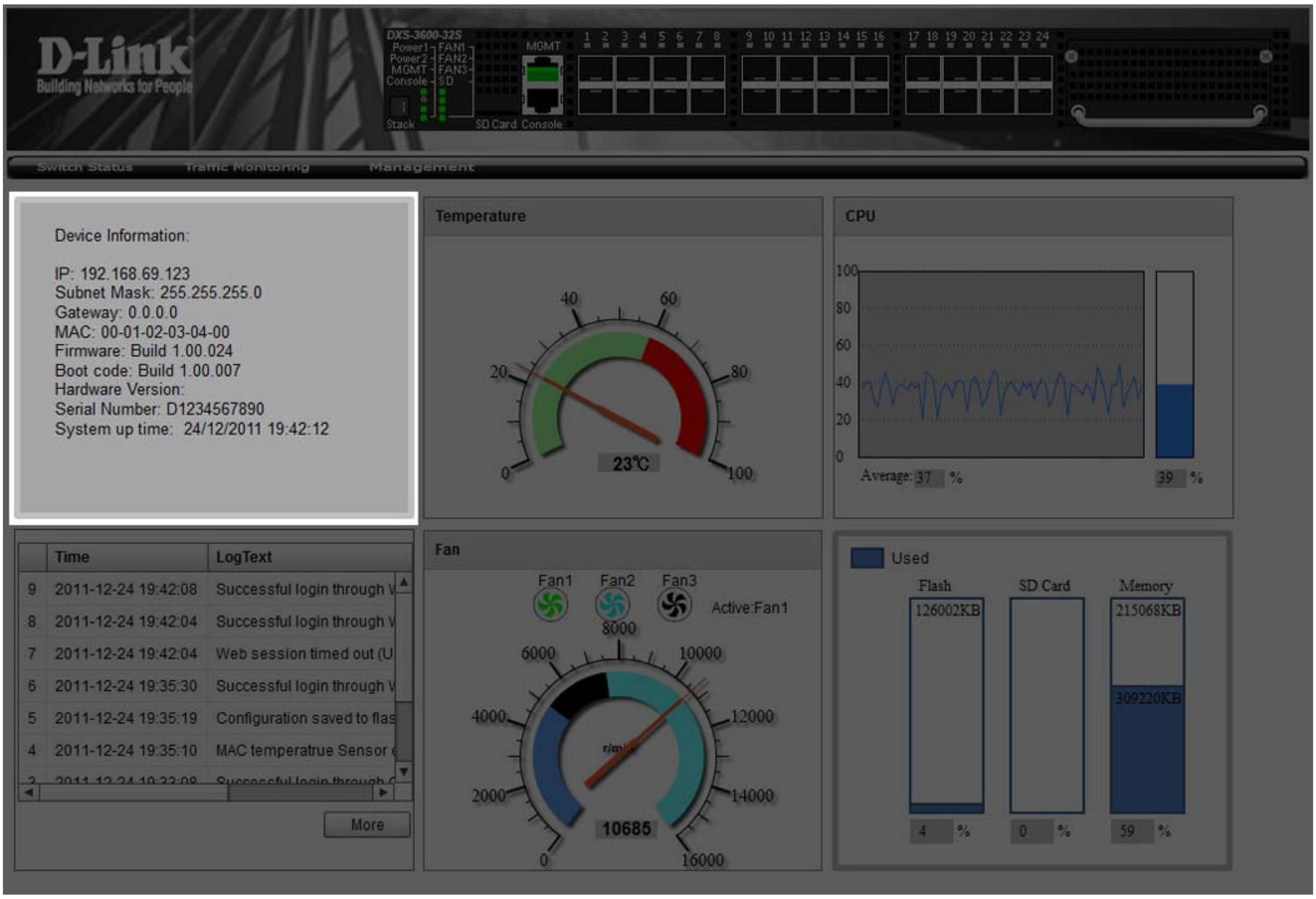
Device Information:

IP: 192.168.69.123
Subnet Mask: 255.255.255.0
Gateway: 0.0.0.0
MAC: 00-01-02-03-04-00
Firmware: Build 1.00.024
Boot code: Build 1.00.007
Hardware Version:
Serial Number: D1234567890
System up time: 24/12/2011 19:42:12

	Time	LogText
9	2011-12-24 19:42:08	Successful login through V
8	2011-12-24 19:42:04	Successful login through V
7	2011-12-24 19:42:04	Web session timed out (U
6	2011-12-24 19:35:30	Successful login through V
5	2011-12-24 19:35:19	Configuration saved to flas
4	2011-12-24 19:35:10	MAC temperatrue Sensor (
3	2011-12-24 19:33:08	Successful login through (

Device Information

In the **Device Information** section, the user can view a list of basic information regarding the switch.



Device Information:

IP: 192.168.69.123
Subnet Mask: 255.255.255.0
Gateway: 0.0.0.0
MAC: 00-01-02-03-04-00
Firmware: Build 1.00.024
Boot code: Build 1.00.007
Hardware Version:
Serial Number: D1234567890
System up time: 24/12/2011 19:42:12

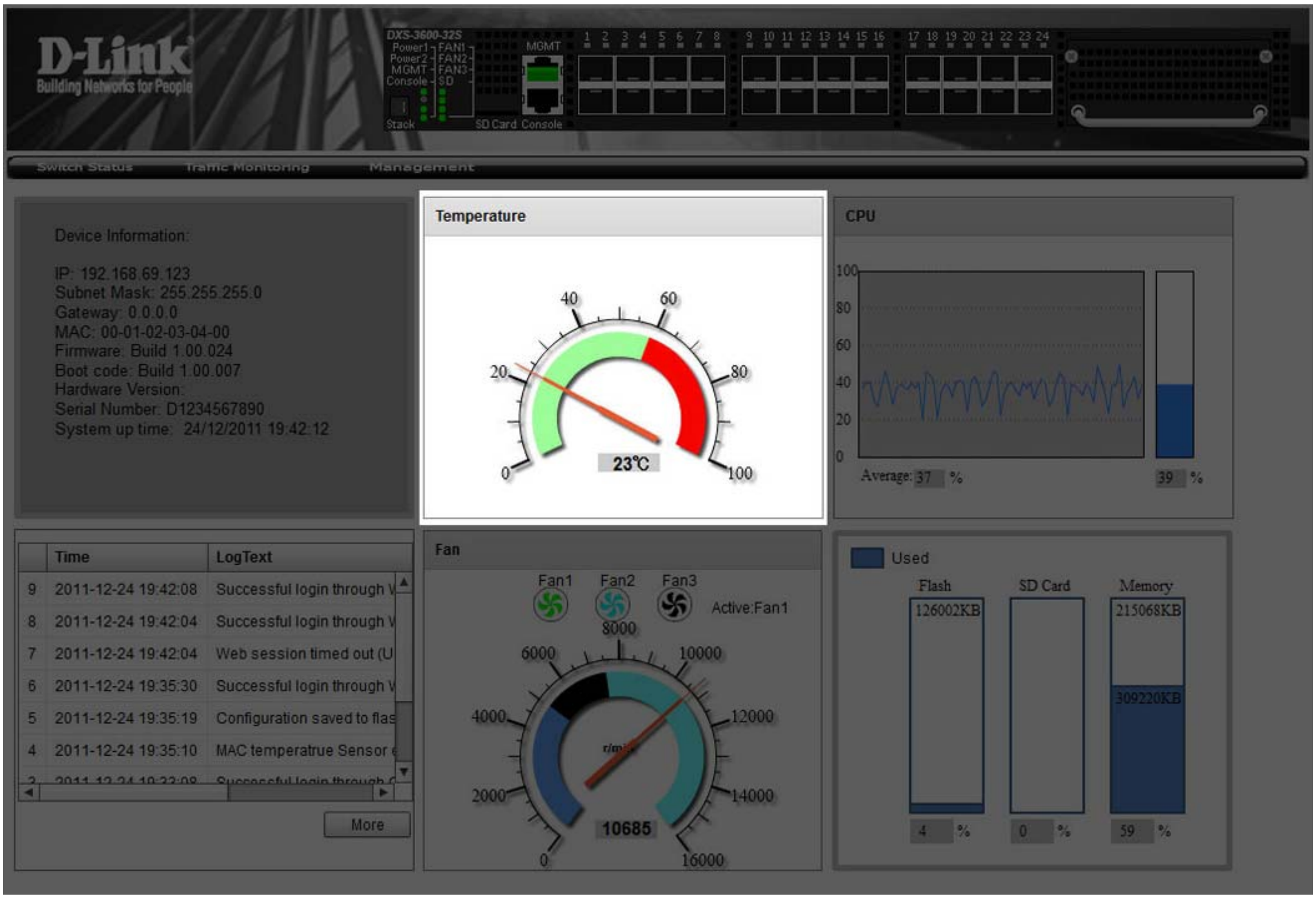
	Time	LogText
9	2011-12-24 19:42:08	Successful login through W
8	2011-12-24 19:42:04	Successful login through W
7	2011-12-24 19:42:04	Web session timed out (U
6	2011-12-24 19:35:30	Successful login through W
5	2011-12-24 19:35:19	Configuration saved to flas
4	2011-12-24 19:35:10	MAC temperatrue Sensor (

In the **Device Information** section, the following display parameters are available:

Parameter	Description
IP Address	Here the IP address of the switch's main interface is displayed.
Subnet Mask	Here the Subnet Mask of the switch's main interface is displayed.
Gateway	Here the Gateway IP address of the switch's main interface is displayed.
MAC Address	Here the MAC address of the switch is displayed.
Firmware Version	Here the Firmware version of the switch is displayed.
Boot Code Version	Here the Boot Code of the switch is displayed.
Hardware Version	Here the Hardware version of the switch is displayed.
Serial Number	Here the Serial number of the switch is displayed.
System Up Time	Here the System's up time is displayed.

Temperature Status

In the **Temperature** section, the user can view a real-time display of the switch's internal temperature. The temperature of the switch is mainly influenced by two factors: (1) the enviroment, and (2) the internal air-flow of the switch. In the **Hardware Installation Guide**, there are some guidelines the can assist the user with the installation of this switch in a temperature friendly environment. The fan modules, installed in this switch, have temperature sensors built-in, that automatically controls the air-flow inside the switch.



Device Information:

IP: 192.168.69.123
Subnet Mask: 255.255.255.0
Gateway: 0.0.0.0
MAC: 00-01-02-03-04-00
Firmware: Build 1.00.024
Boot code: Build 1.00.007
Hardware Version:
Serial Number: D1234567890
System up time: 24/12/2011 19:42:12

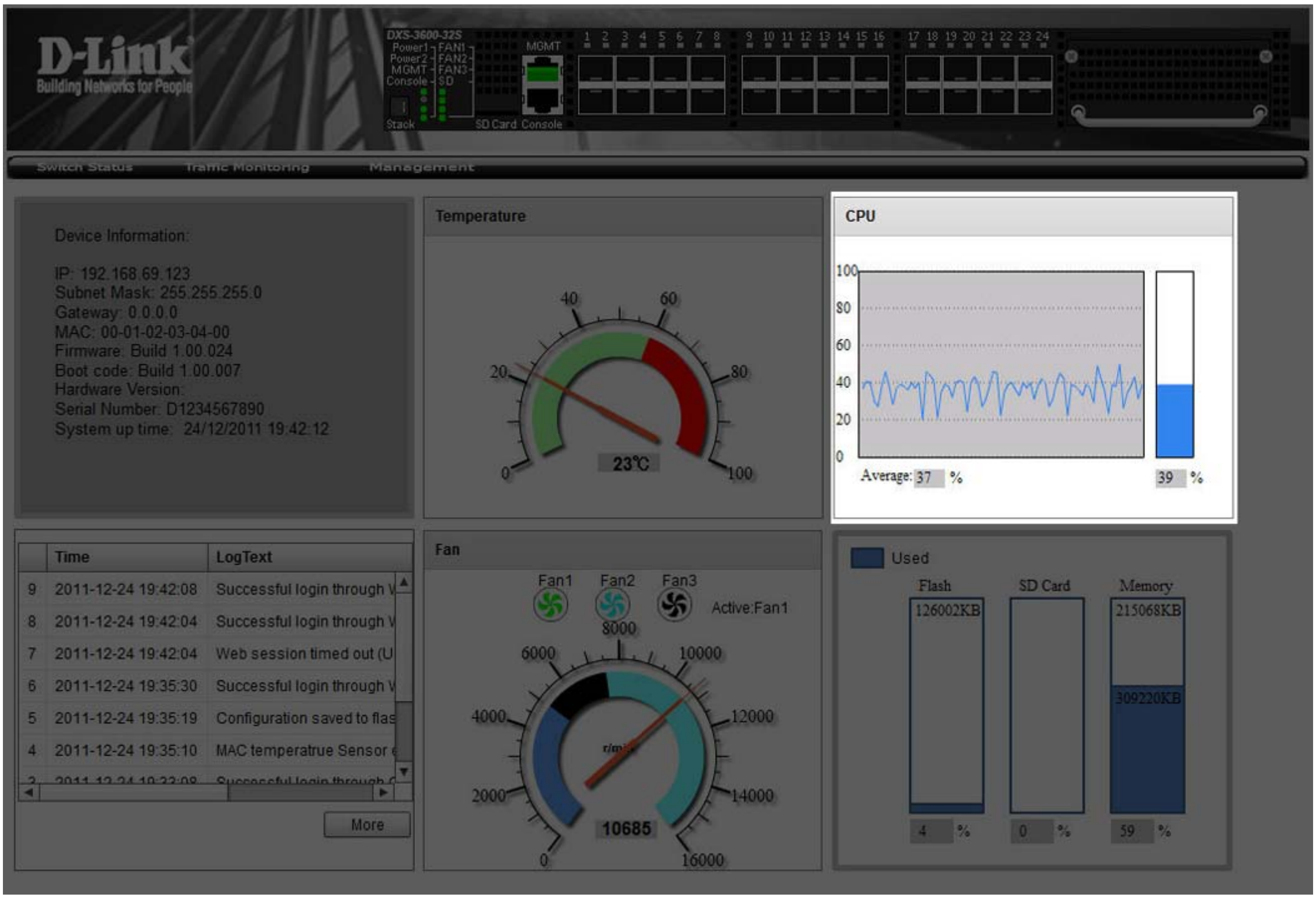
	Time	LogText
9	2011-12-24 19:42:08	Successful login through V
8	2011-12-24 19:42:04	Successful login through V
7	2011-12-24 19:42:04	Web session timed out (U
6	2011-12-24 19:35:30	Successful login through V
5	2011-12-24 19:35:19	Configuration saved to flas
4	2011-12-24 19:35:10	MAC temperatrue Sensor

In the **Temperature** section, the following display parameters are available:

Parameter	Description
Percentage Display	In this graphic, the reading is divided into percentage sections. The **green area** is known as the 'safe' area. This area ranges from 0% to 60%. This is the optimum temperature range recommended for this switch.
Temperature	Below the percentage gauge needle, the accurate temperature reading, for this switch, is displayed in degrees celsius.
Warning Section	In this graphic, the reading is divided into percentage sections. The **red area** is known as the 'warning' area. This area ranges from 60% to 100%. It is recommended not to allow the switch to run this hot, to avoid component damage.

CPU Status

In the **CPU** section, the user can view a real-time display of the switch’s CPU usage. There are a number of factors that can influance a depleted CPU usage. One of those factors are network broadcasts. In the **CLI Reference Guide** there is an abundance of features that can be enabled to prevent this problem from occuring.



Device Information:

IP: 192.168.69.123
Subnet Mask: 255.255.255.0
Gateway: 0.0.0.0
MAC: 00-01-02-03-04-00
Firmware: Build 1.00.024
Boot code: Build 1.00.007
Hardware Version:
Serial Number: D1234567890
System up time: 24/12/2011 19:42:12

	Time	LogText
9	2011-12-24 19:42:08	Successful login through W
8	2011-12-24 19:42:04	Successful login through W
7	2011-12-24 19:42:04	Web session timed out (U
6	2011-12-24 19:35:30	Successful login through W
5	2011-12-24 19:35:19	Configuration saved to flas
4	2011-12-24 19:35:10	MAC temperatrue Sensor
3	2011-12-24 19:33:08	Successful login through C

Average: 37 %

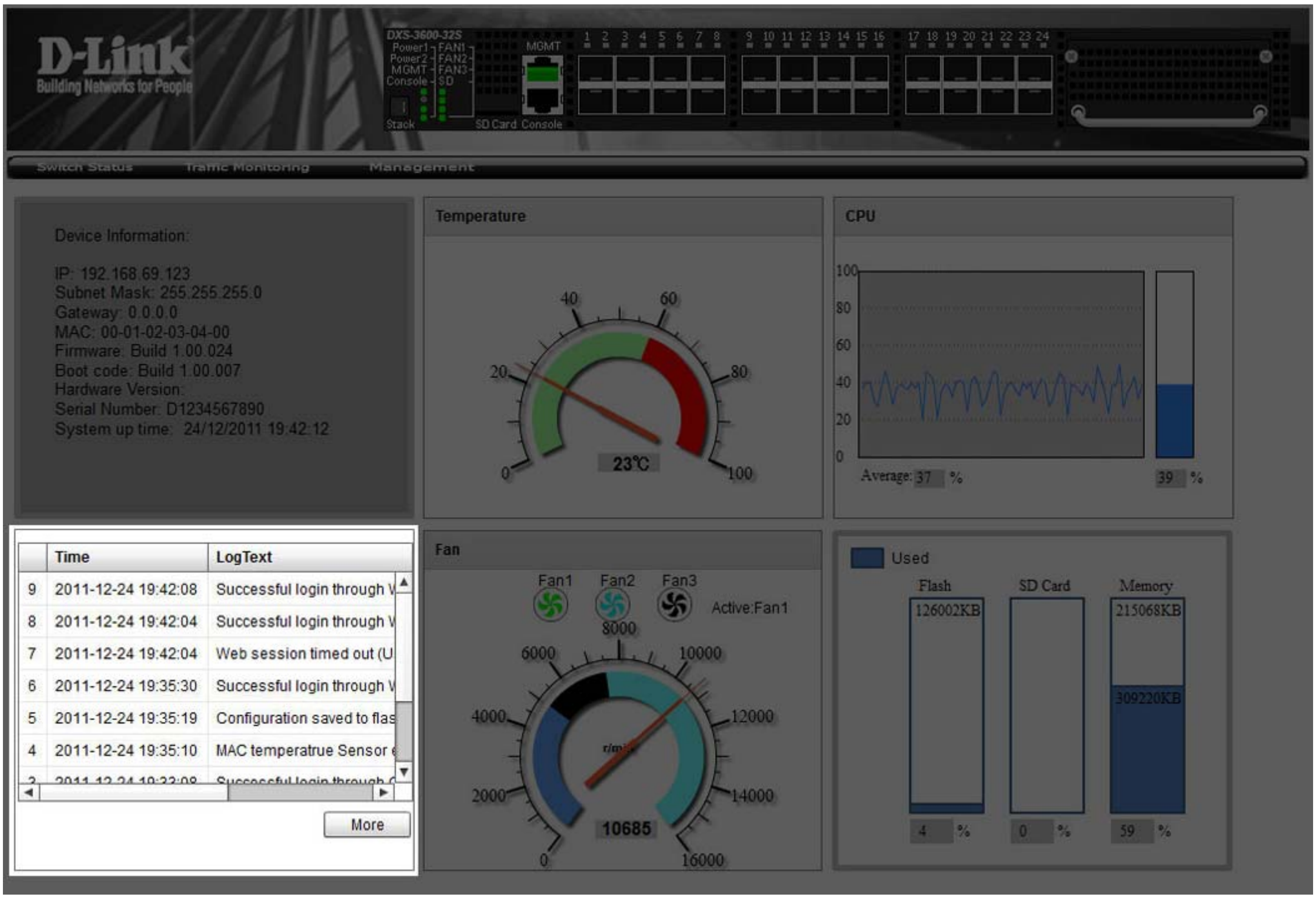
39 %

In the **CPU** section, the following display parameters are available:

Parameter	Description
Percentage Display	In this graphic, the reading is divided into percentage sections. This area ranges from 0% to 100%.
Average	Below the CPU percentage line chart, we find an accurate display of the average CPU usage percentage.
Percentage Bar	In this graphic, an accurate reading of the real-time CPU usage percentage is displayed.

System Log Entries

In the **System Log** section, the user can view a list of System log entries, generated by the switch, when certain events have occured.



Device Information:

IP: 192.168.69.123
Subnet Mask: 255.255.255.0
Gateway: 0.0.0.0
MAC: 00-01-02-03-04-00
Firmware: Build 1.00.024
Boot code: Build 1.00.007
Hardware Version:
Serial Number: D1234567890
System up time: 24/12/2011 19:42:12

	Time	LogText
9	2011-12-24 19:42:08	Successful login through W
8	2011-12-24 19:42:04	Successful login through W
7	2011-12-24 19:42:04	Web session timed out (U
6	2011-12-24 19:35:30	Successful login through W
5	2011-12-24 19:35:19	Configuration saved to flas
4	2011-12-24 19:35:10	MAC temperatrue Sensor e

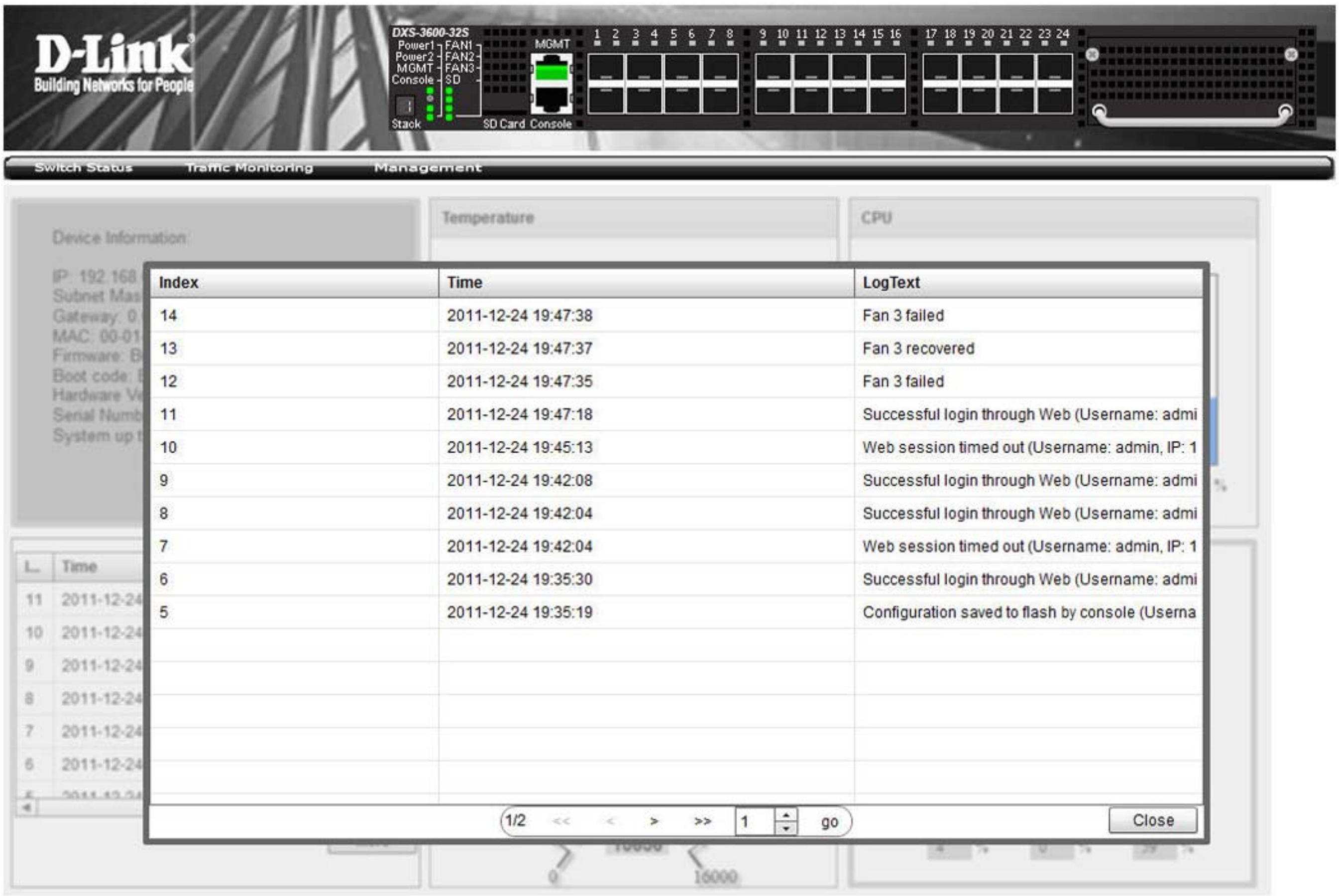
More

In the **System Log** section, the following display parameters are available:

Parameter	Description
Entry Number	Every log entry has a specific entry number, generated when the log entry was added to the System log entry display. Here the System log entry number is displayed in reverse order.
Time	Here the specific date and time of the log entry is displayed.
Log Text	Here the log entry decription is displayed.

Click the **More** button to view a larger display of the complete System Log section.

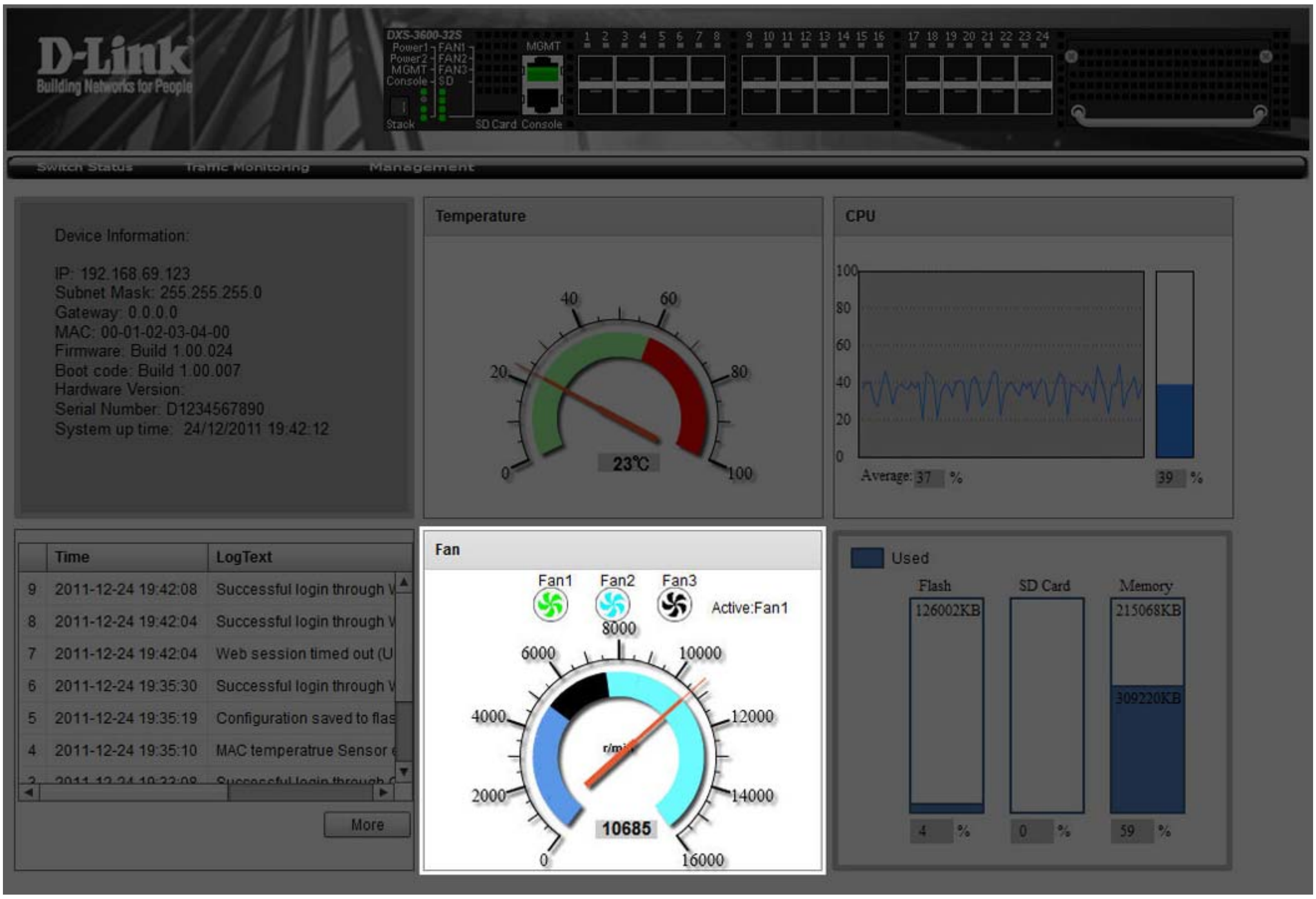
Click the **Close** button to exit the larger display.



Index	Time	LogText
14	2011-12-24 19:47:38	Fan 3 failed
13	2011-12-24 19:47:37	Fan 3 recovered
12	2011-12-24 19:47:35	Fan 3 failed
11	2011-12-24 19:47:18	Successful login through Web (Username: admi
10	2011-12-24 19:45:13	Web session timed out (Username: admin, IP: 1
9	2011-12-24 19:42:08	Successful login through Web (Username: admi
8	2011-12-24 19:42:04	Successful login through Web (Username: admi
7	2011-12-24 19:42:04	Web session timed out (Username: admin, IP: 1
6	2011-12-24 19:35:30	Successful login through Web (Username: admi
5	2011-12-24 19:35:19	Configuration saved to flash by console (Userna

Fan Status

In the **Fan** section, the user can view a real-time display of the switch's fan(s) status. A maximum of 3 fans can be installed in this switch. In this real-time graphic, we observe the status and speed of the three fans installed.



Device Information:

IP: 192.168.69.123
Subnet Mask: 255.255.255.0
Gateway: 0.0.0.0
MAC: 00-01-02-03-04-00
Firmware: Build 1.00.024
Boot code: Build 1.00.007
Hardware Version:
Serial Number: D1234567890
System up time: 24/12/2011 19:42:12

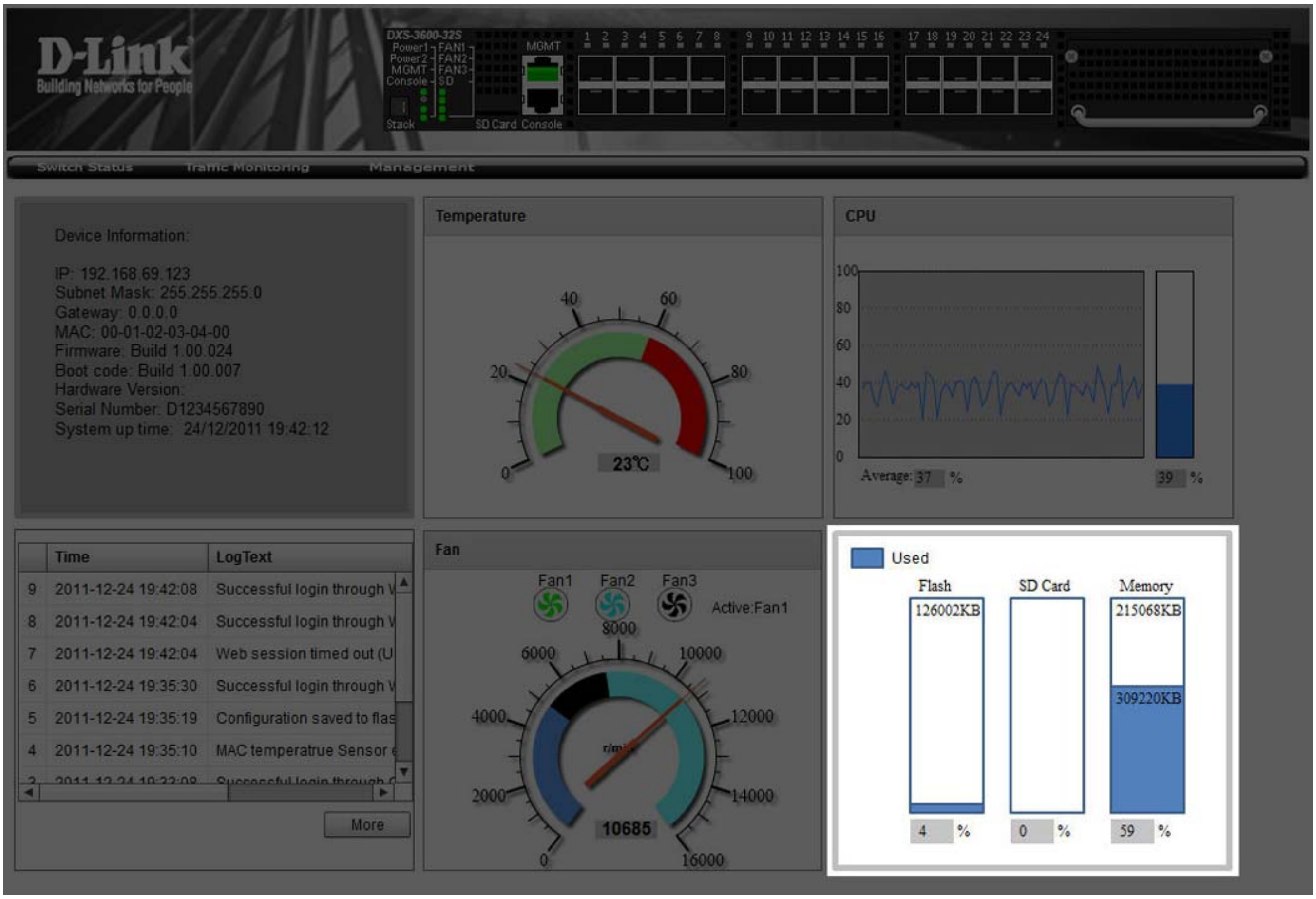
	Time	LogText
9	2011-12-24 19:42:08	Successful login through W
8	2011-12-24 19:42:04	Successful login through W
7	2011-12-24 19:42:04	Web session timed out (U
6	2011-12-24 19:35:30	Successful login through W
5	2011-12-24 19:35:19	Configuration saved to flas
4	2011-12-24 19:35:10	MAC temperatrue Sensor

In the **Fan** section, the following display parameters are available:

Parameter	Description
Fan Number	At the top of this graphic, the list of installed fans are displayed. After clicking on any specific fan icon, the real-time RPM gauge of that fan will be displayed. Also after clicking on a fan icon, the **Active Fan** display parameter will change accordingly.
RPM Graph	In this graph (gauge display), we observe the RPM speed at which the selected fan is working at.
RPM Reading	At the bottom of the graphics, we observe the accurate real-time display of the RPM value for a specific fan.

Flash, SD Card, and Memory Status

In this section, the user can view a real-time graphic that represents the memory usage for the **Flash**, **SD Card**, and **RAM Memory**.



Device Information:

IP: 192.168.69.123
Subnet Mask: 255.255.255.0
Gateway: 0.0.0.0
MAC: 00-01-02-03-04-00
Firmware: Build 1.00.024
Boot code: Build 1.00.007
Hardware Version:
Serial Number: D1234567890
System up time: 24/12/2011 19:42:12

	Time	LogText
9	2011-12-24 19:42:08	Successful login through W
8	2011-12-24 19:42:04	Successful login through W
7	2011-12-24 19:42:04	Web session timed out (U
6	2011-12-24 19:35:30	Successful login through W
5	2011-12-24 19:35:19	Configuration saved to flas
4	2011-12-24 19:35:10	MAC temperatrue Sensor

In this section, the following display parameters are available:

Parameter	Description
Used	This displays the color that represents the used memory allocation.
Flash	This displays the used and unused space of the Flash. The more accurate percentage display can be found below the graphic.
SD Card	This displays the used and unused space of the SD Card. The more accurate percentage display can be found below the graphic.
Memory	This displays the used and unused space of the Memory. The more accurate percentage display can be found below the graphic.

Traffic Monitoring

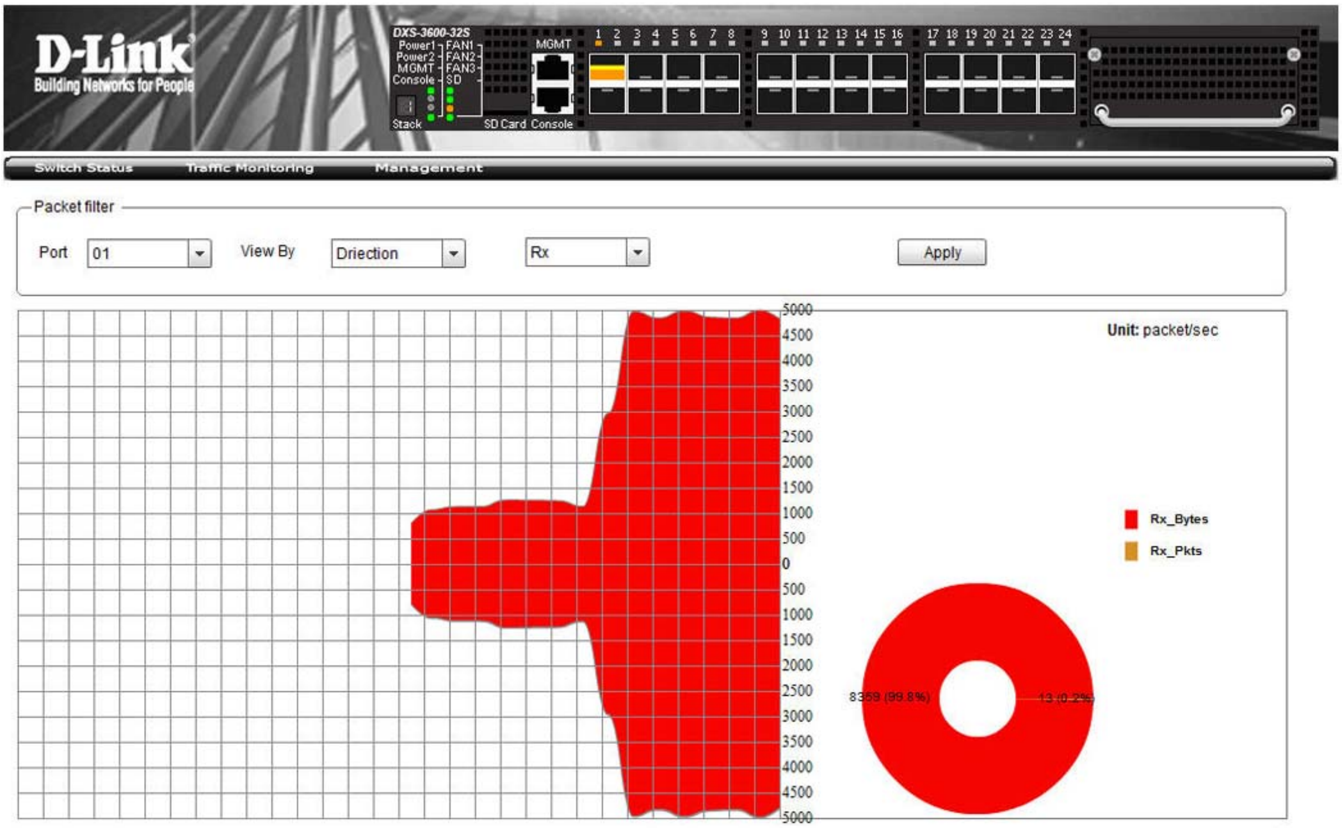
Traffic Monitoring by Direction
Traffic Monitoring by Type
Traffic Monitoring by Size
Traffic Monitoring by Error

After clicking on the **Traffic Monitoring** link, found in the menu, the following pages will be displayed.

Traffic Monitoring by Direction

This page can be used to monitor traffic, per-port, in a certain **direction**. The two directions, that can by selected, are received (Rx) or transmited (Tx) packets.

After selecting a **Port** number and then selecting the **Direction** option, from the drop-down menu, click the **Apply** button to view the page below:



Packet filter
Port: 01
View By: Driection
Rx

The following parameters can be configured on this page:

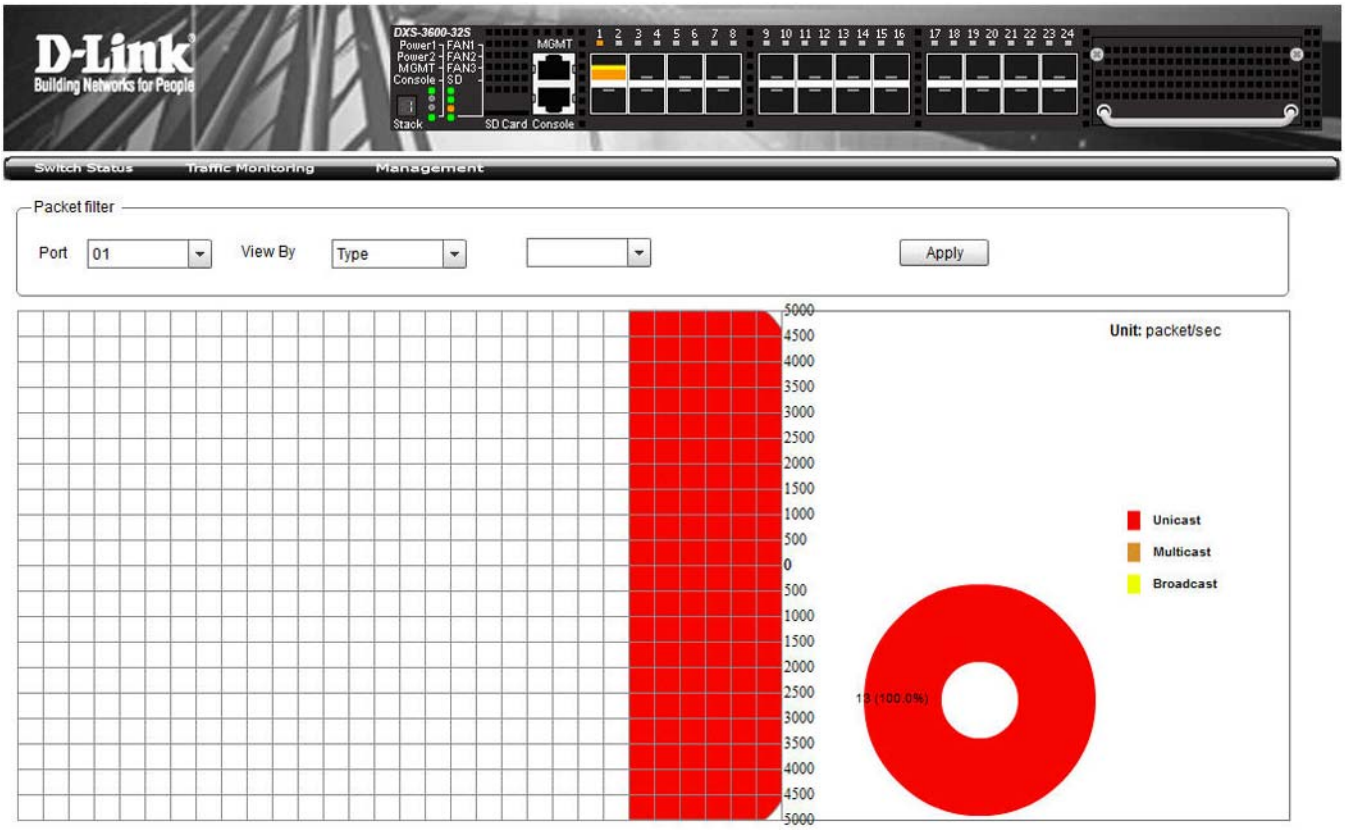
Parameter	Description
Port	Select the port number used here. The list of options are from **01** to **24**.
View By	Select the view type used here. This list of options to choose from are **Direction**, **Type**, **Size**, and **Error**. For this page, select **Direction**.
Direction	Select the traffic flow direction to monitor here. The list of options to choose from are **Rx** and **Tx**.

Click the **Apply** button to accept the changes made.

Traffic Monitoring by Type

This page can be used to monitor traffic, per-port, of a certain **type**.

After selecting a **Port** number and then selecting the **Type** option, from the drop-down menu, click the **Apply** button to view the page below:



Packet filter

Port 01

View By Type

The following parameters can be configured on this page:

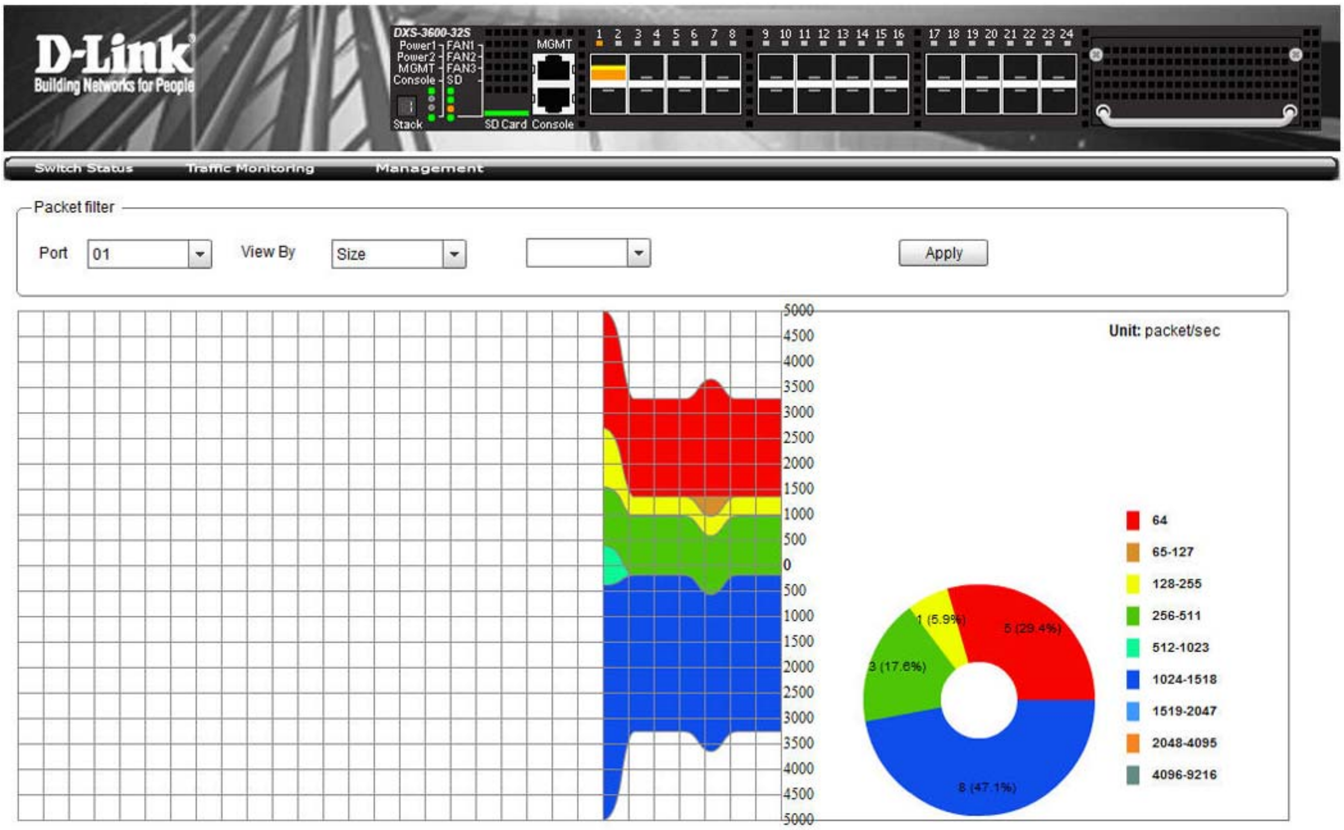
Parameter	Description
Port	Select the port number used here. The list of options are from **01** to **24**.
View By	Select the view type used here. This list of options to choose from are **Direction**, **Type**, **Size**, and **Error**. For this page, select **Type**.
Traffic Type	Select the type of traffic to monitor here. The list of options to choose from are **Multicast**, **Broadcast**, **Unicast**, and **All**. Selecting the **All** option will display all the types of traffic supported by this switch.

Click the **Apply** button to accept the changes made.

Traffic Monitoring by Size

This page can be used to monitor traffic, per-port, of a certain **packet size**.

After selecting a **Port** number and then selecting the **Size** option, from the drop-down menu, click the **Apply** button to view the page below:



Packet filter

Port 01 View By Size Apply

The following parameters can be configured on this page:

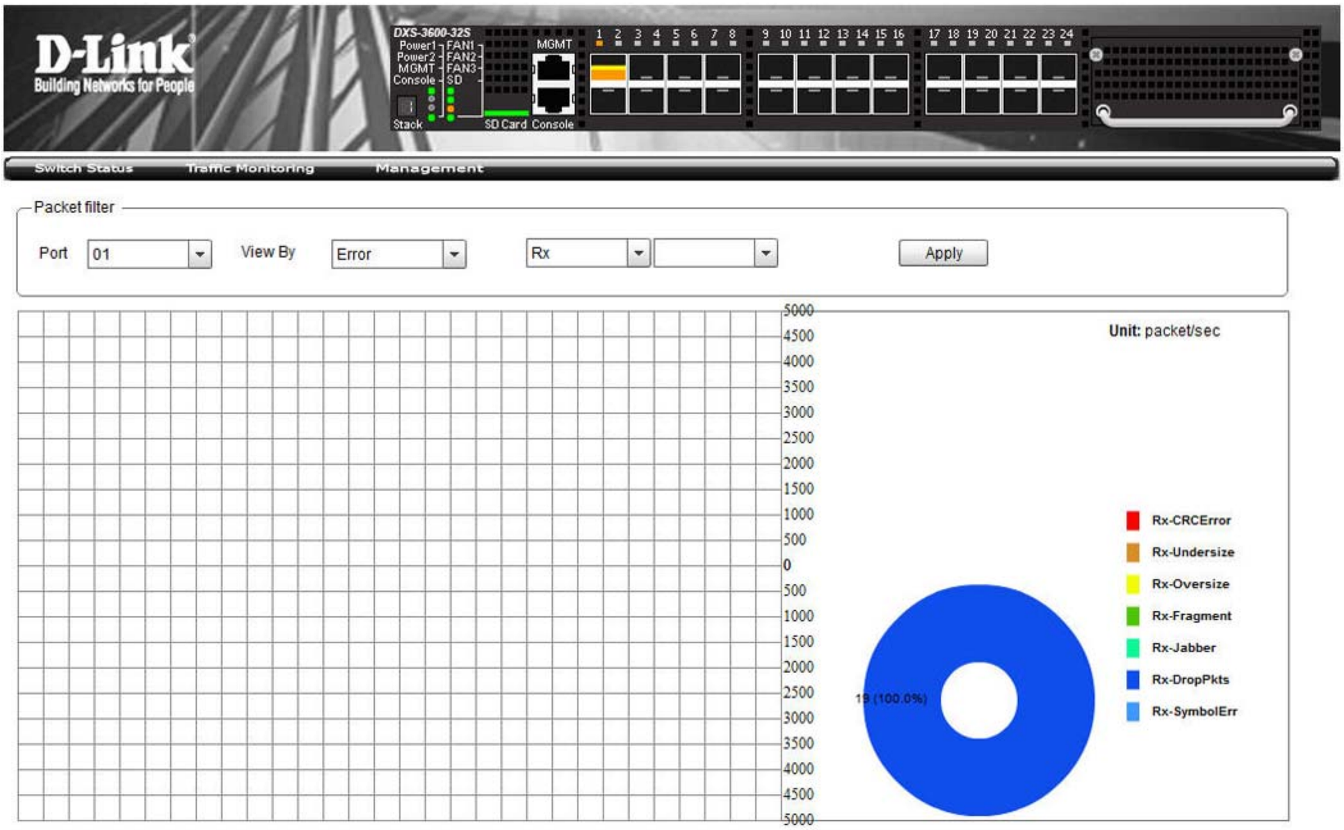
Parameter	Description
Port	Select the port number used here. The list of options are from **01** to **24**.
View By	Select the view type used here. This list of options to choose from are **Direction**, **Type**, **Size**, and **Error**. For this page, select **Size**.
Size	Select the packet size, to monitor, here. This list of options to choose from are **64**, **65-127**, **128-255**, **256-511**, **512-1023**, **1024-1518**, **1519-2047**, **2048-4095**, **4096-9216**, and **All**. Selecting the **All** option, allows the user to monitor all the sizes of packets available on this switch.

Click the **Apply** button to accept the changes made.

Traffic Monitoring by Error

This page can be used to monitor traffic, per-port, of a certain **error type** and **direction**.

After selecting a **Port** number and then selecting the **Error** option, from the drop-down menu, click the **Apply** button to view the page below:



Packet filter

Port 01 View By Error Rx Apply

The following parameters can be configured on this page:

Parameter	Description
Port	Select the port number used here. The list of options are from **01** to **24**.
View By	Select the view type used here. This list of options to choose from are **Direction**, **Type**, **Size**, and **Error**. For this page, select **Error**.
Direction	Select the traffic flow direction to monitor here. The list of options to choose from are **Rx** and **Tx**.
Error Type	Select the type of error to monitor here. The list of options to choose from differs for each direction selected. • For **Rx** the options available are **Rx-CRCError**, **Rx-Undersize**, **Rx-Oversize**, **Rx-Fragment**, **Rx-Jabber**, **Rx-DropPkts**, **Sysbol Error**, **Rx-SymbolErr**, and **All**. • For **Tx** the options available are **Tx-ExDefer**, **Tx-CRCError**, **Tx-LateColl**, **Tx-ExColl**, **Tx-SingleColl**, **Tx-Coll**, and **All**. Select the **All** option for both directions, will allow the user to monitor all error related traffic in the selected direction.

Click the **Apply** button to accept the changes made.

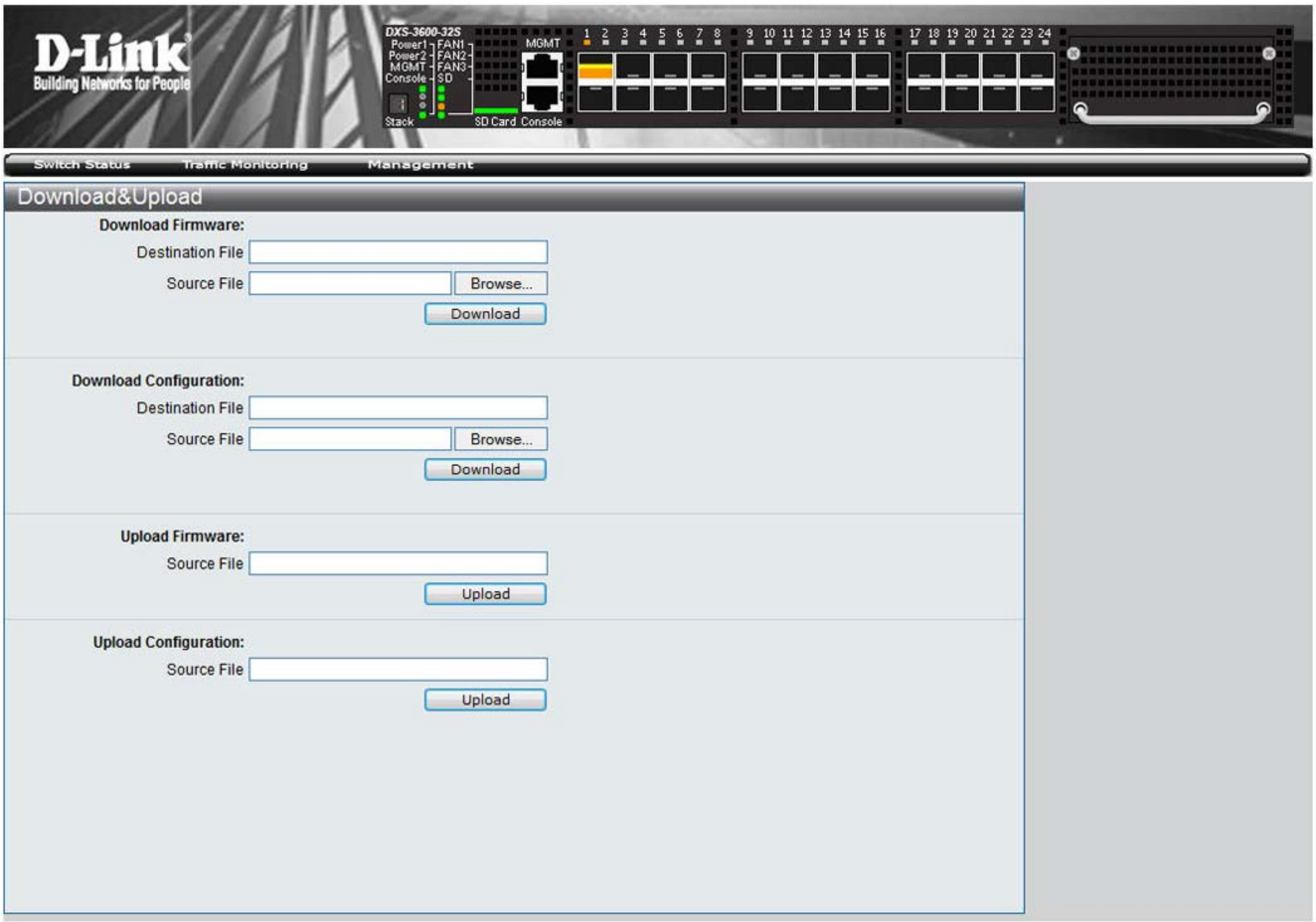
Management

Download Firmware
Download Configuration
Upload Firmware
Upload Configuration

On the **Management** page, the user is allowed to **Download** and **Upload Firmware** or **Configuration** files. Keeping the switch's firmware up-to-date will prevent any future inconvenience caused by minor software bugs. Also from time to time, D-Link provides new features that can only be acquired with a new firmware update.

Keeping a copy of the **configuration** file ensures the convenience of not having to reconfigure the switch if it needs to be replaced.

After clicking on the **Management** link, found in the menu, the following page will be displayed:



Download&Upload

Download Firmware:
Destination File
Source File Browse...
Download

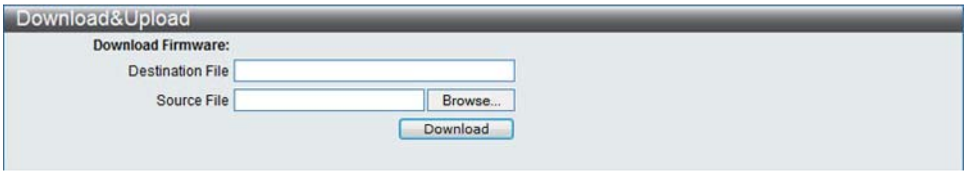
Download Configuration:
Destination File
Source File Browse...
Download

Upload Firmware:
Source File
Upload

Upload Configuration:
Source File
Upload

Download Firmware

In the **Download Firmware** section, the following can be seen:



Download&Upload

Download Firmware:
Destination File
Source File Browse...
Download

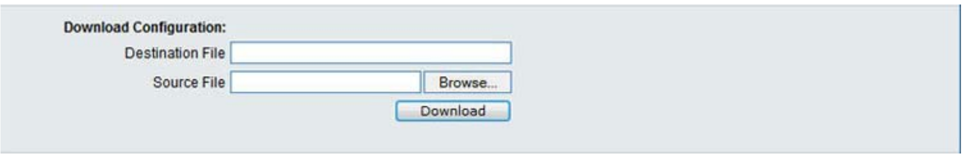
The following parameters can be configured in this section:

Parameter	Description
Destination File	Enter the location and name of the Destination File.
Source File	Enter the location and name of the Source File or click the **Browse** button to navigate to the firmware file for the download.

Click the **Download** button to initiate the download.

Download Configuration

In the **Download Configuration** section, the following can be seen:



Download Configuration:

Destination File

Source File

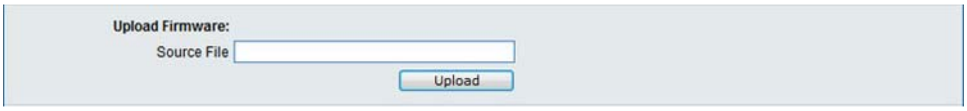
The following parameters can be configured in this section:

Parameter	Description
Destination File	Enter the location and name of the Destination File.
Source File	Enter the location and name of the Source File or click the **Browse** button to navigate to the configuration file for the download**.**

Click the **Download** button to initiate the download.

Upload Firmware

In the **Upload Firmware** section, the following can be seen:



Upload Firmware:

Source File

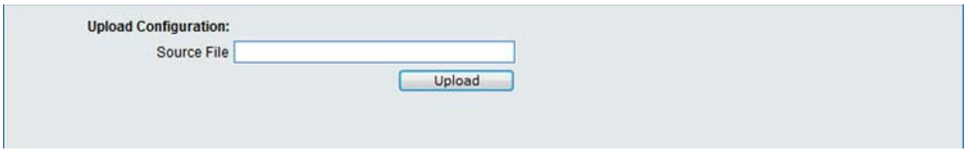
The following parameters can be configured in this section:

Parameter	Description
Source File	Enter the location and name of the Source File or click the **Browse** button to navigate to the firmware file for the upload.

Click the **Upload** button to initiate the upload.

Upload Configuration

In the **Upload Configuration** section, the following can be seen:



Upload Configuration:

Source File

The following parameters can be configured in this section:

Parameter	Description
Source File	Enter the location and name of the Source File for the upload.

Click the **Upload** button to initiate the upload.

Appendix A - Password Recovery Procedure

This section describes the procedure for resetting passwords on the D-Link DXS-3600-32S switch.

Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a **Username** and **Password**. Sometimes, passwords get forgotten or destroyed, so network administrators need to reset these passwords. This section will explain how the Password Recovery feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on this switch to easily recover passwords.

Complete these steps to reset the password:

1. For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the switch.
2. Power on the Switch. After the UART init is loaded to 100%, the Switch will allow 2 seconds for the user to press the hotkey [^] (Shift + 6) to enter the “Password Recovery Mode.” Once the Switch enters the “Password Recovery Mode,” all ports on the Switch will be disabled.

```
  Boot Procedure                                          V1.00.007
-------------------------------------------------------------------------------

  Power On Self Test ........................................  100 %

  MAC Address   : 00-01-02-03-04-00
  H/W Version   :

  Please Wait, Loading V1.00.024 Runtime Image ..............  100 %
  UART init .................................................  100 %
```

```
Password Recovery Mode
>
```

1. In the “Password Recovery Mode” only the following commands can be used.

Command	Parameters
clear configure	This command allows the administrator to clear the configuration of this switch to the factory default settings. This includes resetting the user accounts to the defaults.
clear levelpassword	This command allows the administrator to clear the level password used on this switch to the factory default settings.
clear username	This command allows the administrator to clear the usernames used on this switch to the factory default settings.
reload	This command will restart the switch.

Appendix B - System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

Category	Log Description	Severity	Note
IP Directed-broadcast	Event description: IP Directed-broadcast rate exceed 50 packets per second on a certain subnet. Log Message: IP Directed Broadcast packet rate is high on subnet. [(IP: %s)] Parameters description: IP: the Broadcast IP destination address.	Informational	
	Event description: IP Directed-broadcast rate exceed 100 packets per second Log Message: IP Directed Broadcast rate is high. Parameters description: None.	Informational	
TFTP	Event description: Firmware upgraded successfully. Log Message: [TFTP(1):] Firmware upgraded by <session> was successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user’s session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Informational	
	Event description: Firmware upgrade was unsuccessful. Log Message: [TFTP(2):] Firmware upgrade by <session> was unsuccessfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user’s session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Warning	
	Event description: Firmware successfully uploaded. Log Message: [TFTP(3):]Firmware successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user’s session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Informational	
	Event description: Firmware upload was unsuccessful. Log Message: [TFTP(4):]Firmware upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user’s session. Username: Represent current login user. Ipaddr: Represent client IP address.	Warning	

Category	Log Description	Severity	Note
	Event description: Configuration successfully downloaded. Log Message: [TFTP(5):]Configuration successfully downloaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Informational	
	Event description: Configuration download was unsuccessful. Log Message: [TFTP(6):]Configuration download by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Warning	
	Event description: Configuration successfully uploaded. Log Message: [TFTP(7):]Configuration successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Informational	
	Event description: Configuration upload was unsuccessful. Log Message: [TFTP(8):]Configuration upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Warning	
	Event description: Log message successfully uploaded. Log Message: [TFTP(9):]Log message successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Informational	
	Event description: Log message upload was unsuccessful. Log Message: [TFTP(10):]Log message upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Warning	

Category	Log Description	Severity	Note
	Event description: Attack log message successfully uploaded. Log Message: [TFTP(13):]Attack log message successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user’s session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Informational	
	Event description: Attack log message upload was unsuccessful. Log Message: [TFTP(14):]Attack log message upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user’s session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Warning	
DNS Resolver	Event description: Duplicate Domain name cache added, leads a dynamic domain name cache be deleted Log Message: [DNS_RESOLVER(1):]Duplicate Domain name case name: <domainname>, static IP: <ipaddr>, dynamic IP:<ipaddr> Parameters description: domainame: the domain name string. ipaddr: IP address.	Informational	
TELNET	Event description: Successful login through Telnet. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational	
	Event description: Login failed through Telnet. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Warning	
	Event description: Logout through Telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational	
	Event description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>). Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational	
Interface	Event description: Port link up. Log Message: Port <portNum> link up, <link state> Parameters description: portNum: 1.Interger value;2.Represent the logic port number of the device. link state: for ex: , 100Mbps FULL duplex	Informational	

Category	Log Description	Severity	Note
	Event description: Port link down. Log Message: Port <portNum> link down Parameters description: portNum: 1.Interger value;2.Represent the logic port number of the device.	Informational	
802.1X	Event description: 802.1X Authentication failure. Log Message: 802.1X Authentication failure [for <reason>] from (Username: <username>, <interface-id>, MAC: <macaddr>) Parameters description: reason: The reason for the failed authentication. username: The user that is being authenticated.. interface-id: The interface name. macaddr: The MAC address of thr authenticated device.	Warning	
	Event description: 802.1X Authentication successful. Log Message: 802.1X Authentication successful from (Username: <username>, <interface-id>, MAC: <macaddr>) Parameters description: username: The user that is being authenticated. interface-id: The interface name. macaddr: The MAC address of the authenticated device.	Informational	
RADIUS	Event description: VID assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully .This VID will be assigned to the port and this port will be the VLAN untagged port member. Log Message: RADIUS server <ipaddr> assigned VID :<vlanID> to port <interface-id> (account :<username>) Parameters description: ipaddr: The IP address of the RADIUS server. vlanID: The VID of RADIUS assigned VLAN. interface-id: The interface name. Username: The user that is being authenticated.	Informational	
	Event description: Ingress bandwidth assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully .This Ingress bandwidth will be assigned to the port. Log Message: RADIUS server <ipaddr> assigned ingress bandwith :<ingressBandwidth> to port <interface-id> (account : <username>) Parameters description: ipaddr: The IP address of the RADIUS server. ingressBandwidth: The ingress bandwidth of RADIUS assign. interface-id: The interface name. Username: The user that is being authenticated.	Informational	
	Event description: Egress bandwidth assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully .This egress bandwidth will be assigned to the port. Log Message: RADIUS server <ipaddr> assigned egress bandwith :<egressBandwidth> to port <interface-id> (account: <username>) Parameters description: ipaddr: The IP address of the RADIUS server. egressBandwidth: The egress bandwidth of RADIUS assign. interface-id: The interface name. Username: The user that is being authenticated.	Informational	

Category	Log Description	Severity	Note
	Event description: 802.1p default priority assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully. This 802.1p default priority will be assigned to the port. Log Message: RADIUS server <ipaddr> assigned 802.1p default priority:<priority> to port <interface-id> (account : <username>) Parameters description: ipaddr: The IP address of the RADIUS server. priority: Priority of RADIUS assign. interface-id: The interface name. Username: The user that is being authenticated.	Informational	
	Event description: Failed to assign ACL profiles/rules from RADIUS server. Log Message: RADIUS server <ipaddr> assigns <username> ACL failure at port <interface-id> (<string>) Parameters description: ipaddr: The IP address of the RADIUS server. interface-id: The interface name. Username: The user that is being authenticated. string: The failed RADIUS ACL command string.	Warning	
LLDP-MED	Event description: LLDP-MED topology change detected Log Message: LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) Parameters description: portNum: The port number. chassisType: chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: chassis ID. portType: port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: port ID. deviceClass: LLDP-MED device type.	Notice	

Category	Log Description	Severity	Note
	Event description: Conflict LLDP-MED device type detected Log Message: Conflict LLDP-MED device type detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>) Parameters description: portNum: The port number. chassisType: chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: chassis ID. portType: port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: port ID. deviceClass: LLDP-MED device type.	Notice	
	Event description: Incompatible LLDP-MED TLV set detected Log Message: Incompatible LLDP-MED TLV set detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>) Parameters description: portNum: The port number. chassisType: chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: chassis ID. portType: port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: port ID. deviceClass: LLDP-MED device type.	Notice	

Category	Log Description	Severity	Note
BGP	Event description: BGP FSM with Peer has gone to the successfully established state. Log Message: [BGP(1):] BGP connection is successfully established (Peer:<ipaddr>). Parameters description: ipaddr: IP address of BGP peer.	Informational	
	Event description: BGP connection is normally closed. Log Message:[BGP(2):] BGP connection is normally closed(Peer:<ipaddr>). Parameters description: ipaddr: IP address of BGP peer.	Informational	
	Event description: BGP connection is closed due to error (Error Code, Error Subcode and Data fields Refer to RFC). Log Message: [BGP(3):] BGP connection is closed due to error (Code:<num> Subcode:<num> Field:<field> Peer:<ipaddr>). Parameters description: num: Error Code or Error Subcode is defined in RFC 4271 etc. field: field value when an error happen. ipaddr: IP address of the BGP peer.	Warning	
	Event description: Receive a BGP notify packet with an undefined error code or sub error code in RFC 4271. Log Message: [BGP(4):] BGP Notify: unkown Error code(num), Sub Error code(num), Peer:<ipaddr>. Parameters description: num: Error Code or Error Subcode is defined in RFC 4271 etc. ipaddr: IP address of BGP peer.	Warning	
	Event description: Receive a BGP update packet but the next_hop points to a local interface. Log Message: [BGP(5):] BGP Update Attr NHop: Erroneous NHop <ipaddr> Peer:<ipaddr>. Parameters description: ipaddr: IP address of BGP peer.	Warning	
	Event description: BGP connection is closed due to some events happens. (Event refer to RFC) Log Message: [BGP(6):] BGP connection is closed due to Event: <num> (Peer:<ipaddr>). Parameters description: num: Event is defined in RFC 4271 etc. ipaddr: IP address of BGP peer.	Warning	
	Event description: BGP connection is closed due to receive notify packet. (Error Code and Error Subcode refer to RFC) Log Message: [BGP(7):] BGP connection is closed due to Notify: Code <num> Subcode <num> (Peer:<ipaddr>). Parameters description: num: Error Code or Error Subcode is defined in RFC 4271 etc. ipaddr: IP address of BGP peer.	Warning	

Category	Log Description	Severity	Note
	Event description: The number of bgp prefix received from this neighbor reaches the threshold. Log Message: [BGP(8):] The number of prefix received reaches <num>, max <limit> (Peer < ipaddr >). Parameters description: num: The number of prefix received. limit: Max number of prefix allowed to receive. ipaddr: IP address of BGP peer.	Warning	
	Event description: The total bgp prefix number received exceeds the limit. Log Message: [BGP(9):] The total number of prefix received reaches max prefix limit.	Warning	
	Event description: BGP received unnecessary AS4-PATH attribute from new 4-bytes AS BGP peer Log Message: [BGP(10):] Received AS4-PATH attribute from new (4-bytes AS) peer. (Peer <ipaddr>).	Warning	
	Event description: BGP received unnecessary AS4-AGGREGATOR attribute from new 4-bytes AS BGP peer Log Message: [BGP(11):] Received AS4-AGGREGATOR attribute from new (4-bytes AS) peer. (Peer <ipaddr>).	Warning	
	Event description: BGP received AS_CONFED_SEQUENCE or AS_CONFED_SET path segment type in AS4-PATH attribute. Log Message: [BGP(12):] Received AS_CONFED_SEQUENCE or AS_CONFED_SET path segment type in AS4-PATH attribute. (Peer <ipaddr>).	Warning	
	Event description: BGP received invalid AS4-PATH attribute. Log Message: [BGP(13):] Received invalid AS4-PATH attribute. Value : <STRING> (Peer <ipaddr>).	Warning	
	Event description: BGP received invalid AS4- AGGREGATOR attribute. Log Message: [BGP(14):] Received invalid AS4- AGGREGATOR attribute. Value : <STRING> (Peer <ipaddr>).	Warning	
SNMP	Event Description: SNMP request received with invalid community string Log Message: SNMP request received from <ipaddr> with invalid community string. Parameters Description: ipaddr: The IP address.	Informational	
OSPFv2	Event description: OSPF interface link state changed. Log Message: OSPF interface <intf-name> changed state to [Up | Down] Parameters description: intf-name: Name of OSPF interface.	Informational	
	Event description: OSPF interface administrator state changed. Log Message: OSPF protocol on interface <intf-name> changed state to [Enabled | Disabled] Parameters description: intf-name: Name of OSPF interface.	Informational	
	Event description: One OSPF interface changed from one area to another. Log Message: OSPF interface <intf-name> changed from area <area-id> to area <area-id> Parameters description: intf-name: Name of OSPF interface. area-id: OSPF area ID.	Informational	

Category	Log Description	Severity	Note
	Event description: One OSPF neighbor state changed from Loading to Full. Log Message: OSPF nbr <nbr-id> on interface <intf-name> changed state from Loading to Full Parameters description: intf-name: Name of OSPF interface. nbr-id: Neighbor's router ID.	Notice	
	Event description: One OSPF neighbor state changed from Full to Down. Log Message: OSPF nbr <nbr-id> on interface <intf-name> changed state from Full to Down Parameters description: intf-name: Name of OSPF interface. nbr-id: Neighbor's router ID.	Notice	
	Event description: One OSPF neighbor state's dead timer expired. Log Message: OSPF nbr <nbr-id> on interface <intf-name> dead timer expired Parameters description: intf-name: Name of OSPF interface. nbr-id: Neighbor's router ID.	Notice	
	Event description: One OSPF virtual neighbor state changed from Loading to Full. Log Message: OSPF nbr <nbr-id> on virtual link changed state from Loading to Full Parameters description: nbr-id: Neighbor's router ID.	Notice	
	Event description: One OSPF virtual neighbor state changed from Full to Down. Log Message: OSPF nbr <nbr-id> on virtual link changed state from Full to Down Parameters description: nbr-id: Neighbor's router ID.	Notice	
	Event description: OSPF router ID was changed. Log Message: OSPF router ID changed to <router-id> Parameters description: router-id: OSPF router ID.	Informational	
	Event description: Enable OSPF. Log Message: OSPF state changed to Enabled	Informational	
	Event description: Disable OSPF. Log Message: OSPF state changed to Disabled	Informational	
VRRP Debug	Event description: One virtual router state becomes Master. Log Message: VR <vr-id> at interface <intf-name> switch to Master Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Informational	
	Event description: One virtual router state becomes Backup. Log Message: VR <vr-id> at interface <intf-name> switch to Backup Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Informational	

Category	Log Description	Severity	Note
	Event description: One virtual router state becomes Init. Log Message: VR <vr-id> at interface <intf-name> switch to Init Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Informational	
	Event description: Authentication type mismatch of one received VRRP advertisement message. Log Message: Authentication type mismatch on VR <vr-id> at interface <intf-name> Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Warning	
	Event description: Authentication checking fail of one received VRRP advertisement message. Log Message: Authentication fail on VR <vr-id> at interface <intf-name>. Auth type <auth-type> Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based. Auth-type: VRRP interface authentication type.	Warning	
	Event description: Checksum error of one received VRRP advertisement message. Log Message: Received an ADV msg with incorrect checksum on VR <vr-id> at interface <intf-name> Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Warning	
	Event description: Virtual router ID mismatch of one received VRRP advertisement message. Log Message: Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name> Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Warning	
	Event description: Advertisement interval mismatch of one received VRRP advertisement message. Log Message: Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name> Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Warning	
	Event description: A virtual MAC address is added into switch L2 table Log Message: Added a virtual MAC <vrrp-mac-addr> into L2 table Parameters description: vrrp-mac-addr: VRRP virtual MAC address	Notice	
	Event description: A virtual MAC address is deleted from switch L2 table. Log Message: Deleted a virtual MAC <vrrp-mac-addr> from L2 table Parameters description: vrrp-mac-addr: VRRP virtual MAC address	Notice	

Category	Log Description	Severity	Note
	Event description: A virtual MAC address is adding into switch L3 table. Log Message: Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address	Notice	
	Event description: A virtual MAC address is deleting from switch L3 table. Log Message: Deleted a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from L3 table Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address	Notice	
	Event description: Failed when adding a virtual MAC into switch chip L2 table. Log Message: Failed to add virtual MAC <vrrp-mac-addr> into chip L2 table. Errcode <vrrp-errcode> Parameters description: vrrp-mac-addr: VRRP virtual MAC address vrrp-errcode: Errcode of VRRP protocol behavior.	Error	
	Event description: Failed when deleting a virtual MAC from switch chip L2 table. Log Message: Failed to delete virtual MAC <vrrp-mac-addr> from chip L2 table. Errcode <vrrp-errcode> Parameters description: vrrp-mac-addr: VRRP virtual MAC address vrrp-errcode: Errcode of VRRP protocol behaviour.	Error	
	Event description: Failed when adding a virtual MAC into switch L3 table. The L3 table is full. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. L3 table is full Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address	Error	
	Event description: Failed when adding a virtual MAC into switch L3 table. The port where the MAC is learned from is invalid. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Port <mac-port> is invalid Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address mac-port: port number of VRRP virtual MAC.	Error	
	Event description: Failed when adding a virtual MAC into switch L3 table. The interface where the MAC is learned from is invalid. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Interface <mac-intf> is invalid Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address mac-intf: interface id on which VRRP virtual MAC address is based.	Error	

Category	Log Description	Severity	Note
	Event description: Failed when adding a virtual MAC into switch L3 table. The box where the MAC is learned from is invalid. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Box id <mac-box> is invalid Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address mac-box: stacking box number of VRRP virtual MAC.	Error	
	Event description: Failed when adding a virtual MAC into switch chip's L3 table. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into chip L3 table. Errcode <vrrp-errcode> Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address vrrp-errcode: Err code of VRRP protocol behavior.	Error	
	Event description: Failed when deleting a virtual MAC from switch chip's L3 table. Log Message: Failed to delete virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from chip L3 table. Errcode <vrrp-errcode> Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address vrrp-errcode: Err code of VRRP protocol behavior.	Error	
WEB	Event description: Successful login through Web. Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational	
	Event description: Login failed through Web. Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Warning	
	Event description: Web session timed out. Log Message: Web session timed out (Username: <usrname>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational	
	Event description: Logout through Web. Log Message: Logout through Web (Username: %S, IP: %S). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational	

Category	Log Description	Severity	Note
Port Security	Event description: Address full on a port Log Message: Port security violation (MAC address: < macaddr > on < interface-id >) Parameters description: macaddr: The violation MAC address. interface-id: The interface name.	Warning	
SSH	Event description: SSH server is enabled. Log Message: SSH server is enabled	Informational	
	Event description: SSH server is disabled. Log Message: SSH server is disabled	Informational	
AAA	Event description: Successful login. Log Message: Successful login through <Console | Telnet | Web(SSL) | SSH>(Username: <username>, IP: <ipaddr >). Parameters description: ipaddr: IP address. username: user name.	Informational	
	Event description: Login failed. Log Message: Login failed through <Console | Telnet | Web(SSL) | SSH> (Username: <username>, IP: <ipaddr >). Parameters description: ipaddr: IP address. username: user name.	Warning	
	Event description: Logout. Log Message: Logout through <Console | Telnet | Web(SSL) | SSH> (Username: <username>, IP: <ipaddr >). Parameters description: ipaddr: IP address. username: user name.	Informational	
	Event description: session timed out. Log Message: <Console | Telnet | Web(SSL) | SSH> session timed out (Username: <username>, IP: <ipaddr >). Parameters description: ipaddr: IP address. username: user name.	Informational	
	Event description: Authentication Policy is enabled. Log Message: Authentication Policy is enabled (Module: AAA).	Informational	
	Event description: Authentication Policy is disabled. Log Message: Authentication Policy is disabled (Module: AAA).	Informational	
	Event description: Login failed due to AAA server timeout or improper configuration. Log Message: Login failed through <Console | Telnet | Web(SSL) | SSH> from <ipaddr > due to AAA server <ipaddr> timeout or improper configuration (Username: <username>). Parameters description: ipaddr: IP address. username: user name.	Warning	

Category	Log Description	Severity	Note
	Event description: Successful Enable Admin authenticated by AAA local or none or server. Log Message: Successful Enable Admin through <Console | Telnet | Web(SSL) | SSH> from <ipaddr > authenticated by AAA <local | none | server <ipaddr>> (Username: <username>). Parameters description: local: enable admin by AAA local method. none: enable admin by AAA none method. server: enable admin by AAA server method. ipaddr: IP address. username: user name.	Informational	
	Event description: Enable Admin failed due to AAA server timeout or improper configuration. Log Message: Enable Admin failed through <Console | Telnet | Web(SSL) | SSH> from <ipaddr > due to AAA server <ipaddr > timeout or improper configuration (Username: <username>) Parameters description: ipaddr: IP address. username: user name.	Warning	
	Event description: Enable Admin failed authenticated by AAA local or server. Log Message: Enable Admin failed through <Console | Telnet | Web(SSL) | SSH> from <ipaddr > authenticated by AAA < local | server <ipaddr >> (Username: <username>). Parameters description: local: enable admin by AAA local method. server: enable admin by AAA server method. ipaddr: IP address. username: user name.	Warning	
	Event description: Successful login authenticated by AAA local or none or server. Log Message: Successful login through <Console | Telnet | Web(SSL) | SSH> from < ipaddr > authenticated by AAA <local | none | server <ipaddr >> (Username: <username>). Parameters description: local: specify AAA local method. none: specify none method. server: specify AAA server method. ipaddr: IP address. username: user name.	Informational	
	Event description: Login failed authenticated by AAA local or server. Log Message: Login failed through <Console | Telnet | Web(SSL) | SSH> from <ipaddr> authenticated by AAA <local | server <ipaddr> (Username: <username>). Parameters description: local: specify AAA local method. server: specify AAA server method. ipaddr: IP address. username: user name.	Warning	
Traffic Control	Event description: Broadcast storm occurrence. Log Message: <interface-id> Broadcast storm is occurring. Parameters description: interface-id: The interface name.	Warning	

Category	Log Description	Severity	Note
	Event description: Broadcast storm cleared. Log Message: <interface-id> Broadcast storm has cleared. Parameters description: interface-id: The interface name.	Informational	
	Event description: Multicast storm occurrence. Log Message: <interface-id> Multicast storm is occurring. Parameters description: interface-id: The interface name.	Warning	
	Event description: Multicast Storm cleared. Log Message: <interface-id>Multicast storm has cleared. Parameters description: interface-id: The interface name.	Informational	
	Event description: Unicast storm occurrence. Log Message: <interface-id> Unicast storm is occurring. Parameters description: interface-id: The interface name.	Warning	
	Event description: Unicast Storm cleared. Log Message: <interface-id> Unicast storm has cleared. Parameters description: interface-id: The interface name.	Informational	
	Event description: Port shut down due to a packet storm Log Message: <interface-id> is currently shut down due to a packet storm. Parameters description: interface-id: The interface name.	Warning	
MSTP Debug	Event description: Topology changed. Log Message: Topology changed [([Instance:<InstanceID>] ,port:< portNum> ,MAC: <macaddr>)] Parameters description: InstanceID: Instance ID. portNum:Port ID macaddr: MAC address	Notice	
	Event description: Spanning Tree new Root Bridge Log Message: [CIST | CIST Regional | MSTI Regional] New Root bridge selected([Instance: <InstanceID>]MAC: <macaddr> Priority :<value>) Parameters description: InstanceID: Instance ID. macaddr: Mac address value: priority value	Informational	
	Event description: Spanning Tree Protocol is enabled Log Message: Spanning Tree Protocol is enabled	Informational	
	Event description: Spanning Tree Protocol is disabled Log Message: Spanning Tree Protocol is disabled	Informational	
	Event description: New root port Log Message: New root port selected [([Instance:<InstanceID>], port:< portNum>)] Parameters description: InstanceID: Instance ID. portNum:Port ID	Notice	

Category	Log Description	Severity	Note
	Event description: Spanning Tree port status changed Log Message: Spanning Tree port status changed [([Instance:<InstanceID>], port:< portNum>)] <old_status> -> <new_status> Parameters description: InstanceID: Instance ID. portNum: Port ID old_status: Old status new_status: New status	Notice	
	Event description: Spanning Tree port role changed. Log Message: Spanning Tree port status changed. [([Instance:<InstanceID>], port:<[portNum>)] <old_role> -> <new_role> Parameters description: InstanceID: Instance ID. portNum:Port ID/ old_role: Old role new_status:New role	Informational	
	Event description: Spannnig Tree instance created. Log Message: Spanning Tree instance created. Instance:<InstanceID> Parameters description: InstanceID: Instance ID.	Informational	
	Event description: Spannnig Tree instance deleted. Log Message: Spanning Tree instance deleted. Instance:<InstanceID> Parameters description: InstanceID: Instance ID.	Informational	
	Event description: Spanning Tree Version changed. Log Message: Spanning Tree version changed. New version:<new_version> Parameters description: new_version: New STP version.	Informational	
	Event description: Spanning Tree MST configuration ID name and revision level changed. Log Message: Spanning Tree MST configuration ID name and revision level changed (name:<name> ,revision level <revision_level>). Parameters description: name : New name. revision_level:New revision level.	Informational	
	Event description: Spanning Tree MST configuration ID VLAN mapping table deleted. Log Message: Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> delete vlan <startvlanid> [- <endvlanid>]). Parameters description: InstanceID: Instance ID. startvlanid- endvlanid:VLANlist	Informational	
	Event description: Spanning Tree MST configuration ID VLAN mapping table added. Log Message: Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> add vlan <startvlanid> [- <endvlanid>]). Parameters description: InstanceID: Instance ID. startvlanid- endvlanid:VLANlist	Informational	

Category	Log Description	Severity	Note
Port	Event description: port linkup Log Message: Port <port> link up, <nway> Parameters description: port: Represents the logical port number. nway: Represents the speed and duplex of link.	Informational	
	Event description: port linkdown Log Message: Port <port> link down Parameters description: port: Represents the logical port number.	Informational	
DLMS	Event Description: Input an illegal activation code. Log Message: Illegal activation code (AC: <string25>). Parameters Description: <string25>: Activation Code	Informational	
	Event Description: License Expired. Log Message: License expired (license:<license-model>, AC: <string25>). Parameters Description: <license-model>: License Model Name. <string25>: Activation Code	Critical	
	Event Description: License successfully installed. Log Message: License successfully installed (license:<license-model>, AC: <string25>). Parameters Description: <license-model>: License Model Name. <string25>: Activation Code	Informational	
	Event Description:The Activation Code is unbound. Log Message: Unbound Activation Code (AC: <string25>). Parameters Description: <string25>: Activation Code	Critical	
	Event Description:When a license is going to expire, it will be logged before 30 days. Log Message: License will expire in 30 days. (license:<license-model>, AC: <string25>). Parameters Description: <license-model>: License Model Name. <string25>: Activation Code	Informational	
Peripheral	Event description: Fan Recovered . Log Message: Unit <id>, Fan <id> recovered Parameters description: Unit <id>: The unit ID. Fan <id>: The FAN ID.	Critical	
	Event description: Fan Fail Log Message: Unit <id>, Fan <id> failed. Parameters description: Unit <id>: The unit ID. Fan <id>: The FAN ID.	Critical	

Category	Log Description	Severity	Note
	Event description: Temperature sensor enters alarm state. Log Message: [Uint <unitID>] Temperature sensor <sensorID> enters alarm state (current temperature: <temperature>) Parameters description: unitID: The unit ID. sensorID: The sensor ID. temperature: The temperature.	Warning	
	Event description: Temperature recovers to normal. Log Message: [Uint <unitID>] Temperature sensor <sensorID> recovers to normal state (current temperature: <temperature>) Parameters description: unitID: The unit ID. sensorID: The sensor ID. temperature: The temperature.	Informational	
	Event description: Power failed. Log Message: Unit <id>, Power <id> failed Parameters description: Unit <id>: The unit ID. Power <id>: The Power ID.	Critical	
	Event description: Power is recovered. Log Message: Unit <id>, Power <id> is recovered Parameters description: Unit <id>: The unit ID. Power <id>: The Power ID.	Critical	

Appendix C - Trap Entries

This table lists the trap logs found on the Switch.

Category	Trap Name	Description	OID
UP/Download	agentFirmwareUpgrade	This trap is sent when the process of upgrading the firmware via SNMP has finished. Binding objects: (1) swMultiImageVersion	1.3.6.1.4.1.171.12.1.7.2.0.7
	agentCfgOperCompleteTrap	The trap is sent when the configuration is completely saved, uploaded or downloaded Binding objects: (1) unitID (2) agentCfgOperate (3) agentLoginUserName	1.3.6.1.4.1.171.12.1.7.2.0.9
VRRP	vrrpTrapNewMaster	The newMaster trap indicates that the sending agent has transitioned to 'Master' state. Binding objects: (1) vrrpOperMasterIpAddr	1.3.6.1.2.1.68.0.1
	vrrpTrapAuthFailure	A vrrpAuthFailure trap signifies that a packet has been received from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type. Implementation of this trap is optional. Binding objects: (1) vrrpTrapPacketSrc (2) vrrpTrapAuthErrorType	1.3.6.1.2.1.68.0.2
MSTP	newRoot	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.	1.3.6.1.2.1.17.0.1
	topologyChange	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation ofthis trap is optional.	1.3.6.1.2.1.17.0.2
Port Trap	linkUp	A notification is generated when port linkup. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.4
	linkDown	A notification is generated when port linkdown. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.3

Category	Trap Name	Description	OID
Start Trap	coldStart	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.	1.3.6.1.6.3.1.1.5.1
	warmStart	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.	1.3.6.1.6.3.1.1.5.2
Authentication	authenticationFailure	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.	1.3.6.1.6.3.1.1.5.5
RMON	risingAlarm	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16.0.1
	fallingAlarm	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16.0.2