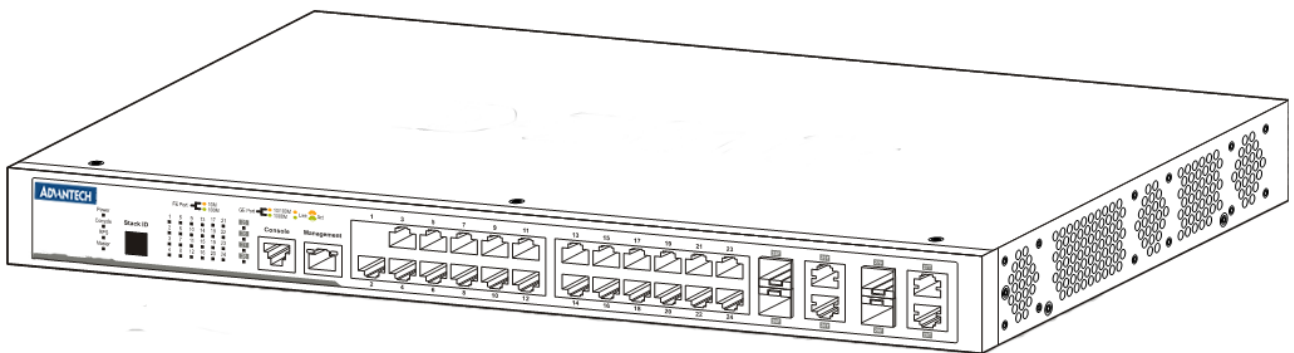


ADVANTECH

ADVANTECH EKI-4668C Industrial Ethernet Switch

Web User Interface Manual Version 1.01



Revision History

Feb 2011 - First release based on 1.10 firmware.

Copyright Statement

Advantech to provide.

Contents

Web-based Switch Configuration	1
Drop-down Menus	7
Save	8
Save Configuration / Log	8
Tools	9
Download Firmware	9
Download Firmware From TFTP	9
Download Firmware From HTTP	10
Download Configuration	11
Download Configuration From TFTP	11
Download Configuration From HTTP	12
Upload Configuration	13
Upload Configuration To TFTP	13
Upload Configuration To HTTP	14
Upload Log File	15
Upload Log To TFTP	15
Upload Log To HTTP	16
Reset	17
Reboot System	18
System Configuration	19
Device Information	20
System Information Settings	21
Port Configuration Folder	22
Port Settings	22
Port Description Settings	25
Jumbo Frame Settings	26
Serial Ports Settings	27
Warning Temperature Settings	28
System Log Settings Folder	29
System Log Settings	29
System Log Server Settings	30
System Log	31
System Log & Trap Settings	33

System Severity Settings.....	34
Time Settings.....	35
User Account Settings	36
Management	38
ARP Folder	39
Static ARP Settings	39
ARP Table	40
IP Interface Folder	41
System IP Address Settings	41
Interface Settings.....	45
Management Settings	48
Out of Band Management Settings.....	49
SNMP Settings Folder	50
SNMP Global Settings.....	52
SNMP Traps Settings	53
SNMP Link Change Traps Settings	54
SNMP View Table Settings.....	55
SNMP Community Table Settings	56
SNMP Group Table Settings	57
SNMP Engine ID Settings.....	58
SNMP User Table Settings.....	59
SNMP Host Table Settings.....	60
RMON Settings.....	61
Telnet Settings.....	62
Web Settings.....	63
L2 Features	64
VLAN (802.1Q) Folder.....	65
802.1Q VLAN Settings.....	72
GVRP Folder.....	75
GVRP Global Settings	75
GVRP Port Settings.....	76
VLAN Counter Settings.....	78
Spanning Tree Folder.....	79
STP Bridge Global Settings	82

STP Port Settings	84
MST Configuration Identification.....	86
STP Instance Settings	87
MSTP Port Information	88
Link Aggregation Folder	89
Port Trunking Settings	91
LACP Port Settings.....	93
FDB Folder	95
Static DFDB Settings Folder	95
Unicast Static FDB Settings	95
Multicast Static FDB Settings	96
MAC Address Aging Time Settings	97
MAC Address Table.....	98
ARP and FDB Table	99
L2 Multicast Control Folder	100
IGMP Snooping Folder	100
IGMP Snooping Settings	100
IGMP Snooping Static Group Settings	104
IGMP Router Port.....	106
IGMP Snooping Group	107
IGMP Snooping Forwarding Table	108
IGMP Host Table.....	109
IP Multicast VLAN Replication Folder.....	110
IP Multicast VLAN Replication Global Settings	111
IP Multicast VLAN Replication Settings.....	112
Multicast Filtering Folder	114
Multicast Filtering Mode.....	114
LLDP Folder	115
LLDP Folder	116
LLDP Global Settings	116
LLDP Port Settings	117
LLDP Management Address List.....	118
LLDP Basic TLVs Settings	119
LLDP Dot1 TLVs Settings.....	120
LLDP Dot3 TLVs Settings.....	121
LLDP Statistics System	122
LLDP Local Port Information	123
LLDP Remote Port Information	125

LLDP-MED Folder	126
LLDP-MED System Settings	127
LLDP-MED Port Settings.....	128
LLDP-MED Local Port Information	129
LLDP-MED Remote Port Information	130
L3 Features	131
IPv4 Static/Default Route Settings.....	132
IPv4 Route Table	134
IP Forwarding Table.....	135
Route Preference Settings.....	137
ECMP Algorithm Settings	138
Route Redistribution Settings	139
OSPF Folder	140
OSPFv2 Folder	140
OSPF Global Settings	140
OSPF Area Settings	141
OSPF Interface Settings.....	143
OSPF Virtual Link Settings.....	145
OSPF Area Aggregation Settings.....	147
OSPF Host Router Settings.....	148
OSPF Default Information Originate Settings.....	149
OSPF LSDB Table	150
OSPF Neighbor Table	151
OSPF Virtual Neighbor Table	152
RIP Folder.....	153
RIP Settings.....	153
IP Multicast Routing Protocol Folder	155
IGMP Interface Settings.....	155
IGMP Check Subscriber Source Network Settings.....	157
IGMP Group Table.....	158
IGMP Static Group Settings.....	159
MD5 Settings	160
Quality of Service (QoS)	161
802.1p Settings Folder	164
802.1p Default Priority Settings	164
802.1p User Priority Settings	165

Bandwidth Control Folder	166
Bandwidth Control Settings	166
Queue Bandwidth Control Settings page.....	168
Storm Control Settings.....	169
DSCP Folder.....	173
DSCP Trust Settings.....	173
DSCP Map Settings.....	174
HOL Blocking Prevention.....	175
Scheduling Settings Folder	176
Scheduling Profile Settings.....	176
Scheduling Group Settings.....	177
CPU RX Rate Limit Settings	178
Access Control List (ACL).....	179
ACL Flow Meter	180
ACL Port Settings	181
Access Profile Settings	182
Security	198
802.1X Folder	199
802.1X Global Settings	203
802.1X Port Settings.....	204
802.1X User Settings.....	206
RADIUS Folder	209
Authentication RADIUS Server Settings.....	209
RADIUS Authentication	210
IP-MAC-Port Binding (IMPB) Folder.....	212
IMPB Port Settings	213
IMPB Entry Settings.....	215
DHCP Snooping Folder	216
DHCP Snooping Max Entry Settings	216
DHCP Snooping Entries.....	217
Port Security Folder	218
Port Security Settings	218
Port Security Entries.....	220

Loopback Detection Settings	221
Traffic Segmentation Settings.....	223
SSL Settings	224
Trusted Host Settings	227
Network Application Folder.....	228
DHCP Folder	229
DHCP Relay Folder	229
DHCP Relay Global Settings.....	229
DHCP Relay Interface Settings	232
DHCP Relay Option 60 Server Settings	233
DHCP Relay Option 60 Settings.....	234
DHCP Relay Option 61 Settings.....	235
DHCP Server Folder	236
DHCP Server Global Settings	236
DHCP Server Exclude Address Settings.....	237
DHCP Server Pool Settings.....	238
DHCP Server Manual Binding.....	240
DHCP Server Dynamic Binding.....	241
DHCP Conflict IP	242
SMTP Settings	243
SNTP Folder	246
SNTP Settings	246
Time Zone Settings.....	247
Monitoring.....	251
Utilization Folder	252
CPU Utilization.....	252
DRAM & Flash Utilization	253
Port Utilization.....	254
Statistics Folder.....	255
Packets Folder	255
Received (RX)	255
UMB_Cast (RX).....	257
Transmitted (TX).....	259

Errors Folder	261
Received (RX)	261
Transmitted (TX).....	263
Packet Size.....	265
VLAN Counter Statistics	267
Mirror Folder	268
Port Mirror Settings.....	268
Ping Test.....	269
Trace Route	271
Device Environment.....	272
X-Ring.....	273
X-Ring Settings	274
Appendix A - Password Recovery Procedure	276
Appendix B - Trap Logs.....	278
Appendix C - Logs.....	281
Switch Log Syntax:	281
System Logs	281
Peripheral Function Logs	282
SNMP Logs.....	283
Interface Logs	283
Debug Funtion Logs.....	283
TFTP Client Logs	283
MSTP Debug Enhancement Logs	285
LLDP-MED Logs	287
8021X Logs.....	290
Port Security Logs.....	291
IMPB Logs	291
LD Logs.....	292
Traffic Control Logs.....	293
IP and Password Change Logs	294

Intended Readers

Typographical Conventions

Notes, Notices, and Cautions

Safety Instructions

The **EKI-4668C User Guide** contains information for setup and management of the Switch. This manual is intended for network managers familiar with network management concepts and terminology.

Typographical Conventions

Convention	Description
[]	In a command line, square brackets indicate an optional entry. For example: [copy filename] means that optionally you can type copy followed by the name of the file. Do not type the brackets.
Bold font	Indicates a button, a toolbar icon, menu, or menu item. For example: Open the File menu and choose Cancel . Used for emphasis. May also indicate system messages or prompts appearing on screen. For example: You have mail . Bold font is also used to represent filenames, program names and commands. For example: use the copy command .
Boldface Typewriter Font	Indicates commands and responses to prompts that must be typed exactly as printed in the manual.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Click Enter.
Italics	Indicates a window name or a field. Also can indicate a variables or parameter that is replaced with an appropriate word or string. For example: type <i>filename</i> means that the actual filename should be typed instead of the word shown in italic.
Menu Name > Menu Option	Menu Name > Menu Option Indicates the menu structure. Device > Port > Port Properties means the Port Properties menu option under the Port menu option that is located under the Device menu.

Table 1. Typographical Conventions

Notes, Notices, and Cautions



A **NOTE** indicates important information that helps make better use of the device




A **CAUTION** indicates a potential for property damage, personal injury, or death



A **NOTICE** indicates either potential damage to hardware or loss of data and tells how to avoid the problem.

Safety Instructions

Use the following safety guidelines to ensure your own personal safety and to help protect your system from potential damage. Throughout this safety section, the caution icon () is used to indicate cautions and precautions that need to be reviewed and followed.

Safety Cautions

To reduce the risk of bodily injury, electrical shock, fire, and damage to the equipment observe the following precautions:

- Observe and follow service markings.
 - Do not service any product except as explained in the system documentation.
 - Opening or removing covers that are marked with the triangular symbol with a lightning bolt 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 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.
- Keep your 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, see the appropriate section in the troubleshooting guide or 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.
- Use the product only with approved equipment.
- Allow the product to cool before removing covers 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.
- To help avoid damaging the system, be sure the voltage selection switch (if provided) on the power supply is set to match the power available at the Switch's location:

- 115 volts (V)/60 hertz (Hz) in most of North and South America and some Far Eastern countries such as South Korea and Taiwan
 - 100 V/50 Hz in eastern Japan and 100 V/60 Hz in western Japan
 - 230 V/50 Hz in most of Europe, the Middle East, and the Far East
- Also, 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 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/national wiring rules.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, 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; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.

General Precautions for Rack-Mountable Products

Observe the following precautions for rack stability and safety. Also, refer to the rack installation documentation accompanying the system and the rack for specific caution statements and procedures.

- Systems are considered to be components in a rack. Thus, "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 bodily injury under certain circumstances. Therefore, always install the stabilizers before installing components in the rack. 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.



NOTE: A qualified electrician must perform all connections to DC power and to safety grounds. All electrical wiring must comply with applicable local or national codes and practices.



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):

1. 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.
2. When transporting a sensitive component, first place it in an antistatic container or packaging.
3. Handle all sensitive components in a static-safe area. If possible, use anti-static floor pads, workbench pads and an antistatic grounding strap.

Web-based Switch Configuration

Introduction — 2

Logging in to the Web Manager — 3

Web-based User Interface — 4

Areas of the User Interface — 5

Web Pages — 6

Introduction

All software functions of the EKI-4668C switch can be managed, configured and monitored via the embedded web-based (HTML) interface. Manage the Switch from remote stations anywhere on the network through a standard browser. The browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol.

The Web-based management module and the Console program (and Telnet) are different ways to access the same internal switching software and configure it. Thus, all settings encountered in web-based management are the same as those found in the console program.

Logging in to the Web Manager

To begin managing the Switch, simply run the browser installed on your computer and point it to the IP address you have defined for the device. The URL in the address bar should read something like: `http://123.123.123.123`, where the numbers 123 represent the IP address of the Switch.



NOTE: The factory default IP address is 10.90.90.90.

This opens the management module's user authentication window, as seen below.



Leave both the **User Name** field and the **Password** field blank and click **OK**. This will open the Web-based user interface. The Switch management features available in the web-based manager are explained below.

Web-based User Interface

The user interface provides access to various Switch configuration and management screens, allows the user to view performance statistics, and permits graphical monitoring of the system status.

Areas of the User Interface

The figure below shows the user interface. Three distinct areas divide the user interface, as described in the table.

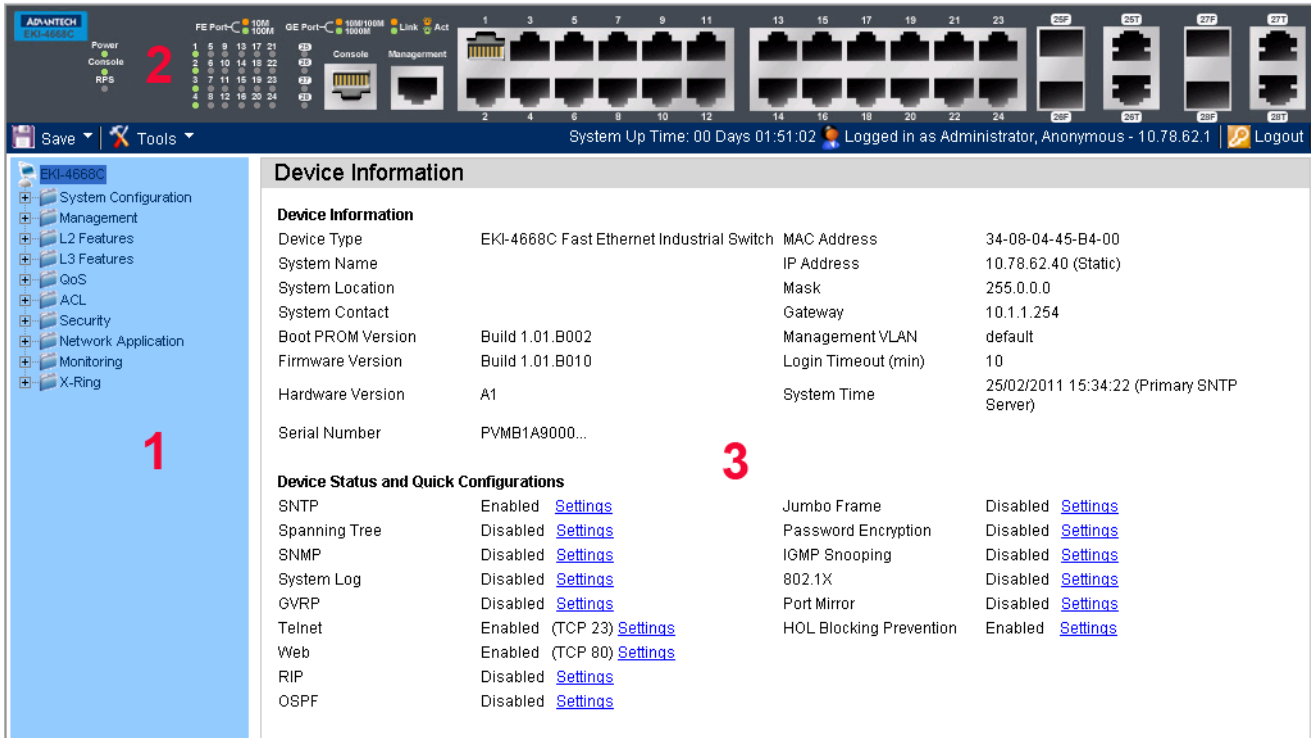


Figure 2. Main Web-Manager Screen

Area Number	Function
Area 1	Select the menu or window to display. Open folders and click the hyperlinked menu buttons and subfolders contained within them to display menus. Click the Advantech logo to go to the Advantech website.
Area 2	Presents a graphical near real-time image of the front panel of the Switch. This area displays the Switch's ports, console and management port, showing port activity. Some management functions, including save, reboot, download and upload are accessible here.
Area 3	Presents switch information based on user selection and the entry of configuration data.

Table 2. Areas of the User Interface

Web Pages

When connecting to the management mode of the Switch with a web browser, a login screen is displayed. Enter a user name and password to access the Switch's management mode.

Below is a list of the main folders available in the Web interface:

System Configuration - In this section the user will be able to configure features regarding the Switch's configuration.

Management - In this section the user will be able to configure features regarding the Switch's management.

L2 Features - In this section the user will be able to configure features regarding the Layer 2 functionality of the Switch.

L3 Features - In this section the user will be able to configure features regarding the Layer 3 functionality of the Switch.

QoS - In this section the user will be able to configure features regarding the Quality of Service functionality of the Switch.

ACL - In this section the user will be able to configure features regarding the Access Control List functionality of the Switch.

Security - In this section the user will be able to configure features regarding the Switch's security.

Network Application - In this section the user will be able to configure features regarding network applications handled by the Switch.

Monitoring - In this section the user will be able to monitor the Switch's configuration and statistics.

X-Ring - In this section the user will be able to



NOTE: Be sure to configure the user name and password in the User Accounts menu before connecting the Switch to the greater network.

Drop-down Menus

Save Configuration / Log — 8

Download Firmware — 9

Download Configuration — 11

Upload Configuration — 13

Upload Log File — 15

Reset — 17

Reboot System — 18

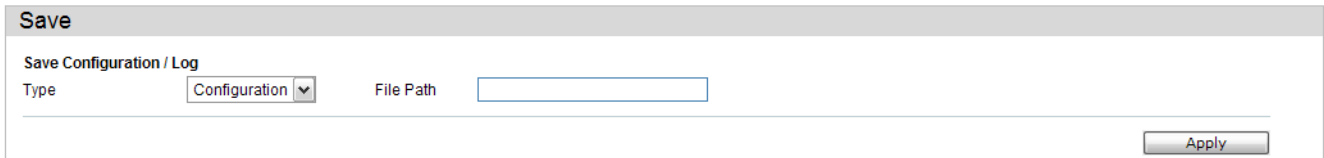
System Up Time: 00 Days 00:12:59 Logged in as Administrator, Anonymous - 10.78.62.1 Logout

Device Information			
Device Type	EKI-4668C Fast Ethernet Industrial Switch	MAC Address	34-08-04-45-B4-00
System Name		IP Address	10.78.62.40 (Static)
System Location		Mask	255.0.0.0
System Contact		Gateway	10.1.1.254
Boot PROM Version	Build 1.01.B002	Management VLAN	default
Firmware Version	Build 1.01.B010	Login Timeout (min)	10
Hardware Version	A1	System Time	02/03/2011 09:49:50 (Primary SNTP Server)

Save

Save Configuration / Log

Save Configuration allows the user to backup the configuration of the switch to a folder on the computer. Select **Configuration** from the **Type** field and enter the **File Path** in the space provided and click **Apply**.



The screenshot shows a web interface titled "Save". Below the title is a section labeled "Save Configuration / Log". There are two fields: "Type" with a dropdown menu showing "Configuration" and "File Path" with an empty text input box. An "Apply" button is located at the bottom right of the section.

Save Log allows the user to backup the log file of the switch. Select **Log** from the **Type** field and click **Apply**.



The screenshot shows the same "Save" dialog box. The "Type" dropdown menu now shows "Log". The "File Path" field is empty. The "Apply" button is at the bottom right.

Save All allows the user to permanently save changes made to the configuration. This option will allow the changes to be kept after the switch has rebooted. Select **All** from the **Type** field and click **Apply**.



The screenshot shows the "Save" dialog box with the "Type" dropdown menu set to "All". The "File Path" field is empty. The "Apply" button is at the bottom right.

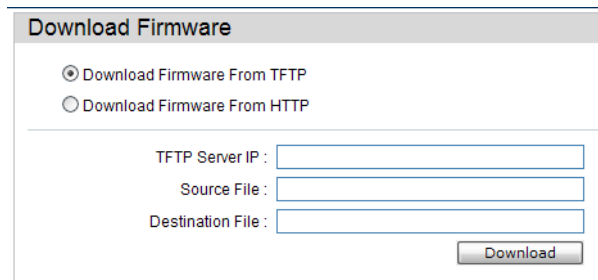
Tools

Download Firmware

The following window is used to download firmware for the Switch.

Download Firmware From TFTP

This page allows the user to download firmware from a TFTP Server to the Switch and updates the switch.



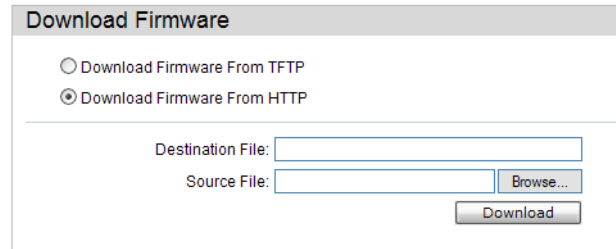
The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Here the user can enter the TFTP Server IP Address used. The user can select IPv4 to input an IPv4 address or select IPv6 to input an IPv6 address in the space provided.
Source File	Here the user can enter the location and name of the Source File.
Destination Fil	Here the user can enter the location and name of the Destination File.

Click **Download** to initiate the download.

Download Firmware From HTTP

This page allows the user to download firmware from a computer to the Switch and updates the switch.



The fields that can be configured are described below

Parameter	Description
Destination File	Here the user can enter the location of the Destination File.
Source File	Here the user can enter the location of the Source File. Click on the Browse button to navigate to the firmware file for the download

Click **Download** to initiate the download.

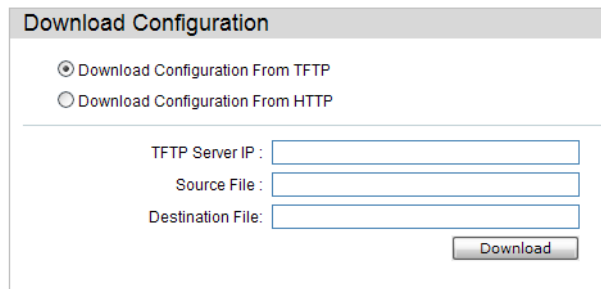
Click **Upload** to initiate the upload.

Download Configuration

The following window is used to download the configuration file for the Switch.

Download Configuration From TFTP

This page allows the user to download the configuration file from a TFTP Server to the Switch and updates the switch.



The fields that can be configured are described below:

Parameter	Description
TFTP Server IP:	Here the user can enter the TFTP Server IP Address used. The user can select IPv4 to input an IPv4 address or select IPv6 to input an IPv6 address in the space provided.
Destination File:	Here the user can enter the location and name of the Destination File.
Source File:	Here the user can enter the location and name of the Source File.

Click **Download** to initiate the download.

Download Configuration From HTTP

This page allows the user to download the configuration file from a computer to the Switch and updates the switch.

Download Configuration

Download Configuration From TFTP

Download Configuration From HTTP

Destination File:

Source File:

The fields that can be configured are described below:

Parameter	Description
Destination File:	Here the user can enter the location and name of the Destination File.
Source File:	Here the user can enter the location and name of the Source File. Click on the Browse button to navigate to the configuration file for the download.

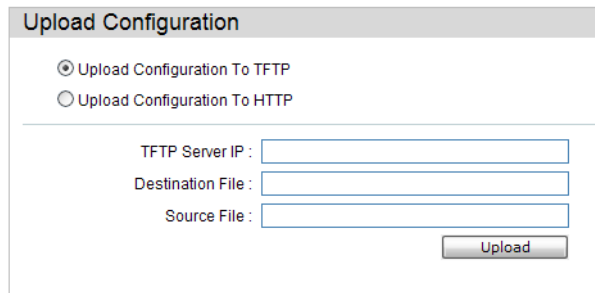
Click **Download** to initiate the download.

Upload Configuration

The following window is used to upload the configuration file from the Switch.

Upload Configuration To TFTP

This page allows the user to upload the configuration file from the Switch to a TFTP Server.



The fields that can be configured are described below:

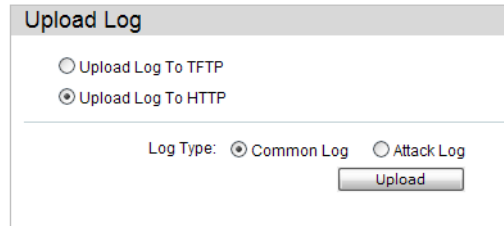
Parameter	Description
TFTP Server IP:	Here the user can enter the TFTP Server IP Address used. The user can select IPv4 to input an IPv4 address or select IPv6 to input an IPv6 address in the space provided.
Destination File:	Here the user can enter the location and name of the Destination File.
Source File:	Here the user can enter the location and name of the Source File.
Filter:	Here the user can specify to <i>include</i> , <i>begin</i> or <i>exclude</i> a filter like SNMP, VLAN or STP. Select the appropriate Filter action and enter the service name in the space provided.

Click **Upload** to initiate the upload.

Click **Upload** to initiate the upload.

Upload Configuration To HTTP

This page allows the user to upload the configuration file from the Switch to a computer.



Upload Log

Upload Log To TFTP

Upload Log To HTTP

Log Type: Common Log Attack Log

Upload

The fields that can be configured are described below:

Parameter	Description
Destination File:	Here the user can enter the location and name of the Destination File.

Click **Upload** to initiate the upload.

Upload Log File

The following window is used to upload the log file from the Switch.

Upload Log To TFTP

This page allows the user to upload the log file from the Switch to a TFTP Server.

The screenshot shows a web form titled "Upload Log". It contains two radio buttons for selection: "Upload Log To TFTP" (which is selected) and "Upload Log To HTTP". Below these are two text input fields: "TFTP Server IP:" and "Destination File:". Underneath the input fields is a "Log Type:" section with two radio buttons: "Common Log" (selected) and "Attack Log". An "Upload" button is located at the bottom right of the form.

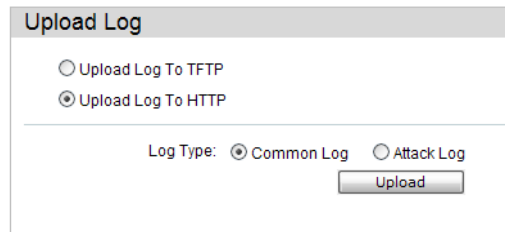
The fields that can be configured are described below:

Parameter	Description
TFTP Server IP:	Here the user can enter the TFTP Server IP Address used. The user can select IPv4 to input an IPv4 address or select IPv6 to input an IPv6 address in the space provided.
Destination File:	Here the user can enter the location and name of the Destination File.
Log Type:	Here the user can select the type of log to be transferred. Selecting the Common Log option here will upload the common log entries. Selecting the Attack Log option here will upload the log concerning attacks.

Click **Upload** to initiate the upload.

Upload Log To HTTP

This page allows the user to upload the log file from the Switch to a computer.



Upload Log

Upload Log To TFTP

Upload Log To HTTP

Log Type: Common Log Attack Log

Upload

The fields that can be configured are described below:

Parameter	Description
Log Type:	Here the user can select the type of log to be transferred. Selecting the Common Log option here will upload the common log entries. Selecting the Attack Log option here will upload the log concerning attacks.

Click **Upload** to initiate the upload.

Reset

The Reset function has several options when resetting the Switch. Some of the current configuration parameters can be retained while resetting all other configuration parameters to their factory defaults.



NOTE: Only the Reset System option will enter the factory default parameters into the Switch's non-volatile RAM, and then restart the Switch. All other options enter the factory defaults into the current configuration, but do not save this configuration. Reset System will return the Switch's configuration to the state it was when it left the factory

Reset gives the option of retaining the Switch's User Accounts and History Log while resetting all other configuration parameters to their factory defaults. If the Switch is reset using this window, and **Save Changes** is not executed, the Switch will return to the last saved configuration when rebooted.

Reset System

Reset Proceed with system reset except IP address, log, user account and banner.

Reset Config Switch will be reset to factory defaults.

Reset System Switch will be reset to factory defaults and reboot.

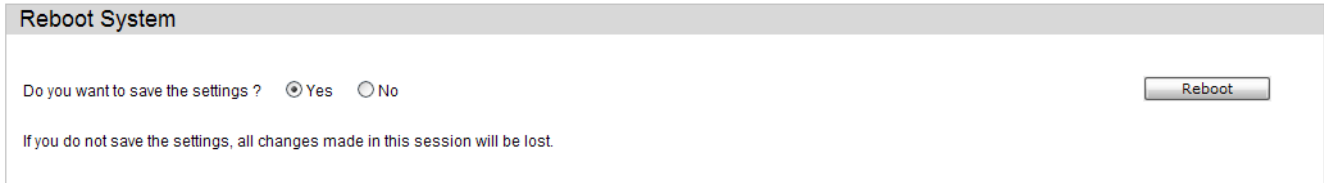
The fields that can be configured are described below:

Parameter	Description
Reset:	Selecting this option will factory reset the Switch but not the <i>IP Address, User Accounts</i> and the <i>Banner</i> .
Reset Config:	Selecting this option will factory reset the Switch but not perform a Reboot.
Reset System:	Selecting this option will factory reset the Switch and perform a Reboot.

Click the **Apply** button to initiate the Reset action.

Reboot System

The following window is used to restart the Switch.

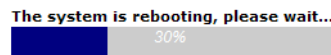


The screenshot shows a dialog box titled "Reboot System". It contains the text "Do you want to save the settings ?" followed by two radio buttons: "Yes" (which is selected) and "No". To the right of these options is a button labeled "Reboot". Below the radio buttons, there is a warning message: "If you do not save the settings, all changes made in this session will be lost."

Selecting the **Yes** radio button will instruct the Switch to save the current configuration to non-volatile RAM before restarting the Switch.

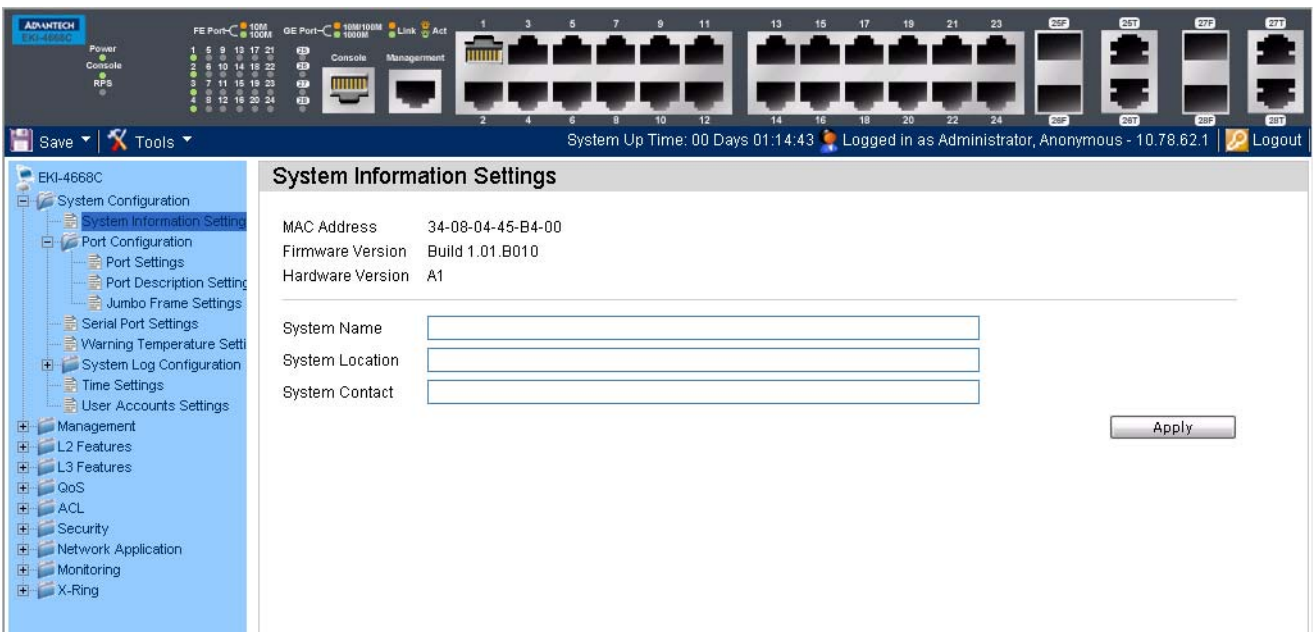
Selecting the **No** radio button instructs the Switch not to save the current configuration before restarting the Switch. All of the configuration information entered from the last time **Save Changes** was executed will be lost.

Click the Reboot button to restart the Switch.



System Configuration

- Device Information — 20***
- System Information Settings — 21***
- Port Configuration Folder — 22***
- Serial Ports Settings — 27***
- Warning Temperature Settings — 28***
- System Log Settings Folder — 29***
- Time Settings — 35***
- User Account Settings — 36***



Device Information

This window contains the main settings for all the major functions for the Switch. It appears automatically when you log on to the Switch. To return to the **Device Information** window after viewing other windows, click the **EKI-4668C** link.

The **Device Information** window shows the Switch’s MAC Address (assigned by the factory and unchangeable), the Boot PROM Version, Firmware Version, Hardware Version, and many other important types of information. This is helpful to keep track of PROM and firmware updates and to obtain the Switch’s MAC address for entry into another network device’s address table, if necessary. In addition, this window displays the status of functions on the Switch to quickly assess their current global status.

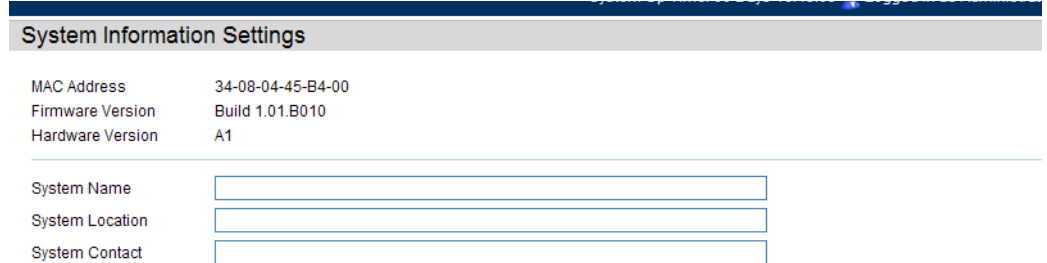
Many functions are hyper-linked for easy access to enable quick configuration from this window.

Device Information					
Device Information					
Device Type	EKI-4668C Fast Ethernet Industrial Switch	MAC Address	34-08-04-45-B4-00		
System Name		IP Address	10.78.62.40 (Static)		
System Location		Mask	255.0.0.0		
System Contact		Gateway	10.1.1.254		
Boot PROM Version	Build 1.01.B002	Management VLAN	default		
Firmware Version	Build 1.01.B010	Login Timeout (min)	10		
Hardware Version	A1	System Time	25/02/2011 15:34:22 (Primary SNTP Server)		
Serial Number	PVMB1A9000...				
Device Status and Quick Configurations					
SNTP	Enabled	Settings	Jumbo Frame	Disabled	Settings
Spanning Tree	Disabled	Settings	Password Encryption	Disabled	Settings
SNMP	Disabled	Settings	IGMP Snooping	Disabled	Settings
System Log	Disabled	Settings	802.1X	Disabled	Settings
GVRP	Disabled	Settings	Port Mirror	Disabled	Settings
Telnet	Enabled (TCP 23)	Settings	HOL Blocking Prevention	Enabled	Settings
Web	Enabled (TCP 80)	Settings			
RIP	Disabled	Settings			
OSPF	Disabled	Settings			

Click on the [Settings](#) link to navigate to the appropriate feature page for configuration.

System Information Settings

The user can enter a **System Name**, **System Location**, and **System Contact** to aid in defining the Switch. To view the following window, click **System Configuration > System Information Settings**:



MAC Address	34-08-04-45-B4-00
Firmware Version	Build 1.01.B010
Hardware Version	A1
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>

The fields that can be configured are described below:

System Name:	Enter a system name for the Switch, if so desired. This name will identify it in the Switch network.
System Location:	Enter the location of the Switch, if so desired.
System Contact:	Enter a contact name for the Switch, if so desired.

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

Port Configuration Folder

Port Settings

This page used to configure the details of the switch ports.

Port Settings

From Port: 01 To Port: 01 State: Enabled Speed/Duplex: Auto Flow Control: Disabled Address Learning: Enabled MDIX: Auto Medium Type: Copper Apply Refresh

Port	State	Speed/Duplex	Flow Control	Connection	MDIX	Address Learning
01	Enabled	Auto	Disabled	100M/Full/None	Auto	Enabled
02	Enabled	Auto	Disabled	Link Down	Auto	Enabled
03	Enabled	Auto	Disabled	Link Down	Auto	Enabled
04	Enabled	Auto	Disabled	Link Down	Auto	Enabled
05	Enabled	Auto	Disabled	Link Down	Auto	Enabled
06	Enabled	Auto	Disabled	Link Down	Auto	Enabled
07	Enabled	Auto	Disabled	Link Down	Auto	Enabled
08	Enabled	Auto	Disabled	Link Down	Auto	Enabled
09	Enabled	Auto	Disabled	Link Down	Auto	Enabled
10	Enabled	Auto	Disabled	Link Down	Auto	Enabled
11	Enabled	Auto	Disabled	Link Down	Auto	Enabled
12	Enabled	Auto	Disabled	Link Down	Auto	Enabled
13	Enabled	Auto	Disabled	Link Down	Auto	Enabled
14	Enabled	Auto	Disabled	Link Down	Auto	Enabled
15	Enabled	Auto	Disabled	Link Down	Auto	Enabled
16	Enabled	Auto	Disabled	Link Down	Auto	Enabled
17	Enabled	Auto	Disabled	Link Down	Auto	Enabled
18	Enabled	Auto	Disabled	Link Down	Auto	Enabled
19	Enabled	Auto	Disabled	Link Down	Auto	Enabled
20	Enabled	Auto	Disabled	Link Down	Auto	Enabled
21	Enabled	Auto	Disabled	Link Down	Auto	Enabled
22	Enabled	Auto	Disabled	Link Down	Auto	Enabled
23	Enabled	Auto	Disabled	Link Down	Auto	Enabled

To configure switch ports:

1. Choose the port or sequential range of ports using the From Port and To Port pull-down menus.
2. Use the remaining pull-down menus to configure the parameters described below:

The fields that can be configured are described below:

Parameter	Description
From Port – To Port:	Select the appropriate port range used for the configuration here.
State:	Toggle the State field to either enable or disable a given port or group of ports.

Speed/Duplex:	<p>Toggle the Speed/Duplex field to either select the speed and duplex/half-duplex state of the port. <i>Auto</i> denotes auto-negotiation between 10 and 100 Mbps devices, in full- or half-duplex. The <i>Auto</i> setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. The other options are <i>10M Half</i>, <i>10M Full</i>, <i>100M Half</i>, <i>100M Full</i>, <i>1000M Full_Master</i>, <i>1000M Full_Slave</i>, and <i>1000M Full</i>. There is no automatic adjustment of port settings with any option other than <i>Auto</i>.</p> <p>The Switch allows the user to configure three types of gigabit connections; <i>1000M Full_Master</i>, <i>1000M Full_Slave</i>, and <i>1000M Full</i>. Gigabit connections only support full duplex connections and take on certain characteristics that are different from the other choices listed.</p> <p>The <i>1000M Full_Master</i> and <i>1000M Full_Slave</i> parameters refer to connections running a 1000BASE-T cable for connection between the Switch port and other device capable of a gigabit connection. The master setting (<i>1000M Full_Master</i>) will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The slave setting (<i>1000M Full_Slave</i>) uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for <i>1000M Full_Master</i>, the other side of the connection must be set for <i>1000M Full_Slave</i>. Any other configuration will result in a link down status for both ports.</p>
Flow Control:	<p>Displays the flow control scheme used for the various port configurations. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control, and Auto ports use an automatic selection of the two. The default is <i>Disabled</i>.</p>
Connection:	<p>Here the current connection speed will be displayed.</p>
MDIX:	<p><i>auto</i> - Select auto for auto sensing of the optimal type of cabling.</p> <p><i>normal</i> - Select normal for normal cabling. If set to normal state, the port is in MDI mode and can be connected to a PC NIC using a straight-through cable or a port (in MDI mode) on another switch through a cross-over cable.</p> <p><i>cross</i> - Select cross for cross cabling. If set to cross state, the port is in MDIX mode, and can be connected to a port (in MDI mode) on another switch through a straight cable.</p>
Address Learning:	<p>Enable or disable MAC address learning for the selected ports. When <i>Enabled</i>, destination and source MAC addresses are automatically listed in the forwarding table. When address learning is <i>Disabled</i>, MAC addresses must be manually entered into the forwarding table. This is sometimes done for reasons of security or efficiency. See the section on Forwarding/Filtering for information on entering MAC addresses into the forwarding table. The default setting is <i>Enabled</i>.</p>
Medium:	<p>If configuring the Combo ports, this defines the type of transport medium to be used, whether <i>Copper</i> or <i>Fiber</i>.</p>

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

Click the **Refresh** button to refresh the display section of this page.

Port Description Settings

The Switch supports a port description feature where the user may name various ports.

Port Description Settings

From Port: To Port: Medium Type: Description:

Port	Description
01	
02	
03	
04	
05	
06	
07	
08	
09	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	

The fields that can be configured are described below:

Parameter	Description
From Port – To Port:	Select the appropriate port range used for the configuration here.
Medium Type:	Specify the medium type for the selected ports. If configuring the Combo ports, the Medium Type defines the type of transport medium to be used, whether <i>Copper</i> or <i>Fiber</i> .
Description:	Users may then enter a description for the chosen port(s).

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

Jumbo Frame Settings

The Switch supports jumbo frames. Jumbo frames are Ethernet frames with more than 1,500 bytes of payload. The Switch supports jumbo frames with a maximum frame size of up to 10240 bytes.

Jumbo Frame Settings

Jumbo Frame Enabled Disabled

Current Status: The maximum size of frame is 1536 bytes. Apply

The fields that can be configured are described below:

Parameter	Description
Jumbo Frame:	This field will enable or disable the Jumbo Frame function on the Switch. The default is Disabled. The maximum frame size is 1536 bytes.

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

Serial Ports Settings

Here the user can adjust the Baud Rate and the Auto Logout values.

Serial Port Settings

Baud Rate	115200 ▼
Auto Logout	Never ▼
Data Bits	8
Parity Bits	None
Stop Bits	1

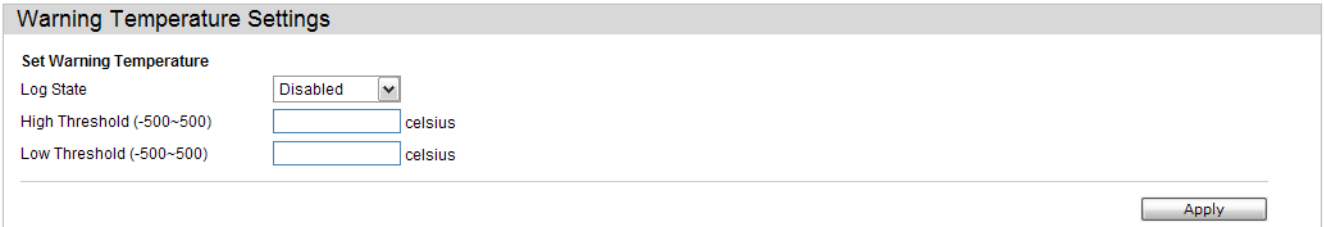
The fields that can be configured are described below:

Parameter	Description
Baud Rate:	This field specifies the baud rate for the serial port on the Switch. There are four possible baud rates to choose from, <i>9600</i> , <i>19200</i> , <i>38400</i> and <i>115200</i> . For a connection to the Switch using the console port, the baud rate must be set to <i>115200</i> , which is the default setting.
Auto Logout:	Select the logout time used for the console interface. This automatically logs the user out after an idle period of time, as defined. Choose from the following options: <i>2</i> , <i>5</i> , <i>10</i> , <i>15 minutes</i> or <i>Never</i> . The default setting is <i>10 minutes</i> .
Data Bits:	Displays the data bits used for the serial port connection.
Parity Bits:	Displays the parity bits used for the serial port connection.
Stop Bits:	Displays the stop bits used for the serial port connection.

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

Warning Temperature Settings

On this page the user can configure the system warning temperature parameters.



The image shows a web interface for 'Warning Temperature Settings'. It includes a title bar, a 'Set Warning Temperature' section, a 'Log State' dropdown menu set to 'Disabled', two input fields for 'High Threshold (-500~500)' and 'Low Threshold (-500~500)' both labeled 'celsius', and an 'Apply' button at the bottom right.

The fields that can be configured are described below:

Parameter	Description
Traps State:	Here the user can enable or disable the traps state option of the warning temperature setting.
Log State:	Here the user can enable or disable the log state option of the warning temperature setting.
High Threshold:	Here the user can enter the high threshold value of the warning temperature setting.
Low Threshold:	Here the user can enter the low threshold value of the warning temperature setting.

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

System Log Settings Folder

System Log Settings

The Switch allow users to choose a method for which to save the switch log to the flash memory of the Switch.



The fields that can be configured are described below:

Parameter	Description
System Log:	Here the user can enable or disable the system log settings. Select Enable or Disable and click to Apply button to accept the changes made.
Save Mode:	Use the pull-down menu to choose the method for saving the switch log to the flash memory. The user has three options: Time Interval – Users who choose this method can configure a time interval by which the Switch will save the log files, in the box adjacent to this configuration field. The user may set a time between 1 and 65535 minutes. On Demand – Users who choose this method will only save log files when they manually tell the Switch to do so, either using the Save Log link in the Save folder or clicking the Save Log Now button on this window. Log Trigger – Users who choose this method will have log files saved to the Switch every time a log event occurs on the Switch.

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

System Log Server Settings

The Switch can send Syslog messages to up to four designated servers using the System Log Server.

Add System Log Server

Server ID	<input type="text" value="1"/>	Severity	<input type="text" value="Emergency (0)"/>
Server IPv4 Address	<input type="text"/>	UDP Port (514 or 6000-65535)	<input type="text" value="514"/>
Facility	<input type="text" value="Local 0"/>	<input type="button" value="Apply"/> <input type="button" value="Delete All"/>	

System Log Server List

Server ID	Server IP Address	Severity	Facility	UDP Port

The fields that can be configured are described below:

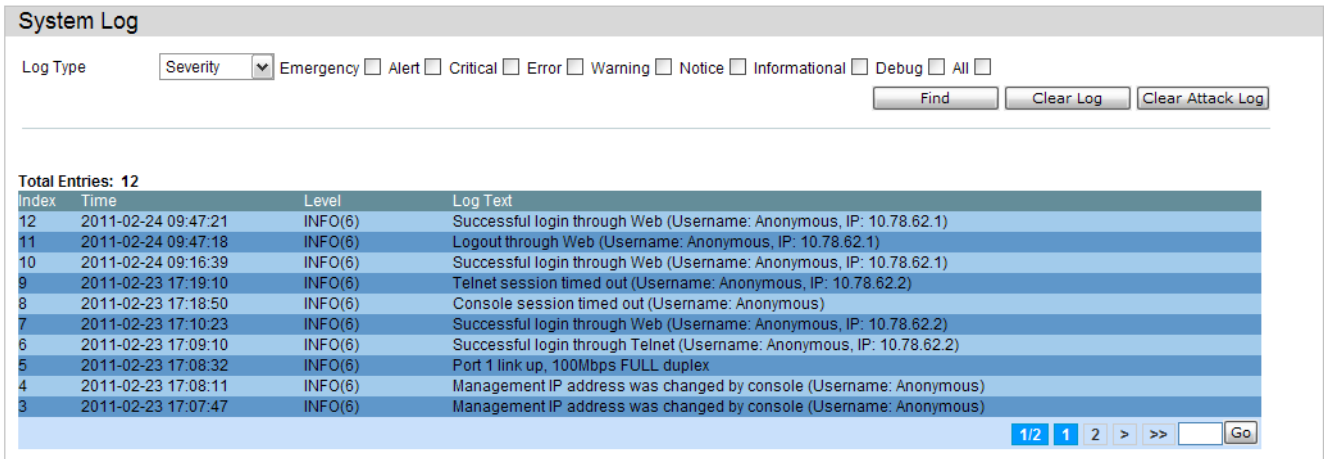
Parameter	Description
Server ID:	Syslog server settings index (1 to 4).
Server IPv4 Address:	The IPv4 address of the Syslog server.
Severity:	This drop-down menu allows you to select the higher level of messages that will be sent. All messages which level is higher than selecting level will be sent. The options are Emergency, Alert, Critical, Error, Warning, Notice, Informational and Debug.
Server IPv6 Address:	The IPv6 address of the Syslog server.
Facility:	Use the drop-down menu to select Local 0, Local 1, Local 2, Local 3, Local 4, Local 5, Local 6, or Local 7.
UDP Port:	Type the UDP port number used for sending Syslog messages. The default is 514.
Status:	Choose Enabled or Disabled to activate or deactivate.

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

Click the **Delete All** button to remove all servers configured.

System Log

Users can view and delete the local history log as compiled by the Switch's management agent.



The Switch can record event information in its own log. Click **Go** to go to the next page of the **System Log** window.

The fields that can be configured are described below:

Parameter	Description
Log Type:	In the drop-down menu the user can select the log type that will be displayed. Severity - When the user selects Severity then a secondary tick must be made. Secondary ticks are Emergency , Alert , Critical , Error , Warning , Notice , Informational and Debug . To view all information in the log simply select the All option. Module List – When the user selects Module List , the module name must be manually entered like MSTP or ERPS. Attack Log – When the user selects Attack Log all attacks will be listed.
Index:	A counter incremented whenever an entry to the Switch's history log is made. The table displays the last entry (highest sequence number) first.
Time:	Displays the time in days, hours, minutes, and seconds since the Switch was last restarted.
Level:	Here the level of the log entry is displayed.
Log Text:	Displays text describing the event that triggered the history log entry.

Click the **Find** button to display the log in the display section according to the selection made.

Click the **Clear Log** button to clear the entries from the log in the display section.

Click the **Clear Attack Log** button to clear the entries from the attack log in the display section.

System Log & Trap Settings

The Switch allows users to configure the system log source IP interface addresses here.

System Log & Trap Settings

System Log Source IP Interface Settings

IP Interface

IPv4 Address

Trap Source IP Interface Settings

IP Interface

IPv4 Address

The fields that can be configured are described below:

Parameter	Description
IP Interface:	Here the user can enter the IP interface name used.
IPv4 Address:	Here the user can enter the IPv4 address used
IPv6 Address:	Here the user can enter the IPv6 address used

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

Click the **Clear** button to clear all the information entered in the fields.

System Severity Settings

The Switch can be configured to allow alerts be logged or sent as a trap to an SNMP agent or both. The level at which the alert triggers either a log entry or a trap message can be set as well. Use the **System Severity Settings** window to set the criteria for alerts. The current settings are displayed below the System Severity Table.

System Severity Settings

System Severity: Trap ▼

Severity Level: Emergency (0) ▼ Apply

System Severity Table

System Severity	Severity Level
Trap	Information (6)
Log	Information (6)

The fields that can be configured are described below:

Parameter	Description
System Severity:	Choose how the alerts are used from the drop-down menu. Select <i>Log</i> to send the alert of the Severity Type configured to the Switch’s log for analysis. Choose <i>Trap</i> to send it to an SNMP agent for analysis, or select <i>All</i> to send the chosen alert type to an SNMP agent and the Switch’s log for analysis.
Severity Level:	This drop-down menu allows you to select the level of messages that will be sent. The options are <i>Emergency</i> , <i>Alert</i> , <i>Critical</i> , <i>Error</i> , <i>Warning</i> , <i>Notice</i> , <i>Informational</i> and <i>Debug</i> .

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

Time Settings

Users can configure the time settings for the Switch.



Time Settings

Set Current Time

Date (DD / MM / YYYY)

Time (HH: MM: SS)

The fields that can be configured are described below:

Parameter	Description
Date (DD/MM/YYYY):	Enter the current day, month, and year to update the system clock.
Time (HH:MM:SS):	Enter the current time in hours, minutes, and seconds.

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

User Account Settings

The Switch allows the control of user privileges.

User Accounts Settings

Add User Accounts

User Name Password

Access Right Confirm Password

Note: Password / User Name should be less than 16 characters.

Total Entries: 0

User Name	Access Right

To add a new user, type in a User Name and New Password and retype the same password in the Confirm New Password field. Choose the level of privilege (Admin, Operator or User) from the Access Right drop-down menu.

Configuration	Read/Write	Read/Write–partly	No
Network Monitoring	Read/Write	Read/Write	Read-only
Community Strings and Trap Stations	Read/Write	Read-only	Read-only
Update Firmware and Configuration Files	Read/Write	No	No
System Utilities	Read/Write	No	No
Factory Reset	Read/Write	No	No
Add/Update/Delete User Accounts	Read/Write	No	No
View User Accounts	Read/Write	No	No

The fields that can be configured are described below:

Parameter	Description
User Name:	Here the user can type in a new user name for the switch.
Password:	Here the user can type in a new password for the switch.
Confirm Password:	Here the user can re-type in a new password for the switch.
Access Right:	Here the user can specify the access right for this user.

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



CAUTION: In case of lost passwords or password corruption, please refer to the appendix chapter entitled, "Password Recovery Procedure," which will guide you through the steps necessary to resolve this issue.



NOTE: The username and password should be less than 16 characters.

Management

ARPIP Interface Folder — 41

IP Interface Folder — 41

Management Settings — 48

Out of Band Management Settings — 49

SNMP Settings Folder — 50

Telnet Settings — 62

Web Settings — 63

The screenshot displays the 'Static ARP Settings' page in a network management web interface. At the top, there is a status bar showing 'System Up Time: 00 Days 01:05:24' and 'Logged in as Administrator, Anonymous - 10.78.62.1'. A left-hand navigation tree is visible, with 'Static ARP Settings' selected under the 'ARP' folder. The main content area is titled 'Static ARP Settings' and contains the following sections:

- Global Settings:** Includes 'ARP Aging Time (0-65535)' set to 20 min, with an 'Apply' button.
- Add Static ARP Entry:** A form with 'IP Address' and 'MAC Address' input fields, an 'Apply' button, and a 'Delete All' button.
- Total Entries: 3:** A table listing existing entries with columns for Interface, IP Address, MAC Address, and Type. Each entry has 'Edit' and 'Delete' buttons.

Interface	IP Address	MAC Address	Type	Edit	Delete
System	10.0.0.0	FF-FF-FF-FF-FF-FF	Local/Broadcast		
System	10.78.62.40	34-08-04-45-B4-00	Local		
System	10.255.255.255	FF-FF-FF-FF-FF-FF	Local/Broadcast		

ARP Folder

Static ARP Settings

The Address Resolution Protocol is a TCP/IP protocol that converts IP addresses into physical addresses. This table allows network managers to view, define, modify, and delete ARP information for specific devices. Static entries can be defined in the ARP table. When static entries are defined, a permanent entry is entered and is used to translate IP addresses to MAC addresses.

Global Settings

ARP Aging Time (0-65535) min

Add Static ARP Entry

IP Address MAC Address

Total Entries: 3

Interface	IP Address	MAC Address	Type		
mgmt_ipif	10.0.0.0	FF-FF-FF-FF-FF-FF	Local/Broadcast	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
mgmt_ipif	10.78.62.41	34-08-04-45-B4-00	Local	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
mgmt_ipif	10.255.255.255	FF-FF-FF-FF-FF-FF	Local/Broadcast	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

The fields that can be configured are described below:

Parameter	Description
ARP Aging Time (0-65535)	The ARP entry age-out time, in minutes. The default is 20 minutes.
IP Address:	The IP address of the ARP entry.
MAC Address:	The MAC address of the ARP entry.

Click the **Apply** button, located in the **Global Settings** section to accept the changes made in this section.

Click the **Apply** button, located in the **Add Static ARP Entry** section to accept the changes made in this section.

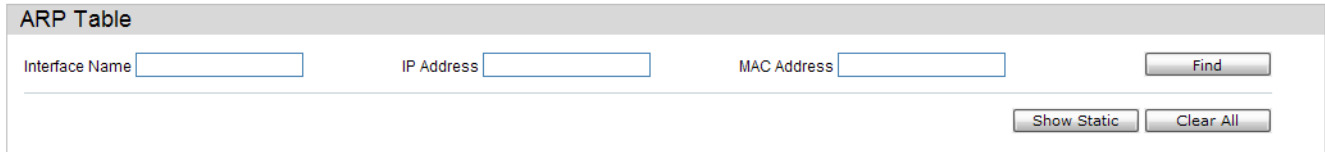
Click the **Delete All** button to remove all the entries listed.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

ARP Table

Users can display current ARP entries on the Switch.



ARP Table

Interface Name IP Address MAC Address

The fields that can be configured are described below:

Parameter	Description
Interface Name:	Here the user can enter or view the Interface name used.
IP Address:	Here the user can enter or view the IP Address used.
MAC Address:	Here the user can enter or view the MAC Address used.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show Static** button to display only the static entries in the display table.

Click the **Clear All** button to remove all the entries listed in the table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

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

IP Interface Folder

System IP Address Settings

The IP address may initially be set using the console interface prior to connecting to it through the Ethernet. The Web manager will display the Switch’s current IP settings.



NOTE: The Switch’s factory default IP address is 10.90.90.90 with a subnet mask of 255.0.0.0 and a default gateway of 0.0.0.0.

System IP Address Settings

Static
 DHCP
 BOOTP

IP Interface:

Management VLAN Name:

Interface Admin State: ▾

IP Address:

Subnet Mask:

Gateway:

IP Interface:

IP Address:

Subnet Mask:

Gateway:

Status: **Enabled**

Link Status: **Link Up**

The fields that can be configured are described below:

Parameter	Description
Static:	Allows the entry of an IP address, subnet mask, and a default gateway for the Switch. These fields should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal form) between 0 and 255. This address should be a unique address on the network assigned for use by the network administrator.
DHCP:	The Switch will send out a DHCP broadcast request when it is powered up. The DHCP protocol allows IP addresses, network masks, and default gateways to be assigned by a DHCP server. If this option is set, the Switch will first look for a DHCP server to provide it with this information before using the default or previously entered settings.

BOOTP:	The Switch will send out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the Switch will first look for a BOOTP server to provide it with this information before using the default or previously entered settings.
---------------	---

The following table will describe the fields that are about the **System** Interface.

Parameter	Description
IP Interface:	Here the System interface name will be displayed.
Management VLAN Name:	This allows the entry of a VLAN name from which a management station will be allowed to manage the Switch using TCP/IP (in-band via Web manager or Telnet). Management stations that are on VLANs other than the one entered here will not be able to manage the Switch in-band unless their IP addresses are entered in the Trusted Host window (Security > Trusted Host). If VLANs have not yet been configured for the Switch, the default VLAN contains all of the Switch's ports. There are no entries in the Trusted Host table, by default, so any management station that can connect to the Switch can access the Switch until a management VLAN is specified or Management Station IP addresses are assigned.
Interface Admin State:	Use the drop-down menu to enable or disable the configuration on this interface.
IP Address:	This field allows the entry of an IPv4 address to be assigned to this IP interface.
Subnet Mask:	A Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.
Gateway:	IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.

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

The following table will describe the fields that are about the **Management** Interface. The management interface can be accessed by connecting to the **Management port**.

Parameter	Description
IP Interface:	Here the management interface name will be displayed.
IP Address:	This field allows the entry of an IPv4 address to be assigned to this IP interface.

Subnet Mask:	A Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.
Gateway:	IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.
Status:	Specifies whether the management port is enabled or disabled.
Link Status:	Specifies whether a physical connection is made to the Management Port.

Setting the Switch's IP Address using the Console Interface

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP, TFTP). The Switch's default IP address is 10.90.90.90. The default Switch IP address can be changed to meet the specification of your networking address scheme.

The IP address for the Switch must be set before the Web-based manager can manage the switch. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known. The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:

Starting at the command line prompt, enter the commands

```
EKI-4668C:15# configure terminal
EKI-4668C:15(config)#out-band interface ip xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy
```

Where the x's represent the IP address to be assigned to the IP interface named System and the y's represent the corresponding subnet mask.

Alternatively, the user can enter:

```
EKI-4668C:15# configure terminal
EKI-4668C:15(config)#ip interface System
EKI-4668C:15(config-ip-if)# ip address ip xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy
EKI-4668C:15(config-ip-if)#
```

Where the x's represent the IP address to be assigned to the IP interface named **System** and the z represents the corresponding number of subnets in CIDR notation.

The IP interface named System on the Switch can be assigned an IP address and subnet mask, which can then be used to connect a management station to the Switch's Telnet or Web-based management agent.

The user may now utilize this address to configure or manage the Switch through Telnet, the Command Line Interface (CLI) or the Web-based management (GUI).

Interface Settings

Users can display the Switch's current IP interface settings.

Interface Settings

IP Interface Name Find

Add Delete All

Total Entries: 1

IP Interface	VLAN Name	Admin.State	Secondary
System	default	Enabled	No

Edit Delete

The fields that can be configured are described below:

Parameter	Description
IP Interface Name:	Here the user can enter the name of the IP interface to search for.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete All** button to remove all the entries listed.

Click the **IPv4 Edit** button to edit the IPv4 settings for the specific entry.

Click the **IPv6 Edit** button to edit the IPv6 settings for the specific entry.

Click the **Delete** button to remove the specific entry.



NOTE: To create IPv6 interfaces, the user has to create an IPv4 interface then edit it to IPv6.

After clicking the **Add** button, the following page will appear:

IPv4 Interface Settings

IP Interface Name (Max: 12 characters)

IPv4 Address (e.g.: 172.18.211.10)

Subnet Mask (e.g.: 255.255.255.254 or 0-32)

VLAN Name (Max: 32 characters)

Interface Admin State ▼

Secondary Interface

<<Back Apply

The fields that can be configured are described below:

Parameter	Description
IP Interface Name:	Here the user can enter the name of the IP interface being created.
IPv4 Address:	Here the user can enter the IPv4 address used.
Subnet Mask:	Here the user can enter the IPv4 subnet mask used.
VLAN Name:	Here the user can enter the VLAN Name used.
Interface Admin State:	Here the user can select to enable or disable the Interface Admin State.
Secondary Interface:	The user can select this option to use this Interface as a Secondary Interface. When the primary IP is not available, the VLAN will switch to the secondary interface. It will switch back when the primary IP was recovered.

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

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Edit** button, the following page will appear:

IPv4 Interface Settings

Get IP From: ▼

IP Interface Name:

IPv4 Address: (e.g.: 172.18.211.10)

Subnet Mask: (e.g.: 255.255.255.254 or 0-32)

VLAN Name:

Interface Admin State: ▼

The fields that can be configured are described below:

Parameter	Description
Get IP From:	Here the user can specify the method this Interface will use to acquire an IP Address.
IP Interface Name:	Here the user can enter the name of the IP interface being configured.
IPv4 Address:	Here the user can enter the IPv4 address used.
Subnet Mask:	Here the user can enter the IPv4 subnet mask used.
VLAN Name:	Here the user can enter the VLAN Name used.
IPv4 State:	Here the user can select to enable or disable IPv4 State.
Interface Admin State:	Here the user can select to enable or disable the Interface Admin State.

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

Click the <<Back button to discard the changes made and return to the previous page.

Management Settings

Users can stop the scrolling of multiple pages beyond the limits of the console when using the Command Line Interface.

This window is also used to enable the DHCP auto configuration feature on the Switch. When enabled, the Switch is instructed to receive a configuration file from a TFTP server, which will set the Switch to become a DHCP client automatically on boot-up. To employ this method, the DHCP server must be set up to deliver the TFTP server IP address and configuration file name information in the DHCP reply packet. The TFTP server must be up and running and hold the necessary configuration file stored in its base directory when the request is received from the Switch. For more information about loading a configuration file for use by a client, see the DHCP server and/or TFTP server software instructions. The user may also consult the **Upload Log File** window description located in the **Tools** section of this manual.

If the Switch is unable to complete the DHCP auto configuration, the previously saved configuration file present in the Switch’s memory will be used.

This window also allows the user to implement the Switch’s built-in power saving feature. When power saving is Enabled, a port which has a link down status will be turned off to save power to the Switch. This will not affect the port’s capabilities when the port status is link up.

Users can also configure Password Encryption on the Switch.



The fields that can be configured are described below:

Parameter	Description
Password Encryption State:	Password encryption will encrypt the password configuration in configuration files. Password encryption is Disabled by default. To enable password encryption, click the Enabled radio button.

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

Out of Band Management Settings

On this page the user can configure the details of the RJ-45 out of band management port.

Out of Band Management Settings

IP Address	<input type="text" value="10"/>	<input type="text" value="78"/>	<input type="text" value="62"/>	<input type="text" value="41"/>
Subnet Mask	<input type="text" value="255"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Gateway	<input type="text" value="10"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="254"/>
Status	<input type="text" value="Enabled"/>			
Link Status	<input type="text" value="Link Up"/>			

The fields that can be configured are described below:

Parameter	Description
IP Address:	The user can enter the IP address used here.
Subnet Mask:	The user can enter the subnet mask used here.
Gateway:	The user can enter the Gateway IP address used here.
Status:	The user can enable or disable the out of band management status here.
Link Status:	The user can view the link status here.

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

Click the **Refresh** button to refresh the display table so that new entries will appear.

SNMP Settings Folder

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, switch group or network.

Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The Switch supports the SNMP versions 1, 2c, and 3. The three versions of SNMP vary in the level of security provided between the management station and the network device.

In SNMP v.1 and v.2, user authentication is accomplished using 'community strings', which function like passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped).

The default community strings for the Switch used for SNMP v.1 and v.2 management access are:

- **public** – Allows authorized management stations to retrieve MIB objects.
- **private** – Allows authorized management stations to retrieve and modify MIB objects.

SNMPv3 uses a more sophisticated authentication process that is separated into two parts. The first part is to maintain a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user on that list can do as an SNMP manager.

The Switch allows groups of users to be listed and configured with a shared set of privileges. The SNMP version may also be set for a listed group of SNMP managers. Thus, you may create a group of SNMP managers that are allowed to view read-only information or receive traps using SNMPv1 while assigning a higher level of security to another group, granting read/write privileges using SNMPv3.

Using SNMPv3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions. The functions allowed or restricted are defined using the Object Identifier (OID) associated with a specific MIB. An additional layer of security is available for SNMPv3 in that SNMP messages may be encrypted. To read more about how to configure SNMPv3 settings for the Switch read the next section.

Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port status change. The Switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change and Broadcast\Multicast Storm.

MIBs

The Switch in the Management Information Base (MIB) stores management and counter information. The Switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. In addition to the standard MIB-II, the Switch also supports its own proprietary enterprise MIB as an extended Management Information Base. Specifying the MIB Object Identifier may also retrieve the proprietary MIB. MIB values can be either read-only or read-write.

The Switch incorporates a flexible SNMP management for the switching environment. SNMP management can be customized to suit the needs of the networks and the preferences of the network administrator. Use the SNMP V3 menus to select the SNMP version used for specific tasks.

The Switch supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The administrator can specify the SNMP version used to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

SNMP settings are configured using the menus located on the SNMP V3 folder of the Web manager. Workstations on the network that are allowed SNMP privileged access to the Switch can be restricted with the Management Station IP Address menu.

SNMP Global Settings

SNMP global state settings can be enabled or disabled.



SNMP Global Settings

SNMP Global Settings

SNMP State Enabled Disabled

Apply

The fields that can be configured are described below:

Parameter	Description
SNMP State:	Enable this option to use the SNMP feature.

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

SNMP Traps Settings

Users can enable and disable the SNMP trap support function of the switch and SNMP authentication failure trap support, respectively.

SNMP Traps Settings

SNMP Traps Enabled Disabled

SNMP Authentication Trap Enabled Disabled

Linkchange Traps Enabled Disabled

Coldstart Traps Enabled Disabled

Warmstart Traps Enabled Disabled

The fields that can be configured are described below:

Parameter	Description
SNMP Traps:	Enable this option to use the SNMP Traps feature.
SNMP Authentication Trap:	Enable this option to use the SNMP Authentication Traps feature.
Linkchange Traps:	Enable this option to use the SNMP Link Change Traps feature.
Coldstart Traps:	Enable this option to use the SNMP Cold Start Traps feature.
Warmstart Traps:	Enable this option to use the SNMP Warm Start Traps feature.

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

SNMP Link Change Traps Settings

On this page the user can configure the SNMP link change trap settings

SNMP Linkchange Traps Settings

From Port

To Port

State

Linkchange Traps: Enabled

Port	State
1	Enabled
2	Enabled
3	Enabled
4	Enabled
5	Enabled
6	Enabled
7	Enabled
8	Enabled
9	Enabled
10	Enabled
11	Enabled
12	Enabled
13	Enabled
14	Enabled
15	Enabled
16	Enabled
17	Enabled
18	Enabled
19	Enabled
20	Enabled
21	Enabled
22	Enabled

The fields that can be configured are described below:

Parameter	Description
From Port – To Port:	Here the user can select the starting and ending ports to use.
State:	Here the user can enable or disable the SNMP link change Trap.

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

SNMP View Table Settings

Users can assign views to community strings that define which MIB objects can be accessed by a remote SNMP manager. The SNMP Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous window.

SNMP View Table Settings

View Name:

Subtree OID:

View Type: Included

Total Entries: 8

View Name	Subtree	View Type	
restricted	1.3.6.1.2.1.1	Included	<input type="button" value="Delete"/>
restricted	1.3.6.1.2.1.11	Included	<input type="button" value="Delete"/>
restricted	1.3.6.1.6.3.10....	Included	<input type="button" value="Delete"/>
restricted	1.3.6.1.6.3.11....	Included	<input type="button" value="Delete"/>
restricted	1.3.6.1.6.3.15....	Included	<input type="button" value="Delete"/>
CommunityView	1	Included	<input type="button" value="Delete"/>
CommunityView	1.3.6.1.6.3	Excluded	<input type="button" value="Delete"/>
CommunityView	1.3.6.1.6.3.1	Included	<input type="button" value="Delete"/>

The fields that can be configured are described below:

Parameter	Description
View Name:	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created.
Subtree OID:	Type the Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
View Type:	Select Included to include this object in the list of objects that an SNMP manager can access. Select Excluded to exclude this object from the list of objects that an SNMP manager can access.

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

Click the **Delete** button to remove the specific entry.

SNMP Community Table Settings

Users can create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string:

- An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch's SNMP agent.
- Any MIB view that defines the subset of all MIB objects will be accessible to the SNMP community.
- Read/write or read-only level permission for the MIB objects accessible to the SNMP community.

Add Community

Community Name

View Name

Access Right

Total Entries: 2

Community Name	View Name	Access Right
private	CommunityView	read_write

The fields that can be configured are described below:

Parameter	Description
Community Name:	Type an alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
View Name:	Type an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. The view name must exist in the SNMP View Table.
Access Right:	<p><i>Read Only</i> – Specifies that SNMP community members using the community string created can only read the contents of the MIBs on the Switch.</p> <p><i>Read Write</i> – Specifies that SNMP community members using the community string created can read from, and write to the contents of the MIBs on the Switch.</p>

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

Click the **Delete** button to remove the specific entry.

SNMP Group Table Settings

An SNMP Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous window.

Notify View Name
 User-based Security Model
 Security Level

Total Entries: 9

Group Name	Read View Name	Write View Name	Notify View Name	User-based Security Model	Security Level	
public	CommunityV...		CommunityV...	SNMPv1	NoAuthNoPriv	<input type="button" value="Delete"/>
public	CommunityV...		CommunityV...	SNMPv2	NoAuthNoPriv	<input type="button" value="Delete"/>
initial	restricted		restricted	SNMPv3	NoAuthNoPriv	<input type="button" value="Delete"/>

The fields that can be configured are described below:

Parameter	Description
Group Name:	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP group of SNMP users.
Read View Name:	This name is used to specify the SNMP group created can request SNMP messages.
Write View Name:	Specify a SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent.
Notify View Name:	Specify a SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.
User-based Security Model:	<p><i>SNMPv1</i> – Specifies that SNMP version 1 will be used.</p> <p><i>SNMPv2</i> – Specifies that SNMP version 2c will be used. The SNMPv2 supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.</p> <p><i>SNMPv3</i> – Specifies that the SNMP version 3 will be used. SNMPv3 provides secure access to devices through a combination of authentication and encrypting packets over the network.</p>
Security Level:	<p>The Security Level settings only apply to SNMPv3.</p> <p><i>NoAuthNoPriv</i> – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>AuthNoPriv</i> – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>AuthPriv</i> – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.</p>

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

Click the **Delete** button to remove the specific entry.

SNMP Engine ID Settings

The Engine ID is a unique identifier used for SNMP V3 implementations on the Switch.

SNMP Engine ID Settings

Engine ID

Note: Engine ID length is 10-64, the accepted character is from 0 to F.

To change the Engine ID, type the new Engine ID value in the space provided.

The fields that can be configured are described below:

Parameter	Description
Engine ID:	The SNMP engine ID displays the identification of the SNMP engine on the Switch. The default value is suggested in RFC2271. The very first bit is 1, and the first four octets are set to the binary equivalent of the agent's SNMP management private enterprise number as assigned by IANA (Advantech is 171). The fifth octet is 03 to indicate the rest is the MAC address of this device. The sixth to eleventh octets is the MAC address.

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



NOTE: The Engine ID length is 10-64 and accepted characters can range from 0 to F.

SNMP User Table Settings

This window displays all of the SNMP User's currently configured on the Switch.

User Name	<input type="text"/>	Group Name	<input type="text"/>
SNMP Version	V3	SNMP V3 Encryption	None
Auth-Protocol by Password	MD5	Password	<input type="password"/>
Priv-Protocol by Password	None	Password	<input type="password"/>
Auth-Protocol by Key	MD5	Key	<input type="password"/>
Priv-Protocol by Key	None	Key	<input type="password"/>

Total Entries: 1

The fields that can be configured are described below:

Parameter	Description
User Name:	An alphanumeric string of up to 32 characters. This is used to identify the SNMP users.
Group Name:	This name is used to specify the SNMP group created can request SNMP messages.
SNMP Version:	V3 – Indicates that SNMP version 3 is in use.
SNMP V3 Encryption:	Use the drop-down menu to enable encryption for SNMP V3. This is only operable in SNMP V3 mode. The choices are <i>None</i> , <i>Password</i> , or <i>Key</i> .
Auth-Protocol:	<p><i>MD5</i> – Specifies that the HMAC-MD5-96 authentication level will be used. This field is only operable when V3 is selected in the SNMP Version field and the Encryption field has been checked. This field will require the user to enter a password.</p> <p><i>SHA</i> – Specifies that the HMAC-SHA authentication protocol will be used. This field is only operable when V3 is selected in the SNMP Version field and the Encryption field has been checked. This field will require the user to enter a password.</p>
Priv-Protocol:	<p><i>None</i> – Specifies that no authorization protocol is in use.</p> <p><i>DES</i> – Specifies that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field is only operable when V3 is selected in the SNMP Version field and the Encryption field has been checked. This field will require the user to enter a password.</p>

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

Click the **Delete** button to remove the specific entry.

SNMP Host Table Settings

Users can set up SNMP trap recipients for IPv4.

Add Host Table

Host IP Address

User-based Security Model

Security Level

Community String / SNMPv3 User Name

Total Entries: 0

The fields that can be configured are described below:

Parameter	Description
Host IP Address:	Type the IP address of the remote management station that will serve as the SNMP host for the Switch.
User-based Security Model:	<p><i>SNMPv1</i> – Specifies that SNMP version 1 will be used.</p> <p><i>SNMPv2</i> – Specifies that SNMP version 2 will be used.</p> <p><i>SNMPv3</i> – Specifies that SNMP version 3 will be used.</p>
Security Level:	<p><i>NoAuthNoPriv</i> – To specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level.</p> <p><i>AuthNoPriv</i> – To specify that the SNMP version 3 will be used, with an Auth-NoPriv security level.</p> <p><i>AuthPriv</i> – To specify that the SNMP version 3 will be used, with an Auth-Priv security level.</p>
Community String / SNMP V3 User Name:	Type in the community string or SNMP V3 user name as appropriate.

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

Click the **Delete** button to remove the specific entry.

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

Click the **Delete** button to remove the specific entry.

RMON Settings

On this page the user can enable or disable remote monitoring (RMON) for the rising and falling alarm trap feature for the SNMP function on the Switch.



RMON Settings

RMON Rising Alarm Trap Enabled Disabled

RMON Falling Alarm Trap Enabled Disabled

Apply


The fields that can be configured are described below:

Parameter	Description
RMON Rising Alarm Trap:	Enable this option to use the RMON Rising Alarm Trap Feature.
RMON Falling Alarm Trap:	Enable this option to use the RMON Falling Alarm Trap Feature.

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

Telnet Settings

Users can configure Telnet Settings on the Switch.



Telnet Settings

Telnet State Enabled Disabled

Port (1-65535)

Apply

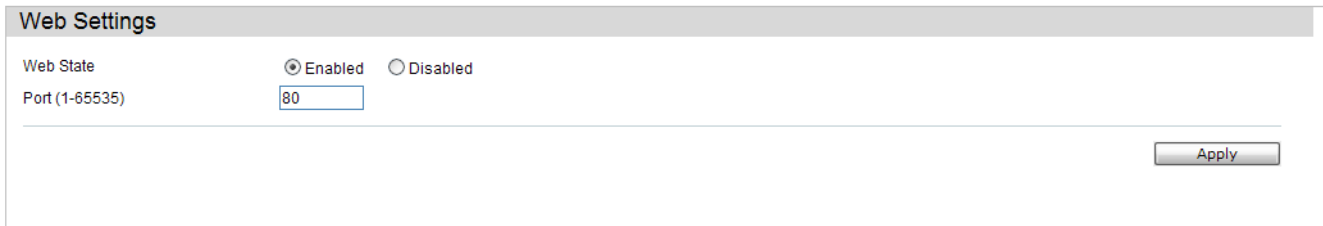
The fields that can be configured are described below:

Parameter	Description
Telnet State:	Telnet configuration is Enabled by default. If you do not want to allow configuration of the system through Telnet choose Disabled.
Port (1-65535):	The TCP port number used for Telnet management of the Switch. The “well-known” TCP port for the Telnet protocol is 23.

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

Web Settings

Users can configure the Web settings on the Switch.



Web Settings

Web State Enabled Disabled

Port (1-65535)

Apply

The fields that can be configured are described below:

Parameter	Description
Web Status:	Web-based management is Enabled by default. If you choose to disable this by clicking Disabled, you will lose the ability to configure the system through the web interface as soon as these settings are applied
Port (1-65535):	The TCP port number used for web-based management of the Switch. The “well-known” TCP port for the Web protocol is 80.

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

L2 Features

VLAN (802.1Q) Folder — 65

Spanning Tree Folder — 79

Link Aggregation Folder — 89

FDB Folder — 95

L2 Multicast Control Folder — 100

Multicast Filtering Folder — 114

LLDP Folder — 115

The screenshot shows the '802.1Q VLAN Settings' page in a network management web interface. The interface includes a top status bar with port information (FE Port-C, GE Port-C, Link Act) and a left navigation tree. The main content area displays a table of VLAN configurations.

VID	VLAN Name	Advertisement	Tagged Ports	Untagged Ports	Forbidden Ports	
1	default	Enabled		1-28		Edit Delete
99	Sales	Disabled				Edit Delete

Below the table, there is a pagination control showing '1/1' and a 'Go' button.

VLAN (802.1Q) Folder

Understanding IEEE 802.1p Priority

Priority tagging is a function defined by the IEEE 802.1p standard designed to provide a means of managing traffic on a network where many different types of data may be transmitted simultaneously. It is intended to alleviate problems associated with the delivery of time critical data over congested networks. The quality of applications that are dependent on such time critical data, such as video conferencing, can be severely and adversely affected by even very small delays in transmission.

Network devices that are in compliance with the IEEE 802.1p standard have the ability to recognize the priority level of data packets. These devices can also assign a priority label or tag to packets. Compliant devices can also strip priority tags from packets. This priority tag determines the packet's degree of expeditiousness and determines the queue to which it will be assigned.

Priority tags are given values from 0 to 7 with 0 being assigned to the lowest priority data and 7 assigned to the highest. The highest priority tag 7 is generally only used for data associated with video or audio applications, which are sensitive to even slight delays, or for data from specified end users whose data transmissions warrant special consideration.

The Switch allows you to further tailor how priority tagged data packets are handled on your network. Using queues to manage priority tagged data allows you to specify its relative priority to suit the needs of your network. There may be circumstances where it would be advantageous to group two or more differently tagged packets into the same queue. Generally, however, it is recommended that the highest priority queue, Queue 7, be reserved for data packets with a priority value of 7. Packets that have not been given any priority value are placed in Queue 0 and thus given the lowest priority for delivery.

Strict mode and weighted round robin system are employed on the Switch to determine the rate at which the queues are emptied of packets. The ratio used for clearing the queues is 4:1. This means that the highest priority queue, Queue 7, will clear 4 packets for every 1 packet cleared from Queue 0.

Remember, the priority queue settings on the Switch are for all ports, and all devices connected to the Switch will be affected. This priority queuing system will be especially beneficial if your network employs switches with the capability of assigning priority tags.

VLAN Description

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLANs can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLANs also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the

VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLANs can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

Notes about VLANs on the Switch

- No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLANs without a network device performing a routing function between the VLANs.
- The Switch supports IEEE 802.1Q VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.
- The Switch's default is to assign all ports to a single 802.1Q VLAN named "default."
- The "default" VLAN has a VID = 1.
- The member ports of Port-based VLANs may overlap, if desired.

IEEE 802.1Q VLANs

Some relevant terms:

- **Tagging** – The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** – The act of stripping 802.1Q VLAN information out of the packet header.
- **Ingress port** – A port on a switch where packets are flowing into the Switch and VLAN decisions must be made.
- **Egress port** – A port on a switch where packets are flowing out of the Switch, either to another switch or to an end station, and tagging decisions must be made.

IEEE 802.1Q (tagged) VLANs are implemented on the Switch. 802.1Q VLANs require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLANs allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

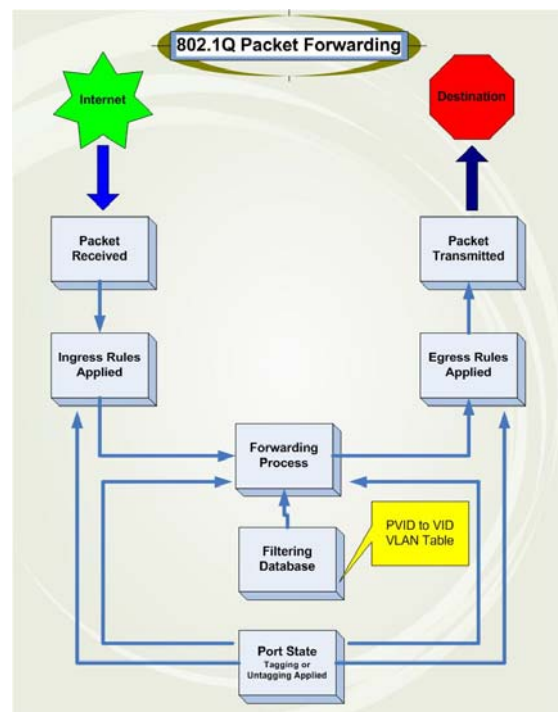
VLANs can also provide a level of security to your network. IEEE 802.1Q VLANs will only deliver packets between stations that are members of the VLAN.

Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLANs allows VLANs to work with legacy switches that don't recognize VLAN tags in packet headers. The tagging feature allows VLANs to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

The IEEE 802.1Q standard restricts the forwarding of untagged packets to the VLAN the receiving port is a member of.

The main characteristics of IEEE 802.1Q are as follows:

- Assigns packets to VLANs by filtering.
- Assumes the presence of a single global spanning tree.
- Uses an explicit tagging scheme with one-level tagging.
- 802.1Q VLAN Packet Forwarding
- Packet forwarding decisions are made based upon the following three types of rules:
 - Ingress rules – rules relevant to the classification of received frames belonging to a VLAN.
 - Forwarding rules between ports – decides whether to filter or forward the packet.
 - Egress rules – determines if the packet must be sent tagged or untagged.

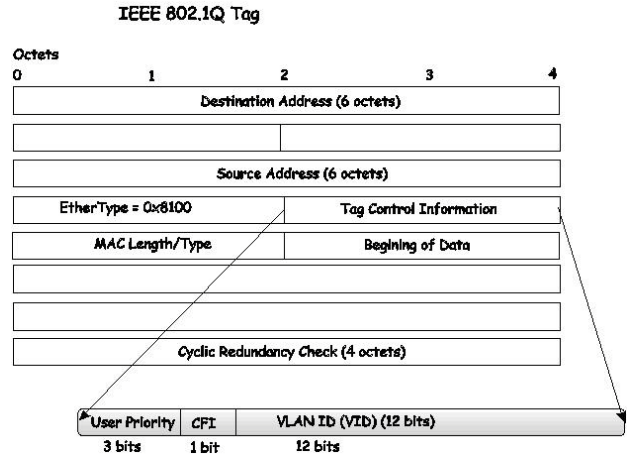


802.1Q VLAN Tags

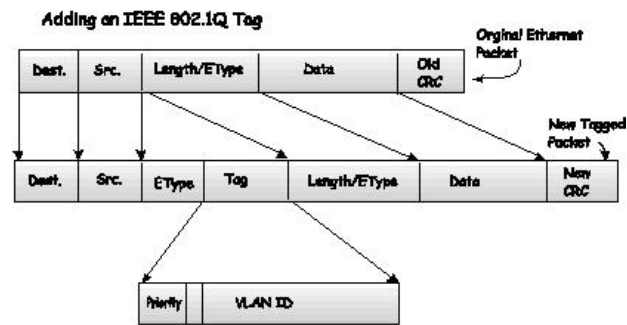
The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the EtherType field. When a packet's EtherType field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical

Format Identifier (CFI – used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of VLAN ID (VID). The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLANs can be identified.

The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.



The EtherType and VLAN ID are inserted after the MAC source address, but before the original EtherType/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.



Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLANs to span network devices (and indeed, the entire network, if all network devices are 802.1Q compliant).

Unfortunately, not all network devices are 802.1Q compliant. These devices are referred to as tag-unaware. 802.1Q devices are referred to as tag-aware.

Prior to the adoption of 802.1Q VLANs, port-based and MAC-based VLANs were in common use. These VLANs relied upon a Port VLAN ID (PVID) to forward packets. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port that corresponded to the packet's destination address (found in the Switch's forwarding table). If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the Switch will drop the packet.

Within the Switch, different PVIDs mean different VLANs (remember that two VLANs cannot communicate without an external router). So, VLAN identification

based upon the PVIDs cannot create VLANs that extend outside a given switch (or switch stack).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the Switch. If no VLANs are defined on the Switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLANs are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet-forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVIDs within the Switch to VIDs on the network. The Switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VIDs are different, the Switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VIDs as the Switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Tagging and Untagging

Every port on an 802.1Q compliant switch can be configured as tagging or untagging.

Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into and out of it.

If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. Other 802.1Q compliant devices on the network to make packet-forwarding decisions can then use the VLAN information in the tag.

Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into and out of those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Ingress Filtering

A port on a switch where packets are flowing into the Switch and VLAN decisions must be made is referred to as an ingress port. If ingress filtering is enabled for a port, the Switch will examine the VLAN information in the packet header (if present) and decide whether or not to forward the packet.

If the packet is tagged with VLAN information, the ingress port will first determine if the ingress port itself is a member of the tagged VLAN. If it is not, the packet will be dropped. If the ingress port is a member of the 802.1Q VLAN, the Switch then determines if the destination port is a member of the 802.1Q VLAN. If it is not, the packet is dropped. If the destination port is a member of the 802.1Q VLAN, the packet is forwarded and the destination port transmits it to its attached network segment.

If the packet is not tagged with VLAN information, the ingress port will tag the packet with its own PVID as a VID (if the port is a tagging port). The switch then determines if the destination port is a member of the same VLAN (has the same VID) as the ingress port. If it does not, the packet is dropped. If it has the same VID, the packet is forwarded and the destination port transmits it on its attached network segment.

This process is referred to as ingress filtering and is used to conserve bandwidth within the Switch by dropping packets that are not on the same VLAN as the ingress port at the point of reception. This eliminates the subsequent processing of packets that will just be dropped by the destination port.

Default VLANs

The Switch initially configures one VLAN, VID = 1, called “default.” The factory default setting assigns all ports on the Switch to the “default.” As new VLANs are configured in Port-based mode, their respective member ports are removed from the “default.”

Packets cannot cross VLANs. If a member of one VLAN wants to connect to another VLAN, the link must be through an external router.



NOTE: If no VLANs are configured on the Switch, then all packets will be forwarded to any destination port. Packets with unknown source addresses will be flooded to all ports. Broadcast and multicast packets will also be flooded to all ports.

An example is presented below:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7
Engineering	2	9, 10
Sales	5	1, 2, 3, 4

Port-based VLANs

Port-based VLANs limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

On port-based VLANs, NICs do not need to be able to identify 802.1Q tags in packet headers. NICs send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another switch port, VLAN considerations come into play to decide if the packet gets dropped by the Switch or delivered.

VLAN Segmentation

Take for example a packet that is transmitted by a machine on Port 1 that is a member of VLAN 2. If the destination lies on another port (found through a normal forwarding table lookup), the Switch then looks to see if the other port (Port 10) is a member of VLAN 2 (and can therefore receive VLAN 2 packets). If Port 10 is not a member of VLAN 2, then the packet will be dropped by the Switch and will not reach its destination. If Port 10 is a member of VLAN 2, the packet will go through. This selective forwarding feature based on VLAN criteria is how VLANs segment networks. The key point being that Port 1 will only transmit on VLAN 2.

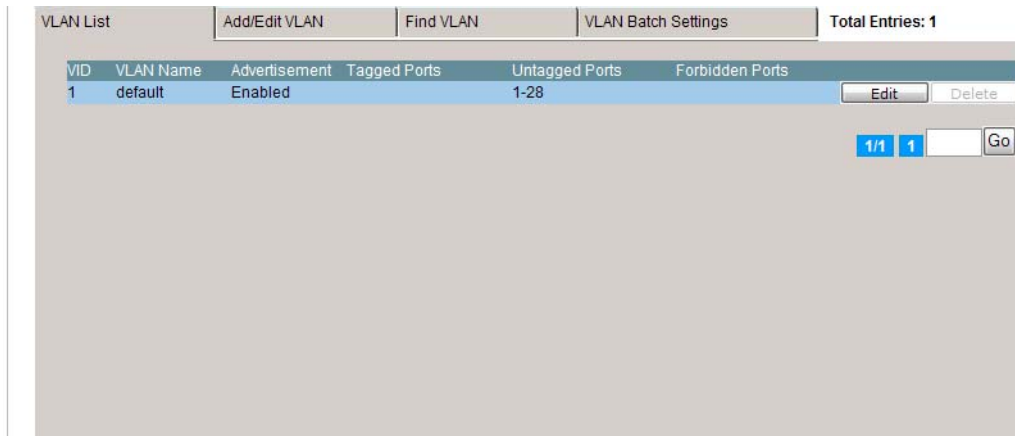
The members of a trunk group have the same VLAN setting. Any VLAN setting on the members of a trunk group will apply to the other member ports.



NOTE: In order to use VLAN segmentation in conjunction with port trunk groups, first set the port trunk group(s), and then configure the VLAN settings. To change the port trunk grouping with VLANs already in place it is unnecessary to reconfigure the VLAN settings after changing the port trunk group settings. VLAN settings will automatically change in conjunction with the change of the port trunk group settings.

802.1Q VLAN Settings

The **VLAN List** tab lists all previously configured VLANs by VLAN ID and VLAN Name.



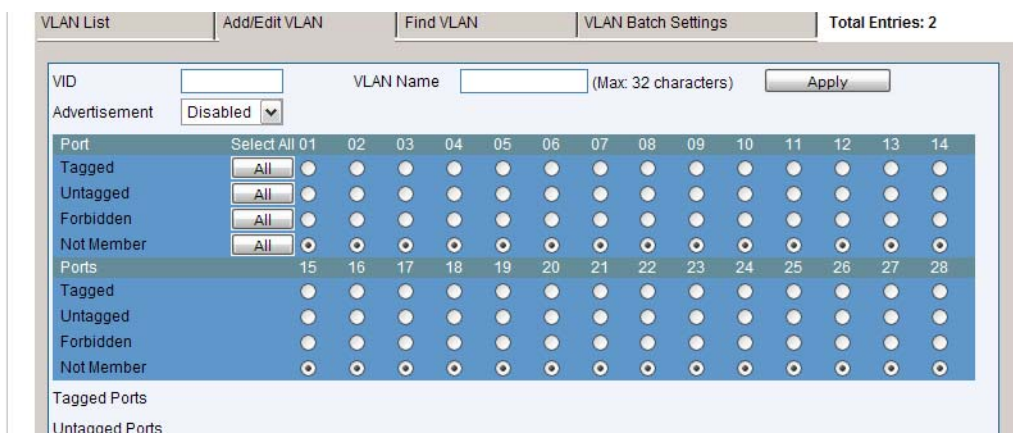
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

To create a new 802.1Q VLAN or modify an existing 802.1Q VLAN, click the **Add/Edit VLAN** tab.

A new tab will appear, as shown below, to configure the port settings and to assign a unique name and number to the new VLAN.

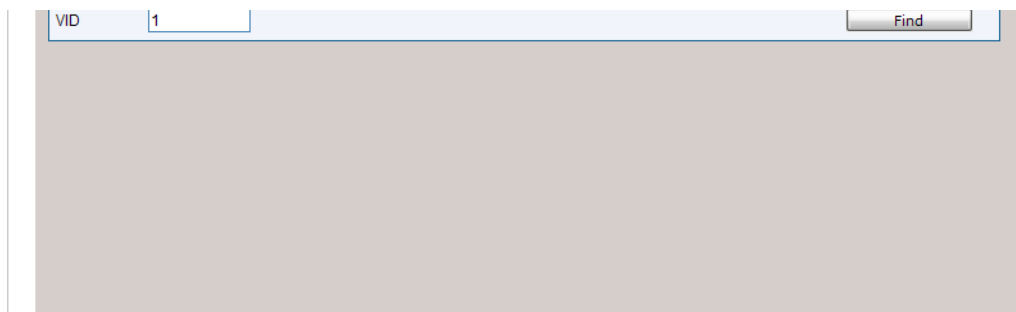


The fields that can be configured are described below:

Parameter	Description
VID (VLAN ID):	Allows the entry of a VLAN ID or displays the VLAN ID of an existing VLAN in the Add/Edit VLAN tab. VLANs can be identified by either the VID or the VLAN name.

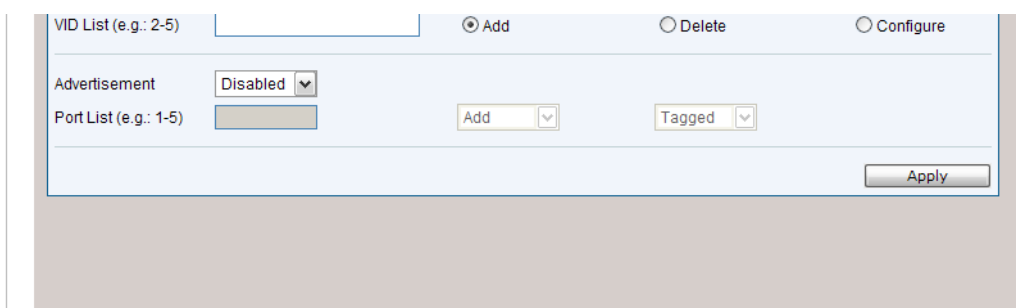
VLAN Name:	Allows the entry of a name for the new VLAN or for editing the VLAN name in the Add/Edit VLAN tab.
Advertisement:	Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Port:	Shows all ports of the Switch for the configuration option.
Tagged:	Specifies the port as 802.1Q tagging. Clicking the radio button will designate the port as tagged. Click the All button to select all ports.
Untagged:	Specifies the port as 802.1Q untagged. Clicking the radio button will designate the port as untagged. Click the All button to select all ports.
Forbidden:	Click the radio button to specify the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically. Click the All button to select all ports.
Not Member	Click the radio button to allow an individual port to be specified as a non-VLAN member. Click the All button to select all ports.

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



Enter the VLAN ID number in the field offered and then click the **Find** button. You will be redirected to the **VLAN List** tab.

To create, delete and configure a VLAN Batch entry click the **VLAN Batch Settings** tab, as shown below.



The fields that can be configured are described below:

Parameter	Description
-----------	-------------

VID List (e.g.: 2-5):	Enter a VLAN ID List that can be added, deleted or configured.
Advertisement:	Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Port List (e.g.: 1-5):	Allows an individual port list to be added or deleted as a member of the VLAN.
Tagged:	Specifies the port as 802.1Q tagged. Use the drop-down menu to designate the port as tagged.
Untagged:	Specifies the port as 802.1Q untagged. Use the drop-down menu to designate the port as untagged.
Forbidden:	Specifies the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically. Use the drop-down menu to designate the port as forbidden.

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



NOTE: The Switch supports up to 4k static VLAN entries.

GVRP Folder

GVRP Global Settings

Users can determine whether the Switch will share its VLAN configuration information with other GARP VLAN Registration Protocol (GVRP) enabled switches. In addition, Ingress Checking can be used to limit traffic by filtering incoming packets whose PVID does not match the PVID of the port. Results can be seen in the table under the configuration settings.

GVRP Global Settings

GVRP Global Settings

GVRP State Enabled Disabled Apply

The fields that can be configured are described below:

Parameter	Description
GVRP State:	Here the user can enable or disable the GVRP State.
Join Time:	Here the user can enter the Join Time value in milliseconds.
Leave Time:	Here the user can enter the Leave Time value in milliseconds.
Leave All Time:	Here the user can enter the Leave All Time value in milliseconds.
NNI BPDU Address:	Used to determine the BPDU protocol address for GVRP in service provide site. It can use an 802.1d GVRP address, 802.1ad service provider GVRP address or a user defined multicast address.

Click the **Apply** button to accept the changes made for each individual section.



NOTE: The **Leave Time** value should be greater than twice the **Join Time** value. The **Leave All Time** value should be greater than the **Leave Time** value.

GVRP Port Settings

On this page the user can configure the GVRP port parameters.

GVRP Port Settings

From Port: To Port: PVID (1-4094):
 GVRP: Ingress Checking:
 Acceptable Frame Type:

Port	PVID	GVRP	Ingress Checking	Acceptable Frame Type
1	1	Disabled	Enabled	All
2	1	Disabled	Enabled	All
3	1	Disabled	Enabled	All
4	1	Disabled	Enabled	All
5	1	Disabled	Enabled	All
6	1	Disabled	Enabled	All
7	1	Disabled	Enabled	All
8	1	Disabled	Enabled	All
9	1	Disabled	Enabled	All
10	1	Disabled	Enabled	All
11	1	Disabled	Enabled	All
12	1	Disabled	Enabled	All
13	1	Disabled	Enabled	All
14	1	Disabled	Enabled	All
15	1	Disabled	Enabled	All
16	1	Disabled	Enabled	All
17	1	Disabled	Enabled	All
18	1	Disabled	Enabled	All
19	1	Disabled	Enabled	All
20	1	Disabled	Enabled	All
21	1	Disabled	Enabled	All
22	1	Disabled	Enabled	All
23	1	Disabled	Enabled	All
24	1	Disabled	Enabled	All

The fields that can be configured are described below:

Parameter	Description
From Port:	This drop-down menu allows the selection of the beginning port for a range of ports that will be included in the Port-based VLAN.
To Port:	This drop-down menu allows the selection of the ending port for a range of ports that will be included in the Port-based VLAN.
PVID:	This field is used to manually assign a PVID to a VLAN. The Switch's default is to assign all ports to the default VLAN with a VID of 1. The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified to accept only tagged frames - as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If the port receives a packet, and Ingress filtering is <i>Enabled</i> , the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.
GVRP:	The GARP VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is <i>Disabled</i> by default.

Ingress Checking:	This drop-down menu allows the user to enable the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet. <i>Disabled</i> disables ingress filtering. Ingress checking is <i>Enabled</i> by default.
Acceptable Frame Type:	This field denotes the type of frame that will be accepted by the port. The user may choose between <i>Tagged Only</i> , which means only VLAN tagged frames will be accepted, and <i>All</i> , which mean both tagged and untagged frames will be accepted. <i>All</i> is enabled by default.

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

VLAN Counter Settings

The user can create control entry to count statistics for a specific VLAN, or to count statistics for a specific port on a specific VLAN. The statistics can be either byte count or packet count. The statistics can be counted for different frame types.

The fields that can be configured are described below:

Parameter	Description
VID List:	Specifies a list of VLANs by VLAN ID.
VLAN Name:	Specifies the VLAN name.
Ports:	To enable to count statistics by specific port on specific VLAN.
Packet Type:	This option specifies the Packet Type: <i>Broadcast</i> - Specifies to count broadcast packets. <i>Multicast</i> - Specifies to count multicast packets. <i>Unicast</i> – Specifies to count unicast packets. <i>All</i> - The statistics will be counted for all packets.
Counter Type:	This option specifies the Counter Type: <i>Packet</i> - Specifies to count at packet level. <i>Byte</i> - Specifies to count at byte level.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specific entry based on the information entered.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **View All** button to display all the existing entries.

Click the **Delete All** button to remove all the entries listed.

Spanning Tree Folder

This Switch supports three versions of the Spanning Tree Protocol: 802.1D-1998 STP, 802.1D-2004 Rapid STP, and 802.1Q-2005 MSTP. 802.1D-1998 STP will be familiar to most networking professionals. However, since 802.1D-2004 RSTP and 802.1Q-2005 MSTP have been recently introduced to Advantech managed Ethernet switches, a brief introduction to the technology is provided below followed by a description of how to set up 802.1D-1998 STP, 802.1D-2004 RSTP, and 802.1Q-2005 MSTP.

802.1Q-2005 MSTP

Multiple Spanning Tree Protocol, or MSTP, is a standard defined by the IEEE community that allows multiple VLANs to be mapped to a single spanning tree instance, which will provide multiple pathways across the network. Therefore, these MSTP configurations will balance the traffic load, preventing wide scale disruptions when a single spanning tree instance fails. This will allow for faster convergences of new topologies for the failed instance. Frames designated for these VLANs will be processed quickly and completely throughout interconnected bridges utilizing any of the three spanning tree protocols (STP, RSTP or MSTP).

This protocol will also tag BPDU packets so receiving devices can distinguish spanning tree instances, spanning tree regions and the VLANs associated with them. An MSTI ID will classify these instances. MSTP will connect multiple spanning trees with a Common and Internal Spanning Tree (CIST). The CIST will automatically determine each MSTP region, its maximum possible extent and will appear as one virtual bridge that runs a single spanning tree. Consequentially, frames assigned to different VLANs will follow different data routes within administratively established regions on the network, continuing to allow simple and full processing of frames, regardless of administrative errors in defining VLANs and their respective spanning trees.

Each switch utilizing the MSTP on a network will have a single MSTP configuration that will have the following three attributes:

1. A configuration name defined by an alphanumeric string of up to 32 characters (defined in the **MST Configuration Identification** window in the Configuration Name field).
2. A configuration revision number (named here as a Revision Level and found in the **MST Configuration Identification** window) and;
3. A 4094-element table (defined here as a VID List in the **MST Configuration Identification** window), which will associate each of the possible 4094 VLANs supported by the Switch for a given instance.

To utilize the MSTP function on the Switch, three steps need to be taken:

1. The Switch must be set to the MSTP setting (found in the **STP Bridge Global Settings** window in the STP Version field)

2. The correct spanning tree priority for the MSTP instance must be entered (defined here as a Priority in the **MSTI Config Information** window when configuring MSTI ID settings).
3. VLANs that will be shared must be added to the MSTP Instance ID (defined here as a VID List in the **MST Configuration Identification** window when configuring an MSTI ID settings).

802.1D-2004 Rapid Spanning Tree

The Switch implements three versions of the Spanning Tree Protocol, the Multiple Spanning Tree Protocol (MSTP) as defined by the IEEE 802.1Q-2005, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1D-2004 specification and a version compatible with the IEEE 802.1D-1998 STP. RSTP can operate with legacy equipment implementing IEEE 802.1D-1998; however the advantages of using RSTP will be lost.

The IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D-1998 STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 functions that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Port Transition States

An essential difference between the three protocols is in the way ports transition to a forwarding state and in the way this transition relates to the role of the port (forwarding or not forwarding) in the topology. MSTP and RSTP combine the transition states disabled, blocking and listening used in 802.1D-1998 and creates a single state Discarding. In either case, ports do not forward packets. In the STP port transition states disabled, blocking or listening or in the RSTP/MSTP port state discarding, there is no functional difference, the port is not active in the network topology. Table 7-3 below compares how the three protocols differ regarding the port state transition.

All three protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All bridges listen for BPDU packets. However, BPDU packets are sent more frequently - with every Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and thus faster topology adjustment. A drawback of 802.1D-1998 is this absence of immediate feedback from adjacent bridges.

802.1Q-2005 MSTP	802.1D-2004 RSTP	802.1D-1998 STP	Forwarding	Learning
Disabled	Disabled	Disabled	No	No
Discarding	Discarding	Blocking	No	No

Discarding	Discarding	Listening	No	No
Learning	Learning	Listening	No	Yes
Forwarding	Forwarding	Forwarding	Yes	Yes

RSTP is capable of a more rapid transition to a forwarding state - it no longer relies on timer configurations - RSTP compliant bridges are sensitive to feedback from other RSTP compliant bridge links. Ports do not need to wait for the topology to stabilize before transitioning to a forwarding state. In order to allow this rapid transition, the protocol introduces two new variables: the edge port and the point-to-point (P2P) port.

Edge Port

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

P2P Port

A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP/MSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration.

802.1D-1998/802.1D-2004/802.1Q-2005 Compatibility

MSTP or RSTP can interoperate with legacy equipment and is capable of automatically adjusting BPDU packets to 802.1D-1998 format when necessary. However, any segment using 802.1D-1998 STP will not benefit from the rapid transition and rapid topology change detection of MSTP or RSTP. The protocol also provides for a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP or MSTP.

The Spanning Tree Protocol (STP) operates on two levels:

1. On the switch level, the settings are globally implemented.
2. On the port level, the settings are implemented on a per-user-defined group of ports basis.

STP Bridge Global Settings

On this page the user can configure the STP bridge global parameters.

The fields that can be configured are described below:

Parameter	Description
STP Status:	Use the radio button to globally enable or disable STP.
STP Version:	Use the pull-down menu to choose the desired version of STP: <i>STP</i> - Select this parameter to set the Spanning Tree Protocol (STP) globally on the switch. <i>RSTP</i> - Select this parameter to set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. <i>MSTP</i> - Select this parameter to set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch.
Forwarding BPDU:	This field can be <i>Enabled</i> or <i>Disabled</i> . When <i>Enabled</i> , it allows the forwarding of STP BPDU packets from other network devices. The default is <i>Enabled</i> .
Bridge Max Age (6 – 40):	The Max Age may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. The user may choose a time between 6 and 40 seconds. The default value is 20 seconds.
Bridge Hello Time (1 – 2):	The Hello Time can be set from 1 to 2 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. This field will only appear here when STP or RSTP is selected for the STP Version. For MSTP, the Hello Time must be set on a port per port basis. The default is 2 seconds.
Bridge Forward Delay (4 – 30):	The Forward Delay can be from 4 to 30 seconds. Any port on the Switch spends this time in the listening state while moving from the blocking state to the forwarding state. The default is 15 seconds
Tx Hold Count (1- 10):	Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from 1 to 10. The default is 6.

Max Hops (6-40):	Used to set the number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out. The user may set a hop count from 6 to 40. The default is 20.
NNI BPDU Address:	Here the user can enter the NNI BPDU Address used. Among the options, the user can select either Dot1d or Dot1adb .

Click the **Apply** button to accept the changes made for each individual section.



The Bridge Hello Time cannot be longer than the Bridge Max Age. Otherwise, a configuration error will occur. Observe the following formulas when setting the above parameters:

Bridge Max Age \leq 2 x (Bridge Forward Delay - 1 second)

NOTE: Bridge Max Age $>$ 2 x (Bridge Hello Time + 1 second)

STP Port Settings

STP can be set up on a port per port basis.

External Cost (0 = Auto)	<input type="text" value="0"/>	Migrate	<input type="button" value="Yes"/>	Edge	<input type="button" value="Auto"/>
P2P	<input type="button" value="Auto"/>	Port STP	<input type="button" value="Enabled"/>	Restricted Role	<input type="button" value="False"/>
Restricted TCN	<input type="button" value="False"/>	Forward BPDU	<input type="button" value="Enabled"/>	<input type="button" value="Apply"/>	

Port	External Cost	Edge	P2P	Port STP	Restricted Role	Restricted TCN	Forward BPDU	Hello Time
1	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
2	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
3	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
4	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
5	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
6	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
7	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
8	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
9	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
10	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
11	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2

It is advisable to define an STP Group to correspond to a VLAN group of ports.

The fields that can be configured are described below:

Parameter	Description
From Port:	The beginning port in a consecutive group of ports to be configured.
To Port:	The ending port in a consecutive group of ports to be configured.
External Cost (0=Auto):	This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is 0 (auto). Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. The default port cost for a 100Mbps port is 200000 and the default port cost for a Gigabit port is 20000. Enter a value between 1 and 200000000 to determine the External Cost. The lower the number, the greater the probability the port will be chosen to forward packets.
P2P:	Choosing the <i>True</i> parameter indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports; however they are restricted in that a P2P port must operate in full duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A P2P value of <i>False</i> indicates that the port cannot have P2P status. <i>Auto</i> allows the port to have P2P status whenever possible and operate as if the P2P status were <i>True</i> . If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the P2P status changes to operate as if the P2P value were <i>False</i> . The default setting for this parameter is <i>Auto</i> .
Restricted TCN:	Topology Change Notification is a simple BPDU that a bridge sends out to its root port to signal a topology change. Restricted TCN can be toggled between <i>True</i> and <i>False</i> . If set to <i>True</i> , this stops the port from propagating received topology change notifications and topology changes to other ports. The default is <i>False</i> .
Migrate:	When operating in RSTP mode, selecting <i>Yes</i> forces the port that has been selected to transmit RSTP BPDUs.

Port STP:	This drop-down menu allows you to enable or disable STP for the selected group of ports. The default is <i>Enabled</i> .
Forward BPDU:	Use the pull-down menu to enable or disable the flooding of BPDU packets when STP is disabled.
Edge:	Choosing the <i>True</i> parameter designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge port status. Choosing the <i>False</i> parameter indicates that the port does not have edge port status. Alternatively, the <i>Auto</i> option is available.
Restricted Role:	Use the drop-down menu to toggle Restricted Role between <i>True</i> and <i>False</i> . If set to <i>True</i> , the port will never be selected to be the Root port. The default is <i>False</i> .
Hello Time (sec):	This is a per-Bridge parameter in RSTP, but it becomes a per-Port parameter in MSTP. The default value is 2 seconds.

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

MST Configuration Identification

This window allows the user to configure a MSTI instance on the Switch. These settings will uniquely identify a multiple spanning tree instance set on the Switch. The Switch initially possesses one CIST, or Common Internal Spanning Tree, of which the user may modify the parameters for but cannot change the MSTI ID for, and cannot be deleted.

MST Configuration Identification

MST Configuration Identification Settings

Configuration Name: 34:08:04:45:B4:00

Revision Level (0-65535): 0 Apply

Instance ID Settings

MSTI ID (1-15):

Type: Add VID ▼

VID List (1-4094):

Apply

Total Entries: 1

MSTI ID	VID List	
CIST	1-4094	Edit Delete

The fields that can be configured are described below:

Parameter	Description
Configuration Name:	This name uniquely identifies the MSTI (Multiple Spanning Tree Instance). If a Configuration Name is not set, this field will show the MAC address to the device running MSTP.
Revision Level (0-65535):	This value, along with the Configuration Name, identifies the MSTP region configured on the Switch.
MSTI ID:	Enter a number between 1 and 15 to set a new MSTI on the Switch.
Type:	This field allows the user to choose a desired method for altering the MSTI settings. The user has two choices: <i>Add VID</i> - Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter. <i>Remove VID</i> - Select this parameter to remove VIDs from the MSTI ID, in conjunction with the VID List parameter.
VID List (1-4094):	This field is used to specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number 1 to 4094.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

STP Instance Settings

This window displays MSTIs currently set on the Switch and allows users to change the Priority of the MSTIs.

STP Instance Settings

STP Priority Settings

MSTI ID Priority

Total Entries: 1

Instance Type	Instance Status	Instance Priority	
CIST	Disabled	32768(Bridge Priority : 32768, SYS ID Ext : 0)	<input type="button" value="Edit"/> <input type="button" value="View"/>

STP Instance Operational Status

MSTP ID	--	Designated Root Bridge	--
External Root Cost	--	Regional Root Bridge	--
Internal Root Cost	--	Designated Bridge	--
Root Port	--	Max Age	--
Forward Delay	--	Remaining Hops	--
Last Topology Change	--	Topology Changes Count	--

The fields that can be configured are described below:

Parameter	Description
MSTI ID:	Enter the MSTI ID in this field. An entry of 0 denotes the CIST (default MSTI).
Priority:	Enter the priority in this field. The available range of values is from 0 to 61440.

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

Click the **Edit** button to re-configure the specific entry.

Click the **View** button to display the information of the specific entry.

MSTP Port Information

This window displays the current MSTI configuration information and can be used to update the port configuration for an MSTI ID. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Remember that lower priority values mean higher priorities for forwarding packets.

To view the MSTI settings for a particular port, use the drop-down menu to select the Port number. To modify the settings for a particular MSTI instance, enter a value in the Instance ID field, an Internal Path Cost, and use the drop-down menu to select a Priority.

The fields that can be configured are described below:

Parameter	Description
Instance ID:	The MSTI ID of the instance to be configured. Enter a value between 0 and 15. An entry of 0 in this field denotes the CIST (default MSTI).
Internal Path Cost:	This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within an STP instance. Selecting this parameter with a value in the range of 1 to 200000000 will set the quickest route when a loop occurs. A lower Internal cost represents a quicker transmission. Selecting 0 (zero) for this parameter will set the quickest route automatically and optimally for an interface.
Priority:	Enter a value between 0 and 240 to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.

Click the **Find** button to locate a specific entry based on the information entered.

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

Click the **Edit** button to re-configure the specific entry.

Link Aggregation Folder

Understanding Port Trunk Groups

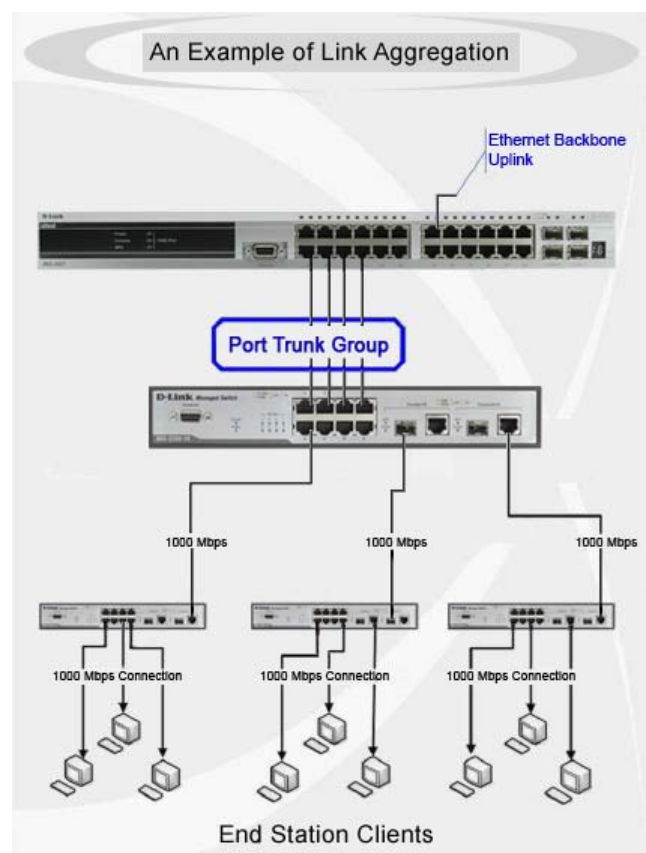
Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline. The Switch supports up to fourteen port trunk groups with two to eight ports in each group. A potential bit rate of 800 Mbps can be achieved.

The Switch treats all ports in a trunk group as a single port. Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent.

Link aggregation allows several ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single link's bandwidth.

Link aggregation is most commonly used to link a bandwidth intensive network device or devices, such as a server, to the backbone of a network.

The Switch allows the creation of up to fourteen link aggregation groups, each group consisting of 2 to 8 links (ports). The (optional) Gigabit ports can only belong to a single link aggregation group.



All of the ports in the group must be members of the same VLAN, and their STP status, static multicast, traffic control; traffic segmentation and 802.1p default priority configurations must be identical. Port locking, port mirroring and 802.1X must not be enabled on the trunk group. Further, the LACP aggregated links must all be of the same speed and should be configured as full duplex.

The Master Port of the group is to be configured by the user, and all configuration options, including the VLAN configuration that can be applied to the Master Port, are applied to the entire link aggregation group.

Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

The Spanning Tree Protocol will treat a link aggregation group as a single link, on the switch level. On the port level, the STP will use the port parameters of the Master Port in the calculation of port cost and in determining the state of the link aggregation group. If two redundant link aggregation groups are configured on the Switch, STP will block one entire group; in the same way STP will block a single port that has a redundant link.



NOTE: If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load shared among the other linked ports of the link aggregation group.

Port Trunking Settings

On this page the user can configure the port trunk settings for the switch.

Port Trunking Settings

Algorithm: Apply

Total Entries: 0

Group ID	Type	Master Port	Member Ports	Active Ports	Status	Flooding Ports

Edit Trunking Information

Group ID (1-14): Type: Master Port: State: Clear All Add

Port	01	02	03	04	05	06	07	08	09	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"/>
	<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"/>
	<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"/>

Ports

Note: Maximum 8 ports in a static trunk or LACP group.

The fields that can be configured are described below:

Parameter	Description
Algorithm:	This is the traffic hash algorithm among the ports of the link aggregation group. Options to choose from are MAC Source Dest, IP Source Dest and Lay4 Source Dest.
Group ID (1-5):	Select an ID number for the group, between 1 and 14.
Type:	This pull-down menu allows users to select between <i>Static</i> and <i>LACP</i> (Link Aggregation Control Protocol). <i>LACP</i> allows for the automatic detection of links in a Port Trunking Group.
Master Port:	Choose the Master Port for the trunk group using the pull-down menu.
State:	Use the drop-down menu to toggle between <i>Enabled</i> and <i>Disabled</i> . This is used to turn a port trunking group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control.
Member Ports:	Choose the members of a trunked group. Up to eight ports per group can be assigned to a group.
Active Ports:	Shows the ports that are currently forwarding packets.

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

Click the **Clear All** button to clear out all the information entered.

Click the **Add** button to add a new entry based on the information entered.



NOTE: The maximum number of ports that can be configured in one Static Trunk or LACP Group are **8 ports**.

LACP Port Settings

In conjunction with the Trunking window, users can create port trunking groups on the Switch. Using the following window, the user may set which ports will be active and passive in processing and sending LACP control frames.

From Port	To Port	Activity
01	01	Passive

Port	Activity
1	Passive
2	Passive
3	Passive
4	Passive
5	Passive
6	Passive
7	Passive
8	Passive
9	Passive
10	Passive
11	Passive
12	Passive
13	Passive
14	Passive
15	Passive
16	Passive
17	Passive
18	Passive
19	Passive
20	Passive
21	Passive
22	Passive
23	Passive

The fields that can be configured are described below:

Parameter	Description
From Port:	The beginning port of a consecutive group of ports may be configured starting with the selected port.
To Port:	The ending port of a consecutive group of ports may be configured ending with the selected port.
Activity:	<p><i>Active</i> - Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.</p> <p><i>Passive</i> - LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports (see above).</p>

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

FDB Folder

Static DFDB Settings Folder

Unicast Static FDB Settings

Users can set up static unicast forwarding on the Switch.

Unicast Static FDB Settings

Unicast Forwarding Settings

VLAN Name MAC Address Port

Total Entries: 0

VID	VLAN Name	MAC Address	Port

The fields that can be configured are described below:

Parameter	Description
VLAN Name:	The VLAN name of the VLAN on which the associated unicast MAC address resides.
MAC Address:	The MAC address to which packets will be statically forwarded. This must be a unicast MAC address.
Port/Drop:	Allows the selection of the port number on which the MAC address entered above resides This option could also drop the MAC address from the unicast static FDB.

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

Click the **Delete** button to remove the specific entry.

Multicast Static FDB Settings

Users can set up static multicast forwarding on the Switch.

Multicast Forwarding Settings

VID

Multicast MAC Address

Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
None	<input type="button" value="All"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	
Egress	<input type="button" value="All"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	

Egress Ports

Total Entries: 0

The fields that can be configured are described below:

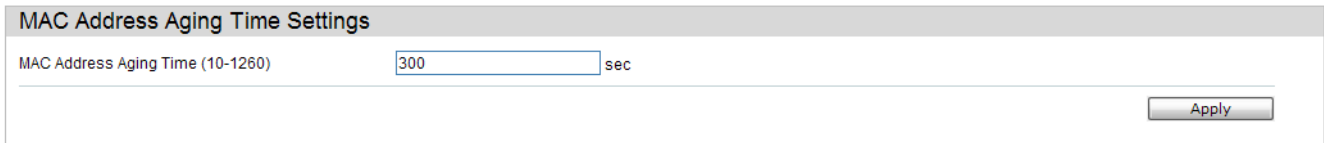
Parameter	Description
VID:	The VLAN ID of the VLAN the corresponding MAC address belongs to.
Multicast MAC Address:	The static destination MAC address of the multicast packets. This must be a multicast MAC address.
Port:	Allows the selection of ports that will be members of the static multicast group and ports that are either forbidden from joining dynamically, or that can join the multicast group dynamically, using GMRP. The options are: <i>None</i> - No restrictions on the port dynamically joining the multicast group. When <i>None</i> is chosen, the port will not be a member of the Static Multicast Group. Click the All button to select all the ports. <i>Egress</i> - The port is a static member of the multicast group. Click the All button to select all the ports.

Click the **Clear All** button to clear out all the information entered.

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

MAC Address Aging Time Settings

Users can configure the MAC Address aging time on the Switch.



MAC Address Aging Time (10-1260) sec Apply

The fields that can be configured are described below:

Parameter	Description
MAC Address Aging Time (10-1260):	This field specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). To change this option, type in a different value representing the MAC address' age-out time in seconds. The MAC Address Aging Time can be set to any value between 10 and 1260 seconds. The default setting is 300 seconds.

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

MAC Address Table

This allows the Switch's MAC address forwarding table to be viewed. When the Switch learns an association between a MAC address, VLAN and a port number, it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch.

Port: 01

VLAN Name:

MAC Address: 00-00-00-00-00-00

Total Entries: 1

VID	VLAN Name	MAC Address	Port	Type
1	default	34-08-04-45-B4-00	CPU	Self

The fields that can be configured are described below:

Parameter	Description
Port:	The port to which the MAC address below corresponds.
VLAN Name:	Enter a VLAN Name for the forwarding table to be browsed by.
MAC Address:	Enter a MAC address for the forwarding table to be browsed by.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear Dynamic Entries** button to delete all dynamic entries of the address table.

Click the **View All Entries** button to display all the existing entries.

Click the **Clear All Entries** button to remove all the entries listed in the table.

Click the **Add to Static MAC table** button to add the specific entry to the Static MAC table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ARP and FDB Table

On this page the user can find the ARP and FDB table parameters.

ARP & FDB Table

Port

MAC Address

IP Address

Total Entries: 0

Interface	IP Address	MAC Address	VLAN Name	Port

The fields that can be configured are described below:

Parameter	Description
Port:	Here the user can select the port number to use for this configuration.
MAC Address:	Here the user can enter the MAC address to use for this configuration.
IP Address:	Here the user can enter the IP address the use for this configuration.

Click the **Find by Port** button to locate a specific entry based on the port number selected.

Click the **Find by MAC** button to locate a specific entry based on the MAC address entered.

Click the **Find by IP Address** button to locate a specific entry based on the IP address entered.

Click the **View All Entries** button to display all the existing entries.

Click the **Add to IP MAC Port Binding Table** to add the specific entry to the IP MAC Port Binding Table.

L2 Multicast Control Folder

IGMP Snooping Folder

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host. When enabled for IGMP snooping, the Switch can open or close a port to a specific device based on IGMP messages passing through the Switch.

IGMP Snooping Settings

In order to use IGMP Snooping it must first be enabled for the entire Switch under IGMP Global Settings at the top of the window. You may then fine-tune the settings for each VLAN by clicking the corresponding **Edit** button. When enabled for IGMP snooping, the Switch can open or close a port to a specific multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa. The Switch monitors IGMP messages and discontinues forwarding multicast packets when there are no longer hosts requesting that they continue.

The fields that can be configured are described below:

Parameter	Description
IGMP Snooping State:	Here the user can enable or disable the IGMP Snooping state.
Max Learning Entry Value:	Here the user can enter the maximum learning entry value.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Edit** button to configure the IGMP Snooping Parameters Settings.

Click the [Modify Router Port](#) link to configure the IGMP Snooping Router Port Settings.

After clicking the **Edit** button, the following page will appear:

IGMP Snooping Parameters Settings			
VID	1	VLAN Name	default
Querier IP	0.0.0.0		
Querier Expiry Time	0 secs	Query Interval (1-65535)	125 sec
Max Response Time (1-25)	10 sec	Robustness Value (1-255)	2
Last Member Query Interval (1-25)	1 sec	Data Driven Group Expiry Time (1-65535)	260 sec
Querier State	Disabled	Fast Leave	Disabled
State	Disabled	Report Suppression	Enabled
Data Driven Learning State	Enabled	Data Driven Learning Aged Out	Disabled
Version	3	Querier Role	Non-Querier

The fields that can be configured are described below:

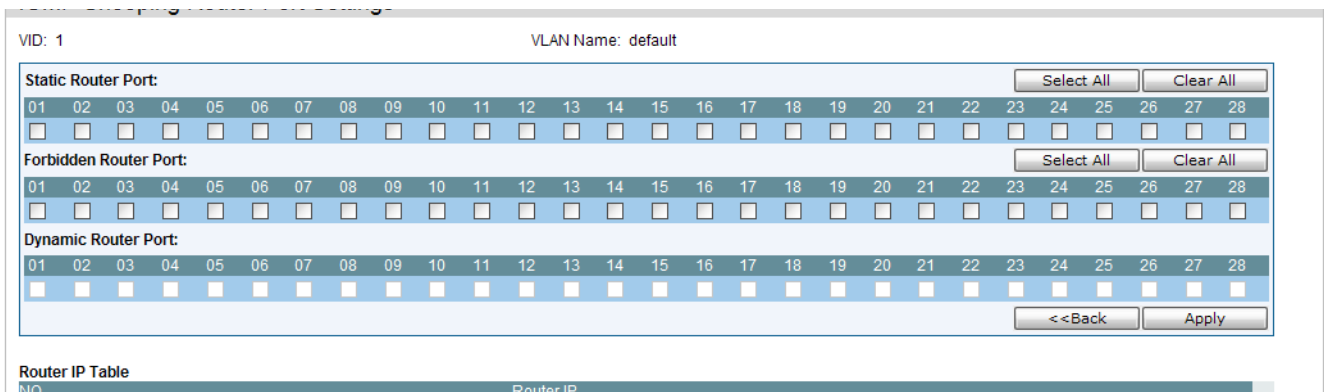
Parameter	Description
VID:	Specify the name of the VLAN ID.
VLAN Name:	Specify the name of the VLAN for which IGMP snooping querier is to be configured.
Rate Limit:	Here is displayed the rate of IGMP control packets that the switch can process on a specific port/VLAN. The rate is specified in packet per second. The packets that exceed the limited rate will be dropped.
Querier IP:	Displays the querier IP address
Querier Expiry Time:	Displays the querier expiry time.
Query Interval:	Specify the amount of time in seconds between general query transmissions. The default setting is 125 seconds..
Max Response Time:	Specify the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.
Robustness Value:	Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness value is used in calculating the following IGMP message intervals: By default, the robustness variable is set to 2.
Last Member Query Interval:	Specify the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group.
Data Drive Group Expiry Time:	Specify the data driven group lifetime in seconds.
Querier State:	Specify to enable or disable the querier state.
Fast Leave:	Enable or disable the IGMP snooping fast leave function. If enabled, the membership is immediately removed when the system receive the IGMP leave message.

State:	<p>If the state is enable, it allows the switch to be selected as a IGMP Querier (sends IGMP query packets). If the state is disabled, then the switch can not play the role as a querier.</p> <p>NOTE: that if the Layer 3 router connected to the switch provides only the IGMP proxy function but does not provide the multicast routing function, then this state must be configured as disabled. Otherwise, if the Layer 3 router is not selected as the querier, it will not send the IGMP query packet. Since it will not also send the multicast-routing protocol packet, the port will be timed out as a router port.</p>
Report Suppression:	When enabled, multiple IGMP reports or leave for a specific (S, G) will be integrated into one report only before sending to the router port.
Data Driven Learning State:	Specify to enable or disable the data driven learning state.
Data Drive Learning Aged Out:	Specify to enable or disable the data drive learning aged out option.
Version:	Specify the version of IGMP packet that will be sent by this port. If a IGMP packet received by the interface has a version higher than the specified version, this packet will be dropped.
Querier Role:	Displays the querier role.

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

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the [Modify Router Port](#) link, the following page will appear:



The fields that can be configured are described below:

Parameter	Description
Static Router Port:	This section is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router regardless of the protocol.

Forbidden Router Port:	This section is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.
Dynamic Router Port:	Displays router ports that have been dynamically configured.
Ports:	Select the appropriate ports individually to include them in the Router Port configuration.

Click the Select All button to select all the ports for configuration.

Click the Clear All button to unselect all the ports for configuration.

Click the Apply button to accept the changes made.

Click the <<Back button to discard the changes made and return to the previous page.

IGMP Snooping Static Group Settings

Users can view the Switch's IGMP Snooping Group Table. IGMP Snooping allows the Switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the Switch.

The fields that can be configured are described below:

Parameter	Description
VLAN Name:	The <i>VLAN Name</i> of the multicast group.
VID List:	The <i>VID List</i> of the multicast group.
IPv4 Address:	Enter the IPv4 address.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Create** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specific entry based on the information entered.

Click the **View All** button to display all the existing entries.

Click the **Edit** button to re-configure the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following page will appear:

Click the **Select All** button to select all the ports for configuration.

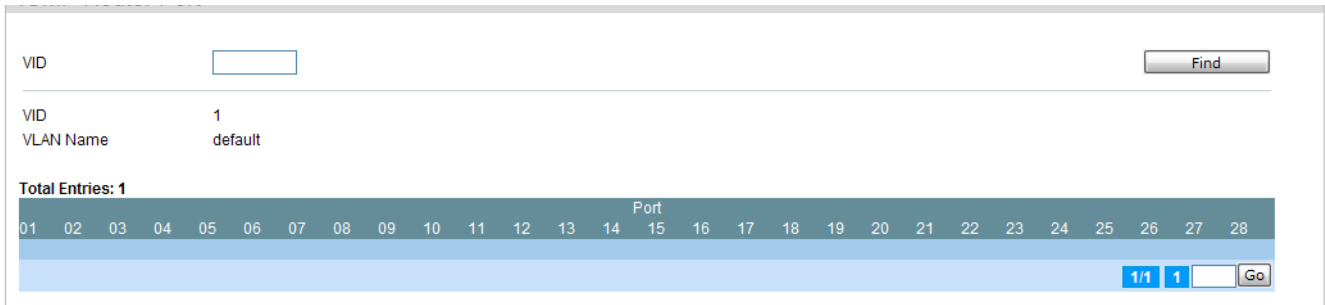
Click the **Clear All** button to unselect all the ports for configuration.

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

Click the **<<Back** button to discard the changes made and return to the previous page.

IGMP Router Port

Users can display which of the Switch's ports are currently configured as router ports. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by S. A router port that is dynamically configured by the Switch is designated by D, while a Forbidden port is designated by F.



VID

VID 1
VLAN Name default

Total Entries: 1

Port																											
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

1/1 1

Enter a VID (VLAN ID) in the field at the top of the window.

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.



NOTE: The abbreviations used on this page are **Static Router Port (S)**, **Dynamic Router Port (D)** and **Forbidden Router Port (F)**.

IGMP Snooping Group

Users can view the Switch's IGMP Snooping Group Table. IGMP Snooping allows the Switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the Switch.

The screenshot shows the 'IGMP Snooping Group' configuration page. It includes search filters for VLAN Name, VID List, Port List, and Group IPv4 Address. There are also checkboxes for 'Data Driven' and buttons for 'Find', 'Clear Data Driven', 'View All', and 'Clear All Data Driven'. Below the search area, it indicates 'Total Entries: 0' and shows a table header with columns: VID, VLAN Name, Source, Group, Member Port, Router Port, Group Type, Up Time, Expiry Time, and Filter Mode.

The user may search the IGMP Snooping Group Table by either *VLAN Name* or *VID List* by entering it in the top left hand corner and clicking **Find**.

The fields that can be configured are described below:

Parameter	Description
VLAN Name:	The VLAN Name of the multicast group.
VID List:	The VLAN ID list of the multicast group.
Port List:	Specifies the port number(s) used to find a multicast group.
Group IPv4 Address:	Enter the IPv4 address.
Data Driven:	If Data Drive is selected, only data driven groups will be displayed.

Click the **Clear Data Driven** button to delete the specific IGMP snooping group which is learned by the Data Driven feature of the specified VLAN.

Click the **View All** button to display all the existing entries.

Click the **Clear All Data Driven** button to delete all IGMP snooping groups which is learned by the Data Driven feature of specified VLANs.

IGMP Snooping Forwarding Table

This page displays the switch's current IGMP snooping forwarding table. It provides an easy way for user to check the list of ports that the multicast group comes from and specific sources that it will be forwarded to. The packet comes from the source VLAN. They will be forwarded to the forwarding VLAN. The IGMP snooping further restricts the forwarding ports.

IGMP Snooping Forwarding Table

VLAN Name
 VID List (e.g.: 1, 4-6)

Total Entries: 0

VLAN Name	Source IP	Multicast Group	Port Member

The fields that can be configured are described below:

Parameter	Description
VLAN Name:	The VLAN Name of the multicast group.
VID List:	The VLAN ID list of the multicast group.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **View All** button to display all the existing entries.

IGMP Host Table

On this page the user can view the IGMP host table.

IGMP Host Table

VLAN Name
 VID List (e.g.: 1, 4-6)
 Port List (e.g.: 1, 3-5)
 Group Address (e.g.: 224.1.1.1)

Total Entries: 0

VID	Group	Port	Host

The fields that can be configured are described below:

Parameter	Description
VLAN Name:	The VLAN Name of the multicast group.
VID List:	The VLAN ID list of the multicast group.
Port List:	The <i>Port List</i> of the multicast group.
Group Address:	The <i>Group Address</i> of the multicast group.

Click the **Find** button to locate a specific entry based on the information entered.

IP Multicast VLAN Replication Folder

In a switching environment, multiple VLANs may exist. Every time a multicast query passes through the Switch, the switch must forward separate different copies of the data to each VLAN on the system, which, in turn, increases data traffic and may clog up the traffic path. To lighten the traffic load, multicast VLANs may be incorporated. These multicast VLANs will allow the Switch to forward this multicast traffic as one copy to recipients of the multicast VLAN, instead of multiple copies.

Regardless of other normal VLANs that are incorporated on the Switch, users may add any ports to the multicast VLAN where they wish multicast traffic to be sent. Users are to set up a source port, where the multicast traffic is entering the switch, and then set the ports where the incoming multicast traffic is to be sent. The source port cannot be a recipient port and if configured to do so, will cause error messages to be produced by the switch. Once properly configured, the stream of multicast data will be relayed to the receiver ports in a much more timely and reliable fashion.

Restrictions and Provisos:

The Multicast VLAN feature of this Switch does have some restrictions and limitations, such as:

1. Multicast VLANs can be implemented on edge and non-edge switches.
2. Member ports and source ports can be used in multiple ISM VLANs. But member ports and source ports cannot be the same port in a specific ISM VLAN.
3. The Multicast VLAN is exclusive with normal 802.1q VLANs, which means that VLAN IDs (VIDs) and VLAN Names of 802.1q VLANs and ISM VLANs cannot be the same. Once a VID or VLAN Name is chosen for any VLAN, it cannot be used for any other VLAN.
4. The normal display of configured VLANs will not display configured Multicast VLANs.
5. Once an ISM VLAN is enabled, the corresponding IGMP snooping state of this VLAN will also be enabled. Users cannot disable the IGMP feature for an enabled ISM VLAN.
6. One IP multicast address cannot be added to multiple ISM VLANs, yet multiple Ranges can be added to one ISM VLAN.

IP Multicast VLAN Replication Global Settings

On this page the user can configure the IP multicast VLAN replication parameters.

IP Multicast VLAN Replication Global Settings

Global State Enabled Disabled

TTL Decrease No Decrease

Source MAC Address Replace No Replace

The fields that can be configured are described below:

Parameter	Description
Global State:	Here the user can enable or disable the global state feature.
TTL:	Here the user can select to decrease or no decrease the Time to live (TTL) value in the packets.
Source MAC Address:	Here the user can select to replace or not to replace the Source MAC Address of the packet.

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

IP Multicast VLAN Replication Settings

On this page the user can add and view the IP multicast VLAN replication table.

The fields that can be configured are described below:

Parameter	Description
Entry Name:	Here the user can enter a Multicast VLAN Replication entry name.

Click the **Add** button to add a new entry based on the information entered.

Click the **Find by Hardware** the find an entry based on the hardware.

Click the **View All** button to display all the existing entries.

Click the **Edit** button under **Source** to re-configure the specific entry.

Click the **Edit** button under **Destination** to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

After clicking the **Edit** button under **Source**, the following page will appear:

The fields that can be configured are described below:

Parameter	Description
Entry Name:	Here the IP Multicast VLAN Replication Source entry name will be displayed.
VID / VLAN Name:	Here the user can choose to enter a VLAN Name, VID value or Group value.

Action:	Here the user can select the action to be taken.
Multicast Address List:	Here the user can enter the multicast address list.
Source Address:	Here the user can enter the source address.

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

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Edit** button under **Destination**, the following page will appear:

IP Multicast VLAN Replication Destination Settings

Entry Name:

VID List / VLAN Name: VID List VLAN Name

Action: ▼

Port List (e.g.: 1, 6-9):

Total Entries: 0

Entry NO.	VID	VLAN Name	PortList

The fields that can be configured are described below:

Parameter	Description
Entry Name:	Here the IP Multicast VLAN Replication Destination entry name will be displayed.
VID / VLAN Name:	Here the user can choose to enter a VLAN Name, VID value or Group value.
Action:	Here the user can select the action to be taken.
Multicast Address List:	Here the user can enter the multicast address list.
Source Address:	Here the user can enter the source address.

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

Click the **<<Back** button to discard the changes made and return to the previous page.

Multicast Filtering Folder

Multicast Filtering Mode

Users can configure the multicast filtering mode.

The fields that can be configured are described below:

Parameter	Description
VLAN Name/VID List:	The VLAN to which the specified filtering action applies. Tick the All option to apply this feature to all the VLANs.
Multicast Filtering Mode:	This drop-down menu allows you to select the action the Switch will take when it receives a multicast packet that requires forwarding to a port in the specified VLAN. <i>Forward Unregistered Groups</i> – This will instruct the Switch to forward a multicast packet whose destination is an unregistered multicast group residing within the range of ports specified above. <i>Filter Unregistered Groups</i> – This will instruct the Switch to filter any multicast packets whose destination is an unregistered multicast group residing within the range of ports specified above.

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

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

LLDP Folder

The Link Layer Discovery Protocol (LLDP) allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN. The major capabilities provided by this system is that it incorporates the station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station's point of attachment to the IEEE 802 LAN required by those management entity or entities.

The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) through a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP Folder

LLDP Global Settings

On this page the user can configure the LLDP global parameters.

LLDP State	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled	<input type="button" value="Apply"/>
LLDP Forward Message	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled	<input type="button" value="Apply"/>
Message TX Interval (5-32768)	<input type="text" value="30"/>	sec	
Message TX Hold Multiplier (2-10)	<input type="text" value="4"/>		
LLDP Reinit Delay (1-10)	<input type="text" value="2"/>	sec	
LLDP TX Delay (1-8192)	<input type="text" value="2"/>	sec	
LLDP Notification Interval (5-3600)	<input type="text" value="5"/>	sec	<input type="button" value="Apply"/>
LLDP System Information			
Chassis ID Subtype	MAC Address		
Chassis ID	34-08-04-45-B4-00		
System Name			

The fields that can be configured are described below:

Parameter	Description
LLDP State:	Here the user can enable or disable the LLDP feature.
LLDP Forward Message:	When LLDP is disabled this function controls the LLDP packet forwarding message based on individual ports. If LLDP is enabled on a port it will flood the LLDP packet to all ports that have the same port VLAN and will advertise to other stations attached to the same IEEE 802 LAN.
Message TX Interval:	This interval controls how often active ports retransmit advertisements to their neighbors. To change the packet transmission interval, enter a value in seconds (5 to 32768).
Message TX Hold Multiplier:	This function calculates the Time-to-Live for creating and transmitting the LLDP advertisements to LLDP neighbors by changing the multiplier used by an LLDP Switch. When the Time-to-Live for an advertisement expires the advertised data is then deleted from the neighbor Switch's MIB.
LLDP Reinit Delay:	The LLDP re-initialization delay interval is the minimum time that an LLDP port will wait before reinitializing after receiving an LLDP disable command. To change the LLDP re-init delay, enter a value in seconds (1 to 10).
LLDP TX Delay:	LLDP TX Delay allows the user to change the minimum time delay interval for any LLDP port which will delay advertising any successive LLDP advertisements due to change in the LLDP MIB content. To change the LLDP TX Delay, enter a value in seconds (1 to 8192).
LLDP Notification interval:	LLDP Notification Interval is used to send notifications to configured SNMP trap receiver(s) when an LLDP change is detected in an advertisement received on the port from an LLDP neighbor. To set the LLDP Notification Interval, enter a value in seconds (5 to 3600).

Click the **Apply** button to accept the changes made for each individual section.

LLDP Port Settings

On this page the user can configure the LLDP port parameters.

Note: The IPv4 address should be the switch's address.

Port ID	Notification	Admin Status	IPv4 Address
1	Disabled	TX and RX	
2	Disabled	TX and RX	
3	Disabled	TX and RX	
4	Disabled	TX and RX	
5	Disabled	TX and RX	
6	Disabled	TX and RX	
7	Disabled	TX and RX	
8	Disabled	TX and RX	
9	Disabled	TX and RX	
10	Disabled	TX and RX	
11	Disabled	TX and RX	
12	Disabled	TX and RX	

The fields that can be configured are described below:

Parameter	Description
From Port – To Port:	Here the user can select the ports used for this configuration.
Notification:	Use the pull-down menu to enable or disable the status of the LLDP notification. This function controls the SNMP trap however it cannot implement traps on SNMP when the notification is disabled.
Admin Status:	<p>This function controls the local LLDP agent and allows it to send and receive LLDP frames on the ports. This option contains TX, RX, TX And RX or Disabled.</p> <p><i>TX</i>: the local LLDP agent can only transmit LLDP frames.</p> <p><i>RX</i>: the local LLDP agent can only receive LLDP frames.</p> <p><i>TX And RX</i>: the local LLDP agent can both transmit and receive LLDP frames.</p> <p><i>Disabled</i>: the local LLDP agent can neither transmit nor receive LLDP frames. The default value is TX And RX.</p>
Subtype:	Here the user can select the type of the IP address information will be sent.
Action:	Here the user can enable or disable the action field.
Address:	Here the user can enter the IP address will that be sent.

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



NOTE: The IPv4 or IPv6 address entered here should be an existing LLDP management IP address.

LLDP Management Address List

On this page the user can view the LLDP management address list.

LLDP Management Address List

IPv4 Address

Subtype	Address	IF Type	OID	Advertising Ports
IPv4	12.78.62.41	IfIndex	1.3.6.1.4.1.10297.2....	

The fields that can be configured are described below:

Parameter	Description
IPv4/IPv6:	Here the user can select either IPv4 or IPv6.
Address:	Enter the management IP address or the IP address of the entity you wish to advertise to here. The IPv4 address is a management IP address so the IP information will be sent with the frame when the mgt_addr config is enabled.

Click the **Find** button to locate a specific entry based on the information entered.

LLDP Basic TLVs Settings

TLV stands for Type-length-value, which allows the specific sending information as a TLV element within LLDP packets. This window is used to enable the settings for the Basic TLVs Settings. An active LLDP port on the Switch always included mandatory data in its outbound advertisements. There are four optional data types that can be configured for an individual port or group of ports to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type includes four basic types of information (end of LLDPDU TLV, chassis ID TLV, port ID TLV, and Time to Live TLV). The mandatory data types cannot be disabled. There are also four data types which can be optionally selected. These include Port Description, System Name, System Description and System Capability.

Port	Port Description	System Name	System Description	System Capabilities
1	Disabled	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled	Disabled
3	Disabled	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled	Disabled
9	Disabled	Disabled	Disabled	Disabled
10	Disabled	Disabled	Disabled	Disabled
11	Disabled	Disabled	Disabled	Disabled
12	Disabled	Disabled	Disabled	Disabled
13	Disabled	Disabled	Disabled	Disabled
14	Disabled	Disabled	Disabled	Disabled
15	Disabled	Disabled	Disabled	Disabled

The fields that can be configured are described below:

Parameter	Description
From Port – To Port:	Here the user can enter the port range to use for this configuration.
Port Description:	Here the user can enable or disable the Port Description option.
System Name:	Here the user can enable or disable the System Name option.
System Description:	Here the user can enable or disable the System Description option.
System Capabilities:	Here the user can enable or disable the System Capabilities option.

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

LLDP Dot1 TLVs Settings

LLDP Dot1 TLVs are organizationally specific TLVs which are defined in IEEE 802.1 and used to configure an individual port or group of ports to exclude one or more of the IEEE 802.1 organizational port VLAN ID TLV data types from outbound LLDP advertisements.

Port	PVID State	VID	VLAN Name State	VID	Protocol Identity State	Protocol Identity
1	Disabled		Disabled		Disabled	
2	Disabled		Disabled		Disabled	
3	Disabled		Disabled		Disabled	
4	Disabled		Disabled		Disabled	
5	Disabled		Disabled		Disabled	
6	Disabled		Disabled		Disabled	
7	Disabled		Disabled		Disabled	
8	Disabled		Disabled		Disabled	
9	Disabled		Disabled		Disabled	
10	Disabled		Disabled		Disabled	
11	Disabled		Disabled		Disabled	
12	Disabled		Disabled		Disabled	
13	Disabled		Disabled		Disabled	

The fields that can be configured are described below:

Parameter	Description
From Port – To Port:	Here the user can enter the port range to use for this configuration.
Dot1 TLV PVID:	Here the user can enable or disable and configure the Dot1 TLV PVID option.
Dot1 TLV Protocol VLAN:	Here the user can enable or disable and configure the Dot1 TLV Protocol VLAN option. After enabling this option to the user can select to use either VLAN Name , VID List or All in the next drop-down menu. After selecting this, the user can enter either the VLAN Name or VID List value in the space provided.
Dot1 TLV VLAN:	Here the user can enable or disable and configure the Dot1 TLV VLAN option. After enabling this option to the user can select to use either VLAN Name , VID List or All in the next drop-down menu. After selecting this, the user can enter either the VLAN Name or VID List value in the space provided.
Dot1 TLV Protocol Identity:	Here the user can enable or disable and configure the Dot1 TLV Protocol Identity option. After enabling this option the user can select to either use EAPOL , LACP , GVRP , STP , or All .

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

LLDP Dot3 TLVs Settings

This window is used to configure an individual port or group of ports to exclude one or more IEEE 802.3 organizational specific TLV data type from outbound LLDP advertisements.

Port	MAC / PHY Configuration Status	Link Aggregation	Maximum Frame Size
1	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled
3	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled
9	Disabled	Disabled	Disabled
10	Disabled	Disabled	Disabled
11	Disabled	Disabled	Disabled
12	Disabled	Disabled	Disabled
13	Disabled	Disabled	Disabled
14	Disabled	Disabled	Disabled
15	Disabled	Disabled	Disabled

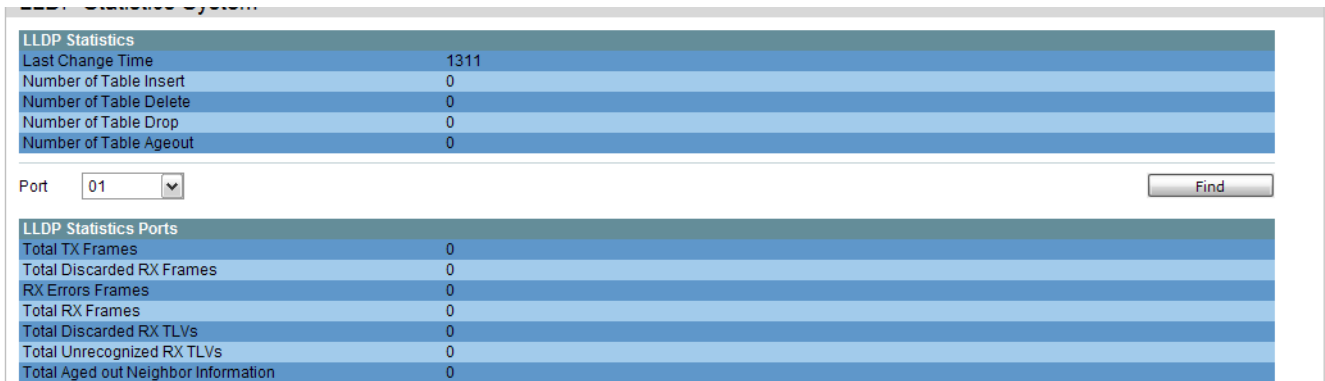
The fields that can be configured are described below:

Parameter	Description
From Port – To Port:	Here the user can enter the port range to use for this configuration.
MAC / PHY Configuration Status:	This TLV optional data type indicates that the LLDP agent should transmit the MAC/PHY configuration/status TLV. This indicates it is possible for two ends of an IEEE 802.3 link to be configured with different duplex and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port supports the auto-negotiation function, whether the function is enabled, whether it has auto-negotiated advertised capability, and what is the operational MAU type. The default state is Disabled.
Link Aggregation:	The Link Aggregation option indicates that LLDP agents should transmit 'Link Aggregation TLV'. This indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in an aggregated link, and what is the aggregated port ID. The default state is Disabled.
Maximum Frame Size:	The Maximum Frame Size indicates that LLDP agent should transmit 'Maximum-frame-size TLV'. The default state is Disabled.

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

LLDP Statistics System

The LLDP Statistics System page allows you an overview of the neighbor detection activity, LLDP Statistics and the settings for individual ports on the Switch. Select a **Port** number and click the **Find** button to view statistics for a certain port.



LLDP Statistics	
Last Change Time	1311
Number of Table Insert	0
Number of Table Delete	0
Number of Table Drop	0
Number of Table Ageout	0

Port:

LLDP Statistics Ports	
Total TX Frames	0
Total Discarded RX Frames	0
RX Errors Frames	0
Total RX Frames	0
Total Discarded RX TLVs	0
Total Unrecognized RX TLVs	0
Total Aged out Neighbor Information	0

LLDP Local Port Information

The LLDP Local Port Information page displays the information on a per port basis currently available for populating outbound LLDP advertisements in the local port brief table shown below.

Port	MAC Address	Port ID	Neighbor Port
2	MAC Address	34-08-04-45-B4-65	Advantech EKI-4...
3	MAC Address	34-08-04-45-B4-66	Advantech EKI-4...
4	MAC Address	34-08-04-45-B4-67	Advantech EKI-4...
5	MAC Address	34-08-04-45-B4-68	Advantech EKI-4...
6	MAC Address	34-08-04-45-B4-69	Advantech EKI-4...
7	MAC Address	34-08-04-45-B4-6A	Advantech EKI-4...
8	MAC Address	34-08-04-45-B4-6B	Advantech EKI-4...
9	MAC Address	34-08-04-45-B4-6C	Advantech EKI-4...
10	MAC Address	34-08-04-45-B4-6D	Advantech EKI-4...
11	MAC Address	34-08-04-45-B4-6E	Advantech EKI-4...
12	MAC Address	34-08-04-45-B4-6F	Advantech EKI-4...
13	MAC Address	34-08-04-45-B4-70	Advantech EKI-4...
14	MAC Address	34-08-04-45-B4-71	Advantech EKI-4...
15	MAC Address	34-08-04-45-B4-72	Advantech EKI-4...
16	MAC Address	34-08-04-45-B4-73	Advantech EKI-4...
17	MAC Address	34-08-04-45-B4-74	Advantech EKI-4...
18	MAC Address	34-08-04-45-B4-75	Advantech EKI-4...

To view the normal LLDP Local Port information page per port, click the **Show Normal** button.

To view the brief LLDP Local Port information page per port, click the **Show Brief** button.

LLDP Local Port Information

LLDP Local Port Normal Table

Port:

LLDP Normal Ports	
Port ID Subtype	MAC Address
Port ID	34-08-04-45-B4-64
Port Description	Advantech EKI-4668C R1.01.B010 Port 1 on Unit 1
Port PVID	1
Management Address Count	Show Detail
VLAN Entries	Show Detail
Protocol Identity Entries Count	Show Detail
MAC / PHY Configuration/Status	Show Detail
Link Aggregation	Show Detail
Maximum Frame Size	1536

Select a **Port** number and click the **Find** button to locate a specific entry.

To view more details about, for example, the **Management Address Count**, click on the [Show Detail](#) hyperlink.

LLDP Local Port Information

LLDP Local Management Address Detail Table

Total Entries: 2

Port	Subtype	Address	IF Type	OID
1	IPv4	10.78.62.40	IfIndex	1.3.6.1.4.1.10297.2....
1	IPv4	47.100.100.99	IfIndex	1.3.6.1.4.1.10297.2....

Click the **<<Back** button to return to the previous page.

LLDP Remote Port Information

This page displays port information learned from the neighbors. The switch receives packets from a remote station but is able to store the information as local.

LLDP Remote Port Information

LLDP Remote Port Brief Table

Port

Total Entries: 0

Entity	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description
--------	--------------------	------------	-----------------	---------	------------------

Select a **Port** number and click the **Find** button to locate a specific entry.

To view the normal LLDP Remote Port information page per port, click the **Show Normal** button.

LLDP Remote Port Information

LLDP Remote Entity Information Table

Total Entries: 0

Entity	Information
--------	-------------

Click the **<<Back** button to return to the previous page.

LLDP-MED Folder

LLDP-MED (Media-Endpoint-Discovery) extends the LLDP industry standard to support advanced features on the network edges with specialized capabilities and LLDP-MED standards-based functionality.

LLDP-MED System Settings

On this page the user can configure the fast start repeat count.

LLDP-MED System Settings

LLDP-MED Log State Enabled Disabled Apply

Fast Start Repeat Count (1-10) Apply

LLDP-MED System Information :

Device Class	Network Connectivity Device
Hardware Revision	A1
Firmware Revision	1.01.B002
Software Revision	1.01.B010
Serial Number	PVMB1A9000003
Manufacturer Name	Advantech
Model Name	EKI-4668C Fast Ethernet Industri
Asset ID	

The fields that can be configured are described below:

Parameter	Description
LLDP-MED Log State:	Here the user can enable or disable the LLDP-MED Log State.
Fast Start Repeat Count:	The repeat count range is from 1 to 10. The default value is 4.
LLDP-MEP System Information:	Here a list of information regarding the LLDP-MEP system will be displayed.

Click the **Apply** button to accept the changes made for each individual section.

LLDP-MED Port Settings

On this page the user can enable or disable transmit LLDP-MED TLVs. Setting non-supported capability shall have no functional effect and will result in an inconsistent value error returned to the management application. It effectively disables LLDP-MED on a per-port basis by disabling transmission of capabilities TLV. In this case the remote table's objects in the LLDP-MED MIB corresponding to the respective port will not be populated.

LLDP-MED Port Settings

From Port: To Port: NTCS: State: Capabilities Inventory All

Note: NTCS: Notification Topology Change Status

Port	NTCS	Capabilities	Inventory
1	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled
3	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled
9	Disabled	Disabled	Disabled
10	Disabled	Disabled	Disabled
11	Disabled	Disabled	Disabled
12	Disabled	Disabled	Disabled
13	Disabled	Disabled	Disabled
14	Disabled	Disabled	Disabled
15	Disabled	Disabled	Disabled
16	Disabled	Disabled	Disabled
17	Disabled	Disabled	Disabled
18	Disabled	Disabled	Disabled
19	Disabled	Disabled	Disabled
20	Disabled	Disabled	Disabled

The fields that can be configured are described below:

Parameter	Description
From Port – To Port:	Specified a range of ports to be configured.
NTCS:	Here the user can enable or disable the notification topology change status.
State:	Here the user can enable or disable TLVs.
Capabilities:	This TLV type indicates that LLDP agent should transmit 'LLDP-MED capabilities TLV'. If user wants to transmit LLDP-MED PDU, this TLV type should be enabled. Otherwise, this port cannot transmit LLDP-MED PDU.
Network Policy:	This TLV type indicates that LLDP agent should transmit 'LLDP-MED network policy TLV'.
Inventory:	This TLV type indicates that LLDP agent should transmit 'LLDP-MED inventory TLV'.
All:	Select this option to include Capabilities , Network Policy and Inventory in the configuration.

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

LLDP-MED Local Port Information

On this page the LLDP-MED local port information will be displayed per port.

LLDP-MED Local Port Information

Port

Port 1	
LLDP-MED Capabilities Support:	
LLDP-MED Capabilities	Support
Network Policy	Not Support
Location Identification	Not Support
Extended Power Via MDI PSE	Not Support
Extended Power Via MDI PD	Not Support
Inventory	Support

Click the **Find** button to locate a specific entry based on the information entered.

LLDP-MED Remote Port Information

On this page the LLDP-MEP Remote Port Information will be displayed.

LLDP-MED Remote Port Information

LLDP-MED Remote Port Brief Table

Port

Total Entries: 0

Entity	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID
--------	--------------------	------------	-----------------	---------

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show Normal** button to view the normal layout of the Remote Port Information.

LLDP Remote Port Information

LLDP Remote Entity Information Table

Total Entries: 0

Entity	Information
--------	-------------

Click the **<<Back** button to return to the previous page.

L3 Features

IPv4 Static/Default Route Settings — 132

IPv4 Route Table — 134

IP Forwarding Table/ IP Forwarding Table — 135

Route Preference Settings/ Route Preference Settings — 137

ECMP Algorithm Settings/ ECMP Algorithm Settings — 138

Route Redistribution Settings/ Route Preference Settings — 137

OSPFv2/ OSPF Folder — 140

RIP/ RIP Folder — 153

IP Multicast Routing Protocol/ IP Multicast Routing Protocol Folder — 155

IGMP Static Group Settings/ IGMP Static Group Settings — 159

MD5 Settings/ MD5 Settings — 160

The screenshot displays the web management interface for an ADVANTECH EKI-4668C switch. The top navigation bar shows the device name and various status indicators. The left sidebar contains a tree view of configuration categories, with 'L3 Features' expanded to show 'IPv4 Static/Default Route Settings'. The main content area is titled 'IPv4 Static/Default Route Settings' and contains the following configuration fields:

- IPv4 Static/Default Route Settings**
 - IP Address:
 - Netmask: (e.g.: 255.255.255.254 or 0-32)
 - Gateway: (e.g.: 172.18.211.10)
 - Metric (1-65535):
 - Backup State:
 - NULL Interface:

Below the configuration fields, there is a table titled 'Total Entries: 1' with the following data:

IP Address	Netmask	Gateway	Cost	Backup	Weight	Status	
0.0.0.0	0.0.0.0	10.1.1.254	1	Primary	None	Active	<input type="button" value="Delete"/>

The bottom status bar shows 'System Up Time: 00 Days 00:59:46' and 'Logged in as Administrator, Anonymous - 10.78.62.1'.

IPv4 Static/Default Route Settings

The Switch supports static routing for IPv4 and IPv6 formatted addressing. Users can create up to 256 static route entries for IPv4 and 128 static route entries for IPv6. For IPv4 static routes, once a static route has been set, the Switch will send an ARP request packet to the next hop router that has been set by the user. Once an ARP response has been retrieved by the switch from that next hop, the route becomes enabled. However, if the ARP entry already exists, an ARP response will not be sent.

The Switch also supports a floating static route, which means that the user may create an alternative static route to a different next hop. This secondary next hop device route is considered as a backup static route for when the primary static route is down. If the primary route is lost, the backup route will uplink and its status will become Active.

Entries into the Switch's forwarding table can be made using both an IP address subnet mask and a gateway.

IPv4 Static/Default Route Settings

IPv4 Static/Default Route Settings

IP Address Default

Netmask (e.g.: 255.255.255.254 or 0-32)

Gateway (e.g.: 172.18.211.10)

Metric (1-65535)

Backup State

NULL Interface

Total Entries: 0

IP Address	Netmask	Gateway	Cost	Backup	Weight	Status
Total Entries: 0						

The fields that can be configured are described below:

Parameter	Description
IP Address:	This field allows the entry of an IPv4 address to be assigned to the Static or Default route.
Netmask:	This field allows the entry of a subnet mask to be applied to the corresponding subnet mask of the IP address.
Gateway:	This field allows the entry of a Gateway IP Address to be applied to the corresponding gateway of the IP address.
Metric:	Represents the metric value of the IP interface entered into the table. This field may read a number between 1 and 65535.
Backup State:	Each IP address can only have one primary route, while other routes should be assigned to the backup state. When the primary route failed, switch will try the backup routes according to the order learnt by the routing table until route success. The field represents the Backup state that the Static and Default Route is configured for.
NULL Interface:	Specify to enable or disable the NULL function for the routes.. The null interface provides an alternative method of filtering traffic. Packets send to null interface will be dropped by the switch.

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

IPv4 Route Table

The IP routing table stores all the external routes information of the switch. On this page the user can view all the external route information on the switch.

IPv4 Route Table

Network Address (e.g.: 172.18.208.11/24)
 IP Address (e.g.: 172.18.208.11)
 RIP OSPF

Total Entries: 2

IP Address	Netmask	Gateway	Interface Name	Cost	Protocol
10.0.0.0	255.0.0.0	10.1.1.254	mgmt_ipif	1	Local
12.0.0.0	255.0.0.0	0.0.0.0	System	1	Local

1/1 1

Select the **Hardware** option to display only the routes that have been written into the chip.

Click the **Find** button to locate a specific entry based on the information entered.

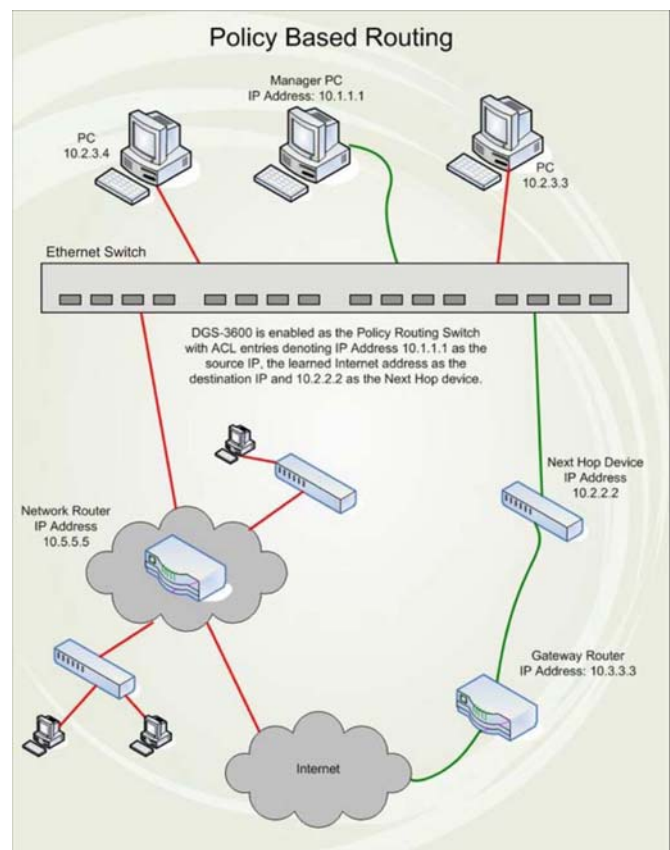
Click the **Apply** button to accept the changes made.

Click the **Delete All** button to remove all the entries listed.

IP Forwarding Table

Policy Based routing is a method used by the Switch to give specified devices a cleaner path to the Internet. Used in conjunction with the Access Profile feature, the Switch will identify traffic originating from a device using the Access Profile feature and forward it on to a next hop router that has a more direct connection to the Internet than the normal routing scheme of your network.

Take the example adjacent picture. Let's say that the PC with IP address 10.1.1.1 belongs to the manager of a company while the other PCs belong to employees. The network administrator hopes to circumvent network traffic by configuring the Policy Routing Switch to make a more direct connection to the Internet using a next hop router (10.2.2.2) that is directly attached to a Gateway router (10.3.3.3), thus totally avoiding the normal network and its related traffic. To accomplish this, the user must configure the Access Profile feature of the Switch to have the PC, with IP address 10.1.1.1 as the Source IP address and the Internet address as the destination IP address (learned through routing protocols), along with other pertinent information. Next, the administrator must configure the Policy Route window to be enabled for this Access Profile and its associated rule, and the Next Hop Router's IP address (10.2.2.2) must be set. Finally, this Policy Route entry must be enabled.

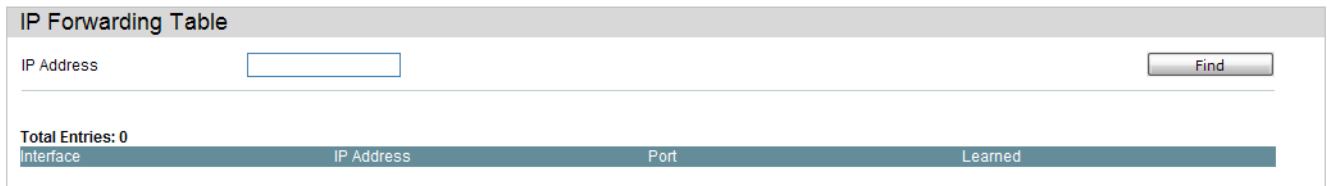


Once completed, the Switch will identify the IP address using the Access Profile function, recognize that it has a Policy Based route, and then forward the information on to the specified next hop router, that will, in turn, relay packets to the gateway router. Thus, the new, cleaner path to the Internet has been formed.

There are some restrictions and cautions when implementing this feature.

1. The access profile must first be created, along with the accompanying rule. If the administrator attempts to enable this feature without the access profile, an error message will be produced.
2. If the access profile is configured as Deny, the packet will be dropped and not forwarded to the next hop destination.
3. If the administrator deletes a rule or profile that is directly linked to a configured policy route, and error message will be prompted to the administrator.

The IP forwarding table stores all the direct connected IP information. On this page the user can view all the direct connected IP information.



The screenshot shows a web interface titled "IP Forwarding Table". At the top, there is a search section with the label "IP Address" followed by an empty text input field and a "Find" button. Below this, it displays "Total Entries: 0". Underneath is a table with a teal header row containing the following columns: "Interface", "IP Address", "Port", and "Learned". The table body is currently empty.

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Route Preference Settings

This window is used to configure the route type preference. The route with smaller preference has higher priority. The preference for local routes is fixed to 0.

To view the following window, click **L3 Features > Route Preference Settings**, as shown below:

Route Preference Settings	
Static (1-999)	<input type="text" value="60"/>
Default (1-999)	<input type="text" value="1"/>
RIP (1-999)	<input type="text" value="100"/>
OSPF Intra (1-999)	<input type="text" value="80"/>
OSPF Inter (1-999)	<input type="text" value="90"/>
OSPF ExtT1 (1-999)	<input type="text" value="110"/>
OSPF ExtT2 (1-999)	<input type="text" value="115"/>
Local	0

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

ECMP Algorithm Settings

This window is used to configure the ECMP OSPF state and ECMP route load-balancing algorithm.

To view the following window, click **L3 Features > ECMP Algorithm Settings**, as shown below:

The fields that can be configured are described below:

Parameter	Description
ECMP OSPF State	Click the radio buttons to enable or disable the ECMP OSPF state.
Destination IP	Tick the check box so that the ECMP algorithm will include the destination IP.
Source IP	Tick the check box so that the ECMP algorithm will include the lower 5 bits of the source IP. This attribution is mutually exclusive with CRC Low and CRC High. If it is set, CRC Low and CRC High will be excluded.
CRC Low	Tick the check box so that the ECMP algorithm will include the lower 5 bits of the CRC. This attribution is mutually exclusive with Source IP and CRC High. If it is set, Source IP and CRC High will be excluded.
CRC High	Tick the check box so that the ECMP algorithm will include the upper 5 bits of the CRC. This attribution is mutually exclusive with Source IP and CRC Low. If it is set, Source IP and CRC Low will be excluded.
TCP/UDP Port	Tick the check box so that the ECMP algorithm will include the TCP or UDP port.

Click the **Apply** button to accept the changes made for each individual section.f

Route Redistribution Settings

This window is used to redistribute the routing information from other routing protocols to RIP, OSPF or BGP.

To view the following window, click **L3 Features > Route Redistribution Settings**, as shown below:

The screenshot shows the 'Route Redistribution Settings' window. At the top, there are four configuration fields: 'Destination Protocol' (set to RIP), 'Source Protocol' (set to RIP), 'Type' (set to All), and 'Metric (0-16)' (empty). An 'Apply' button is located to the right of these fields. Below the fields, it displays 'Total Entries: 0' and a table header with columns: Source Protocol, Destination Protocol, Type, and Metric.

The fields that can be configured are described below:

Parameter	Description
Destination Protocol	Use the drop-down menu to select the destination protocol.
Source Protocol	Use the drop-down menu to select the source protocol.
Type	When OSPF is select in the Source Protocol drop-down menu, this is able to configure. <i>All</i> - To redistribute both OSPF AS-internal and OSPF AS-external routes to RIP. <i>Internal</i> - To redistribute only the OSPF AS-internal routes. <i>External</i> - To redistribute only the OSPF AS-external routes, including Ext Type1 and Ext Type2 routes. <i>Ext Type1</i> - To redistribute only the OSPF AS-external type-1 routes. <i>Ext Type2</i> - To redistribute only the OSPF AS-external type-2 routes. <i>Inter-E1</i> - To redistribute only the OSPF AS-external type-1 and OSPF AS-internal routes. <i>Inter-E2</i> - To redistribute only the OSPF AS-external type-2 and OSPF AS-internal routes.
Metric (0-16)	Enter the RIP metric value for the redistributed routes.
Route Map Name	Enter a route map which will be used as the criteria to determine whether to redistribute specific routes.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

OSPF Folder

OSPFv2 Folder

OSPF Global Settings

This window is used to configure the OSPF Global settings for the Switch.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPF Global Settings**, as shown below:

The fields that can be configured or displayed are described below:

Parameter	Description
OSPF State	Click the radio buttons to enable or disable the OSPF global state.
OSPF Router ID	A 32-bit number (in the same format as an IP address - xxx.xxx.xxx.xxx) that uniquely identifies the Switch in the OSPF domain. It is common to assign the highest IP address assigned to the Switch (router).
Current Router ID	Display the OSPF Route ID currently in use by the Switch. This Route ID is displayed as a convenience to the user when changing the Switch's OSPF Route ID.

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

OSPF Area Settings

This window is used to configure the OSPF Area settings for the Switch. OSPF allows collections of contiguous networks and hosts to be grouped together. Such a group, together with the routers having interfaces to any one of the included networks, is called an area.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPF Area Settings**, as shown below:

Area ID	Type	Stub Import Summary LSA	Stub Default Cost	Translate	
0.0.0.0	Normal	None	None	None	View Detail <input type="button" value="Edit"/> <input type="button" value="Delete"/>

The fields that can be configured are described below:

Parameter	Description
Area ID	A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Type	OSPF area operation Normal , Stub , or NSSA . In some Autonomous Systems, the majority of the topological database may consist of AS external advertisements. An OSPF AS external advertisement is usually flooded throughout the entire AS. However, OSPF allows certain areas to be configured as "stub areas". AS external advertisements are not flooded into or throughout stub areas. Routing to AS external destinations in these areas is based on a (per-area) default only. This reduces the topological database size, and therefore the memory requirements, for a stub area's internal routers.
Translate	Use the drop-down menu to enable or disable the translating of Type-7 LSAs into Type-5 LSAs, so that they can be distributed outside of the NSSA. The default is Disabled. This field can only be configured if NSSA is chosen in the Type field.
Stub Summary	Display whether or not the selected Area will allow Summary Link-State Advertisements (Summary LSAs) to be imported into the area from other areas.
Metric (0-65535)	Enter the metric (1 - 65535; 0 for auto cost) of this area. For NSSA areas, the metric field determines the cost of traffic entering the NSSA area.

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

Click the [View Detail](#) link to view a display of the OSPF Area settings.

Click the **Edit** button to re-configure the selected entry.

Click the **Delete** button to remove the selected entry.

After click the [View Detail](#) link, the following window will appear.

OSPF Area Settings	
OSPF Area Detail Information	
Area ID	0.0.0.0
Area Type	Normal
Import Summary for Stub	-----
Default Cost for Stub	-----
SPF Algorithm Runs for Area 0.0.0.0	1 time
Number of LSA in This Area	0
Checksum Sum	0x0
Number of ABR in This Area	0
Number of ASBR in This Area	0

This window is used to display the OSPF Area settings.

Click the <<Back button to return to the previous window.

OSPF Interface Settings

This window is used to configure the OSPF Interface settings for this Switch.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPF Interface Settings**, as shown below:

The screenshot shows the 'OSPF Interface Settings' window. At the top, there is an 'Interface Name' search box with a 'Find' button to its right. Below the search box is a 'View All' button. A summary line indicates 'Total Entries: 1'. Below this is a table with the following columns: Interface Name, IP Address, Area ID, Administrative State, Link Status, and Metric. The table contains one entry for 'System' with IP Address 12.78.62.41/8, Area ID 0.0.0.0, Administrative State Disabled, Link Status Link Up, and Metric 1. An 'Edit' button is located to the right of the table entry.

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the name of the IP interface here

Click the **Find** button to find the interface entered.

Click the **View All** button to view all the interfaces configured on this switch.

Click the **Edit** button to re-configure the selected entry.

After clicking the **Edit** button, the following window will appear.

The screenshot shows the 'OSPF Interface Settings' window in edit mode. The 'Interface Name' is set to 'System'. Other fields include: Priority (0-255) set to 1, Metric (1-65535) set to 1, Authentication set to None, and Administrative State set to Disabled. On the right side, there are fields for Area ID (0.0.0.0), Hello Interval (1-65535) set to 10 sec, Dead Interval (1-65535) set to 40 sec, Password (empty), and Passive set to Disabled. Below these fields is a section titled 'OSPF Interface Detail Information' which contains a table with the following data:

OSPF Interface Detail Information			
Interface Name	System	IP Address	10.90.90.90/8 (Link Up)
Network Medium Type	Broadcast	Metric	1
Area ID	0.0.0.0	Administrative State	Disabled
Priority	1	DR State	Down
DR Address	None	Backup DR Address	None
Hello Interval	10 sec	Dead Interval	40 sec
Transmit Delay	1 sec	Retransmit Time	5 sec
Authentication	None	Passive Mode	Disabled

The fields that can be configured are described below:

Parameter	Description
Priority (0-255)	Enter the priority for the Designated Router election. If a Router Priority of 0 is set, the Switch cannot be elected as the DR for the network.
Metric (1-65535)	Enter the interface metric used.

Authentication	Select the authentication used. Options to choose from are None , Simple and MD5 . When choosing Simple authentication, a password must be entered. When choosing MD5 authentication, a Key ID must be entered.
Administrative State	Use the drop-down menu to enable or disable the administrative state.
Area ID	Enter the area to which the interface is assigned. An Area ID is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Hello Interval (1-65535)	Enter the specification of the interval between the transmissions of OSPF Hello packets, in seconds. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.
Dead Interval (1-65535)	Enter the specification of the length of time between the receipts of Hello packets from a neighbor router before the selected area declares that router down. The Dead Interval must be evenly divisible by the Hello Interval.
Password	When <i>Simple</i> is selected in the Authentication drop-down menu, enter a simple text password.
Passive	Assign the designated entry to be a passive interface. A passive interface will not advertise to any other routers than those within its OSPF intranet.

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

Click the <<Back button to return to the previous window

OSPF Virtual Link Settings

This window is used to configure the OSPF virtual interface settings for this switch.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPF Virtual Link Settings**, as shown below:

The fields that can be configured are described below:

Parameter	Description
Transit Area ID	A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Neighbor Router ID	The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. This is the router ID of the neighbor router.
Hello Interval (1-65535)	Enter the specification of the interval between the transmissions of OSPF Hello packets, in seconds. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.
Dead Interval (1-65535)	Enter the specification of the length of time between the receipts of Hello packets from a neighbor router before the selected area declares that router down. The Dead Interval must be evenly divisible by the Hello Interval.
Authentication	Select the authentication used. Options to choose from are None , Simple and MD5 . When choosing Simple authentication, a password must be entered. When choosing MD5 authentication, a Key ID must be entered.
Password	When <i>Simple</i> is selected in the Authentication drop-down menu, enter a simple text password.

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

Click the **Edit** button to re-configure the selected entry.

Click the **Delete** button to remove the selected entry.

After clicking the **Edit** button, the following window will appear.f

OSPF Virtual Link Settings			
Transit Area ID	10.90.90.6	Neighbor Router ID	10.90.90.8
Hello Interval (1-65535)	30 sec	Dead Interval (1-65535)	300 sec
Authentication	None	Password	
OSPF Virtual Link Detail Information			
Transit Area ID	10.90.90.6	Virtual Neighbor Router ID	10.90.90.8
Hello Interval	30 sec	Dead Interval	300 sec
Transmit Delay	1 sec	Retransmit Time	5 sec
Authentication	None	Virtual Link Status	Link Down

The fields that can be configured are described below:

Parameter	Description
Hello Interval (1-65535)	Enter the specification of the interval between the transmissions of OSPF Hello packets, in seconds. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.
Dead Interval (1-65535)	Enter the specification of the length of time between the receipts of Hello packets from a neighbor router before the selected area declares that router down. The Dead Interval must be evenly divisible by the Hello Interval.
Authentication	Select the authentication used. Options to choose from are None , Simple and MD5 . When choosing Simple authentication, a password must be entered. When choosing MD5 authentication, a Key ID must be entered.
Password	When <i>Simple</i> is selected in the Authentication drop-down menu, enter a simple text password.

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

Click the **<<Back** button to return to the previous window.

OSPF Area Aggregation Settings

This window is used to configure the OSPF area aggregation settings.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPF Area Aggregation Settings**, as shown below:

The fields that can be configured are described below:

Parameter	Description
Area ID	Enter a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
IP Address	Enter the IP address that uniquely identifies the network that corresponds to the OSPF Area.
Network Mask	Enter the network mask that uniquely identifies the network that corresponds to the OSPF Area.
LSDB Type	Use the drop-down menu to select the type of address aggregation. Options to choose from are <i>NSSA Ext</i> and <i>Summary</i> .
Advertise	Use the drop-down menu to enable or disable the advertisement trigger.

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

Click the **Edit** button to re-configure the selected entry.

Click the **Delete** button to remove the selected entry.

OSPF Host Router Settings

This window is used to configure OSPF host route settings.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPF Host Router Settings**, as shown below:

The fields that can be configured are described below:

Parameter	Description
Host Address	Enter the host's IP address used.
Metric	Enter a metric between 1 and 65535, which will be advertised.
Area ID	Enter a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

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

Click the **Edit** button to re-configure the selected entry.

Click the **Delete** button to remove the selected entry.

OSPF Default Information Originate Settings

??????????f

OSPF Default Information Originate Settings

Always	<input type="text" value="Off"/>
State	<input type="text" value="Disabled"/>
Metric (1-65535)	<input type="text" value="1"/>

OSPF LSDB Table

This window is used to display the OSPF Link State Database (LSDB).

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPF LSDB Table**, as shown below:

OSPF LSDB Table

Area ID Advertise Router ID LSDB Type

Total Entries: 0

Area ID	LSDB Type	Advertising Router ID	Link State ID	Cost	Sequence Number
---------	-----------	-----------------------	---------------	------	-----------------

The fields that can be configured are described below:

Parameter	Description
Area ID	Enter a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Advertise Router ID	Enter the router ID of the advertising router.
LSDB Type	Use the drop-down menu to select the LSDB type to be displayed. Options to choose from are <i>None</i> , <i>RTRLink</i> , <i>NETLink</i> , <i>Summary</i> , <i>ASSummary</i> , <i>ASExtLink</i> , <i>NSSA Ext</i> and <i>Stub</i> .

Click the **Find** button to find the specified entry.

Click the **View All** button to view all the OSPF Link State Database entries.

Click the [View Detail](#) link to view the OSPF LSDB details of the specific entry.

After clicking the [View Detail](#) link, the following window will appear.

OSPF LSDB Table

OSPF Internal LSDB Detail Information

Area ID	1.0.0.1	Link State Type	Network Link
Link State ID	10.90.90.110/8	Advertising Router	18.0.0.1
Link State Age	698	Checksum	0xBB1E
Link State Sequence Number	0x80000001		

Click the **<<Back** button to return to the previous window.

OSPF Neighbor Table

This window is used to display OSPF-neighbor information on a per-interface basis.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPF Neighbor Table**, as shown below:

OSPF Neighbor Table

Neighbor IP Address Find

View All

Total Entries: 0

Neighbor Address	Neighbor Router ID	Neighbor Options	Neighbor Priority	Neighbor State	State Changes
------------------	--------------------	------------------	-------------------	----------------	---------------

The fields that can be configured are described below:

Parameter	Description
Neighbor IP Address	Enter the IP address of the neighbor router.

Click the **Find** button to find the specified entry.

Click the **View All** button to view all the entries.

OSPF Virtual Neighbor Table

This window is used to display OSPF-neighbor information of OSPF virtual links.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPF Virtual Neighbor Table**, as shown below:

The fields that can be configured are described below:

Parameter	Description
Transit Area ID	A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Virtual Neighbor Router ID	The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router.

Click the **Find** button to find the specified entry.

Click the **View All** button to view all the entries.f

RIP Folder

RIP Settings

This window is used to configure the RIP settings for one or more IP interfaces.

To view the following window, click **L3 Features > RIP > RIP Settings**, as shown below:

RIP Settings					
RIP Global Settings					
RIP State	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled				
Update Time (5-65535)	<input type="text" value="30"/>	sec			
Timeout Time (5-65535)	<input type="text" value="180"/>	sec			
Garbage Collection Time (5-65535)	<input type="text" value="120"/>	sec			
Interface Name	<input type="text"/>				
Total Entries: 1					
Interface Name	IP Address	TX Mode	RX Mode	Authentication	State
System	10.90.90.90/8	Disabled	Disabled	Disabled	Disabled

Figure 5-61 RIP Settings window

The fields that can be configured are described below:

Parameter	Description
RIP State	Specifies that the RIP state will be enabled or disabled. If the state is disabled, then RIP packets will not be either transmitted or received by the interface. The network configured on this interface will not be in the RIP database.
Update Time (5-65535)	Enter the value of the rate at which RIP updates are sent.
Timeout Time (5-65535)	Enter the value of the time after which a RIP route is declared to be invalid.
Garbage Collection Time (5-65535)	Enter the value of the time for which a RIP route will be kept before it is removed from routing table.
Interface Name	Specifies the IP interface name used for this configuration.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Find** button to find the specified entry.

Click the **View All** button to view all the entries.

Click the **Edit** button to re-configure the selected entry.

After clicking the **Edit** button, the following window will appear.

RIP Settings

Interface Name: System

TX Mode: Disabled

RX Mode: Disabled

State: Disabled

Authentication: Disabled (Max:16 characters)

RIP Interface Detail Information

Interface Name	System	IP Address	10.90.90.90/8 (Link Up)
Interface Metric	1	Administrative State	Disabled
TX Mode	Disabled	RX Mode	Disabled
Authentication	Disabled		

The fields that can be configured are described below:

Parameter	Description
TX Mode	Specifies the RIP transmission mode. Options to choose from are v1 Only , v1 Compatible and v2 Only . Select Disable to disable this option.
RX Mode	Specifies the RIP receive mode Options to choose from are v1 Only , v2 Only and v1 or v2 . Select Disable to disable this option.
State	Specifies that the RIP state will be enabled or disabled. If the state is disabled, then RIP packets will not be either transmitted or received by the interface. The network configured on this interface will not be in the RIP database.
Authentication	Specifies to set the state of authentication. When the authentication state is enabled, enter the password used in the space provided.

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

Click the **<<Back** button to return to the previous window.

RIP Global Settings

RIP State: Enabled Disabled

Update Time (5-65535): sec

Timeout Time (5-65535): sec

Garbage Collection Time (5-65535): sec

Interface Name:

Total Entries: 1

Interface Name	IP Address	TX Mode	RX Mode	Authentication	State	
System	12.78.62.41/8	Disabled	Disabled	Disabled	Disabled	<input type="button" value="Edit"/>

IP Multicast Routing Protocol Folder

IGMP Interface Settings

The Internet Group Management Protocol (IGMP) can be configured on the Switch on a per-IP interface basis. Each IP interface configured on the Switch is displayed in the below IGMP Interface Settings window.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Interface Settings**, as shown below:

IGMP Interface Settings							
Total Entries: 1							
Interface Name	Network Address	Version	Query Interval	Max RT	RV	LMQI	State
System	12.78.62.4...	3	125	10	2	1	Disabled

Click the **Edit** button to re-configure the specific entry.

Click the **Edit** button to see the following window.

IGMP Interface Settings	
Interface Name	System
Version	3
State	Disabled
Query Interval (1-31744)	125
Max Response Time (1-25)	10 sec
Robustness Variable (1-7)	2
Last Member Query Interval (1-25)	1

Figure 5-68 IGMP Interface Settings – Edit window

The fields that can be configured are described below:

Parameter	Description
Version	Use the drop-down menu to select the IGMP version that will be used to interpret IGMP queries on the interface.
State	Use the drop-down menu to enables or disables IGMP for the IP interface. The default is Disabled.
Query Interval (1-31744)	Enter a value between 1 and 31744 seconds, with a default of 125 seconds. This specifies the length of time between sending IGMP queries.
Max Response Time (1-25)	Enter a value between 1 and 25 to specify the maximum amount of time allowed before sending an IGMP response report. The default time is 10 seconds.

Robustness Variable (1-7)	A tuning variable to allow for subnetworks that are expected to lose a large number of packets. A value between 1 and 7 can be entered, with larger values being specified for subnetworks that are expected to lose larger numbers of packets. The default setting is 2.
Last Member Query Interval (1-25)	Enter a value between 1 and 25 to specify the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. The default is 1 second.

Click the **<<Back** button to return to the previous window.

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

IGMP Check Subscriber Source Network Settings

This window allows users to configure IGMP check subscriber source network settings. When Check Subscriber Source Network is enabled on an interface, every IGMP report/leave message received by the interface will be checked to see whether its source IP is in the same network as the interface. If the check is disabled, an IGMP report/leave message with any source IP can be processed by IGMP protocol.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Check Subscriber Source Network Settings**, as shown below:

IGMP Check Subscriber Source Network Settings

Interface Name Find

View All

Total Entries: 1

Interface Name	IP Address	Network Address	Check Subscriber Source Network
System	12.78.62.41	255.0.0.0	Enabled

Edit

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the IP interface name used for this configuration.

Click the **Find** button to find the interface entered.

Click the **View All** button to view all the interfaces configured on this switch.

Click the **Edit** button to re-configure the selected entry.

IGMP Group Table

The window is used to display the IGMP static groups on the Switch.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Group Table**, as shown below:

IGMP Group Table

Interface Name Multicast Group

Total Entries: 0

Interface Name	Multicast Group	Last Reporter	IP Querier	IP Expire
----------------	-----------------	---------------	------------	-----------

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the IP interface name used for this configuration.
Multicast Group	Enter the multicast group IP address.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **View All** button to view all the interfaces configured on this switch.

Click the [View Detail](#) link to view more information regarding the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the [View Detail](#) link to see the following window.

IGMP Group Detail Information

IGMP Group Detail Information Table

Interface Name	System
Multicast Group	239.1.1.0
Last Reporter	10.3.0.1
IP Querier	SELF
IP Expire	0
Filter Mode	Include
v1 Host Time	0
v2 Host Time	0

Total Entries: 1

Source List	Timer
10.2.0.1	134

Click the **<<Back** button to return to the previous window.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IGMP Static Group Settings

This window is used to create an IGMP static group on the switch.
To view the following window, click **L3 Features > IGMP Static Group Settings**, as shown below:

The fields that can be configured are described below:

Parameter	Description
Interface	Enter the IP interface on which the IGMP static group resides. The IP interface must be the primary IP interface.
Multicast Group	Enter the multicast IP address.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove a specific entry listed.

Click the **Find** button to find the information entered.

MD5 Settings

The MD5 Configuration allows the entry of a 16 character Message Digest version 5 (MD5) key which can be used to authenticate every packet exchanged between OSPF routers. It is used as a security mechanism to limit the exchange of network topology information to the OSPF routing domain. This page is used to configure an MD5 key and password.

To view the following window, click **L3 Features > MD5 Settings**, as shown below:

The fields that can be configured are described below:

Parameter	Description
Key ID	Specifies a number from 1 to 255 used to identify the MD5 Key.
Password	Specifies an alphanumeric string of between 1 and 16 case-sensitive characters used to generate the Message Digest which is in turn, used to authenticate OSPF packets within the OSPF routing domain.

Click the **Add** button to add a new Key ID with its corresponding password.

Click the **Find** button to search for the Key ID entered.

Click the **View All** button to view all the entries.

Click the **Edit** button to re-configure a specific entry listed.

Click the **Delete** button to remove a specific entry listed.

Quality of Service (QoS)

802.1p Settings Folder — 164

Bandwidth Control Folder — 166

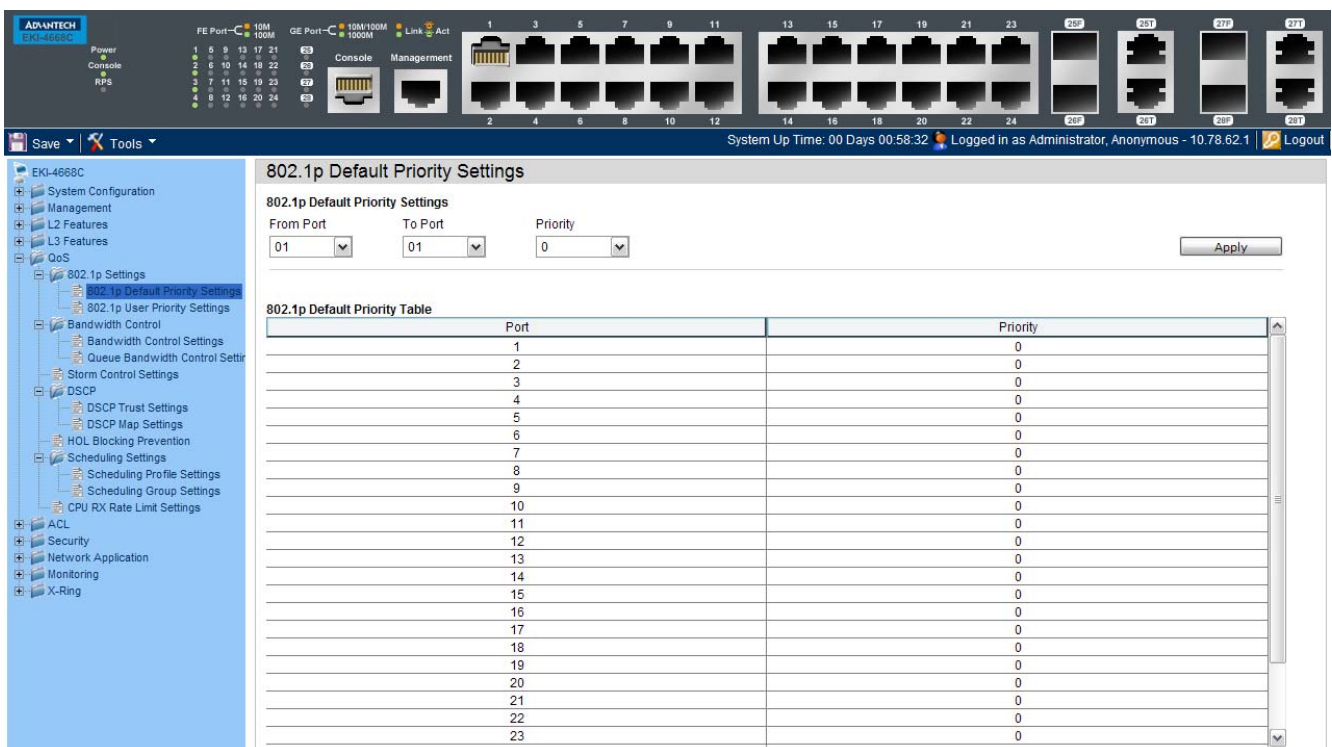
Storm Control Settings — 169s

DSCP Folder — 173

HOL Blocking Prevention — 175

Scheduling Settings Folder — 176

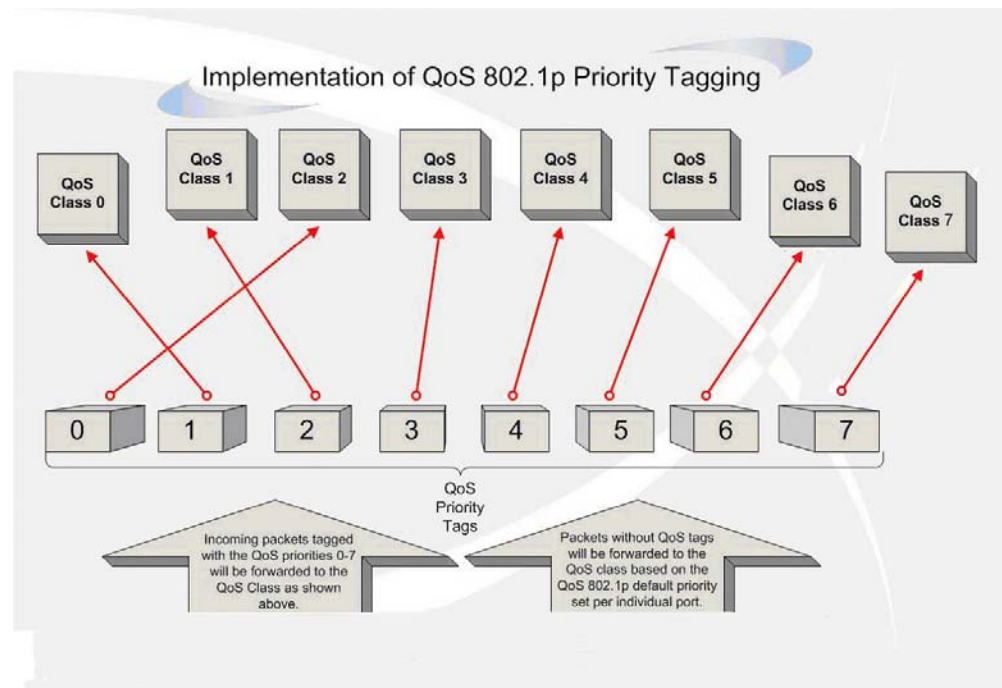
CPU RX Rate Limit Settings — 178



The screenshot displays the '802.1p Default Priority Settings' configuration page. At the top, there are dropdown menus for 'From Port' (set to 01), 'To Port' (set to 01), and 'Priority' (set to 0). Below this is an 'Apply' button. The main content is a table titled '802.1p Default Priority Table' with two columns: 'Port' and 'Priority'. The table lists ports from 1 to 23, all of which have a priority value of 0.

Port	Priority
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0
22	0
23	0

QoS is an implementation of the IEEE 802.1p standard that allows network administrators a method of reserving bandwidth for important functions that require a large bandwidth or have a high priority, such as VoIP (voice-over Internet Protocol), web browsing applications, file server applications or video conferencing. Not only can a larger bandwidth be created, but other less critical traffic can be limited, so excessive bandwidth can be saved. The Switch has separate hardware queues on every physical port to which packets from various applications can be mapped to, and, in turn prioritized. View the following map to see how the Switch implements basic 802.1P priority queuing.



The picture above shows the default priority setting for the Switch. Class-7 has the highest priority of the seven priority classes of service on the Switch. In order to implement QoS, the user is required to instruct the Switch to examine the header of a packet to see if it has the proper identifying tag. Then the user may forward these tagged packets to designated classes of service on the Switch where they will be emptied, based on priority.

For example, let's say a user wishes to have a video conference between two remotely set computers. The administrator can add priority tags to the video packets being sent out, utilizing the Access Profile commands. Then, on the receiving end, the administrator instructs the Switch to examine packets for this tag, acquires the tagged packets and maps them to a class queue on the Switch. Then in turn, the administrator will set a priority for this queue so that will be emptied before any other packet is forwarded. This result in the end user receiving all packets sent as quickly as possible, thus prioritizing the queue and allowing for an uninterrupted stream of packets, which optimizes the use of bandwidth available for the video conference.

Understanding QoS

The Switch supports 802.1p priority queuing. The Switch has eight priority queues. These priority queues are numbered from 7 (Class 7) — the highest priority queue — to 0 (Class 0) — the lowest priority queue. The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority queues as follows:

- Priority 0 is assigned to the Switch's Q2 queue.
- Priority 1 is assigned to the Switch's Q0 queue.
- Priority 2 is assigned to the Switch's Q1 queue.

- Priority 3 is assigned to the Switch's Q3 queue.
- Priority 4 is assigned to the Switch's Q4 queue.
- Priority 5 is assigned to the Switch's Q5 queue.
- Priority 6 is assigned to the Switch's Q6 queue.
- Priority 7 is assigned to the Switch's Q7 queue.

For strict priority-based scheduling, any packets residing in the higher priority classes of service are transmitted first. Multiple strict priority classes of service are emptied based on their priority tags. Only when these classes are empty, are packets of lower priority transmitted.

For weighted round-robin queuing, the number of packets sent from each priority queue depends upon the assigned weight. For a configuration of eight CoS queues, A~H with their respective weight value: 8~1, the packets are sent in the following sequence: A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1.

For weighted round-robin queuing, if each CoS queue has the same weight value, then each CoS queue has an equal opportunity to send packets just like round-robin queuing.

For weighted round-robin queuing, if the weight for a CoS is set to 0, then it will continue processing the packets from this CoS until there are no more packets for this CoS. The other CoS queues that have been given a nonzero value, and depending upon the weight, will follow a common weighted round-robin scheme.

Remember that the Switch has eight configurable priority queues (and eight Classes of Service) for each port on the Switch.



NOTICE: The Switch contains eight classes of service for each port on the Switch. One of these classes is reserved for internal use on the Switch and is therefore not configurable. All references in the following section regarding classes of service will refer to only the eight classes of service that may be used and configured by the administrator.

802.1p Settings Folder

802.1p Default Priority Settings

The Switch allows the assignment of a default 802.1p priority to each port on the Switch. This page allows the user to assign a default 802.1p priority to any given port on the switch that will insert the 802.1p priority tag to untagged packets received. The priority and effective priority tags are numbered from 0, the lowest priority, to 7, the highest priority. The effective priority indicates the actual priority assigned by RADIUS. If the RADIUS assigned value exceeds the specified limit, the value will be set at the default priority. For example, if the RADIUS assigns a limit of 8 and the default priority is 0, the effective priority will be 0.

802.1p Default Priority Settings

802.1p Default Priority Settings

From Port: To Port: Priority:

802.1p Default Priority Table

Port	Priority
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0
22	0

To implement a new default priority, first choose a port range by using the From Port and To Port pull-down menus and then use the Priority drop-down menu to select a value from 0 to 7.

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

802.1p User Priority Settings

The Switch allows the assignment of a class of service to each of the 802.1p priorities.

802.1p User Priority Settings

802.1p User Priority Settings

Priority Class ID

802.1p User Priority Table

Priority	Class ID
0	Class-2
1	Class-0
2	Class-1
3	Class-3
4	Class-4
5	Class-5
6	Class-6
7	Class-7

Once a priority has been assigned to the port groups on the Switch, then a Class may be assigned to each of the eight levels of 802.1p priorities using the drop-down menus on this window. User priority mapping is not only for the default priority configured in the last page, but also for all the incoming tagged packets with 802.1p tag.

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

Bandwidth Control Folder

The bandwidth control settings are used to place a ceiling on the transmitting and receiving data rates for any selected port.

Bandwidth Control Settings

The Effective RX/TX Rate refers to the actual bandwidth of the switch port, if it does not match the configured rate. This usually means that the bandwidth has been assigned by a higher priority resource, such as a RADIUS server.

Bandwidth Control Settings

From Port: To Port: Type: No Limit: Rate (64-1024000): Kbit/sec

Bandwidth Control Table

Port	RX Rate (Kbit/sec)	TX Rate (Kbit/sec)
1	No Limit	No Limit
2	No Limit	No Limit
3	No Limit	No Limit
4	No Limit	No Limit
5	No Limit	No Limit
6	No Limit	No Limit
7	No Limit	No Limit
8	No Limit	No Limit
9	No Limit	No Limit
10	No Limit	No Limit
11	No Limit	No Limit
12	No Limit	No Limit
13	No Limit	No Limit
14	No Limit	No Limit
15	No Limit	No Limit
16	No Limit	No Limit
17	No Limit	No Limit
18	No Limit	No Limit
19	No Limit	No Limit
20	No Limit	No Limit
21	No Limit	No Limit

The fields that can be configured are described below:

Parameter	Description
From Port:	The beginning port of a consecutive group of ports to be configured.
To Port:	The ending port of a consecutive group of ports to be configured.
Type:	This drop-down menu allows a selection between <i>RX</i> (receive), <i>TX</i> (transmit), and <i>Both</i> . This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.
No Limit:	This drop-down menu allows the user to specify that the selected port will have no bandwidth limit or not. NOTE: If the configured number is larger than the port speed, it means no bandwidth limit.
Rate (64-1024000):	This field allows the input of the data rate that will be the limit for the selected port. The user may choose a rate between 64 and 1024000 Kbits per second.

Effective RX:	If a RADIUS server has assigned the RX bandwidth, then it will be the effective RX bandwidth. The authentication with the RADIUS sever can be per port or per user. For per user authentication, there may be multiple RX bandwidths assigned if there are multiple users attached to this specific port. The final RX bandwidth will be the largest one among these multiple RX bandwidths.
Effective TX:	If a RADIUS server has assigned the TX bandwidth, then it will be the effective TX bandwidth. The authentication with the RADIUS sever can be per port or per user. For per user authentication, there may be multiple TX bandwidths assigned if there are multiple users attached to this specific port. The final TX bandwidth will be the largest one among these multiple TX bandwidths.

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

Queue Bandwidth Control Settings page

Queue Bandwidth Control Settings

From Port: To Port:
 From CoS: To CoS:
 Max Rate (64-1024000): No Limit

Queue Bandwidth Control Table On Port 1

Queue	Max Rate (Kbit/sec)
0	No Limit
1	No Limit
2	No Limit
3	No Limit
4	No Limit
5	No Limit
6	No Limit
7	No Limit

Queue Bandwidth Control Table On Port 2

Queue	Max Rate (Kbit/sec)
0	No Limit
1	No Limit
2	No Limit
3	No Limit
4	No Limit
5	No Limit
6	No Limit
7	No Limit

Queue Bandwidth Control Table On Port 3

Queue	Max Rate (Kbit/sec)
0	No Limit
1	No Limit
2	No Limit
3	No Limit

The fields that can be configured are described below:

Parameter	Description
From Port – To Port:	Here the user can select the port range to use for this configuration.
From CoS – To CoS:	Here the user can select the queue range to use for this configuration.
Max Rate:	Here the user can enter the maximum rate for the queue. For no limit select the No Limit option.

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



NOTE: The minimum granularity of queue bandwidth control is 1.85Mbps. The system will adjust the number to the multiple of 1850 automatically.

Storm Control Settings

On a computer network, packets such as Multicast packets and Broadcast packets continually flood the network as normal procedure. At times, this traffic may increase due to a malicious end station on the network or a malfunctioning device, such as a faulty network card. Thus, switch throughput problems will arise and consequently affect the overall performance of the switch network. To help rectify this packet storm, the Switch will monitor and control the situation.

Packet storms are monitored to determine if too many packets are flooding the network based on threshold levels provided by the user. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided. This method can be utilized by selecting the *Drop* option of the Action parameter in the window below.

The Switch will also scan and monitor packets coming into the Switch by monitoring the Switch's chip counter. This method is only viable for Broadcast and Multicast storms because the chip only has counters for these two types of packets. Once a storm has been detected (that is, once the packet threshold set below has been exceeded), the Switch will shut down the port to all incoming traffic, with the exception of STP BPDU packets, for a time period specified using the Count Down parameter.

If a Time Interval parameter times-out for a port configured for traffic control and a packet storm continues, that port will be placed in Shutdown Forever mode, which will cause a warning message to be sent to the Trap Receiver. Once in Shutdown Forever mode, the method of recovering the port is to manually recoup it using the **Port Settings** window in the **Configuration** folder or automatic recovering after 5 minutes. Select the disabled port and return its State to *Enabled* status. To utilize this method of Storm Control, choose the *Shutdown* option of the Action parameter in the window below.

Use this window to enable or disable storm control and adjust the threshold for multicast and broadcast storms.

Storm Control Settings

Storm Control Settings

From Port: To Port:

Action: Countdown (0 or 5-30): min

Time Interval (5-30): sec Threshold (0-255000): pkt/s

Storm Control Type:

Port	Storm Control Type	Action	Threshold	Countdown	Interval	Shutdown Forever
1	None	Drop	131072	0	5	
2	None	Drop	131072	0	5	
3	None	Drop	131072	0	5	
4	None	Drop	131072	0	5	
5	None	Drop	131072	0	5	
6	None	Drop	131072	0	5	
7	None	Drop	131072	0	5	
8	None	Drop	131072	0	5	
9	None	Drop	131072	0	5	
10	None	Drop	131072	0	5	
11	None	Drop	131072	0	5	
12	None	Drop	131072	0	5	
13	None	Drop	131072	0	5	
14	None	Drop	131072	0	5	
15	None	Drop	131072	0	5	
16	None	Drop	131072	0	5	
17	None	Drop	131072	0	5	
18	None	Drop	131072	0	5	

Note: For unicast storm traffic, the violated action is always 'drop'.

The fields that can be configured are described below:

Parameter	Description
From Port:	Select the beginning port of the range of port(s) to be configured.
To Port:	Select the ending port of the range of port(s) to be configured.
Action:	<p>Select the method of traffic control from the pull-down menu. The choices are:</p> <p><i>Drop</i> – Utilizes the hardware Traffic Control mechanism, which means the Switch’s hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved.</p> <p><i>Shutdown</i> – Utilizes the Switch’s software Traffic Control mechanism to determine the Packet Storm occurring. Once detected, the port will deny all incoming traffic to the port except STP BPDU packets, which are essential in keeping the Spanning Tree operational on the Switch. If the Count Down timer has expired and yet the Packet Storm continues, the port will be placed in Shutdown Forever mode and is no longer operational until the port recovers after 5 minutes automatically or the user manually resets the port using the Port Settings window (Configuration> Port Configuration> Port Settings). Choosing this option obligates the user to configure the Time Interval setting as well, which will provide packet count samplings from the Switch’s chip to determine if a Packet Storm is occurring.</p>
Count Down (0 or 5-30):	The Count Down timer is set to determine the amount of time, in minutes, that the Switch will wait before shutting down the port that is experiencing a traffic storm. This parameter is only useful for ports configured as <i>Shutdown</i> in their Action field and therefore will not operate for hardware-based Traffic Control implementations. The possible time settings for this field are 0 and 5 to 30 minutes.
Time Interval (5-30):	The Time Interval will set the time between Multicast and Broadcast packet counts sent from the Switch’s chip to the Traffic Control function. These packet counts are the determining factor in deciding when incoming packets exceed the Threshold value. The Time Interval may be set between 5 and 30 seconds, with a default setting of 5 seconds.
Threshold (0-255000):	Specifies the maximum number of packets per second that will trigger the Traffic Control function to commence. The configurable threshold range is from 0-255000 with a default setting of 130560 packets per second.
Storm Control Type:	Specifies the desired Storm Control Type: <i>None, Broadcast, Multicast, Unknown Unicast, Broadcast + Multicast, Broadcast + Unknown Unicast, Multicast + Unknown Unicast, and Broadcast + Multicast + Unknown Unicast.</i>

Traffic Trap Settings:

Enable sending of Storm Trap messages when the type of action taken by the Traffic Control function in handling a Traffic Storm is one of the following:

None – Will send no Storm trap warning messages regardless of action taken by the Traffic Control mechanism.

Storm Occurred – Will send Storm Trap warning messages upon the occurrence of a Traffic Storm only.

Storm Cleared – Will send Storm Trap messages when a Traffic Storm has been cleared by the Switch only.

Both – Will send Storm Trap messages when a Traffic Storm has been both detected and cleared by the Switch.

This function cannot be implemented in the hardware mode. (When *Drop* is chosen for the Action parameter)

Click the **Apply** button to accept the changes made for each individual section.



NOTE: Traffic Control cannot be implemented on ports that are set for Link Aggregation (Port Trunking).



NOTE: Ports that are in the Shutdown Forever mode will be seen as Discarding in Spanning Tree windows and implementations though these ports will still be forwarding BPDUs to the Switch's CPU.



NOTE: Ports that are in Shutdown Forever mode will be seen as link down in all windows and screens until the user recovers these ports.



NOTE: The minimum granularity of storm control on a GE port is 640pps.

DSCP Folder

DSCP Trust Settings

This page is to configure the DSCP trust state of ports. When ports are under the DSCP trust mode, the switch will insert the priority tag to untagged packets by using the DSCP Map settings instead of the default port priority.

DSCP Trust Settings

From Port: To Port: State:

Port	DSCP Trust
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled

The fields that can be configured are described below:

Parameter	Description
From Port – To Port:	Here the user can select a range of port to configure.
State:	Enable/disable to trust DSCP. By default, DSCP trust is disabled.

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

DSCP Map Settings

The mapping of DSCP to queue will be used to determine the priority of the packet (which will be then used to determine the scheduling queue) when the port is in DSCP trust state.

The DSCP-to-DSCP mapping is used in the swap of DSCP of the packet when the packet is ingresses to the port. The remaining processing of the packet will base on the new DSCP. By default, the DSCP is mapped to the same DSCP.

DSCP Map Settings

DSCP Map: DSCP List (0-63): Priority:

Priority	DSCP List
0	0-7
1	8-15
2	16-23
3	24-31
4	32-39
5	40-47
6	48-55
7	56-63

The fields that can be configured are described below:

Parameter	Description
DSCP Map:	Here the user can select one of two options: <i>DSCP Priority</i> – Specifies a list of DSCP values to be mapped to a specific priority. <i>DSCP DSCP</i> – Specifies a list of DSCP value to be mapped to a specific DSCP.
DSCP List:	Here the user can enter a DSCP List value.
Priority:	Here the user can select a Priority value.

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

HOL Blocking Prevention

HOL (Head of Line) Blocking happens when one of the destination ports of a broadcast or multicast packet are busy. The switch will hold this packet in the buffer while the other destination port will not transmit the packet even they are not busy.

The HOL Blocking Prevention will ignore the busy port and forward the packet directly to have lower latency and better performance.

On this page the user can enable or disable HOL Blocking Prevention.



The fields that can be configured are described below:

Parameter	Description
HOL Blocking Prevention Global Settings:	Here the user can enable or disable the HOL blocking prevention global settings.

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

Scheduling Settings Folder

Scheduling Profile Settings

Changing the output scheduling used for the hardware queues in the Switch can customize the QoS. As with any changes to the QoS implementation, careful consideration should be given to how network traffic in lower priority queues are affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delays. If you choose to customize this setting, it is important to the monitor network performance, especially during peak demand, as bottlenecks can quickly develop if the QoS settings are not suitable.

Profile ID	CoS	Mechanism	Weight
1	0	Strict	1
1	1	Strict	2
1	2	Strict	3
1	3	Strict	4
1	4	Strict	5
1	5	Strict	6
1	6	Strict	7
1	7	Strict	8
2	0	Strict	1
2	1	Strict	2
2	2	Strict	3
2	3	Strict	4
2	4	Strict	5
2	5	Strict	6
2	6	Strict	7
2	7	Strict	8
3	0	Strict	1
3	1	Strict	2
3	2	Strict	3
3	3	Strict	4
3	4	Strict	5
3	5	Strict	6
3	6	Strict	7
3	7	Strict	8

The fields that can be configured are described below:

Parameter	Description
Profile ID:	Here the user can select the profile ID to configure.
From CoS – To CoS:	Here the user can select the range on CoS to configure.
Scheduling Mechanism:	<p>Here the user can select one of two Scheduling Mechanisms:</p> <p><i>Strict</i> – The queue will operate in strict mode. The highest class of service is the first to process traffic. That is, the highest class of service will finish before other queues empty.</p> <p><i>Weight</i> – Specifies the weights for weighted round robin. A value between 1 and n can be specified. The queue will operate in WRR mode if port mode is WRR. It will operate in strict mode if port mode is strict.</p> <p>Determination of n is project dependent.</p>

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

Scheduling Group Settings

On this page the user can configure the scheduling group parameters.\

Scheduling Group Settings	
Profile ID	2
Port List (e.g.: 1, 4-9)	
<input type="button" value="Add"/> <input type="button" value="Delete"/>	
QoS Output Scheduling Group List	
Profile ID	Group Port List
1	1-28
2	
3	
4	
5	
6	
7	
8	

The fields that can be configured are described below:

Parameter	Description
Profile ID:	Here the user can select the profile ID to configure.
Port List:	Here the user can enter the port range to configure.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specific entry based on the information entered.

CPU RX Rate Limit Settings

The CPU RX Rate Limit Settings help to protect the CPU from receiving too many packets(ARP Request/Broadcast IP) over a short period. To many of these packet types can exhaust the CPU resources.

Use this window to configure CPU RX rate limit for ARP request and broadcast IP packets..

CPU RX Rate Limit Settings

CPU RX Rate Limit Settings

ARP Request (1-10000) No Limit

Broadcast IP (1-10000) No Limit

Apply

The fields that can be configured are described below:

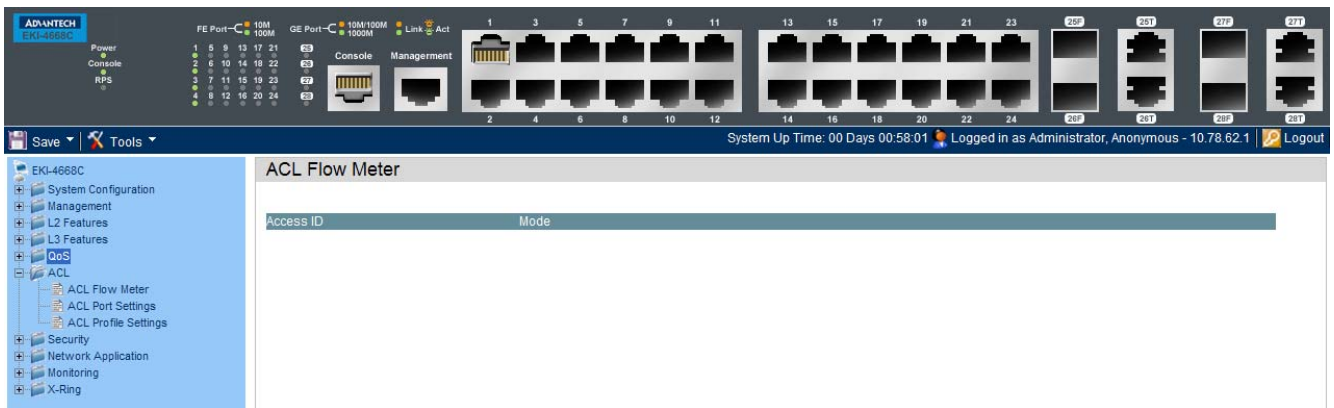
Parameter	Description
arp:	Specifies the rate limit will be applied to ARP request packets received on CPU. The setting is from 1 to 10000 CPU RX packets per second.
bcip:	Specifies the rate limit will be applied to broadcast IP packets received on CPU. The settings is from 1 to 10000 CPU RX packets per second.

Access Control List (ACL)

ACL Flow Meter — 180

ACL Port Settings — 181

Access Profile Settings — 182



ACL Flow Meter

??????????????

ACL Flow Meter	
Access ID	Mode

ACL Port Settings

Click on the View links to display the ACL configuration for each individual port.

ACL Port Settings	
ACL Interface List	
Interface	View
01	View
02	View
03	View
04	View
05	View
06	View
07	View
08	View
09	View
10	View
11	View
12	View
13	View
14	View
15	View
16	View
17	View
18	View
19	View
20	View
21	View
22	View
23	View
24	View
25	View
26	View
27	View
28	View

Access Profile Settings

Access profiles allow you to establish criteria to determine whether the Switch will forward packets based on the information contained in each packet's header.

The Switch supports four Profile Types, Ethernet ACL, IPv4 ACL, IPv6 ACL, and Packet Content ACL.

Creating an access profile is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below in two parts.

Users can display the currently configured Access Profiles on the Switch.

ACL Profile Table

Access List Name Type Extended

Access List Group Settings

Access List Name Port

Total Entries: 0

Access List Name	Type	Rule List	Add Rule	Delete
Total Entries: 0				

Click the **Add ACL Profile** button to add an entry to the **Access Profile List**.

Click the **Delete All** button to remove all access profiles from this table.

Click the **Show Details** button to display the information of the specific profile ID entry.

Click the **Add/View Rules** button to view or add ACL rules within the specified profile ID.

Click the **Delete** button to remove the specific entry.

Click the **Show Total Entries** button to view the total amount of consumed hardware entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

There are four **Add Access Profile** windows;

one for Ethernet (or MAC address-based) profile configuration,

one for IPv6 address-based profile configuration,

one for IPv4 address-based profile configuration, and

one for packet content profile configuration.

Adding an IPv4 ACL Profile

The window shown below is the **Add ACL Profile** window for IPv4. To use specific filtering masks in this ACL profile, click on the packet filtering mask field to highlight it red. This will add more files to the mask.

After clicking the **Add ACL Profile** button, the following page will appear:

The screenshot shows the 'ACL Profile Table' interface. At the top, there are input fields for 'Access List Name' and 'Type' (set to 'IPv4'), along with an 'Extended' checkbox and 'Add', 'View All', and 'Find' buttons. Below this is the 'Access List Group Settings' section with another 'Access List Name' field, a 'Port' dropdown (set to '01'), and an 'Apply' button. A 'Total Entries: 1' label is present above a table. The table has columns for 'Access List Name', 'Type', 'Rule List', 'Add Rule', and 'Delete'. One entry, 'ACL_1', is listed with type 'ip access-list'. The 'Rule List' column contains a 'View' link, and the 'Add Rule' column contains an 'Add' link. The 'Delete' column contains a 'Delete' link. At the bottom right of the table, there are pagination controls showing '1/1' and '1' items, with a 'Go' button.

The fields that can be configured are described below:

Parameter	Description
Profile ID:	Here the user can enter a unique identifier number for this profile set. This value can be set from 1 to 1024.
Select ACL Type:	<p>Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or packet content. This will change the window according to the requirements for the type of profile.</p> <p>Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header.</p> <p>Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header.</p> <p>Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header.</p> <p>Select Packet Content to instruct the Switch to examine the packet content in each frame's header.</p>
802.1Q VLAN:	Selecting this option instructs the Switch to examine the 802.1Q VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.

IPv4 DSCP:	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
IPv4 Source IP Mask:	Enter an IP address mask for the source IP address.
IPv4 Destination IP Mask:	Enter an IP address mask for the destination IP address.

<p>Protocol:</p>	<p>Selecting this option instructs the Switch to examine the protocol type value in each frame's header. Then the user must specify what protocol(s) to include according to the following guidelines:</p> <p>Select <i>ICMP</i> to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.</p> <p>Select <i>Type</i> to further specify that the access profile will apply an ICMP type value, or specify <i>Code</i> to further specify that the access profile will apply an ICMP code value.</p> <p>Select <i>IGMP</i> to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header.</p> <p>Select <i>Type</i> to further specify that the access profile will apply an IGMP type value.</p> <p>Select <i>TCP</i> to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires that you specify a source port mask and/or a destination port mask.</p> <p><i>src port mask</i> - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter.</p> <p><i>Summer Time port mask</i> - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter.</p> <p><i>flag bit</i> - The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between <i>urg</i> (urgent), <i>ack</i> (acknowledgement), <i>psh</i> (push), <i>rst</i> (reset), <i>syn</i> (synchronize), <i>fin</i> (finish).</p> <p>Select <i>UDP</i> to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask.</p> <p><i>src port mask</i> - Specify a UDP port mask for the source port in hex form (hex 0x0-0xffff).</p> <p><i>Summer Time port mask</i> - Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff).</p> <p>Select <i>Protocol ID</i> - Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xff).</p> <p><i>Protocol ID Mask</i> - Specify that the rule applies to the IP protocol ID traffic.</p> <p><i>User Define</i> - Specify the Layer 4 part mask</p>
-------------------------	---

Click the **Select** button to select an ACL type. Click the **Create** button to create a profile.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

Access Rule Detail Information	
ACL Rule Details	
Access ID	1
Profile Type	IP
Action	Deny
Source IP	10.78.62.1
Destination IP	10.78.62.2
TCP	Yes

Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:

ACL Rule List	
<input type="button" value=" <<Back"/>	
Total Entries: 1	
Rule ID	Delete
1	Delete Detail

1/1 1

Click the **Add Rule** button to create a new ACL rule in this profile.

Click the **<<Back** button to return to the previous page.

Click the **Show Details** button to view more information about the specific rule created.

Click the **Delete Rules** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:

Add Access Rule

Profile Information
 Profile Name: ACL_1

Rule Detail

Access ID (1-1024): Auto Assign

Rule Action Type:

Source IP Address: (e.g.: 192.168.1.10)

Destination IP Address: (e.g.: 192.168.1.10)

Rule Action

Action:

Priority (0-7):

Replace Priority:

Replace DSCP (0-63):

Replace ToS Precedence (0-7):

Rate Control

Rate (0-1000000):

Burst Size (0-16384):

Rate Exceed:

Remark DSCP Value (0-63):

Counter:

The fields that can be configured are described below:

Parameter	Description
Access ID (1-1024):	Type in a unique identifier number for this access. This value can be set from 1 to 1024. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Action:	Select Permit to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select Deny to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered. Select Mirror to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7):	Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority:	Tick this check box to replace the Priority value in the adjacent field.
Replace DSCP (0-63):	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv4 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.

Replace ToS Precedence (0-7):	Specify that the IP precedence of the outgoing packet is changed with the new value. If used without an action priority, the packet is sent to the default TC.
Time Range Name:	Tick the check box and enter the name of the Time Range settings that has been previously configured in the Time Range Settings window. This will set specific times when this access rule will be implemented on the Switch.
Counter:	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports:	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. Ticking the All Ports check box will denote all ports on the Switch.
VLAN Name:	Specify the VLAN name to apply to the access rule.
VLAN ID:	Specify the VLAN ID to apply to the access rule.

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

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:

Access Rule Detail Information	
ACL Rule Details	
Access ID	1
Profile Type	IP
Action	Deny
Source IP	10.78.62.1
Destination IP	10.78.62.2
TCP	Yes
<<Back	

Click the **Show All Rules** button to navigate back to the Access Rule List.

Adding an IPv6 ACL Profile

The window shown below is the **Add ACL Profile** window for IPv6. To use specific filtering masks in this ACL profile, click on the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add ACL Profile** button, the following page will appear:

The fields that can be configured are described below:

Parameter	Description
Profile ID:	Here the user can enter a unique identifier number for this profile set. This value can be set from 1 to 1024.
Select ACL Type:	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or packet content. This will change the window according to the requirements for the type of profile. Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header. Select Packet Content to instruct the Switch to examine the packet content in each frame's header.
IPv6 Class:	Ticking this check box will instruct the Switch to examine the <i>class</i> field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
IPv6 Flow Label:	Ticking this check box will instruct the Switch to examine the <i>flow label</i> field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
IPv6 TCP:	<i>Source Port Mask</i> – Specify that the rule applies to the range of TCP source ports. <i>Destination Port Mask</i> – Specify the range of the TCP destination port range.
IPv6 UDP:	<i>Source Port Mask</i> – Specify the range of the TCP source port range. <i>Destination Port Mask</i> – Specify the range of the TCP destination port mask.
IPv6 Source Address:	The user may specify an IP address mask for the source IPv6 address by ticking the corresponding check box and entering the IP address mask.
IPv6 Destination Address:	The user may specify an IP address mask for the destination IPv6 address by ticking the corresponding check box and entering the IP address mask.

Click the **Select** button to select an ACL type. Click the **Create** button to create a profile.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

Access Rule Detail Information	
ACL Rule Details	
Access ID	1024
Profile Type	IPv6
Action	Deny
Source IPv6	2F::3
Destination IPv6	5B::5
TCP	Yes
<<Back	

Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:

ACL Rule List	
<<Back	
Total Entries: 1	
Rule ID	Delete
1024	Delete Detail
1/1 1 <input type="text"/> Go	

Click the **Add Rule** button to create a new ACL rule in this profile.

Click the **<<Back** button to return to the previous page.

Click the **Show Details** button to view more information about the specific rule created.

Click the **Delete Rules** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:

Add IPv6 Access Rule

Profile Information
 Profile Name: ACLv6_1

Rule Detail
 Access ID (1-1024): Auto Assign
 Rule Action Type:
 Source IPv6 Address: (e.g.: 3EFF::3)
 Destination IPv6 Address: (e.g.: 3EFF::3)

Rule Action
 Action:
 Priority (0-7):
 Replace Priority:
 Replace DSCP (0-63):
 Replace ToS Precedence (0-7):
 Rate Control
 Rate (0-1000000):
 Burst Size (0-16384):
 Rate Exceed:
 Remark DSCP Value (0-63):
 Counter:

The fields that can be configured are described below:

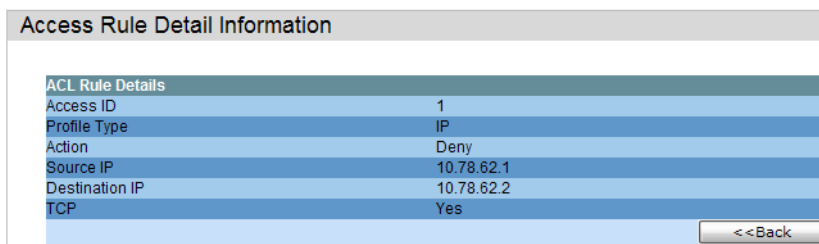
Parameter	Description
Access ID (1-1024):	Type in a unique identifier number for this access. This value can be set from 1 to 1024. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Action:	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify that packets that match the access profile are not forwarded by the Switch and will be filtered. Select <i>Mirror</i> to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7):	Tick the corresponding check box to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority:	Tick this check box to replace the Priority value in the adjacent field.

Replace DSCP (0-63):	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv6 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Replace ToS Precedence (0-7):	Specify that the IP precedence of the outgoing packet is changed with the new value. If used without an action priority, the packet is sent to the default TC.
Time Range Name:	Tick the check box and enter the name of the Time Range settings that has been previously configured in the Time Range Settings window. This will set specific times when this access rule will be implemented on the Switch.
Counter:	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports:	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. Ticking the All Ports check box will denote all ports on the Switch.
VLAN Name:	Specify the VLAN name to apply to the access rule.
VLAN ID:	Specify the VLAN ID to apply to the access rule.

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

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:



Click the **Show All Rules** button to navigate back to the Access Rule List.

Adding a Packet Content (MAC) ACL Profile

The window shown below is the **Add ACL Profile** window for Packet Content: To use specific filtering masks in this ACL profile, click on the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add ACL Profile** button, the following page will appear:

ACL Profile Table

Access List Name Type Mac Extended

Access List Group Settings

Access List Name Port 01

Total Entries: 2

Access List Name	Type	Rule List	Add Rule	Delete
ACL_1	ip access-list	View	Add	Delete
ACLv6_1	ipv6 access-list	View	Add	Delete

1/1 1

The fields that can be configured are described below:

Parameter	Description
Profile ID:	Here the user can enter a unique identifier number for this profile set. This value can be set from 1 to 1024.
Select ACL Type:	<p>Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or packet content. This will change the window according to the requirements for the type of profile.</p> <p>Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header.</p> <p>Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header.</p> <p>Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header.</p> <p>Select Packet Content to instruct the Switch to examine the packet content in each frame's header.</p>

Packet Content:

Source MAC - Specifies the source MAC mask.

Destination MAC - Specifies the destination MAC mask.

Outer Tag - Specifies the outer VLAN tag of the packet to mask. This constitutes only the 12-bit VID fields.

Offset1, Offset2, Offset3, Offset4, Offset5, Offset6 - Defines the UDF fields that the device filters.

Each UDF field consists of 1-byte of data, which is n bytes away from the offset reference (where n is the offset value).

The offset ranges are from 0 to 127.

The offset reference can be one of the following:

L2 – The offset starts counting from the byte after the end of the VLAN tags (start of ether type).

L3 – The offset starts counting right after the ether type field. The packet must have a valid L2 header and a recognizable ether type in order to be recognized.

L4 – The offset starts counting right after the end of the IP header. The packet must have a valid IP header in order to be recognized.

Click the **Select** button to select an ACL type. Click the **Create** button to create a profile.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

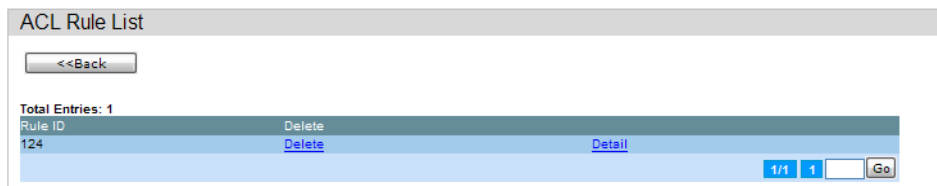
Access Rule Detail Information	
ACL Rule Details	
Access ID	124
Profile Type	MAC Access List
VLAN ID	1
Action	Deny
Source MAC	CB-CB-CB-CB-CB-CB
Source MAC Mask	FF-FF-FF-FF-FF-FF
Destination MAC	1F-1F-1F-1F-1F-1F
Destination MAC Mask	3E-3E-3E-3E-3E-3E
802.1p	0
Ethernet Type	0x8FFF
<input type="button" value="<<Back"/>	

Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.



NOTE: Address Resolution Protocol (ARP) is the standard for finding a host's hardware address (MAC address). However, ARP is vulnerable as it can be easily spoofed and utilized to attack a LAN (i.e. an ARP spoofing attack). For a more detailed explanation on how ARP protocol works and how to employ Advantech's unique Packet Content ACL to prevent ARP spoofing attack, please see Appendix E at the end of this manual.

After clicking the **Add/View Rules** button, the following page will appear:



Click the **Add Rule** button to create a new ACL rule in this profile.

Click the **<<Back** button to return to the previous page.

Click the **Show Details** button to view more information about the specific rule created.

Click the **Delete Rules** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:

The fields that can be configured are described below:

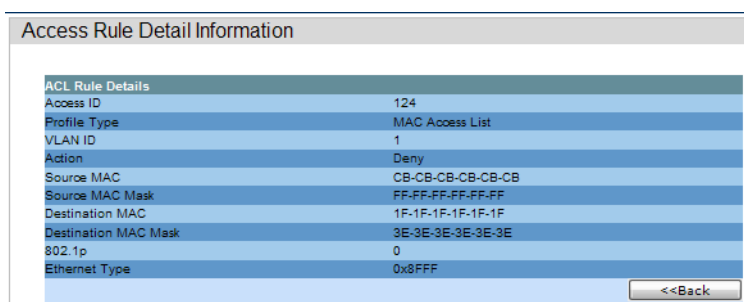
Parameter	Description
Access ID (1-1024):	Type in a unique identifier number for this access. This value can be set from 1 to 1024. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Action:	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered. Select <i>Mirror</i> to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7):	Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority:	Tick this check box to replace the Priority value in the adjacent field.

Replace DSCP (0-63):	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv4 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Replace ToS Precedence (0-7):	Specify that the IP precedence of the outgoing packet is changed with the new value. If used without an action priority, the packet is sent to the default TC.
Time Range Name:	Tick the check box and enter the name of the Time Range settings that has been previously configured in the Time Range Settings window. This will set specific times when this access rule will be implemented on the Switch.
Counter:	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports:	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. Ticking the All Ports check box will denote all ports on the Switch.
VLAN Name:	Specify the VLAN name to apply to the access rule.
VLAN ID:	Specify the VLAN ID to apply to the access rule.

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

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:



Click the **Show All Rules** button to navigate back to the Access Rule List.

Security

802.1X Folder — 199

RADIUS Folder — 209

IP-MAC-Port Binding (IMPB) Folder — 212

Port Security Folder — 218

Loopback Detection Settings — 221

Traffic Segmentation Settings — 223

SSL Settings — 224

Trusted Host Settings — 227

The screenshot displays the web management interface for an ADANTECH EKI-4668C switch. At the top, there is a status bar with system information: "System Up Time: 00 Days 00:56:59" and "Logged in as Administrator, Anonymous - 10.78.62.1". Below this is a navigation menu on the left with categories like System Configuration, Management, L2 Features, L3 Features, QoS, ACL, Security, and Network Application. The main content area is titled "802.1X Global Settings" and contains the following configuration options:

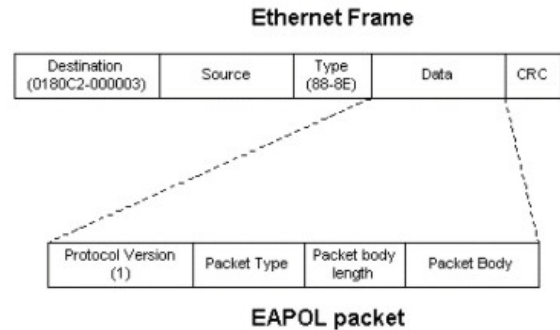
- Authentication State: Disabled
- Authentication Protocol: RADIUS EAP
- Forward EAPOL PDU: Disabled

An "Apply" button is located at the bottom right of the settings area. The top of the interface also shows a physical port layout with labels for FE Port, GE Port, Console, and Management.

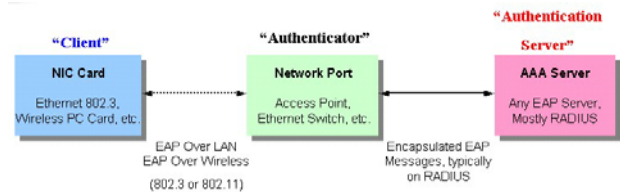
802.1X Folder

802.1X (Port-Based and Host-Based Access Control)

The IEEE 802.1X standard is a security measure for authorizing and authenticating users to gain access to various wired or wireless devices on a specified Local Area Network by using a Client and Server based access control model. This is accomplished by using a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and the Server. The following figure represents a basic EAPOL packet:



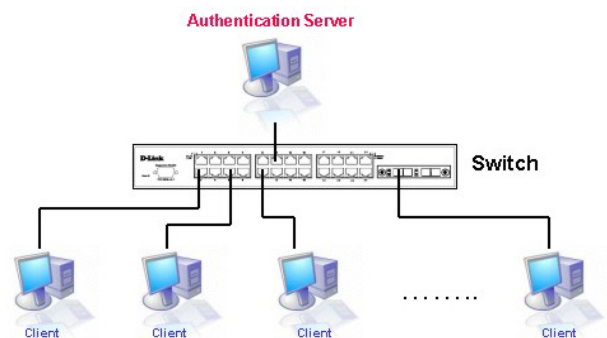
Utilizing this method, unauthorized devices are restricted from connecting to a LAN through a port to which the user is connected. EAPOL packets are the only traffic that can be transmitted through the specific port until authorization is granted. The 802.1X Access Control method has three roles, each of which are vital to creating and up keeping a stable and working Access Control security method.



The following section will explain the three roles of Client, Authenticator and Authentication Server in greater detail.

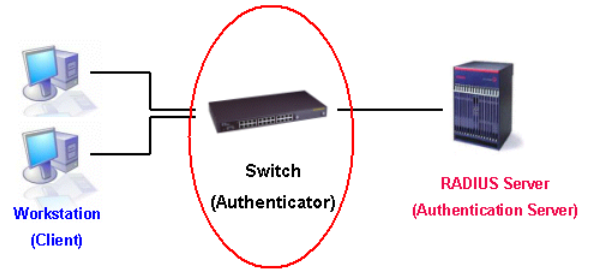
Authentication Server

The Authentication Server is a remote device that is connected to the same network as the Client and Authenticator, must be running a RADIUS Server program and must be configured properly on the Authenticator (Switch). Clients connected to a port on the Switch must be authenticated by the Authentication Server (RADIUS) before attaining any services offered by the Switch on the LAN. The role of the Authentication Server is to certify the identity of the Client attempting to access the network by exchanging secure information between the RADIUS server and the Client through EAPOL packets and, in turn, informs the Switch whether or not the Client is granted access to the LAN and/or switches services.



Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator serves two purposes when utilizing the 802.1X function. The first purpose is to request certification information from the Client through EAPOL packets, which is the only information allowed to pass through the Authenticator before access is granted to the Client. The second purpose of the Authenticator is to verify the information gathered from the Client with the Authentication Server, and to then relay that information back to the Client.

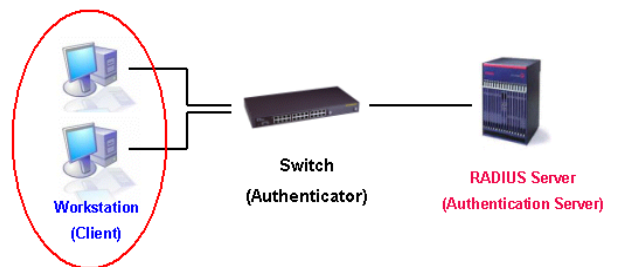


Three steps must be implemented on the Switch to properly configure the Authenticator.

1. The 802.1X State must be *Enabled*. (**Security / 802.1X / 802.1X Settings**)
2. The 802.1X settings must be implemented by port (**Security / 802.1X / 802.1X Settings**)
3. A RADIUS server must be configured on the Switch. (**Security / 802.1X / Authentic RADIUS Server**)

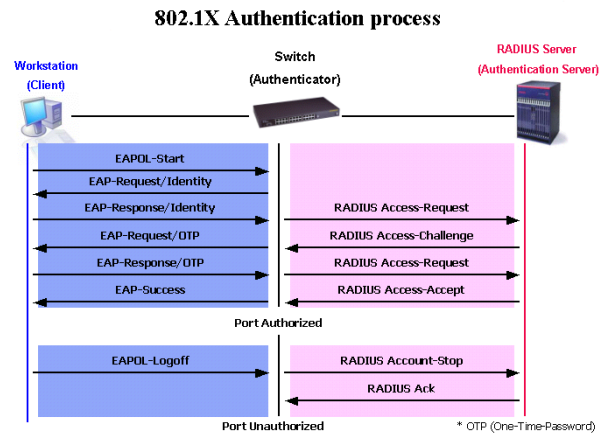
Client

The Client is simply the end station that wishes to gain access to the LAN or switch services. All end stations must be running software that is compliant with the 802.1X protocol. For users running Windows XP and Windows Vista, that software is included within the operating system. All other users are required to attain 802.1X client software from an outside source. The Client will request access to the LAN and or Switch through EAPOL packets and, in turn will respond to requests from the Switch.



Authentication Process

Utilizing the three roles stated above, the 802.1X protocol provides a stable and secure way of authorizing and authenticating users attempting to access the network. Only EAPOL traffic is allowed to pass through the specified port before a successful authentication is made. This port is “locked” until the point when a Client with the correct username and password (and MAC address if 802.1X is enabled by MAC address) is granted access and therefore successfully “unlocks” the port. Once unlocked, normal traffic is allowed to pass through the port. The following figure displays a more detailed explanation of how the authentication process is completed between the three roles stated above.



The Advantech implementation of 802.1X allows network administrators to choose between two types of Access Control used on the Switch, which are:

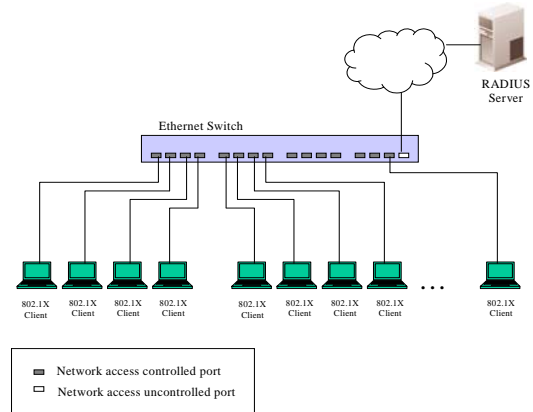
1. **Port-Based Access Control** – This method requires only one user to be authenticated per port by a remote RADIUS server to allow the remaining users on the same port access to the network.
2. **Host-Based Access Control** – Using this method, the Switch will automatically learn up to a maximum of 16 MAC addresses by port and set them in a list. Each MAC address must be authenticated by the Switch using a remote RADIUS server before being allowed access to the Network.

Understanding 802.1X Port-based and Host-based Network Access Control

The original intent behind the development of 802.1X was to leverage the characteristics of point-to-point in LANs. As any single LAN segment in such infrastructures has no more than two devices attached to it, one of which is a Bridge Port. The Bridge Port detects events that indicate the attachment of an active device at the remote end of the link, or an active device becoming inactive. These events can be used to control the authorization state of the Port and initiate the process of authenticating the attached device if the Port is unauthorized. This is the Port-Based Network Access Control.

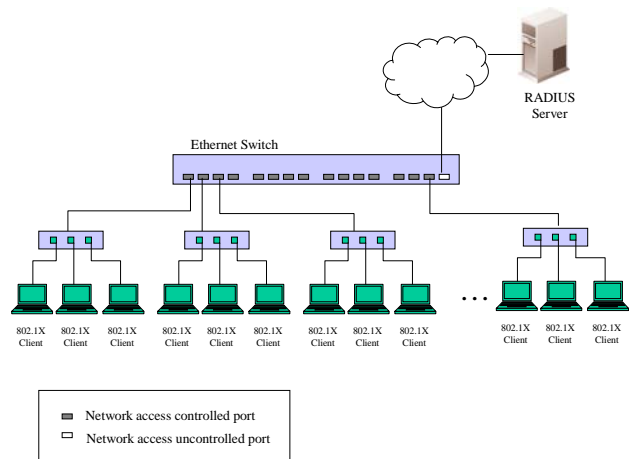
Port-Based Network Access Control

Once the connected device has successfully been authenticated, the Port then becomes Authorized, and all subsequent traffic on the Port is not subject to access control restriction until an event occurs that causes the Port to become Unauthorized. Hence, if the Port is actually connected to a shared media LAN segment with more than one attached device, successfully authenticating one of the attached devices effectively provides access to the LAN for all devices on the shared segment. Clearly, the security offered in this situation is open to attack.



Host-Based Network Access Control

In order to successfully make use of 802.1X in a shared media LAN segment, it would be necessary to create “logical” Ports, one for each attached device that required access to the LAN. The Switch would regard the single physical Port connecting it to the shared media segment as consisting of a number of distinct logical Ports, each logical Port being independently controlled from the point of view of EAPOL exchanges and authorization state. The Switch learns each attached devices’ individual MAC addresses, and effectively creates a logical Port that the attached device can then use to communicate with the LAN via the Switch.



802.1X Global Settings

Users can configure the 802.1X global parameter.vb

802.1X Global Settings

Authentication State

Forward EAPOL PDU

Authentication Protocol

The fields that can be configured are described below:

Parameter	Description
Authentication Mode:	Choose the 802.1X authenticator mode, <i>Disabled</i> , <i>Port Based</i> , or <i>MAC(host)-based</i> .
Authentication Protocol:	Choose the authenticator protocol, <i>Local</i> or <i>RADIUS EAP</i> .
Forward EAPOL PDU:	This is a global setting to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or for a port, and if 802.1X forward PDU is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports for which 802.1X forward PDU is enabled and 802.1X is disabled (globally or just for the port). The default state is disabled.
Max Users:	Specifies the maximum number of users. The limit on the maximum users is 1792 users.
RADIUS Authorization:	This option is used to enable or disable acceptance of authorized configuration. When the authorization is enabled for 802.1X's RADIUS, the authorized data assigned by the RADIUS server will be accepted if the global authorization network is enabled.

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

802.1X Port Settings

Users can configure the 802.1X authenticator port settings.

802.1X Port Settings

802.1X Port Access Control

From Port	<input type="text" value="01"/>	To Port	<input type="text" value="01"/>
QuietPeriod (0-65535)	<input type="text" value="60"/> sec	SuppTimeout (1-65535)	<input type="text" value="30"/> sec
ServerTimeout (1-65535)	<input type="text" value="30"/> sec	MaxReq (1-10)	<input type="text" value="2"/> times
TX Period (1-65535)	<input type="text" value="30"/> sec	ReAuthPeriod (1-65535)	<input type="text" value="3600"/> sec
ReAuthentication	<input type="text" value="Disabled"/>	Port Control	<input type="text" value="Auto"/>
Capability	<input type="text" value="None"/>	Direction	<input type="text" value="Both"/>
Forward EAPOL PDU	<input type="text" value="Disabled"/>	<input type="button" value="Refresh"/> <input type="button" value="Apply"/>	

Port	AdmDir	OpenCrDir	Port Control	Tx Period	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth	Capability	Forward EAPOL PDU
1	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled
2	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled
3	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled
4	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled
5	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled
6	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled
7	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled
8	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled
9	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled
10	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled
11	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled
12	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled
13	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled
14	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled
15	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled

The fields that can be configured are described below:

Parameter	Description
From Port:	Enter the beginning port of the range of ports to be set.
To Port:	Enter the ending port of the range of ports to be set.
QuietPeriod:	This allows the user to set the number of seconds that the Switch remains in the quiet state following a failed authentication exchange with the client. The default setting is 60 seconds.
SuppTimeout:	This value determines timeout conditions in the exchanges between the Authenticator and the client. The default setting is 30 seconds.
ServerTimeout:	This value determines timeout conditions in the exchanges between the Authenticator and the authentication server. The default setting is 30 seconds.
MaxReq:	The maximum number of times that the Switch will retransmit an EAP Request to the client before it times out of the authentication sessions. The default setting is 2.
TxPeriod:	This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. The default setting is 30 seconds.
ReAuthPeriod:	A constant that defines a nonzero number of seconds between periodic re-authentication of the client. The default setting is 3600 seconds.
ReAuthentication:	Determines whether regular re-authentication will take place on this port. The default setting is <i>Disabled</i> .

Port Control:	<p>This allows the user to control the port authorization state.</p> <p>Select <i>ForceAuthorized</i> to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client.</p> <p>If <i>ForceUnauthorized</i> is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface.</p> <p>If <i>Auto</i> is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server.</p> <p>The default setting is <i>Auto</i>.</p>
Capability:	<p>This allows the 802.1X Authenticator settings to be applied on a per-port basis. Select <i>Authenticator</i> to apply the settings to the port. When the setting is activated, a user must pass the authentication process to gain access to the network. Select <i>None</i> disable 802.1X functions on the port.</p>
Direction:	<p>Sets the administrative-controlled direction to <i>Both</i> or <i>In</i>. If <i>Both</i> is selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field. If <i>In</i> is selected, the control is only exerted over incoming traffic through the port the user selected in the first field.</p>
Forward EAPOL PDU:	<p>This is a global setting to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or for a port, and if 802.1X forward PDU is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports for which 802.1X forward PDU is enabled and 802.1X is disabled (globally or just for the port). The default state is disabled.</p>
Max Users:	<p>Specifies the maximum number of users. The maximum user limit is 1792 users. By default, the maximum value is selected.</p>

Click the **Refresh** button to refresh the display table so that new entries will appear.

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

802.1X User Settings

Users can set different 802.1X users in switch's local database.

802.1X User Settings

802.1X User
Password
Confirm Password

Note: 802.1X User and Password should be less than 16 characters.

802.1X User Table
Total Entries: 0

User Name	Password

The fields that can be configured are described below:

Parameter	Description
802.1X User:	The user can enter an 802.1X user's username in here.
Password:	The user can enter an 802.1X user's password in here.
Confirm Password:	The user can re-enter an 802.1X user's password in here.

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

Click the **Delete** button to remove the specific entry.

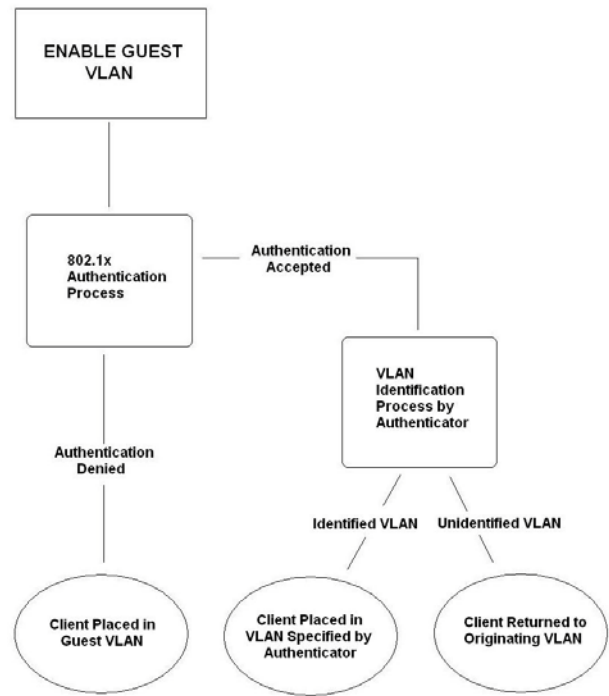


NOTE: The **802.1X User** and **Password** values should be less than 16 characters.

Guest VLAN Settings

On 802.1X security-enabled networks, there is a need for non- 802.1X supported devices to gain limited access to the network, due to lack of the proper 802.1X software or incompatible devices, such as computers running Windows 98 or older operating systems, or the need for guests to gain access to the network without full authorization or local authentication on the Switch. To supplement these circumstances, this switch now implements 802.1X Guest VLANs. These VLANs should have limited access rights and features separate from other VLANs on the network.

To implement 802.1X Guest VLANs, the user must first create a VLAN on the network with limited rights and then enable it as an 802.1X guest VLAN. Then the administrator must configure the guest accounts accessing the Switch to be placed in a Guest VLAN when trying to access the Switch. Upon initial entry to the Switch, the client wishing services on the Switch will need to be authenticated by a remote RADIUS Server or local authentication on the Switch to be placed in a fully operational VLAN.



If authenticated and the authenticator possess the VLAN placement information, that client will be accepted into the fully operational target VLAN and normal switch functions will be open to the client. If the authenticator does not have target VLAN placement information, the client will be returned to its originating VLAN. Yet, if the client is denied authentication by the authenticator, it will be placed in the Guest VLAN where it has limited rights and access. The adjacent figure should give the user a better understanding of the Guest VLAN process.

Limitations Using the Guest VLAN

1. Ports supporting Guest VLANs cannot be GVRP enabled and vice versa.
2. A port cannot be a member of a Guest VLAN and a static VLAN simultaneously.
3. Once a client has been accepted into the target VLAN, it can no longer access the Guest VLAN.

Remember, to set an 802.1X guest VLAN, the user must first configure a normal VLAN, which can be enabled here for guest VLAN status. Only one VLAN may be assigned as the 802.1X guest VLAN.

The fields that can be configured are described below:

Parameter	Description
VLAN Name:	Enter the pre-configured VLAN name to create as an 802.1X guest VLAN.
Port:	Set the ports to be enabled for the 802.1X guest VLAN. Click the All button to select all the ports.

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

Click the **Delete** button to remove the specific entry based on the information entered.

RADIUS Folder

Authentication RADIUS Server Settings

The RADIUS feature of the Switch allows the user to facilitate centralized user administration as well as providing protection against a sniffing, active hacker.

Authentication RADIUS Server Settings

Index: (e.g.: 10.90.90.90)

Server IP:

Authentication Port (1-65535): Default

Accounting Port (1-65535): Default

Timeout (1-255): sec Default

Retransmit (1-20): times Default

Key (Max: 32 characters):

Confirm Key:

RADIUS Server List

Index	IP Address	Auth-Port	Acct-Port	Timeout	Retransmit	Key
1						
2						
3						

The fields that can be configured are described below:

Parameter	Description
Index:	Choose the desired RADIUS server to configure: 1, 2 or 3 and select the IPv4 Address.
Server IP:	Set the RADIUS server IP address.
Authentication Port:	Set the RADIUS authentic server(s) UDP port which is used to transmit RADIUS data between the Switch and the RADIUS server. The default port is 1812.
Accounting Port:	Set the RADIUS account server(s) UDP port which is used to transmit RADIUS accounting statistics between the Switch and the RADIUS server. The default port is 1813.
Timeout:	Set the RADIUS server age-out, in seconds.
Retransmit:	Set the RADIUS server retransmit time, in times.
Key:	Set the key the same as that of the RADIUS server.
Confirm Key:	Confirm the key the same as that of the RADIUS server.

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

RADIUS Authentication

Users can display information concerning the activity of the RADIUS authentication client on the client side of the RADIUS authentication protocol.

AccessRejects	AccessChallenges	AccessResponses	BadAuthenticators	PendingRequests	Timeouts	UnknownTypes	PacketsDropped
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

The user may also select the desired time interval to update the statistics, between 1s and 60s, where “s” stands for seconds. The default value is one second.

The fields that can be configured are described below:

Parameter	Description
InvalidServerAddresses:	The number of RADIUS Access-Response packets received from unknown addresses.
Identifier:	The NAS-Identifier of the RADIUS authentication client.
ServerIndex:	The identification number assigned to each RADIUS Authentication server that the client shares a secret with.
AuthServerAddress:	The (conceptual) table listing the RADIUS authentication servers with which the client shares a secret.
ServerPortNumber:	The UDP port the client is using to send requests to this server.
RoundTripTime:	The time interval (in hundredths of a second) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
AccessRequests:	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
AccessRetransmissions:	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
AccessAccepts:	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
AccessRejects:	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
AccessChallenges:	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.

Click the **Clear** button to clear the current statistics shown.

IP-MAC-Port Binding (IMPB) Folder

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC-port binding is to restrict the access to a switch to a number of authorized users. Authorized clients can access a switch’s port by either checking the pair of IP-MAC addresses with the pre-configured database or if DHCP snooping has been enabled in which case the switch will automatically learn the IP/MAC pairs by snooping DHCP packets and saving them to the IMPB white list. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet. For the xStack® EKI-4668C series of switches, active and inactive entries use the same database. The maximum number of entries is 511. The creation of authorized users can be manually configured by CLI or Web. The function is port-based, meaning a user can enable or disable the function on the individual port.

IMPB Global Settings

Users can enable or disable the Trap/Log State and DHCP Snoop state on the Switch. The Trap/Log field will enable and disable the sending of trap/log messages for IP-MAC-port binding. When enabled, the Switch will send a trap message to the SNMP agent and the Switch log when an ARP packet is received that doesn’t match the IP-MAC-port binding configuration set on the Switch.

The fields that can be configured are described below:

Parameter	Description
Log:	This field will enable and disable the sending of log messages for IP-MAC-port binding. When <i>Enabled</i> , the Switch logs when an ARP packet is received that does not match the IP-MAC-port binding configuration set on the Switch. The default is <i>Disabled</i> .
DHCP Snooping:	Use the pull-down menu to enable or disable DHCP snooping for IP-MAC-port binding. The default is <i>Disabled</i> .

Click the **Apply** button to accept the changes made for each individual section.

IMPB Port Settings

Select a port or a range of ports with the From Port and To Port fields. Enable or disable the port with the State, Allow Zero IP and Forward DHCP Packet field, and configure the port's Max Entry.

IMPB Port Settings

From Port: To Port: State:

Port	State
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled

The fields that can be configured are described below:

Parameter	Description
From Port:	Select a starting port to set for IP-MAC-port binding.
To Port:	Select an ending port to set for IP-MAC-port binding.
State:	Use the pull-down menu to enable or disable these ports for IP-MAC-port binding.
Enabled (Strict):	This mode provides a stricter method of control. If the user selects this mode, all packets will be sent to the CPU, thus all packets will not be forwarded by the hardware until the S/W learns the entries for the ports. The port will check ARP packets and IP packets by IP-MAC-port binding entries. When the packet is found by the entry, the MAC address will be set to dynamic state. If the packet is not found by the entry, the MAC address will be set to block. Other packets will be dropped. The default mode is strict if not specified. The ports with strict mode will capture unicast DHCP packets through the ACL module. If configuring IP-MAC-port binding in strict mode when IP-MAC-port binding DHCP snooping is enabled, it will create an ACL profile and the rules according to the ports. If there is not enough profile or rule space for an ACL profile or rule table, it will return a warning message and will not create an ACL profile and rules to capture unicast DHCP packets.

Enabled (Loose):	This mode provides a looser way of control. If the user selects loose mode, ARP packets and IP broadcast packets will be sent to the CPU. The packets will still be forwarded by the hardware until a specific source MAC address is blocked by the software. The port will check ARP packets and IP broadcast packets by IP-MAC-port binding entries. When the packet is found by the entry, the MAC address will be set to dynamic state. If the packet is not found by the entry, the MAC address will be set to block. Other packets will be bypassed.
Zero IP:	Use the pull-down menu to enable or disable this feature. Allow zero IP configures the state which allows ARP packets with 0.0.0.0 source IP to bypass.
DHCP Packet:	By default, the DHCP packet with broadcast DA will be flooded. When set to disable, the broadcast DHCP packet received by the specified port will not be forwarded in strict mode. This setting is effective when DHCP snooping is enabled, in the case when a DHCP packet which has been trapped by the CPU needs to be forwarded by the software. This setting controls the forwarding behavior in this situation.
Mode:	Toggle between <i>ARP</i> and <i>ACL</i> . When configuring the port mode to <i>ACL</i> , the Switch will create an <i>ACL</i> access entry corresponding to the entries of this port. If the port changes to <i>ARP</i> , all the <i>ACL</i> access entries will be deleted automatically. The default mode is <i>ARP</i> .
Stop Learning Threshold:	Here is displayed the number of blocked entries on the port. The default value is <i>500</i> .

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

IMPB Entry Settings

This table is used to create static IP-MAC-binding port entries and view all IMPB entries on the Switch.

IMPB Entry Settings

IP Address MAC Address Ports All Ports

Total Entries: 0

IP Address	MAC Address	Ports	Mode
------------	-------------	-------	------

The fields that can be configured are described below:

Parameter	Description
IP Address:	Enter the IP address to bind to the MAC address set below.
MAC Address:	Enter the MAC address to bind to the IP Address set above.
Ports:	Specify the switch ports for which to configure this IP-MAC binding entry (IP Address + MAC Address). Click the All Ports check box to configure this entry for all ports on the Switch.

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

Click the **Find** button to locate a specific entry based on the information entered.

Click the **View All** button to display all the existing entries.

Click the **Delete All** button to remove all the entries listed.

DHCP Snooping Folder

DHCP Snooping Max Entry Settings

Users can configure the maximum DHCP snooping entry for ports on this page.

Port	Max Entry
1	5
2	5
3	5
4	5
5	5
6	5
7	5
8	5
9	5
10	5
11	5
12	5
13	5
14	5
15	5
16	5
17	5
18	5
19	5
20	5
21	5
22	5
23	5
24	5
25	5

The fields that can be configured are described below:

Parameter	Description
From Port – To Port:	Here the user can select a range of ports to use.
Max Entry:	Here the user can enter the maximum entry value.

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

DHCP Snooping Entries

This table is used to view dynamic entries on specific ports. To view particular port settings, enter the port number and click **Find**. To view all entries click **View All**, and to delete an entry, click **Clear**.

DHCP Snooping Entry

Port:

Ports (e.g.: 1, 7-12): All

Total Entries: 0

IP Address	MAC Address	Lease Time (sec)	Port	Status
------------	-------------	------------------	------	--------

The fields that can be configured are described below:

Parameter	Description
Port:	Use the drop-down menu to select the desired port.
Ports (e.g.: 1, 7-12):	Specify the ports for which to view DHCP snooping entries. Tick the All check box to clear entries for all ports.

Click the **Find** button to locate a specific entry based on the port number selected.

Click the **Clear** button to clear all the information entered in the fields.

Click the **View All** button to display all the existing entries.

Click the **Apply** button to accept the changes made for each individual section.

Total Entries: 1

MAC Address	VLAN Name	VID	Edit by Name	Apply
00-11-22-33-44-55	default	<input type="text" value="1"/>	<input type="button" value="Edit by Name"/>	<input type="button" value="Apply"/>

1/1

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Port Security Folder

Port Security Settings

A given port's (or a range of ports') dynamic MAC address learning can be locked such that the current source MAC addresses entered into the MAC address forwarding table cannot be changed once the port lock is enabled. The port can be locked by changing the Admin State pull-down menu to *Enabled* and clicking **Apply**.

Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to locking the port (or ports) from connecting to the Switch's locked ports and gaining access to the network.

Port Security Settings

Port Security Log Settings Enabled Disabled Apply

Port Security System Settings

System Maximum Address (1-448) No Limit Apply

From Port To Port State Secure Type Max. No. (0-448) Apply

Interface	State	Secure Type	Max. No.	
1	Disabled	DeleteOnReset	32	Edit
2	Disabled	DeleteOnReset	32	Edit
3	Disabled	DeleteOnReset	32	Edit
4	Disabled	DeleteOnReset	32	Edit
5	Disabled	DeleteOnReset	32	Edit
6	Disabled	DeleteOnReset	32	Edit
7	Disabled	DeleteOnReset	32	Edit
8	Disabled	DeleteOnReset	32	Edit
9	Disabled	DeleteOnReset	32	Edit
10	Disabled	DeleteOnReset	32	Edit
11	Disabled	DeleteOnReset	32	Edit
12	Disabled	DeleteOnReset	32	Edit
13	Disabled	DeleteOnReset	32	Edit
14	Disabled	DeleteOnReset	32	Edit

The fields that can be configured are described below:

Parameter	Description
Port Security Trap/ Log Settings:	Use the radio button to enable or disable Port Security Traps and Log Settings on the Switch.
System Max Address:	Here the user can enter the system maximum address.
From Port:	The beginning port of a consecutive group of ports to be configured.
To Port:	The ending port of a consecutive group of ports to be configured.
Admin State:	This pull-down menu allows the user to enable or disable Port Security (locked MAC address table for the selected ports).

Lock Address Mode:	This pull-down menu allows the option of how the MAC address table locking will be implemented on the Switch, for the selected group of ports. The options are: <i>Permanent</i> – The locked addresses will only age out after the Switch has been reset. <i>DeleteOnTimeout</i> – The locked addresses will age out after the aging timer expires. <i>DeleteOnReset</i> – The locked addresses will not age out until the Switch has been reset or rebooted.
Max Learning Address:	Specifies the maximum value of port security entries that can be learned on this port.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Edit** button to re-configure the specific entry.

Port Security Entries

Users can remove an entry from the port security entries learned by the Switch and entered into the forwarding database.

Port Security Entries

Clear Port Security Entries By Port

VLAN Name
 VID List (e.g.: 1, 4-6)

Port List (e.g.: 1, 4-6) All

Total Entries: 0

VID	MAC Address	Port	Lock Mode
-----	-------------	------	-----------

The fields that can be configured are described below:

Parameter	Description
VLAN Name:	The VLAN Name of the entry in the forwarding database table that has been permanently learned by the Switch.
VID List:	The VLAN ID of the entry in the forwarding database table that has been permanently learned by the Switch.
Port List:	Enter the port number or list here to be used for the port security entry search. When All is selected, all the ports configured will be displayed.
MAC Address:	The MAC address of the entry in the forwarding database table that has been permanently learned by the Switch.
Lock Mode:	The type of MAC address in the forwarding database table. Only entries marked Permanent or Delete on Reset can be deleted.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear** button to clear all the entries based on the information entered.

Click the **Show All** button to display all the existing entries.

Click the **Clear All** button to remove all the entries listed.

Click the **Delete** button to remove the specific entry.

Loopback Detection Settings

The Loopback Detection (LBD) function is used to detect the loop created by a specific port. This feature is used to temporarily shut down a port on the Switch when a CTP (Configuration Testing Protocol) packet has been looped back to the Switch. When the Switch detects CTP packets received from a port or a VLAN, this signifies a loop on the network. The Switch will automatically block the port or the VLAN and send an alert to the administrator. The Loopback Detection port will restart (change to discarding state) when the Loopback Detection Recover Time times out. The Loopback Detection function can be implemented on a range of ports at a time. The user may enable or disable this function using the pull-down menu.

Loopback Detection Settings

Loopback Detection Global Settings

Loopback Detection State Enabled Disabled Apply

Loopback Detection Global Settings

Mode Port-based Interval (1-32767) 10 sec

Trap State None Recover Time (0 or 60-1000000) 60 sec Apply

From Port 01 To Port 01 State Disabled Apply

Port	Loopback Detection State	Loop Status
1	Disabled	Normal
2	Disabled	Normal
3	Disabled	Normal
4	Disabled	Normal
5	Disabled	Normal
6	Disabled	Normal
7	Disabled	Normal
8	Disabled	Normal
9	Disabled	Normal
10	Disabled	Normal
11	Disabled	Normal
12	Disabled	Normal
13	Disabled	Normal
14	Disabled	Normal
15	Disabled	Normal
16	Disabled	Normal

The fields that can be configured are described below:

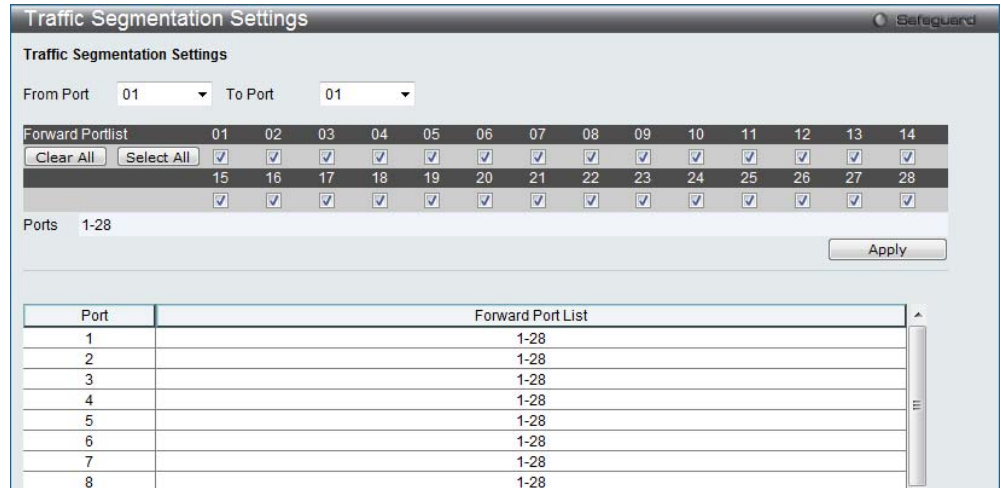
Parameter	Description
LBD State:	Use the radio button to enable or disable loopback detection. The default is Disabled.
Mode:	Use the drop-down menu to toggle between <i>Port Based</i> and <i>VLAN Based</i> .
Trap Status:	Set the desired trap status: <i>None</i> , <i>Loop Detected</i> , <i>Loop Cleared</i> , or <i>Both</i> .
Interval (1-32767):	Set a Loopdetect Interval between 1 and 32767 seconds. The default is 10 seconds.

Recover Time (0 or 60-1000000):	Time allowed (in seconds) for recovery when a Loopback is detected. The Loopdetect Recover Time can be set at 0 seconds, or 60 to 1000000 seconds. Entering 0 will disable the Loopdetect Recover Time. The default is 60 seconds.
From Port:	Use the drop-down menu to select a beginning port number.
To Port:	Use the drop-down menu to select an ending port number.
State:	Use the drop-down menu to toggle between <i>Enabled</i> and <i>Disabled</i> .

Click the **Apply** button to accept the changes made for each individual section.

Traffic Segmentation Settings

Traffic segmentation is used to limit traffic flow from a single or group of ports, to a group of ports. This method of segmenting the flow of traffic is similar to using VLANs to limit traffic, but is more restrictive. It provides a method of directing traffic that does not increase the overhead of the master switch CPU.



The fields that can be configured are described below:

Parameter	Description
From Port –To Port:	Here the user can select the ports to be included in the traffic segmentation setup.
Forward Port List:	Here the user can select the ports to be included in the traffic segmentation setup by simply ticking the corresponding port's tick box. Click the Clear All button to un-select all the ports for the configuration. Click the Select All button to select all the ports for the configuration.
Ports:	Here the ports that have been selected to be included in the traffic segmentation setup will be displayed.

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

SSL Settings

Secure Sockets Layer, or SSL, is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption. These security functions are implemented through the use of a cipher suite, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session and consists of three levels:

1. **Key Exchange:** The first part of the Ciphersuite string specifies the public key algorithm to be used. This switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the DHE DSS Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they “exchange keys” in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
2. **Encryption:** The second part of the cipher suite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:

Stream Ciphers – There are two types of stream ciphers on the Switch, *RC4 with 40-bit keys* and *RC4 with 128-bit keys*. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.

CBC Block Ciphers – CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the *3DES EDE* encryption code defined by the Data Encryption Standard (DES) to create the encrypted text.

1. **Hash Algorithm:** This part of the cipher suite allows the user to choose a message digest function which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports two hash algorithms, *MD5* (Message Digest 5) and *SHA* (Secure Hash Algorithm).

These three parameters are uniquely assembled in four choices on the Switch to create a three-layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the cipher suites available, yet different cipher suites will affect the security level and the performance of the secured connection. The information included in the cipher suites is not included with the Switch and requires downloading from a third source in a file form called a *certificate*. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server. The Switch supports SSLv3. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to host.

The **SSL Settings** window located on the next page will allow the user to enable SSL on the Switch and implement any one or combination of listed cipher suites

on the Switch. A cipher suite is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The Switch possesses four possible cipher suites for the SSL function, which are all enabled by default. To utilize a particular cipher suite, disable the unwanted cipher suites, leaving the desired one for authentication.

When the SSL function has been enabled, the web will become disabled. To manage the Switch through the web based management while utilizing the SSL function, the web browser must support SSL encryption and the header of the URL must begin with https://. (Ex. https://xx.xx.xx.xx) Any other method will result in an error and no access can be authorized for the web-based management.

Users can download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The Switch only supports certificate files with .der file extensions. Currently, the Switch comes with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

SSL Settings

SSL Global Settings

SSL State Enabled Disabled

Cache Timeout (60-86400) sec

Note: Web will be disabled if SSL is enabled. Apply

SSL Ciphersuite Settings

RSA with RC4_128_MD5 Enabled Disabled

RSA with 3DES EDE CBC SHA Enabled Disabled

DHE DSS with 3DES EDE CBC SHA Enabled Disabled

RSA EXPORT with RC4 40 MD5 Enabled Disabled Apply

SSL Certificate Download

Server IP Address

Certificate File Name

Key File Name Download

Current Certificate Loaded with RSA Certificate!

To set up the SSL function on the Switch, configure the parameters in the SSL Settings section described.

The fields that can be configured are described below:

Parameter	Description
SSL Status:	Use the radio buttons to enable or disable the SSL status on the Switch. The default is Disabled.
Cache Timeout (60-86400):	This field will set the time between a new key exchange between a client and a host using the SSL function. A new SSL session is established every time the client and host go through a key exchange. Specifying a longer timeout will allow the SSL session to reuse the master key on future connections with that particular host, therefore speeding up the negotiation process. The default setting is 600 seconds.

Click the Apply button to accept the changes made.

To set up the **SSL cipher suite function** on the Switch, configure the parameters in the SSL Cipher suite Settings section described below:

Parameter	Description
RSA with RC4_128_MD5:	This cipher suite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. Use the radio buttons to enable or disable this cipher suite. This field is Enabled by default.
RSA with 3DES EDE CBC SHA:	This cipher suite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. Use the radio buttons to enable or disable this cipher suite. This field is Enabled by default.
DHS DSS with 3DES EDE CBC SHA:	This cipher suite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. Use the radio buttons to enable or disable this cipher suite. This field is Enabled by default.
RSA EXPORT with RC4 40 MD5:	This cipher suite combines the RSA Export key exchange and stream cipher RC4 encryption with 40-bit keys. Use the radio buttons to enable or disable this cipher suite. This field is Enabled by default.

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

To download SSL certificates, configure the parameters in the SSL Certificate Download section described below.

Parameter	Description
Server IP Address:	Enter the IPv4 address of the TFTP server where the certificate files are located.
Certificate File Name:	Enter the path and the filename of the certificate file to download. This file must have a .der extension. (Ex. c:/cert.der)
Key File Name:	Enter the path and the filename of the key file to download. This file must have a .der extension (Ex. c:/pkey.der)

Click the **Download** button to download the SSL certificate based on the information entered.



NOTE: Certain implementations concerning the function and configuration of SSL are not available on the web-based management of this Switch and need to be configured using the command line interface.



NOTE: Enabling the SSL command will disable the web-based switch management. To log on to the Switch again, the header of the URL must begin with https://. Entering anything else into the address field of the web browser will result in an error and no authentication will be granted.

Trusted Host Settings

Up to ten trusted host secure IP addresses or ranges may be configured and used for remote Switch management. It should be noted that if one or more trusted hosts are enabled, the Switch will immediately accept remote instructions from only the specified IP address or addresses. If you enable this feature, be sure to first enter the IP address of the station you are currently using.

When the user clicks the **Edit** button, one will be able to edit the service allowed to the selected host.

The fields that can be configured are described below:

Parameter	Description
IPv4 Address:	Here the user can enter an IPv4 address to add to the trusted host list.
Net Mask:	Here the user can enter a Net Mask address to add to the trusted host list.
Access Interface:	Here the user can select services that will be allowed to the trusted host.

Click the **Add** button to add a new entry based on the information entered.

Click the Delete All button to remove all the entries listed.

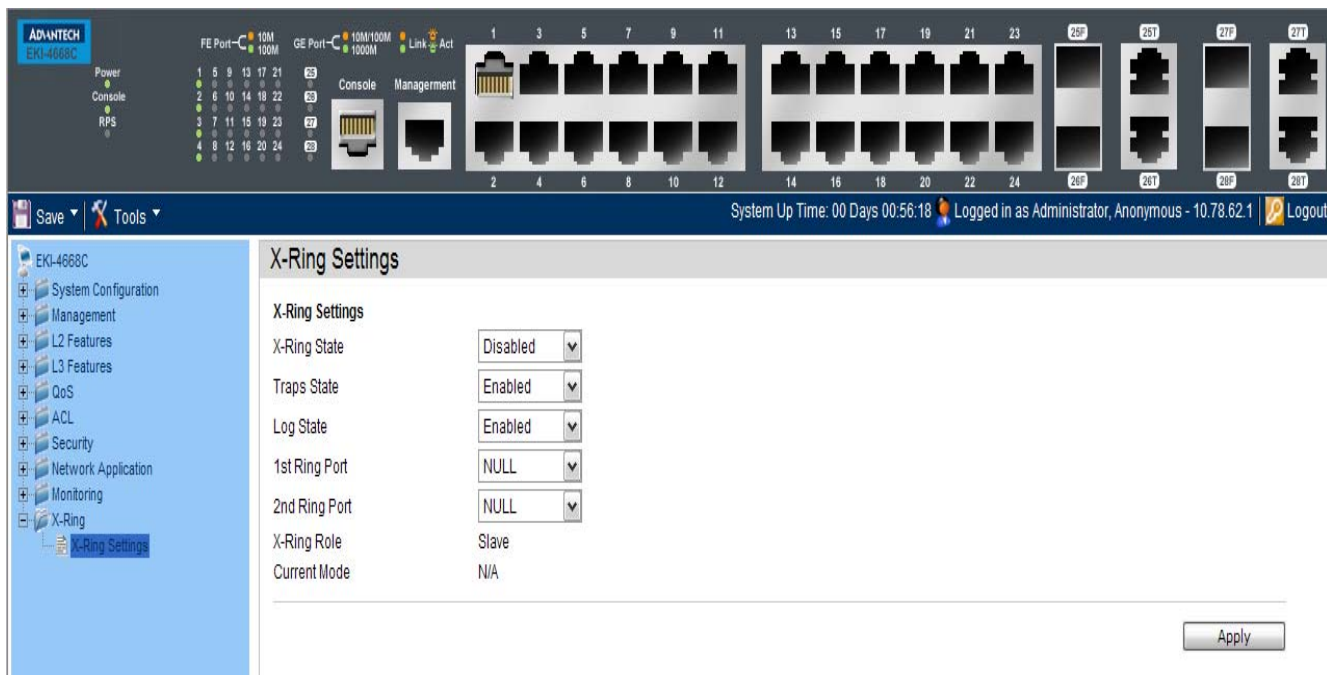
Network Application Folder

DHCP Folder — 229

SMTP Settings — 243

SNTP Folder — 246

Flash File System Settings — 249



DHCP Folder

DHCP Relay Folder

DHCP Relay Global Settings

Users can enable and configure DHCP Relay Global Settings. The relay hops count limit allows the maximum number of hops (routers) that the DHCP messages can be relayed through to be set. If a packet's hop count is more than the hop count limit, the packet is dropped. The range is between 1 and 16 hops, with a default value of 4. The relay time threshold sets the minimum time (in seconds) that the Switch will wait before forwarding a BOOTREQUEST packet. If the value in the seconds' field of the packet is less than the relay time threshold, the packet will be dropped. The range is between 0 and 65,535 seconds, with a default value of 0 seconds.

DHCP Relay Global Settings

DHCP Relay State	Disabled		
DHCP Relay Hops Count Limit (1-16)	4		
DHCP Relay Time Threshold (0-65535)	0	sec	
DHCP Relay Option 82 State	Disabled		
DHCP Relay Agent Information Option 82 Check	Disabled		
DHCP Relay Agent Information Option 82 Policy	Replace		
DHCP Relay Agent Information Option 82 Remote ID	34-08-04-45-B4-00	<input type="checkbox"/> Default	Apply
DHCP Relay Option 60 State	Disabled		
DHCP Relay Option 61 State	Disabled		Apply

The fields that can be configured are described below:

Parameter	Description
DHCP Relay State:	This field can be toggled between <i>Enabled</i> and <i>Disabled</i> using the pull-down menu. It is used to enable or disable the DHCP Relay service on the Switch. The default is <i>Disabled</i> .
DHCP Relay Hops Count Limit (1-16):	This field allows an entry between 1 and 16 to define the maximum number of router hops DHCP messages can be forwarded. The default hop count is 4.

DHCP Relay Time Threshold (0-65535):	Allows an entry between 0 and 65535 seconds, and defines the maximum time limit for routing a DHCP packet. If a value of 0 is entered, the Switch will not process the value in the seconds' field of the DHCP packet. If a non-zero value is entered, the Switch will use that value, along with the hop count to determine whether to forward a given DHCP packet.
DHCP Relay Option 82 State:	<p>This field can be toggled between <i>Enabled</i> and <i>Disabled</i> using the pull-down menu. It is used to enable or disable the DHCP Relay Agent Information Option 82 on the Switch. The default is <i>Disabled</i>.</p> <p><i>Enabled</i> –When this field is toggled to <i>Enabled</i>, the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts the reply back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.</p> <p><i>Disabled</i>- When the field is toggled to <i>Disabled</i>, the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.</p>
DHCP Relay Agent Information Option 82 Check:	<p>This field can be toggled between <i>Enabled</i> and <i>Disabled</i> using the pull-down menu. It is used to enable or disable the Switches ability to check the validity of the packet's option 82 field.</p> <p><i>Enabled</i> – When the field is toggled to <i>Enabled</i>, the relay agent will check the validity of the packet's option 82 field. If the switch receives a packet that contains the option 82 field from a DHCP client, the switch drops the packet because it is invalid. In packets received from DHCP servers, the relay agent will drop invalid messages.</p> <p><i>Disabled</i> – When the field is toggled to <i>Disabled</i>, the relay agent will not check the validity of the packet's option 82 field.</p>
DHCP Relay Agent Information Option 82 Policy:	<p>This field can be toggled between <i>Replace</i>, <i>Drop</i>, and <i>Keep</i> by using the pull-down menu. It is used to set the Switches policy for handling packets when the DHCP Relay Agent Information Option 82 Check is set to <i>Disabled</i>. The default is <i>Replace</i>.</p> <p><i>Replace</i> – The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client.</p> <p><i>Drop</i> – The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client.</p> <p><i>Keep</i> – The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.</p>
DHCP Relay Agent Information Option 82 Remote ID:	Here the user can enter the DHCP Relay Agent Information Option 82 Remote ID.

DHCP Relay Option 60 State:	Here the user can enable or disable the use of the DHCP Relay Option 60 State feature.
DHCP Relay Option 61 State:	Here the user can enable or disable the use of the DHCP Relay Option 61 State feature.

Click the **Apply** button to accept the changes made for each individual section.



NOTE: If the Switch receives a packet that contains the option 82 field from a DHCP client and the information-checking feature is enabled, the Switch drops the packet because it is invalid. However, in some instances, users may configure a client with the option 82 field. In this situation, disable the information check feature so that the Switch does not remove the option 82 field from the packet. Users may configure the action that the Switch takes when it receives a packet with existing option 82 information by configuring the DHCP Agent Information Option 82 Policy.

DHCP Relay Interface Settings

Users can set up a server, by IP address, for relaying DHCP information to the Switch. The user may enter a previously configured IP interface on the Switch that will be connected directly to the DHCP server using this window. Properly configured settings will be displayed in the DHCP Relay Interface Table at the bottom of the window, once the user clicks the Apply button. The user may add up to four server IPs per IP interface on the Switch. Entries may be deleted by clicking the corresponding Delete button.

The fields that can be configured are described below:

Parameter	Description
Interface:	The IP interface on the Switch that will be connected directly to the Server.
Server IP:	Enter the IP address of the DHCP server. Up to four server IPs can be configured per IP Interface.

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

DHCP Relay Option 60 Server Settings

On this page the user can configure the DHCP relay option 60 server parameters.

DHCP Relay Option 60 Server Settings

Relay IP Address (e.g.: 10.90.90.90)

Mode

Server1	Server2	Server3	Server4
---------	---------	---------	---------

The fields that can be configured are described below:

Parameter	Description
Relay IP Address:	Here the user can enter the DHCP Relay Option 60 Server Relay IP Address.
Mode:	Here the user can choose the DHCP Relay Option 60 Server mode.

Click the **Add** button to add a new entry based on the information entered.

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

Click the **Delete** button to remove the specific entry.

Click the **Delete All** button to remove all the entries listed.



NOTE: When there is no matching server found for the packet based on option 60, the relay servers will be determined by the default relay server setting.

DHCP Relay Option 60 Settings

This option decides whether the DHCP Relay will process the DHCP option 60 or not

The screenshot shows a web form titled "DHCP Relay Option 60 Settings". It contains several input fields and buttons. The "String" field has a placeholder "(Max: 255 characters)". The "Server IP" field has a placeholder "(e.g.: 10.90.90.90)". The "Match Type" field is a dropdown menu currently set to "Exact Match". There is an "Add" button to the right of the Match Type dropdown. Below these fields, there is an "IP Address" dropdown menu and an empty input field. To the right of this input field are "Find" and "Delete" buttons. At the bottom right, there are "Show All" and "Delete All" buttons. At the bottom left, it says "Total Entries: 0". Below this, there is a table header with columns for "String", "Match Type", and "IP Address".

The fields that can be configured are described below:

Parameter	Description
String:	Here the user can enter the DHCP Relay Option 60 String value. Different strings can be specified for the same relay server, and the same string can be specified with multiple relay servers. The system will relay the packet to all the matching servers.
Server IP:	Here the user can enter the DHCP Relay Option 60 Server IP address.
Match Type:	Here the user can enter the DHCP Relay Option 60 Match Type value. <i>Exact Match</i> – The option 60 string in the packet must full match with the specified string. <i>Partial Match</i> – The option 60 string in the packet only need partial match with the specified string.
IP Address:	Here the user can enter the DHCP Relay Option 60 IP address.
String:	Here the user can enter the DHCP Relay Option 60 String value.

Click the **Add** button to add a new entry based on the information entered.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete** button to remove the specific entry based on the information entered.

Click the **Show All** button to display all the existing entries.

Click the **Delete All** button to remove all the entries listed.

Click the **Delete** button to remove the specific entry.

DHCP Relay Option 61 Settings

On this page the user can configure, add and delete DHCP relay option 61 parameters.

The fields that can be configured are described below:

Parameter	Description
DHCP Relay Option 61 Default:	Here the user can select the DHCP Relay Option 61 default action. <i>Drop</i> – Specify to drop the packet. <i>Relay</i> – Specify to relay the packet to an IP address. Enter the IP Address of the default relay server. When there is no matching server found for the packet based on option 61, the relay servers will be determined by this default relay server setting.
Client ID:	<i>MAC Address</i> – The client's client-ID which is the hardware address of client. <i>String</i> – The client's client-ID, which is specified by administrator.
Relay Rule:	<i>Drop</i> – Specify to drop the packet. <i>Relay</i> – Specify to relay the packet to an IP address.
Client ID:	<i>MAC Address</i> – The client's client-ID which is the hardware address of client. <i>String</i> – The client's client-ID, which is specified by administrator.

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

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specific entry based on the information entered.

Click the **Delete All** button to remove all the entries listed.

DHCP Server Folder

DHCP, or Dynamic Host Configuration Protocol, allows the switch to delegate IP addresses, subnet masks, default gateways and other IP parameters to devices that request this information. This occurs when a DHCP enabled device is booted on or attached to the locally attached network. This device is known as the DHCP client and when enabled, it will emit query messages on the network before any IP parameters are set. When the DHCP server receives this request, it returns a response to the client, containing the previously mentioned IP information that the DHCP client then utilizes and sets on its local configurations.

The user can configure many DHCP related parameters that it will utilize on its locally attached network, to control and limit the IP settings of clients desiring an automatic IP configuration, such as the lease time of the allotted IP address, the range of IP addresses that will be allowed in its DHCP pool, the ability to exclude various IP addresses within the pool so as not to make identical entries on its network, or to assign the IP address of an important device (such as a DNS server or the IP address of the default route) to another device on the network.

Users also have the ability to bind IP addresses within the DHCP pool to specific MAC addresses in order to keep consistent the IP addresses of devices that may be important to the upkeep of the network that require a static IP address.

DHCP Server Global Settings

On this page the user can configure the DHCP server global parameters.

The fields that can be configured are described below:

Parameter	Description
DHCP Server State:	Here the user can enable or disable the DHCP Server State.
Ping Packets:	Here the user can choose the numbers of ping packet that the Switch will send out on the network containing the IP address to be allotted. If the ping request is not returned, the IP address is considered unique to the local network and then allotted to the requesting client. 0 means there is no ping test. The default value is 2.
Ping Timeout:	Here the user can choose the amount of time the DHCP server must waits before timing out a ping packet. The default value is 100.

Click the **Apply** button to accept the changes made for each individual section.

DHCP Server Exclude Address Settings

The DHCP server assumes that all IP addresses in a DHCP pool subnet are available for assigning to DHCP clients. You must use this page to specify the IP address that the DHCP server should not assign to clients. This command can be used multiple times in order to define multiple groups of excluded addresses.

The fields that can be configured are described below:

Parameter	Description
Begin Address:	Here the user can enter the starting IP Address.
End Address:	Here the user can enter the ending IP Address.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete All** button to remove all the entries listed.

Click the **Delete** button to remove the specific entry.

DHCP Server Pool Settings

On this page the user can add and delete the DHCP server pool.

The fields that can be configured are described below:

Parameter	Description
Pool Name:	Here the user can enter the DHCP Server Pool name.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete All** button to remove all the entries listed.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

After clicking the **Edit** button, the following page will appear:

The fields that can be configured are described below:

Parameter	Description
IP Address:	Here the user can enter the IP address of DNS server.
Netmask:	Here the user can enter the Netmask for the DNS server.
NetBIOS Node Type:	NetBIOS node type for a Microsoft DHCP client.
Domain Name:	Domain name of client. The domain name configured here will be used as the default domain name by the client.

Boot File:	File name of boot image. The boot file is used to store the boot image for the client. The boot image is generally the operating system the client uses to load. If this option is input twice for the same pool, the second command will overwrite the first command. If the boot file is not specified, the boot file information will not be provided to the client.
Next Server:	IP address of next server. The next server used by the DHCP client boot process is typically a TFTP server. If next server information is not specified, it will not be provided to the client. If this option is input twice for the same pool, the second command will overwrite the first command. It is allowed to specify the next server but not specify the boot file, or specify the boot file but not specify the next server.
DNS Server Address:	IP address of DNS server. Specifies the IP address of a DNS server that is available to a DHCP client. Up to three IP addresses can be specified in one command line.
NetBIOS Name Server:	IP address of WINS server. Windows Internet Naming Service (WINS) is a name resolution service that Microsoft DHCP clients use to correlate host names to IP addresses within a general grouping of networks.
Default Router:	IP address of default router. Specifies the IP address of the default router for a DHCP client. Up to three IP addresses can be specified in one command line.
Pool Lease:	By default, each IP address assigned by a DHCP server comes with a one-day lease, which is the amount of time that the address is valid. <i>Days</i> – Days of lease. <i>Hours</i> – Hours of lease. <i>Minutes</i> – Minutes of lease

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

Click the **<<Back** button to discard the changes made and return to the previous page.

DHCP Server Manual Binding

An address binding is a mapping between the IP address and MAC address of a client. The IP address of a client can be assigned manually by an administrator or assigned automatically from a pool by a DHCP server. The dynamic binding entry will be created when an IP address is assigned to the client from the pool network's address.

DHCP Server Manual Binding

Add DHCP Server Manual Binding

Pool Name (Max: 12 characters) IP Address (e.g.: 1.1.1.1)

Hardware Address (e.g.: 00-00-00-00-00-01) Type

Pool Name

Total Entries: 0

Pool Name	IP Address	Hardware Address	Type
-----------	------------	------------------	------

The fields that can be configured are described below:

Parameter	Description
Pool Name:	Here the user can enter the DHCP Server Pool name.
IP Address:	IP address which will be assigned to specified client.
Hardware Address:	Here the user can enter the hardware address.
Type:	Either Ethernet or IEEE802 can be specified.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete All** button to remove all the entries listed.

Click the **Delete** button to remove the specific entry.

DHCP Server Dynamic Binding

On this page the user can delete the DHCP server dynamic binding table.



The screenshot shows a web interface for 'DHCP Server Dynamic Binding'. It features a text input field for 'Pool Name' with a '(Max: 12 characters)' label. To the right of the input field are two buttons: 'Clear' and 'Clear All'.

The fields that can be configured are described below:

Parameter	Description
Pool Name:	Here the user can enter the DHCP Server Pool name.

Click the **Clear** button to clear all the information entered in the fields.

Click the **Clear All** button to remove all the entries listed in the table.

DHCP Conflict IP

The DHCP server will use PING packet to determine whether an IP address is conflict with other host before binding this IP. The IP address which has been identified conflict will be moved to the conflict IP database. The system will not attempt to bind the IP address in the conflict IP database unless the user clears it from the conflict IP database.



Click the **Clear All** button to remove all the entries listed in the table.

SMTP Settings

SMTP or Simple Mail Transfer Protocol is a function of the Switch that will send switch events to mail recipients based on e-mail addresses entered in the window below. The Switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the Switch, place the appropriate information into an e-mail and deliver it to recipients configured on the Switch. This can benefit the Switch administrator by simplifying the management of small workgroups or wiring closets, increasing the speed of handling emergency Switch events, and enhancing security by recording questionable events occurring on the Switch.

Users can set up the SMTP server for the Switch, along with setting e-mail addresses to which switch log files can be sent when a problem arises on the Switch.

The Switch will send out e-mail to recipients when one or more of the following events occur:

- When a cold start occurs on the Switch.
- When a port enters a link down status.
- When a port enters a link up status.
- When SNMP authentication has been denied by the Switch.
- When a switch configuration entry has been saved to the NVRAM by the Switch.
- When an abnormality occurs on TFTP during a firmware download event. This includes in-process, invalid-file, violation, file-not-found, complete and time-out messages from the TFTP server.
- When a system reset occurs on the Switch.

Information within the e-mail from the SMTP server regarding switch events includes:

- The source device name and IP address.
- A timestamp denoting the identity of the SMTP server and the client that sent the message, as well as the time and date of the message received from the Switch. Messages that have been relayed will have timestamps for each relay.
- The event that occurred on the Switch, prompting the e-mail message to be sent.
- When an event is processed by a user, such as save or firmware upgrade, the IP address, MAC address and User Name of the user com-

pleting the task will be sent along with the system message of the event occurred.

- When the same event occurs more than once, the second mail message and every repeating mail message following will have the system’s error message placed in the subject line of the mail message.

The following details events occurring during the Delivery Process.

- Urgent mail will have high priority and be immediately dispatched to recipients while normal mail will be placed in a queue for future transmission.
- The maximum number of un-transmitted mail messages placed in the queue cannot exceed 30 messages. Any new messages will be discarded if the queue is full.
- If the initial message sent to a mail recipient is not delivered, it will be placed in the waiting queue until its place in the queue has been reached, and then another attempt to transmit the message is made. • The maximum attempts for delivering mail to recipients is three. Mail message delivery attempts will be tried every five minutes until the maximum number of attempts is reached. Once reached and the message has not been successfully delivered, the message will be dropped and not received by the mail recipient.
- If the Switch shuts down or reboots, mail messages in the waiting queue will be lost.

SMTP Settings

SMTP Global Settings

SMTP State Enabled Disabled

SMTP Server Address

SMTP Server Port (1-65535)

Self Mail Address

SMTP Mail Receiver Address

Add A Mail Receiver

Send a Test Mail to All

Subject

Content

Index	Mail Receiver Address	
1		Delete
2		Delete
3		Delete
4		Delete
5		Delete
6		Delete
7		Delete
8		Delete

The fields that can be configured are described below:

Parameter	Description
SMTP State:	Use the radio button to enable or disable the SMTP service on this device.
SMTP Server Address:	Enter the IP address of the SMTP server on a remote device. This will be the device that sends out the mail for you.
SMTP Server Port:	Enter the virtual port number that the Switch will connect with on the SMTP server. The common port number for SMTP is 25, yet a value between 1 and 65535 can be chosen.
Self Mail Address:	Enter the e-mail address from which mail messages will be sent. This address will be the "from" address on the e-mail message sent to a recipient. Only one self-mail address can be configured for this Switch. This string can be no more than 64 alphanumeric characters.
Add a Mail Receiver:	Enter an e-mail address and click the Add button. Up to eight e-mail addresses can be added per Switch. To delete these addresses from the Switch, click the corresponding Delete button in the SMTP Mail Receiver Address table at the bottom of the window.
Send a Test Mail to All:	Here the user can send a test mail to all the addresses listed.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specific entry.

SNTP Folder

The Simple Network Time Protocol (SNTP) is a protocol for synchronizing computer clocks through the Internet. It provides comprehensive mechanisms to access national time and frequency dissemination services, organize the SNTP subnet of servers and clients, and adjust the system clock of each participant.

SNTP Settings

Users can configure the time settings for the Switch.

The fields that can be configured are described below:

Parameter	Description
SNTP State:	Use this radio button to enable or disable SNTP.
Current Time:	Displays the Current Time.
Time Source:	Displays the time source for the system.
SNTP First Server:	The IP address of the primary server from which the SNTP information will be taken.
SNTP Second Server:	The IP address of the secondary server from which the SNTP information will be taken.
SNTP Poll Interval In Seconds (30-99999):	The interval, in seconds, between requests for updated SNTP information.

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

Time Zone Settings

Users can configure time zones and Daylight Savings Time settings for SNTP.

Time Zone Settings

Summer Time State: Disabled

Summer Time Offset in Minutes: 60

Time Zone Offset: From GMT in +/-HH:MM: + 00 00

Summer Time Recurring Settings

From: Which Week of the Month: First

From: Day of the Week: Sun

From: Month: Apr

From: Time in HH MM: 00 00

To: Which Week of the Month: Last

To: Day of the Week: Sun

To: Month: Oct

To: Time in HH MM: 00 00

Summer Time Date Settings

From: Month: Apr

From: Day: 29

From: Time in HH MM: 00 00

To: Month: Oct

To: Day: 12

To: Time in HH MM: 00 00

The fields that can be configured are described below:

Parameter	Description
Summer Time State:	Use this pull-down menu to enable or disable the Summer Time Settings.
Summer Time Offset In Minutes:	Use this pull-down menu to specify the amount of time that will constitute your local Summer Time offset – 30, 60, 90, or 120 minutes.
Time Zone Offset From GMT In +/-HH:MM:	Use these pull-down menus to specify your local time zone’s offset from Greenwich Mean Time (GMT.)

Parameter	Description
Summer Time Recurring Settings:	Using repeating mode will enable Summer Time seasonal time adjustment. Repeating mode requires that the Summer Time beginning and ending date be specified using a formula. For example, specify to begin Summer Time on Saturday during the second week of April and end Summer Time on Sunday during the last week of October.
From: Which Week Of The Month:	Enter the week of the month that Summer Time will start.
From: Day Of Week:	Enter the day of the week that Summer Time will start on.
From: Month:	Enter the month Summer Time will start on.

From: Time In HH:MM:	Enter the time of day that Summer Time will start on.
To: Which Week Of The Month:	Enter the week of the month the Summer Time will end.
To: Day Of Week:	Enter the day of the week that Summer Time will end.
To: Month:	Enter the month that Summer Time will end.
To: Time In HH:MM:	Enter the time Summer Time will end.

Parameter	Description
Summer Time Date Settings:	Using annual mode will enable Summer Time seasonal time adjustment. Annual mode requires that the Summer Time beginning and ending date be specified concisely. For example, specify to begin Summer Time on April 3 and end Summer Time on October 14.
From: Month:	Enter the month Summer Time will start on, each year.
From: Day:	Enter the day of the month Summer Time will start on, each year.
From: Time In HH:MM:	Enter the time of day Summer Time will start on, each year.
To: Month:	Enter the month Summer Time will end on, each year.
To: Day:	Enter the day of the month Summer Time will end on, each year.
To: Time In HH:MM:	Enter the time of day that Summer Time will end on, each year.

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

Flash File System Settings

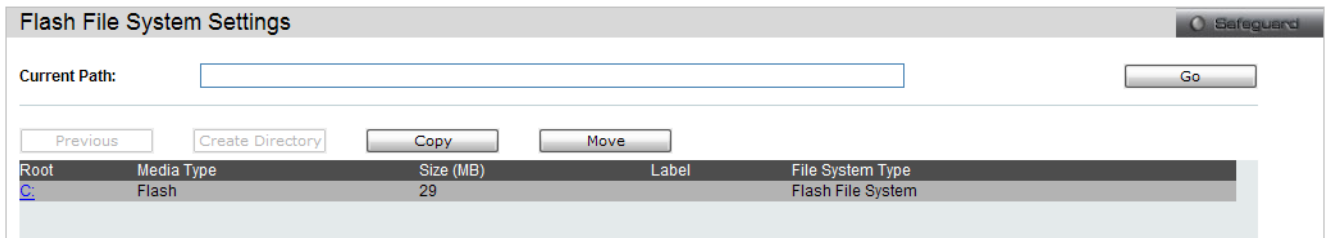
Why use flash file system:

In old switch system, the firmware, configuration and log information are saved in a flash with fixed addresses and size. This means that the maximum configuration file can only be 2Mb, and even if the current configuration is only 40Kb, it will still take up 2Mb of flash storage space. The configuration file number and firmware numbers are also fixed. A compatible issue will occur in the event that the configuration file or firmware size exceeds the originally designed size.

Flash File System in our system:

The Flash File System is used to provide the user with flexible file operation on the Flash. All the firmware, configuration information and system log information are stored in the Flash as files. This means that the Flash space taken up by all the files are not fixed, it is the real file size. If the Flash space is enough, the user could download more configuration files or firmware files and use commands to display Flash file information, rename file names, and delete it. Furthermore, the user can also configure the **boot up runtime image** or the **running configuration file** if needed.

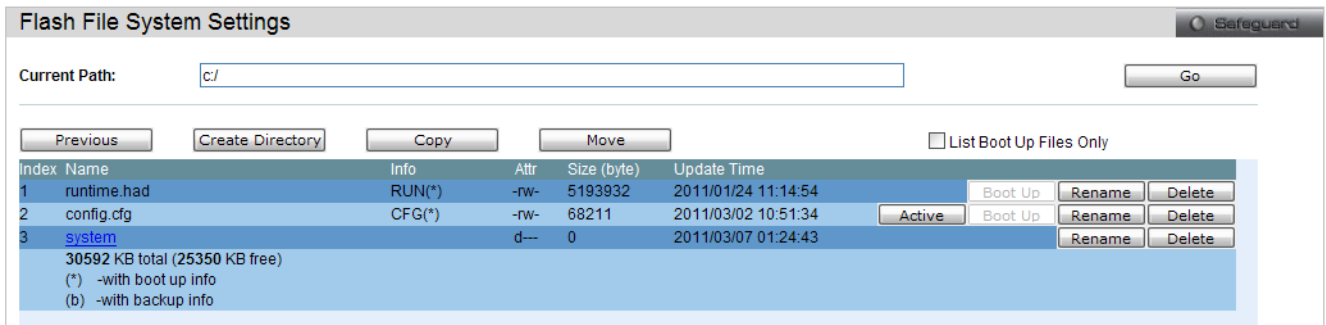
In case the file system gets corrupted, Z-modem can be used to download the backup files directly to the system.



Enter the **Current Path** string and click the **Go** button to navigate to the path entered.

Click the highlighted link to navigate the C: drive

After clicking the C: drive link button, the following page will appear:



Click the **Previous** button to return to the previous page.

Click the **Create Directory** to create a new directory within the file system of the switch.

Click the **Copy** button to copy a specific file to the switch.

Click the **Move** button to move a specific file within the switch.

Tick the **List Boot Up Files Only** option to display only the boot up files.

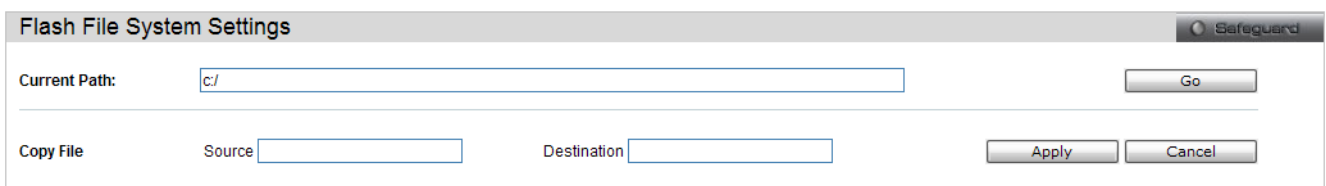
Click the **Active** button to set a specific config file as the active runtime configuration.

Click the **Boot Up** button to set a specific runtime image as the boot up image.

Click the **Rename** button to rename a specific file's name.

Click the **Delete** button to remove a specific file from the file system.

After clicking the **Copy** button, the following page will appear:



When copying a file to the file system of this switch, the user must enter the **Source** and **Destination** path.

Click the **Apply** button to initiate the copy.

Click the **Cancel** button the discard the process.

Monitoring

Utilization Folder — 252

Statistics Folder — 255

Mirror Folder — 268

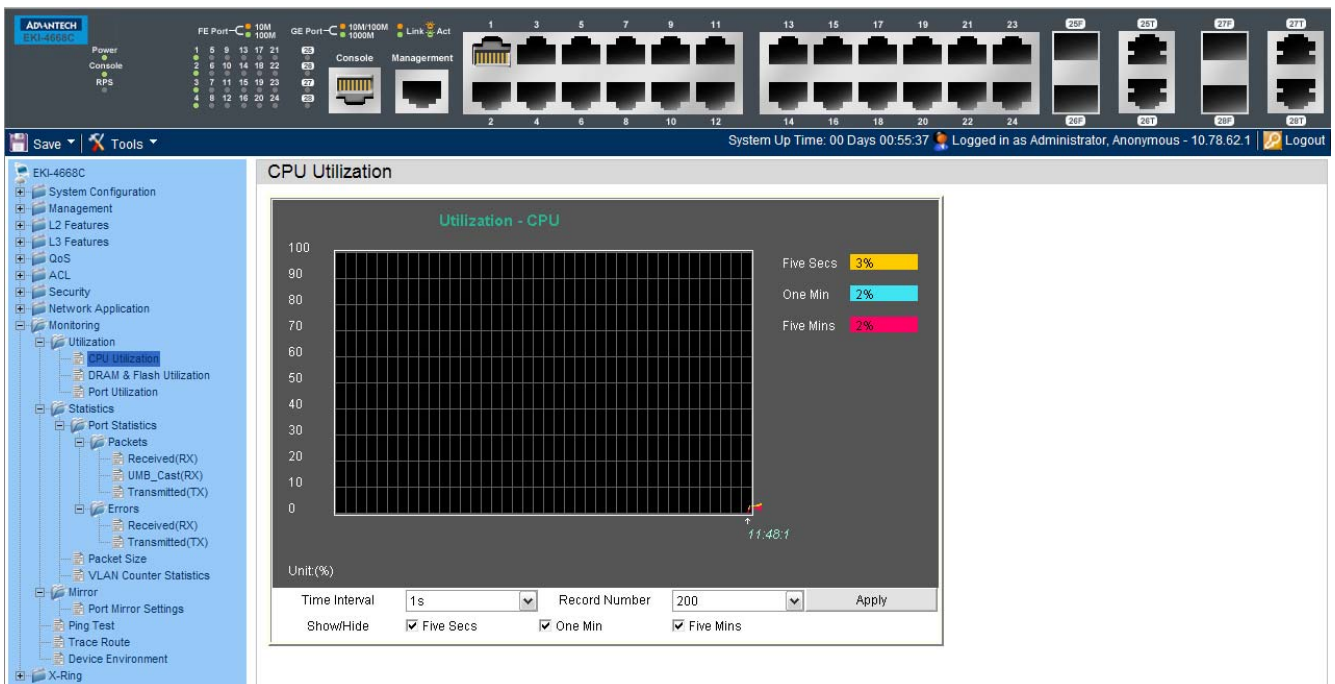
Ping Test — 269

Trace Route — 271

Device Environment — 272



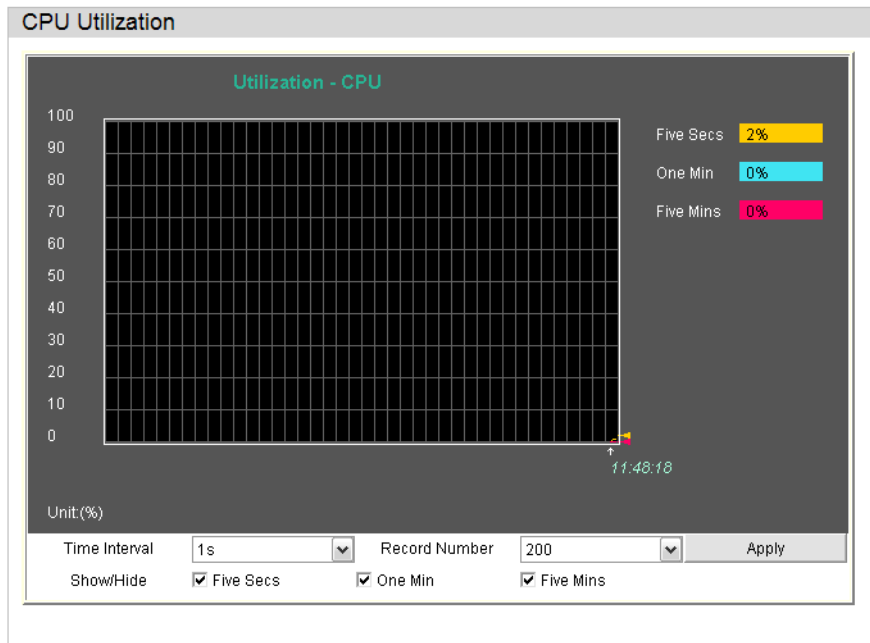
NOTE: The real time monitoring engine requires the JAVA runtime v1.6 or above platform. Please download the software from <http://www.java.com/getjava>



Utilization Folder

CPU Utilization

Users can display the percentage of the CPU being used, expressed as an integer percentage and calculated as a simple average by time interval.



To view the CPU utilization by port, use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port. Click **Apply** to implement the configured settings. The window will automatically refresh with new updated statistics.

The fields that can be configured are described below:

Parameter	Description
Time Interval:	Select the desired setting between <i>1s</i> and <i>60s</i> , where "s" stands for seconds. The default value is one second.
Record Number:	Select number of times the Switch will be polled between <i>20</i> and <i>200</i> . The default value is <i>200</i> .
Show/Hide:	Check whether or not to display Five Seconds, One Minute, and Five Minutes.

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

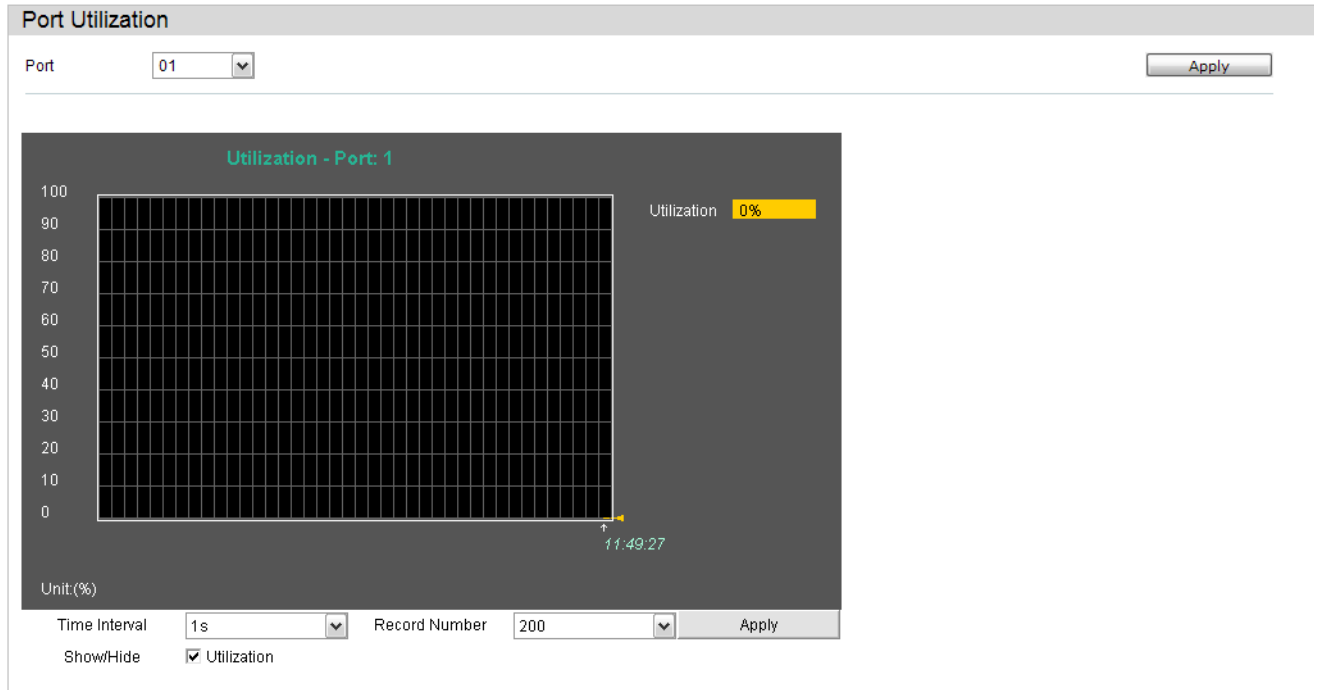
DRAM & Flash Utilization

On this page the user can view information regarding the DRAM and Flash utilization.

DRAM & Flash Utilization	
DRAM	
Total DRAM	0 KB
Used DRAM	0 KB
Utilization	0
Flash	
Total Flash	0 KB
Used Flash	0 KB
Utilization	0

Port Utilization

Users can display the percentage of the total available bandwidth being used on the port.



To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

The fields that can be configured are described below:

Parameter	Description
Port:	Use the drop-down menu to choose the port that will display statistics.
Time Interval:	Select the desired setting between <i>1s</i> and <i>60s</i> , where "s" stands for seconds. The default value is one second.
Record Number:	Select number of times the Switch will be polled between <i>20</i> and <i>200</i> . The default value is <i>200</i> .
Show/Hide:	Check whether or not to display Port Util.

Click the **Apply** button to accept the changes made for each individual section.

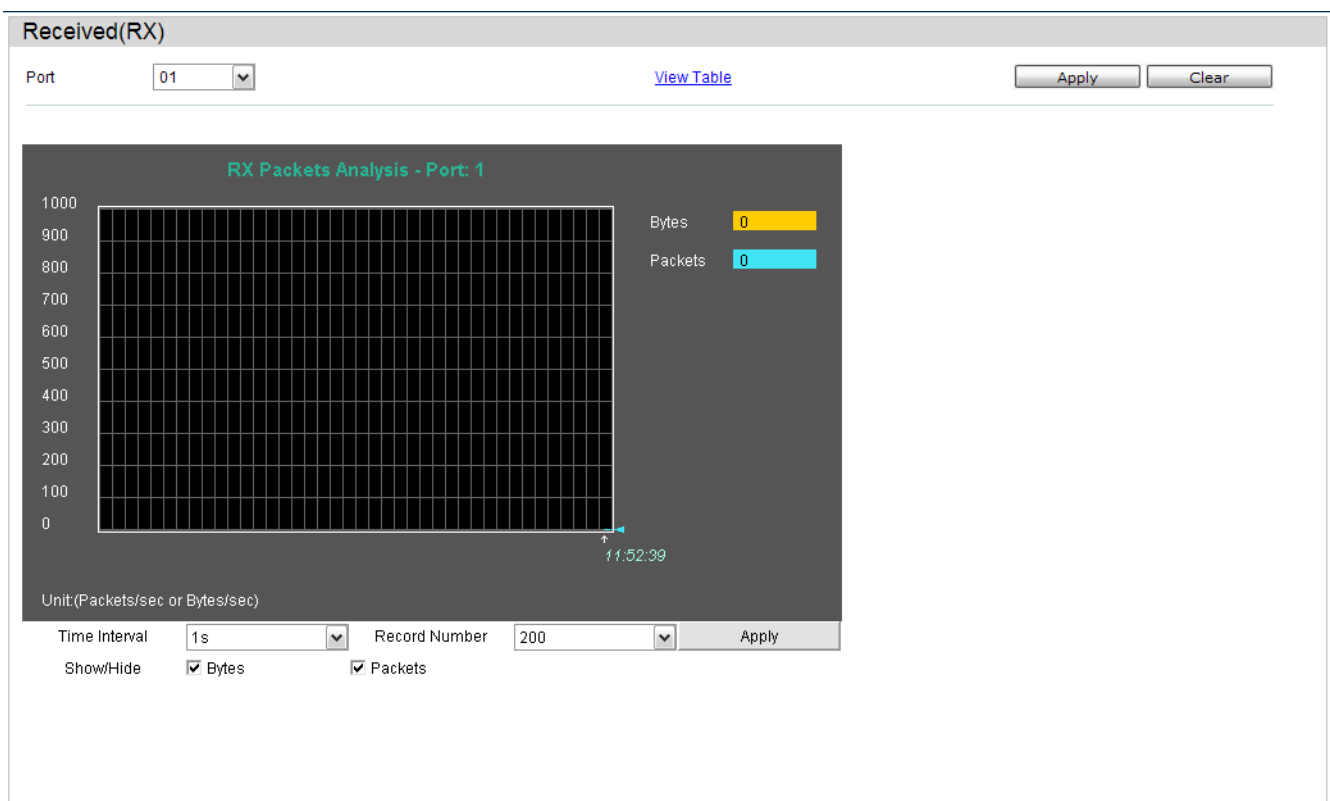
Statistics Folder

Packets Folder

The Web manager allows various packet statistics to be viewed as either a line graph or a table. Six windows are offered.

Received (RX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.



The fields that can be configured are described below:

Parameter	Description
Port:	Use the drop-down menu to choose the port that will display statistics.
Time Interval:	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number:	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
Bytes:	Counts the number of bytes received on the port.
Packets:	Counts the number of packets received on the port.

Unicast:	Counts the total number of good packets that were received by a unicast address.
Multicast:	Counts the total number of good packets that were received by a multicast address.
Broadcast:	Counts the total number of good packets that were received by a broadcast address.
Show/Hide:	Check whether to display Bytes and Packets.

Click the **Apply** button to accept the changes made for each individual section.

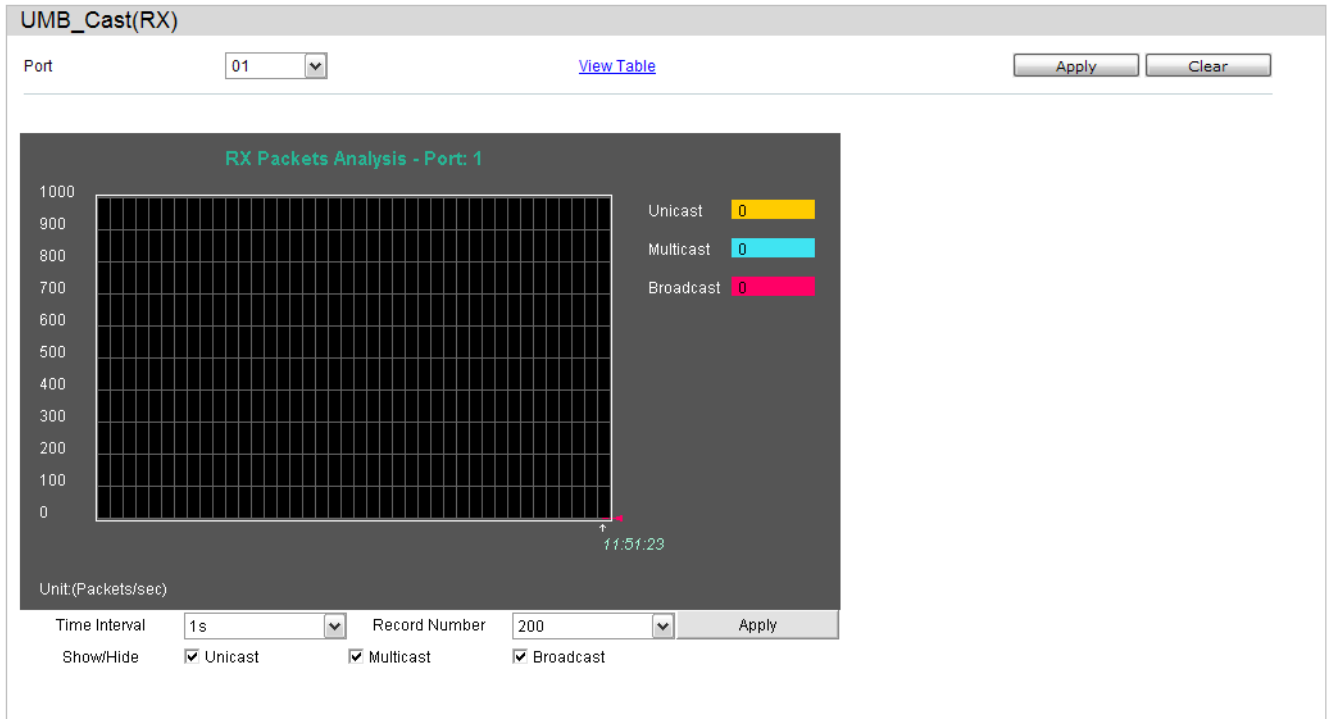
Click the **Clear** button to clear all statistics counters on this window.

Click the [View Table](#) link to display the information in a table rather than a line graph.

Click the [View Graphic](#) link to display the information in a line graph rather than a table.

UMB_Cast (RX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.



The fields that can be configured are described below:

Parameter	Description
Port:	Use the drop-down menu to choose the port that will display statistics.
Time Interval:	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number:	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
Unicast:	Counts the total number of good packets that were received by a unicast address.
Multicast:	Counts the total number of good packets that were received by a multicast address.
Broadcast:	Counts the total number of good packets that were received by a broadcast address.
Show/Hide:	Check whether or not to display Multicast, Broadcast, and Unicast Packets.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear** button to clear all statistics counters on this window.

Click the [View Table](#) link to display the information in a table rather than a line graph.

Click the [View Graphic](#) link to display the information in a line graph rather than a table.

Transmitted (TX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.



The fields that can be configured are described below:

Parameter	Description
Port:	Use the drop-down menu to choose the port that will display statistics.
Time Interval:	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number:	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
Bytes:	Counts the number of bytes successfully sent on the port.
Packets:	Counts the number of packets successfully sent on the port.
Unicast:	Counts the total number of good packets that were transmitted by a unicast address.
Multicast:	Counts the total number of good packets that were transmitted by a multicast address.
Broadcast:	Counts the total number of good packets that were transmitted by a broadcast address.

Show/Hide:Check whether or not to display Bytes and Packets.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear** button to clear all statistics counters on this window.

Click the [View Table](#) link to display the information in a table rather than a line graph.

Click the [View Graphic](#) link to display the information in a line graph rather than a table.

Errors Folder

The Web manager allows port error statistics compiled by the Switch's management agent to be viewed as either a line graph or a table. Four windows are offered.

Received (RX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.



The fields that can be configured are described below:

Parameter	Description
Port:	Use the drop-down menu to choose the port that will display statistics.
Time Interval:	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number:	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
CRCError:	Counts otherwise valid packets that did not end on a byte (octet) boundary.

UnderSize:	The number of packets detected that are less than the minimum permitted packets size of 64 bytes and have a good CRC. Undersize packets usually indicate collision fragments, a normal network occurrence.
OverSize:	Counts valid packets received that were longer than 1518 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536.
Fragment:	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
Jabber:	Counts invalid packets received that were longer than 1518 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536.
Drop:	The number of packets that are dropped by this port since the last Switch reboot.
Symbol:	Counts the number of packets received that have errors received in the symbol on the physical labor.
Show/Hide:	Check whether or not to display CRCError, UnderSize, OverSize, Fragment, Jabber, Drop, and SymbolErr errors.

Click the **Apply** button to accept the changes made for each individual section.

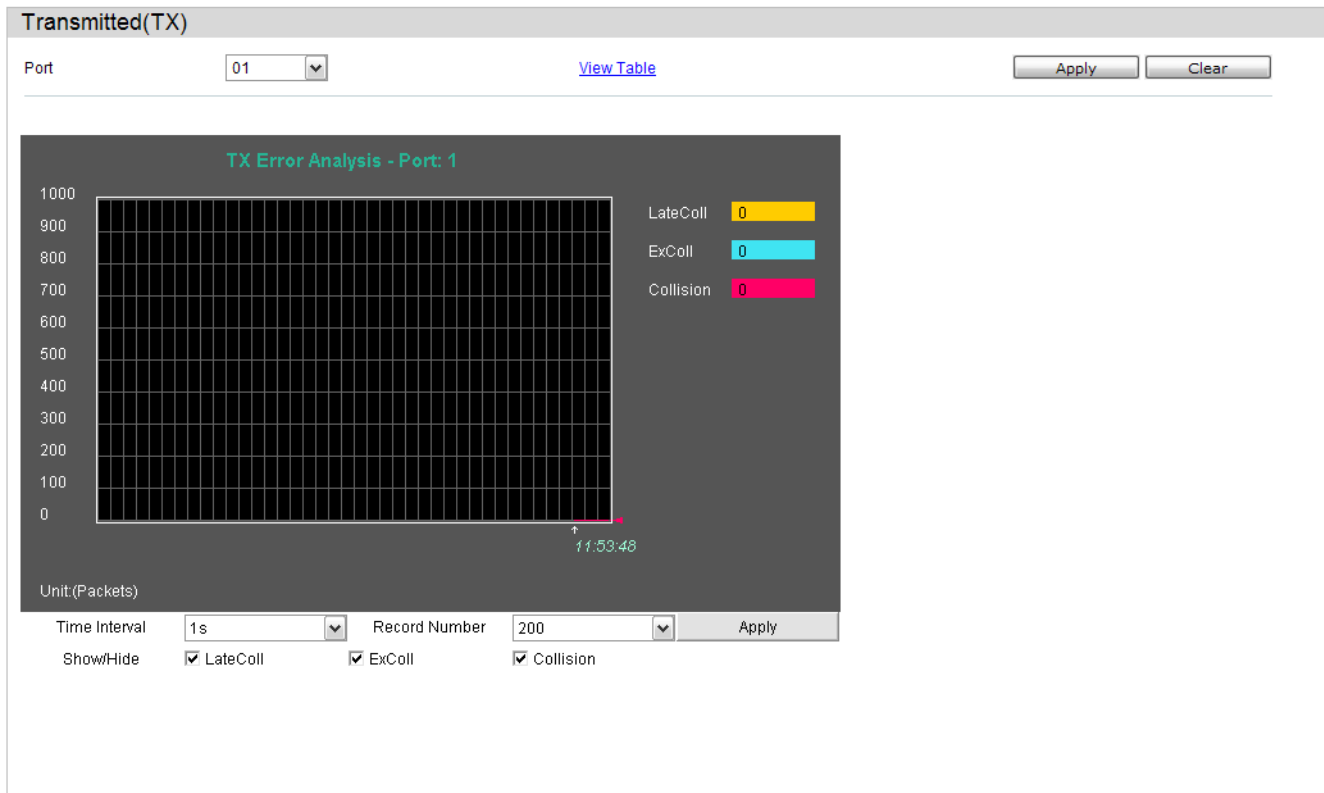
Click the **Clear** button to clear all statistics counters on this window.

Click the [View Table](#) link to display the information in a table rather than a line graph.

Click the [View Graphic](#) link to display the information in a line graph rather than a table.

Transmitted (TX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.



The fields that can be configured are described below:

Parameter	Description
Port:	Use the drop-down menu to choose the port that will display statistics.
Time Interval:	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number:	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
ExDefer:	Counts the number of packets for which the first transmission attempt on a particular interface was delayed because the medium was busy.
CRC Error:	Counts otherwise valid packets that did not end on a byte (octet) boundary.
LateColl:	Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
ExColl:	Excessive Collisions. The number of packets for which transmission failed due to excessive collisions.
SingColl:	Single Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by more than one collision.

Collision:	An estimate of the total number of collisions on this network segment.
Show/Hide:	Check whether or not to display ExDefer, CRCError, LateColl, ExColl, SingColl, and Collision errors.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear** button to clear all statistics counters on this window.

Click the [View Table](#) link to display the information in a table rather than a line graph.

Click the [View Graphic](#) link to display the information in a line graph rather than a table.

Packet Size

Users can display packets received by the Switch, arranged in six groups and classed by size, as either a line graph or a table. Two windows are offered. To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.



The fields that can be configured are described below:

Parameter	Description
Port:	Use the drop-down menu to choose the port that will display statistics.
Time Interval:	Select the desired setting between <i>1s</i> and <i>60s</i> , where "s" stands for seconds. The default value is one second.
Record Number:	Select number of times the Switch will be polled between <i>20</i> and <i>200</i> . The default value is 200.
64:	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65-127:	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

128-255:	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511:	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023:	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518:	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Show/Hide:	Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear** button to clear all statistics counters on this window.

Click the [View Table](#) link to display the information in a table rather than a line graph.

Click the [View Graphic](#) link to display the information in a line graph rather than a table.

VLAN Counter Statistics

On this page the user can view VLAN counter statistics.

VLAN Counter Statistics

VID List (e.g.: 1, 4-6)
 VLAN Name
 Port List (e.g.: 4-6)

Find VLAN Statistics

VID List
 VLAN Name
 Port List

Total Entries: 0

VID	Port	Frame Type	RX Frames / RX Bytes	Frames per Sec / Bytes per Sec

The fields that can be configured are described below:

Parameter	Description
VID List:	Here the user can enter a VID list to view.
VLAN Name:	Here the user can enter VLAN Name to view.
Port List:	Here the user can enter the appropriate port(s) to view.

Click the **Clear** button to clear all the information entered in the fields.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **View All** button to display all the existing entries.

Click the **Clear All** button to remove all the entries listed in the table.

Mirror Folder

The Switch allows you to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes.

Port Mirror Settings

To configure a mirror port:

1. Change the status to Enabled.
2. Select the Source Port from where you want the frames to come from.
3. Select the Target Port, which receives the copies from the source port.
4. Click Apply to let the changes take effect.

Port Mirror Settings

Target Port Settings

State: Enabled Disabled

Target Port:

Source Port:

Sniffer Mode	Ports
TX	
RX	

Source Port Settings

Sniffer Mode	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
TX	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
RX	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Both	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
None	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
TX																												
RX																												



NOTE: You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Also, the target port for the mirroring cannot be a member of a trunk group. Please note a target port and a source port cannot be the same port.

Ping Test



NOTE: If the user wants to change the analyze server ID, he needs to delete the flow sampler and create a new one.

Users can Ping either an IPv4 address or an IPv6 address. Ping is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or “echoes” the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

Ping Test

IPv4 Ping Test

Enter the IP address of the device or station you want to ping, then click **Start**.

Target IP Address

Repeat Pinging for Infinite times
 (1-255 times)

Timeout (1-99 sec)

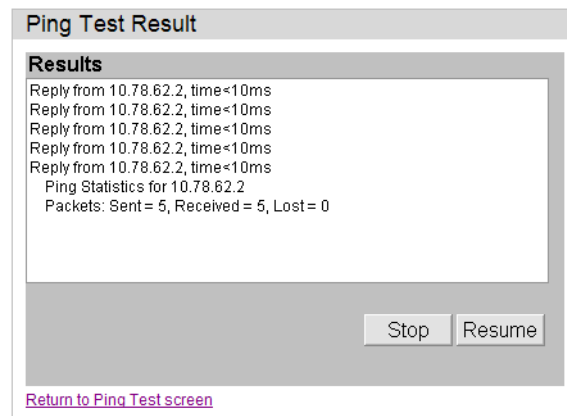
The user may click the Infinite times radio button, in the Repeat Pinging for field, which will tell the ping program to keep sending ICMP Echo packets to the specified IP address until the program is stopped. The user may opt to choose a specific number of times to ping the Target IP Address by clicking its radio button and entering a number between 1 and 255.

The fields that can be configured are described below:

Parameter	Description
Target IP Address:	Enter an IP address to be pinged.
Interface Name:	For IPv6 Link local address only, enter the name of the interface to be Pinged.
Repeat Pinging for:	Enter the number of times desired to attempt to Ping either the IPv4 address or the IPv6 address configured in this window. Users may enter a number of times between 1 and 255.
Size:	For IPv6 only, enter a value between 1 and 6000. The default is 100.
Timeout:	For IPv4, select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. For IPv6, select a timeout period between 1 and 10 seconds for this Ping message to reach its destination. In either case, if the packet fails to find the IP address in this specified time, the Ping packet will be dropped.

Click the **Start** button to initiate the Ping Test

After clicking the **Start** button, the following page will appear:



Click the **Stop** button to halt the Ping Test

Click the **Resume** button to resume the Ping Test

Trace Route

The trace route page allows the user to trace a route between the switch and a given host on the network.

Trace Route

IPv4 Trace Route :
Enter the IP Address of the device or station you want to traceroute, then click **Start**.

IPv4 Address

TTL (1-60)

Port (30000-64900)

Timeout (1-65535) sec

Probe (1-9)

The fields that can be configured are described below:

Parameter	Description
IPv4 Address:	IP address of the destination station.
TTL:	The time to live value of the trace route request. This is the maximum number of routers that a trace route packet can pass. The trace route option will cross while seeking the network path between two devices. The range for the TTL is 1 to 60 hops.
Port:	The port number. The value range is from 30000 to 64900.
Timeout:	Defines the timeout period while waiting for a response from the remote device. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.
Probe:	The number of probing. The range is from 1 to 9. If unspecified, the default value is 1.

Click the **Start** button to initiate the Trace Route

After clicking the **Start** button, the following page will appear:

Trace Route Result

Results

```

20 ms 203.207.46.125
20 ms 203.207.47.49
20 ms 203.79.222.137
20 ms 211.76.96.161
30 ms 72.14.196.13
20 ms 209.85.243.26
20 ms 209.85.243.23
30 ms 72.14.233.122
40 ms 74.125.153.147
Trace complete

```

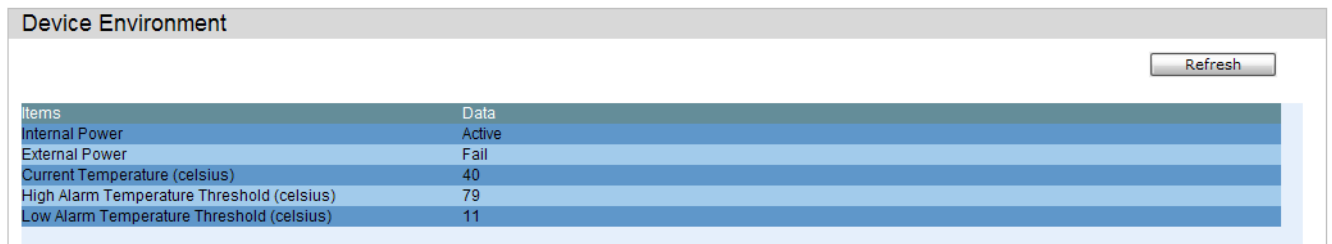
[Return to Trace Route Test screen](#)

Click the **Stop** button to halt the Trace Route

Click the **Resume** button to resume the Trace Route

Device Environment

The device environment feature displays the Switch internal temperature status.

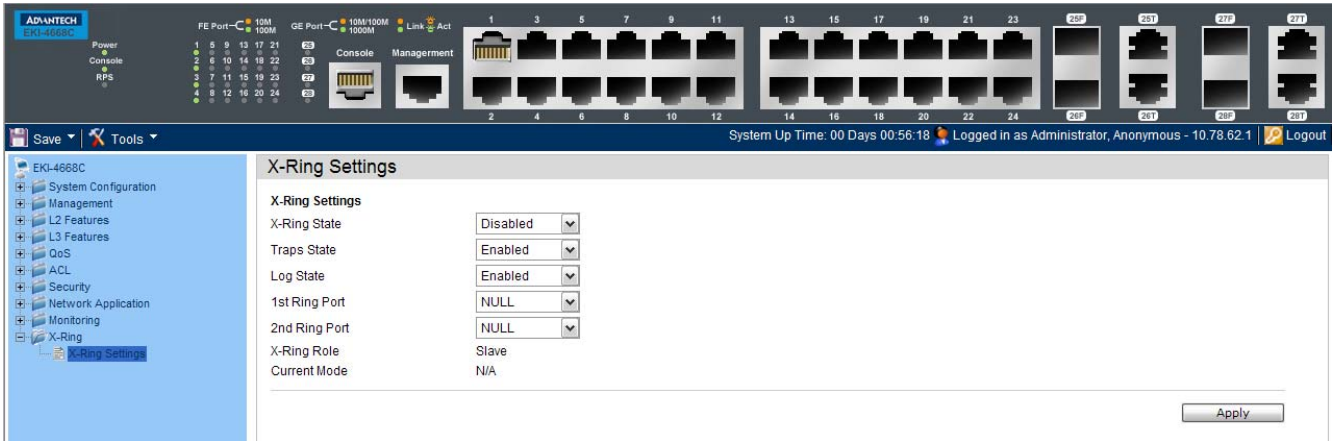


Items	Data
Internal Power	Active
External Power	Fail
Current Temperature (celsius)	40
High Alarm Temperature Threshold (celsius)	79
Low Alarm Temperature Threshold (celsius)	11

Click the **Refresh** button to refresh the display table so that new entries will appear.

X-Ring

Setting up X-Ring with other switches provides a similar redundancy scheme as Spanning Tree provides. The difference is that the recovery time is much faster.



X-Ring Settings

X-Ring provides a faster redundant recovery than Spanning Tree Topology. The action is similar to STP or RSTP but the algorithm used is not the same.

In the X-Ring topology every switch should enable X-Ring function and assign two member ports in the ring. Only one switch in the X-Ring group would be set as the master switch. Each switch has one of its paths (ports) blocked which is called the backup port. Another port is called the working port. When a network connection fails, then the backup port will automatically become a working port in order to recover from the failure.

The switch supports the function and interface for setting the switch as the ring master or slave mode. The ring master can negotiate and issue commands to other switches in the X-Ring group. If there are 2 or more switches in Master mode, then software will select the switch with the lowest MAC address numbers as the X-Ring Master.

This window below allows you to enable the X-Ring protocol and enable the 1st and 2nd Ring ports. Additionally Logs and Traps for X-Ring can be enabled so that they are generated upon appropriated events.

X-Ring Settings	
X-Ring State	Disabled
Traps State	Enabled
Log State	Enabled
1st Ring Port	NULL
2nd Ring Port	NULL
X-Ring Role	Slave
Current Mode	N/A

The fields that can be configured are described below:

Parameter	Description
X-Ring State:	The X-Ring protocol can be disabled or enabled using this setting. To enable X-Ring the 1st and 2nd Ring Ports must be set first
Traps State	Enable this field to allow X-Ring traps to be created.
Log State	Enable this field to allow X-Ring logs to be created.
1st Ring Port	Configures a selected Switch Port as the 1st Ring Port of X-Ring.
2nd Ring Port	Configures a selected Switch Port as the 2nd Ring Port of X-Ring.
1st Ring Port State	Displays the current operational state of the configured 1st Ring Port.
2nd Ring Port State	Displays the current operational state of the configured 2nd Ring Port.
X-Ring Role	Displays whether the Switch is a Master or Slave in the X-Ring topology.
Current Mode	Displays a current operational state for the X-Ring protocol on the Switch.

Appendix A - Password Recovery Procedure

The following steps explain how to use the Password Recovery feature on the Switch to easily recover the username 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 key (esc) 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.B010

Power On Self Test 100%

MAC Address : 00-19-5B-EC-32-15

H/W Version : A1

Please Wait, Loading V1.00.B039 Runtime Image 100 %

. UART init 100 %

Password Recovery Mode

>

In the "Password Recovery Mode" only the following commands can be used.

Command	Parameters
reset config	The reset config command resets the whole configuration back to the default values.
reboot	The reboot command exits the Reset Password Recovery Mode and restarts the switch. A confirmation message will be displayed to allow the user to save the current settings.
reset account	The reset account command deletes all the previously created accounts.

reset password {<username>}	The reset password command resets the password of the specified user. If a username is not specified, the passwords of all users will be reset.
show account	The show account command displays all previously created accounts.

Appendix B - Trap Logs

This table lists the trap logs found on the Switch.

Log Entry	Description	ID
IldpXMedTopologyChangeDetected	<p>A notification generated by the local device sensing a change in the topology that indicates that a new remote device attached to a local port, or a remote device disconnected or moved from one port to another.</p> <p>Binding objects?</p> <p>(1) IldpRemChassisIdSubtype (2) IldpRemChassisId (3) IldpXMedRemDeviceClass</p>	1.0.8802.1.1.2.1.5.4795.0.1
IldpRemTablesChange	<p>A IldpRemTablesChange notification is sent when the value of IldpStatsRemTableLastChangeTime changes. It can be utilized by an NMS to trigger LLDP remote systems table maintenance polls.</p> <p>Binding objects?</p> <p>(1)IldpStatsRemTablesInserts, (2)IldpStatsRemTablesDeletes, (3)IldpStatsRemTablesDrops, (4)IldpStatsRemTablesAgeouts</p>	1.0.8802.1.1.2.0.0.1
colSummer Timeart	<p>A colSummer Timeart trap signifies that the sending protocol entity is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.</p>	1.3.6.1.6.3.1.1.5.1
warmStart	<p>A warmStart trap signifies that the sending protocol entity is reinitializing itself such that neither the agent configuration nor the protocol entity implementation is altered.</p>	1.3.6.1.6.3.1.1.5.2
linkDown	<p>A linkDown trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration.</p> <p>A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state. This other state is indicated by the included value of ifOperStatus.</p> <p>Binding objects:</p> <p>(1)ifIndex (2)ifAdminStatus (3)ifOperStatus</p>	1.3.6.1.6.3.1.1.5.3

linkUp	<p>A linkUp trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up.</p> <p>A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state. This other state is indicated by the included value of ifOperStatus.</p> <p>Binding objects:</p> <ul style="list-style-type: none"> (1)ifIndex (2)ifAdminStatus (3)ifOperStatus 	1.3.6.1.6.3.1.1.5.4
authenticationFailure	<p>An authenticationFailure trap signifies that the sending protocol entity is the address of a protocol message that is not properly authenticated. While implementations of the SNMP must be capable of generating this trap, they must also be capable of suppressing the emission of such traps via an implementation-specific mechanism.</p>	1.3.6.1.6.3.1.1.5.5
RisingAlarm	<p>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.</p> <p>Binding objects?</p> <ul style="list-style-type: none"> (1)alarmIndex, (2)alarmVariable (3)alarmSampleType, (4)alarmValue, (5)alarmRisingThreshold 	1.3.6.1.2.1.16.0.1
FallingAlarmTrap	<p>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.</p> <p>Binding objects?</p> <ul style="list-style-type: none"> (1)alarmIndex, (2)alarmVariable (3)alarmSampleType, (4)alarmValue, (5)alarmFallingThreshold 	1.3.6.1.2.1.16.0.2

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 action 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 of this trap is optional.	1.3.6.1.2.1.17.0.2

Appendix C - Logs

Switch Log Syntax:

Syntac Symbol	Description	Notel
[]	Optional parts of the logs where implentation is dependant on the project.	The syntax symbol can not display in logs
<>	The log's parameters.	The syntax symbol can not display in logs
	Choose one of the options listed	The syntax symbol can not display in logs

System Logs.

ID	Log Description	Severity	Note
1	Event description: System started up Log Message: System started up	Critical	
2	Event description: Configuration saved to flash Log Message: Configuration saved to flash (Username: <username>) Parameters description: username: The user name that save the configuration.	Informational	
3	Event description: System log saved to flash Log Message: System log saved to flash(Username: <username>) Parameters description: username: The user name that save the configuration.	Informational	
4	Event description: Configuration and log saved to flash Log Message: Configuration and log saved to flash (Username: <username>) Parameters description: username: The user name that save the configuration.	Informational	
5	Event description: Successful login through a session. Log Message: Successful login through <Console Telnet Web Web(SSL) >(Username: <username>, IP: <ipaddr>). Parameters description: ipaddr: IP address. username: user name.	Informational	The IP parameter not for Console.

6	<p>Event description: Login failed through a session. Log Message: Login failed through <Console Telnet Web Web(SSL) > (Username: <username>, IP: <ipaddr >).</p> <p>Parameters description: ipaddr: IP address. username: user name.</p>	Warning	The IP parameter not for Console.
7	<p>Event description: Logout through a session. Log Message: Logout through <Console Telnet Web Web(SSL) > (Username: <username>, IP: <ipaddr>).</p> <p>Parameters description: ipaddr: IP address. username: user name.</p>	Informational	The IP parameter not for Console.
8	<p>Event description: session timed out. Log Message: <Console Telnet Web Web(SSL) > session timed out (Username: <username>, IP: <ipaddr >).</p> <p>Parameters description: ipaddr: IP address. username: user name.</p>	Informational	The IP parameter not for Console session.

Peripheral Function Logs

ID	Log Description	Severity	Note
1	<p>Event description: Temperature sensor enters alarm state. Log Message: Temperature sensor <sensorID> enters alarm state (current temperature: <temperature>)</p> <p>Parameters description: sensorID: The sensor ID. temperature: The temperature.</p>	Informational	
2	<p>Event description: Temperature recovers to normal. Log Message: Temperature sensor <sensorID> recovers to normal state (current temperature: <temperature>)</p> <p>Parameters description: sensorID: The sensor ID. temperature: The temperature.</p>	Informational	
3	<p>Event description: Internal Power failed. Log Message: Internal Power failed</p>	Critical	
4	<p>Event description: Internal Power is recovered. Log Message: Internal Power is recovered</p>	Critical	
5	<p>Event description: Redundant Power failed. Log Message: Redundant Power failed</p>	Critical	
6	<p>Event description: Redundant Power is working. Log Message: Redundant Power is working</p>	Critical	

SNMP Logs

ID	Log Description	Severity	Note
1	<p>Event description: SNMP request received with invalid community string</p> <p>Log Message: SNMP request received from <ipAddress> with invalid community string!</p> <p>Parameters description: ipAddress: IP address.</p>	Informational	

Interface Logs

ID	Log Description	Severity	Note
1	<p>Event description: Port link up</p> <p>Log Message: Port <portNum> link up, <link state></p> <p>Parameters description: portNum: The port number link state: port link status, for example: 100Mbps FULL duplex</p>	Informational	
2	<p>Event description: Port link down</p> <p>Log Message: Port <portNum> link down</p> <p>Parameters description: portNum: The port number.</p>	Informational	

Debug Funtion Logs

ID	Log Description	Severity	Note
1	<p>Event description: System fatal error</p> <p>Log Message: System re-start reason: system fatal error</p>	Emergency	
2	<p>Event description: CPU exception</p> <p>Log Message: System re-start reason: CPU exception</p>	Emergency	

TFTP Client Logs

ID	Log Description	Severity	Note
1	<p>Event description: Firmware upgraded successfully.</p> <p>Log Message: Firmware upgrade by <session> successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)</p> <p>Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.</p>	Informational	

2	<p>Event description: Firmware upgrade was unsuccessful. Log Message: Firmware upgrade by <session> was unsuccessful (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)</p> <p>Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.</p>	warning	
3	<p>Event description: Configuration successfully downloaded. Log Message: Configuration successfully downloaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)</p> <p>Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.</p>	informational	
4	<p>Event description: Configuration download was unsuccessful. Log Message: Configuration download by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)</p> <p>Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.</p>	warning	
5	<p>Event description: Configuration successfully uploaded. Log Message: Configuration successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)</p> <p>Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.</p>	informational	
6	<p>Event description: Configuration upload was unsuccessful. Log Message: Configuration upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)</p> <p>Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.</p>	warning	

7	<p>Event description: Log message successfully uploaded. Log Message: Log message successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)</p> <p>Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.</p>	informational	
8	<p>Event description: Log message upload was unsuccessful. Log Message: Log message upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)</p> <p>Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.</p>	warning	

1. The user's session indicates Console, Web, Telnet.
2. If update firmware through Console, there will be no IP and MAC information for logging.

MSTP Debug Enhancement Logs

ID	Log Description	Severity	Note
1	<p>Event description: Topology changed. Log Message: Topology changed [([Instance:<InstanceID>] ,port:<portNum> [,MAC: <macaddr>])]</p> <p>Parameters description: InstanceID: Instance ID. portNum:Port ID macaddr: MAC address</p>	Informational	
2	<p>Event description: New Root selected Log Message: [CIST CIST Region MSTI Region] New Root bridge selected ([Instance: <InstanceID>] MAC:<macaddr>, Priority: <value>)</p> <p>Parameters description: InstanceID: Instance ID. macaddr: root bridge MAC address value: root bridge priority</p>	Informational	
3	<p>Event description: Spanning tree protocol is enabled Log Message: Spanning Tree Protocol is enabled.</p>	Informational	
4	<p>Event description: Spanning tree protocol is disabled Log Message: Spanning Tree Protocol is disabled.</p>	Informational	

5	<p>Event description: Spanning Tree instance created.</p> <p>Log Message: Spanning Tree instance create (Instance:<InstanceID>)</p> <p>Parameters description: InstanceID: Instance ID.</p>	Informational	
6	<p>Event description: Spanning Tree instance deleted.</p> <p>Log Message: Spanning Tree instance delete (Instance:<InstanceID>)</p> <p>Parameters description: InstanceID: Instance ID.</p>	Informational	
7	<p>Event description: Spanning Tree Version changed.</p> <p>Log Message: Spanning Tree version change (new version:<new_version>)</p> <p>Parameters description: new_version: New STP version.</p>	Informational	
8	<p>Event description: Spanning Tree MST configuration ID name and revision level changed.</p> <p>Log Message: Spanning Tree MST configuration ID name and revision level change (name:<name> revision level <revision_level>).</p> <p>Parameters description: name : New name. revision_level:New revision level.</p>	Informational	
9	<p>Event description: Spanning Tree MST configuration ID VLAN mapping table deleted.</p> <p>Log Message: Spanning Tree MST configuration ID VLAN mapping table change (Instance: <InstanceID> delete vlan <startvlanid> [- <endvlanid>]).</p> <p>Parameters description: InstanceID: Instance ID. startvlanid- endvlanid:VLANlist</p>	Informational	
10	<p>Event description: Spanning Tree MST configuration ID VLAN mapping table added.</p> <p>Log Message: Spanning Tree MST configuration ID VLAN mapping table change (Instance: <InstanceID> add vlan <startvlanid> [- <endvlanid>]).</p> <p>Parameters description: InstanceID: Instance ID. startvlanid- endvlanid:VLANlist</p>	Informational	
11	<p>Event description: New root port</p> <p>Log Message: New root port selected [([Instance:<InstanceID>], port:<[unitID:] portNum>)]</p> <p>Parameters description: InstanceID: Instance ID. portNum:Port ID</p>	Notice	

12	<p>Event description: Spanning Tree port status changed Log Message: Spanning Tree port status change [([Instance:<InstanceID>], port:<portNum>)] <old_status> -> <new_status></p> <p>Parameters description: InstanceID: Instance ID. portNum: Port ID old_status: Old status new_status: New status</p>	Notice	
13	<p>Event description: Spanning Tree port role changed. Log Message: Spanning Tree port role change [([Instance:<InstanceID>], port:<portNum>)] <old_role> -> <new_role></p> <p>Parameters description: InstanceID: Instance ID. portNum:Port ID old_role: Old role new_status:New role</p>	Informational	

LLDP-MED Logs

ID	Log Description	Severity	Note
----	-----------------	----------	------

<p>1</p>	<p>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>)</p> <p>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)</p> <p>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)</p> <p>portID: port ID. deviceClass: LLDP-MED device type.</p>	<p>Notice</p>	
----------	--	---------------	--

2	<p>Event description: Conflict LLDP-MED device type detected</p> <p>Log Message: Conflict LLDP-MED device type detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>)</p> <p>Parameters description:</p> <p>portNum: The port number.</p> <p>chassisType: chassis ID subtype.</p> <p>Value list:</p> <ol style="list-style-type: none"> 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) <p>chassisID: chassis ID.</p> <p>portType: port ID subtype.</p> <p>Value list:</p> <ol style="list-style-type: none"> 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) <p>portID: port ID.</p> <p>deviceClass: LLDP-MED device type.</p>	Notice	
---	---	--------	--

3	<p>Event description: Incompatible LLDP-MED TLV set detected</p> <p>Log Message: Incompatible LLDP-MED TLV set detected (on port <portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>)</p> <p>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)</p> <p>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)</p> <p>portID: port ID. deviceClass: LLDP-MED device type.</p>	Notice	
---	--	--------	--

8021X Logs

ID	Log Description	Severity	Note
1	<p>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.</p> <p>Log Message: Radius server <ipaddr> assigned VID :<vlanID> to port <portNum> (account :<username>)</p> <p>Parameters description: ipaddr: The IP address of the RADIUS server. vlanID: the VID of RADIUS assigned VLAN. unitID: The unit ID. portNum: The port number. Username: The user that is being authenticated.</p>	Informational	

2	<p>Event description: 802.1X Authentication failure.</p> <p>Log Message: 802.1X Authentication failure [for <reason>] from (Username: <username>, Port: <portNum>, MAC: <macaddr>)</p> <p>Parameters description: reason: The reason for failed authentication. username: The user that is being authenticated. portNum: The port number. macaddr: the MAC address of authenticated device.</p>	Warning	
3	<p>Event description: 802.1X Authentication success.</p> <p>Log Message: 802.1X Authentication success from (Username: <username>, Port: <portNum>, MAC: <macaddr>)</p> <p>Parameters description: username: The user that being authenticated. portNum: The port number. macaddr: the MAC address of authenticated device.</p>	Informational	

Port Security Logs

ID	Log Description	Severity	Note
1	<p>Event description: Address full on a port</p> <p>Log Message: Port security violation [[([mac address:<macaddr>] on locking address full [port:< portNum>]]]</p> <p>Parameters description: macaddr: The violation MAC address. portNum: The port number.</p>	Warning	

IMPB Logs

ID	Log Description	Severity	Note
1	<p>Event description: Dynamic IMPB entry is conflicting with static ARP</p> <p>Log Message: Dynamic IMPB entry is conflicting with static ARP(IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)</p> <p>Parameters description: ipaddr: IP address macaddr: MAC address portNum : The port number</p>	Warning	

2	<p>Event description: Dynamic IMPB entry is conflicting with static FDB.</p> <p>Log Message: Dynamic IMPB entry is conflicting with static FDB(IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)</p> <p>Parameters description: ipaddr: IP address macaddr: MAC address portNum : The port number</p>	Warning	
3	<p>Event description: Dynamic IMPB entry conflicts with static IMPB.</p> <p>Log Message: Dynamic IMPB entry is conflicting with static IMPB(IP: <ipaddr>, MAC: <macaddr>, Port <portNum>).</p> <p>Parameters description: ipaddr: IP address macaddr: MAC address portNum : The port number</p>	Warning	
4	<p>Event description: Creating IMPB entry failed due to no ACL rule available.</p> <p>Log Message: Creating IMPB entry Failed due to no ACL rule available(IP:<ipaddr>, MAC: <macaddr>, Port <portNum>)</p> <p>Parameters description: ipaddr: IP address macaddr: MAC address portNum : The port number</p>	Warning	

LD Logs

ID	Log Description	Severity	Note
1	<p>Event Description: Loop back is detected under port-based mode.</p> <p>Log Message: Loop is detected on port <portNum> The port is blocked.</p> <p>Parameters Description: portNum: The port number.</p>	Critical	
2	<p>Event Description: Port recovered from LD blocked state under port-based mode.</p> <p>Log Message: Port <portNum> recovers from loop condition. LD is restarted.</p> <p>Parameters Description: portNum: The port number.</p>	Informational	

3	<p>Event Description: Loop back is detected under VLAN-based mode.</p> <p>Log Message: Loop is detected on port <portNum> in VLAN <vlanID >. Packets are discarded.</p> <p>Parameters Description: portNum: The port number. vlanID: the VLAN ID number.</p>	Critical	
4	<p>Event Description: Port recovered from LD blocked state under VLAN-based mode.</p> <p>Log Message: Port <portNum> VID <vlanID> recovers from loop condition. LD is restarted.</p> <p>Parameters Description: portNum: The port number. vlanID: the VLAN ID number.</p>	Informational	
5	<p>Event Description: The number of VLAN in which loop back occurs hit the specified number.</p> <p>Log Message: Looped VLAN number exceed the maximum block VLAN number.</p> <p>Parameters Description: None</p>	Informational	

Traffic Control Logs

ID	Log Description	Severity	Note
1	<p>Event description: Broadcast storm occurrence.</p> <p>Log Message: Port <portNum> Broadcast storm is occurring.</p> <p>Parameters description: portNum: The port number.</p>	Warning	
2	<p>Event description: Broadcast storm cleared.</p> <p>Log Message: Port <portNum> Broadcast storm has cleared.</p> <p>Parameters description: portNum: The port number.</p>	Informational	
3	<p>Event description: Multicast storm occurrence.</p> <p>Log Message: Port <portNum> Multicast storm is occurring.</p> <p>Parameters description: portNum: The port number.</p>	Warning	
4	<p>Event description: Multicast Storm cleared.</p> <p>Log Message: Port <portNum> Multicast storm has cleared.</p> <p>Parameters description: portNum: The port number.</p>	Informational	

5	<p>Event description: Port shut down due to a packet storm</p> <p>Log Message: Port <portNum> is currently shut down due to a packet storm</p> <p>Parameters description: portNum: The port number.</p>	Warning	
---	--	---------	--

IP and Password Change Logs

ID	Log Description	Severity	Note
1	<p>Event description: Password change activity</p> <p>Log Message: Password was changed by console (Username: <username>)</p> <p>Parameters description: username: user name.</p>	Informational	
2	<p>Event description: Management IP change</p> <p>Log Message: Management IP address was changed by console (Username: <username>)</p> <p>Parameters description: username: user name</p>	Informational	

Glossary

1000BASE-SX:	A short laser wavelength on multimode fiber optic cable for a maximum length of 550 meters
1000BASE-LX:	A long wavelength for a "long haul" fiber optic cable for a maximum length of 10 kilometers
100BASE-FX:	100Mbps Ethernet implementation over fiber.
100BASE-TX:	100Mbps Ethernet implementation over Category 5 and Type 1 Twisted Pair cabling.
10BASE-T:	The IEEE 802.3 specification for Ethernet over Unshielded Twisted Pair (UTP) cabling.
ageing:	The automatic removal of dynamic entries from the Switch Database which have timed-out and are no longer valid.
ATM:	Asynchronous Transfer Mode. A connection oriented transmission protocol based on fixed length cells (packets). ATM is designed to carry a complete range of user traffic, including voice, data and video signals.
auto-negotiation:	A feature on a port which allows it to advertise its capabilities for speed, duplex and flow control. When connected to an end station that also supports auto-negotiation, the link can self-detect its optimum operating setup.
backbone port:	A port which does not learn device addresses, and which receives all frames with an unknown address. Backbone ports are normally used to connect the Switch to the backbone of your network. Note that backbone ports were formerly known as designated downlink ports.
backbone:	The part of a network used as the primary path for transporting traffic between network segments.
bandwidth:	Information capacity, measured in bits per second that a channel can transmit. The bandwidth of Ethernet is 10Mbps, the bandwidth of Fast Ethernet is 100Mbps.
baud rate:	The switching speed of a line. Also known as line speed between network segments.
BOOTP:	The BOOTP protocol allows automatic mapping of an IP address to a given MAC address each time a device is started. In addition, the protocol can assign the subnet mask and default gateway to a device.
bridge:	A device that interconnects local or remote networks no matter what higher level protocols are involved. Bridges form a single logical network, centralizing network administration.
broadcast:	A message sent to all destination devices on the network.
broadcast storm:	Multiple simultaneous broadcasts that typically absorb available network bandwidth and can cause network failure.
console port:	The port on the Switch accepting a terminal or modem connector. It changes the parallel arrangement of data within computers to the serial form used on data transmission links. This port is most often used for dedicated local management.
CSMA/CD:	Channel access method used by Ethernet and IEEE 802.3 standards in which devices transmit only after finding the data channel clear for some period of time. When two devices transmit simultaneously, a collision occurs and the colliding devices delay their retransmissions for a random amount of time.
data center switching:	The point of aggregation within a corporate network where a switch provides high-performance access to server farms, a high-speed backbone connection and a control point for network management and security.
Ethernet:	A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks operate at 10Mbps using CSMA/CD to run over cabling.
Fast Ethernet:	100Mbps technology based on the CSMA/CD network access method.
Flow Control:	(IEEE 802.3X) A means of holding packets back at the transmit port of the connected end station. Prevents packet loss at a congested switch port.
forwarding:	The process of sending a packet toward its destination by an internetworking device.
full duplex:	A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

half duplex:	A system that allows packets to be transmitted and received, but not at the same time. Contrast with full duplex.
IP address:	Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with full-stops (periods), and is made up of a network section, an optional subnet section and a host section.
IPX:	Internetwork Packet Exchange. A protocol allowing communication in a NetWare network.
LAN - Local Area Network:	A network of connected computing resources (such as PCs, printers, servers) covering a relatively small geographic area (usually not larger than a floor or building). Characterized by high data rates and low error rates.
latency:	The delay between the time a device receives a packet and the time the packet is forwarded out of the destination port.
line speed:	See baud rate.
main port:	The port in a resilient link that carries data traffic in normal operating conditions.
MDI - Medium Dependent Interface:	An Ethernet port connection where the transmitter of one device is connected to the receiver of another device.
MDI-X - Medium Dependent Interface Cross-over:	Ethernet port connections, where the internal transmit and receive lines are crossed.
MIB - Management Information Base:	Stores a device's management characteristics and parameters. MIBs are used by the Simple Network Management Protocol (SNMP) to contain attributes of their managed systems. The Switch contains its own internal MIB.
multicast:	Single packets copied to a specific subset of network addresses. These addresses are specified in the destination-address field of the packet.
protocol:	A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.
resilient link:	A pair of ports that can be configured so that one will take over data transmission should the other fail. See also main port and standby port.
RJ-45:	Standard 8-wire connectors for IEEE 802.3 10BASE-T networks.
RMON:	Remote Monitoring. A subset of SNMP MIB II that allows monitoring and management capabilities by addressing up to ten different groups of information.
RPS - Redundant Power System:	A device that provides a backup source of power when connected to the Switch.
server farm:	A cluster of servers in a centralized location serving a large user population.
SLIP - Serial Line Internet Protocol:	A protocol which allows IP to run over a serial line connection.
SNMP - Simple Network Management Protocol:	A protocol originally designed to be used in managing TCP/IP internets. SNMP is presently implemented on a wide range of computers and networking equipment and may be used to manage many aspects of network and end station operation.
Spanning Tree Protocol (STP):	A bridge-based system for providing fault tolerance on networks. STP works by allowing the user to implement parallel paths for network traffic, and ensure that redundant paths are disabled when the main paths are operational and enabled if the main paths fail.
standby port:	The port in a resilient link that will take over data transmission if the main port in the link fails.
switch:	A device which filters, forwards and floods packets based on the packet's destination address. The switch learns the addresses associated with each switch port and builds tables based on this information to be used for the switching decision.
TCP/IP:	A layered set of communications protocols providing Telnet terminal emulation, FTP file transfer, and other services for communication among a wide range of computer equipment.

telnet:	A TCP/IP application protocol that provides virtual terminal service, letting a user log in to another computer system and access a host as if the user were connected directly to the host.
TFTP - Trivial File Transfer Protocol:	Allows the user to transfer files (such as software upgrades) from a remote device using your switch's local management capabilities.
UDP - User Datagram Protocol:	An Internet standard protocol that allows an application program on one device to send a datagram to an application program on another device.
VLAN - Virtual LAN:	A group of location and topology-independent devices that communicate as if they are on a common physical LAN.
VLT - Virtual LAN Trunk:	A Switch-to-Switch link which carries traffic for all the VLANs on each Switch.
VT100:	A type of terminal that uses ASCII characters. VT100 screens have a text-based appearance.