



Web UI Reference Guide

Gigabit Ethernet SmartPro Switch

DGS-1510 Series

Information in this document is subject to change without notice. Reproduction of this document in any manner, without the written permission of the D-Link Corporation, is strictly forbidden.

Trademarks used in this text: D-Link and the D-Link logo are trademarks of the D-Link Corporation; Microsoft and Windows are registered trademarks of the Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either as the entities claiming the marks and the names or their products. D-Link Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

© 2024 D-Link Corporation. All rights reserved.

Table of Contents

1.	Introduction	1
	Audience	1
	Other Documentation	1
	Conventions	1
	Notes, Notices, and Cautions	1
2.	Web-based Switch Configuration	2
	Management Options	2
	Connecting using the Web UI	2
	Logging onto the Web UI	3
	Smart Wizard	4
	Step 1 - Web Mode	4
	Step 2 - System IP Information	5
	Step 3 - User Accounts Settings	
	Step 4 - SNMP Settings	7
	Web User Interface (Web UI)	9
	Areas of the User Interface	9
	Standard Mode	9
	Surveillance Mode	10
3.	System	
	Device Information	
	System Information Settings	
	Peripheral Settings	
	Port Configuration	
	Port Settings	
	Port Status	
	Port GBIC	
	Port Auto Negotiation	
	Error Disable Settings	
	Jumbo Frame	
	Interface Description	
	PoE (PoE Switches Only)	
	PoE System	
	PoE Status	
	PoE Configuration	
	PD Alive	
	PoE Statistics	
	PoE Measurement	
	PoE LLDP Classification	
	System Log.	
	System Log Settings	
	System Log Discriminator Settings	
	System Log Server Settings System Log	
	System Attack Log	
	Time and SNTP	
	Clock Settings	
	Time Zone Settings	
	SNTP Settings	
	erri edunge	

Time Range	
Management	
User Account Settings	
Password Encryption	
Login Method	
SNMP	
SNMP Global Settings	
SNMP Linkchange Trap Settings	
SNMP View Table Settings	
SNMP Community Table Settings	
SNMP Group Table Settings	
SNMP Engine ID Local Settings	
SNMP User Table Settings	
SNMP Host Table Settings	
RMON	
RMON Global Settings	
RMON Statistics Settings	
RMON History Settings	
RMON Alarm Settings	
RMON Event Settings	
Telnet/Web	
Session Timeout	
DHCP	
Service DHCP	
DHCP Class Settings	
DHCP Server	
DHCP Server Global Settings	
DHCP Server Pool Settings	
DHCP Server Exclude Address	
DHCP Server Manual Binding	
DHCP Server Dynamic Binding	
DHCP Server IP Conflict	
DHCP Server Statistic	
DHCPv6 Server	
DHCPv6 Server Pool Settings	
DHCPv6 Server Local Pool Settings	
DHCPv6 Server Exclude Address	
DHCPv6 Server Binding	
DHCPv6 Server Interface Settings	
DHCPv6 Server Operational Information	
DHCP Relay	
DHCP Relay Global Settings	
DHCP Relay Pool Settings	
DHCP Relay Information Settings	
DHCP Relay Information Option Format Settings	
DHCP Relay Information Profile Settings	
DHCP Local Relay VLAN	
DHCPv6 Relay	
DHCPv6 Relay Global Settings	
DHCPv6 Relay Interface Settings	
DHCP Auto Configuration	
DHCP Auto Configuration DNS	

DNS Global Settings	
DNS Name Server Settings	
DNS Host Settings	
NTP	
NTP Global Settings	
NTP Server Settings	
NTP Peer Settings	
NTP Access Group Settings	
NTP Key Settings	
NTP Interface Settings	
NTP Associations	
NTP Status	
IP Source Interface	
File System	
Physical Stacking	
Virtual Stacking (SIM)	
Single IP Settings	
Topology	
File	
Print Topology	
Preference	
Group	
Add to Group	
Remove from Group	
Device	
Configure	
View	
Refresh	
Topology	
Help	
About	
Firmware Upgrade	
Configuration File Backup/Restore	
Upload Log File	
D-Link Discovery Protocol	
Layer 2 Features	
FDB	
Static FDB	
Unicast Static FDB	
Multicast Static FDB	
MAC Address Table Settings	
MAC Address Table	
MAC Notification	
VLAN	
VLAN Configuration Wizard	
Create/Configure VLAN	
Create VLAN	
Configure VLAN	
802.1Q VLAN	
VLAN Interface	
VLAN Interface Settings	
Port Summary	
·	

5.

802.1v Protocol VLAN	
Protocol VLAN Profile	
Protocol VLAN Profile Interface	
GVRP	
GVRP Global	
GVRP Port	
GVRP Advertise VLAN	
GVRP Forbidden VLAN	
GVRP Statistics Table	
Asymmetric VLAN	
MÁC VLAN	
L2VLAN Interface Description	
Auto Surveillance VLAN	
Auto Surveillance Properties	
MAC Settings and Surveillance Device	
ONVIF IP-Camera Information	
ONVIF NVR Information	
Voice VLAN	
Voice VLAN Global	
Voice VLAN Port	
Voice VLAN OUI	
Voice VLAN Device	
Voice VLAN LLDP-MED Device	
STP	
STP Global Settings	
STP Port Settings	
MST Configuration Identification	
STP Instance	
MSTP Port Information	
ERPS (G.8032)	
ERPS	
ERPS Profile	
Loopback Detection	
Link Aggregation	
L2 Multicast Control	
IGMP Snooping	
IGMP Snooping Settings	
IGMP Shooping Settings	
IGMP Snooping Mrouter Settings	
IGMP Snooping Statistics Settings	
MLD Snooping	
MLD Shooping Settings	
MLD Shooping Groups Settings	
MLD Shooping Groups Settings	
MLD Shooping Milouter Settings	
Multicast Filtering	
LLDP	
LLDP Global Settings	
LLDP Management Address List LLDP Basic TLVs Settings	
LLDP Dasic TLVS Settings	

	LLDP Dot3 TLVs Settings	170
	LLDP-MED Port Settings	171
	LLDP Statistics Information	172
	LLDP Local Port Information	173
	LLDP Neighbor Port Information	174
6.	Layer 3 Features	176
	ARP	
	ARP Aging Time	
	Static ARP	
	Proxy ARP	177
	ARP Table	
	Gratuitous ARP	179
	UDP Helper	180
	IP Forward Protocol	180
	IP Helper Address	180
	IPv4 Interface	181
	IPv4 Static/Default Route	183
	IPv4 Route Table	184
	IPv6 Interface	185
	IPv6 Neighbor	189
	IPv6 Static/Default Route	189
	IPv6 Route Table	190
	IPMC	191
	IP Multicast Global Settings	191
	IP Multicast Forwarding Cache	191
7.	Quality of Service (QoS)	192
	Basic Settings	192
	Port Default CoS	
		192
	Port Default CoS	192 193
	Port Default CoS Port Scheduler Method	192 193 194
	Port Default CoS Port Scheduler Method Queue Settings	
	Port Default CoS Port Scheduler Method Queue Settings CoS to Queue Mapping	
	Port Default CoS Port Scheduler Method Queue Settings CoS to Queue Mapping Port Rate Limiting	
	Port Default CoS Port Scheduler Method Queue Settings CoS to Queue Mapping Port Rate Limiting Queue Rate Limiting	
	Port Default CoS Port Scheduler Method Queue Settings CoS to Queue Mapping Port Rate Limiting Queue Rate Limiting Advanced Settings	
	Port Default CoS Port Scheduler Method Queue Settings CoS to Queue Mapping Port Rate Limiting Queue Rate Limiting Advanced Settings DSCP Mutation Map	
	Port Default CoS Port Scheduler Method Queue Settings CoS to Queue Mapping Port Rate Limiting Queue Rate Limiting Advanced Settings DSCP Mutation Map Port Trust State and Mutation Binding	
	Port Default CoS Port Scheduler Method Queue Settings CoS to Queue Mapping Port Rate Limiting Queue Rate Limiting Advanced Settings DSCP Mutation Map Port Trust State and Mutation Binding DSCP CoS Mapping	192 193 194 195 195 196 197 198 198 198 199 200
	Port Default CoS Port Scheduler Method Queue Settings CoS to Queue Mapping Port Rate Limiting Queue Rate Limiting Advanced Settings DSCP Mutation Map Port Trust State and Mutation Binding DSCP CoS Mapping CoS Color Mapping	
	Port Default CoS Port Scheduler Method Queue Settings CoS to Queue Mapping Port Rate Limiting Queue Rate Limiting Queue Rate Limiting DSCP Mutation Map Port Trust State and Mutation Binding DSCP CoS Mapping CoS Color Mapping DSCP Color Mapping	192 193 194 195 196 197 198 198 198 199 200 201 201 202 203
	Port Default CoS Port Scheduler Method Queue Settings CoS to Queue Mapping Port Rate Limiting Queue Rate Limiting Advanced Settings DSCP Mutation Map Port Trust State and Mutation Binding DSCP CoS Mapping CoS Color Mapping DSCP Color Mapping DSCP Color Mapping	192 193 194 195 196 197 198 198 198 198 200 201 201 202 203 203
	Port Default CoS Port Scheduler Method Queue Settings CoS to Queue Mapping Port Rate Limiting Queue Rate Limiting Advanced Settings DSCP Mutation Map Port Trust State and Mutation Binding DSCP CoS Mapping CoS Color Mapping DSCP Color Mapping. DSCP Color Mapping. Class Map Aggregate Policer.	192 193 194 195 196 197 198 198 198 199 200 201 201 202 203 203 204 207
8.	Port Default CoS Port Scheduler Method Queue Settings CoS to Queue Mapping. Port Rate Limiting Queue Rate Limiting Advanced Settings DSCP Mutation Map Port Trust State and Mutation Binding DSCP CoS Mapping CoS Color Mapping. DSCP Color Mapping. Class Map Aggregate Policer. Policy Map.	192 193 194 195 196 197 198 198 198 199 200 201 201 202 203 203 204 207 210
8.	Port Default CoS Port Scheduler Method Queue Settings CoS to Queue Mapping Port Rate Limiting Queue Rate Limiting Advanced Settings DSCP Mutation Map Port Trust State and Mutation Binding DSCP CoS Mapping CoS Color Mapping DSCP Color Mapping Class Map Aggregate Policer Policy Map Policy Binding	192 193 194 195 196 197 198 198 198 198 199 200 201 201 202 203 203 204 207 210 210
8.	Port Default CoS Port Scheduler Method Queue Settings CoS to Queue Mapping. Port Rate Limiting Queue Rate Limiting Advanced Settings DSCP Mutation Map Port Trust State and Mutation Binding. DSCP CoS Mapping CoS Color Mapping. DSCP Color Mapping. Class Map Aggregate Policer. Policy Map Policy Binding.	
8.	Port Default CoS Port Scheduler Method Queue Settings CoS to Queue Mapping Port Rate Limiting Queue Rate Limiting Advanced Settings DSCP Mutation Map Port Trust State and Mutation Binding DSCP CoS Mapping CoS Color Mapping DSCP Color Mapping Class Map Aggregate Policer Policy Map Policy Binding ACL Configuration Wizard	
8.	Port Default CoS Port Scheduler Method Queue Settings CoS to Queue Mapping. Port Rate Limiting Queue Rate Limiting Advanced Settings DSCP Mutation Map Port Trust State and Mutation Binding. DSCP CoS Mapping CoS Color Mapping. DSCP Color Mapping. Class Map Aggregate Policer. Policy Map Policy Binding.	192 193 194 195 196 197 198 198 198 198 198 200 201 201 202 203 203 204 203 204 207 210 207 210 211 230 231
8.	Port Default CoS Port Scheduler Method Queue Settings CoS to Queue Mapping Port Rate Limiting Queue Rate Limiting Advanced Settings DSCP Mutation Map Port Trust State and Mutation Binding DSCP CoS Mapping CoS Color Mapping DSCP Color Mapping Class Map Aggregate Policer. Policy Map. Policy Binding. Access Control List (ACL) ACL Configuration Wizard ACL Access List Standard IP ACL	192 193 194 195 196 197 198 198 198 199 200 201 201 202 203 203 204 207 210 207 210 211 230 231 234
8.	Port Default CoS Port Scheduler Method Queue Settings CoS to Queue Mapping Port Rate Limiting. Queue Rate Limiting Advanced Settings DSCP Mutation Map Port Trust State and Mutation Binding DSCP CoS Mapping CoS Color Mapping DSCP Color Mapping Class Map Aggregate Policer. Policy Map. Policy Binding. Access Control List (ACL) ACL Configuration Wizard ACL Access List Standard IP ACL Extended IP ACL	192 193 194 195 196 197 198 198 198 199 200 201 201 202 203 203 204 203 204 207 210 210 211 230 231 234 234

	Extended Expert ACL	
	ACL Interface Access Group	
	ACL VLAN Access Map	
	ACL VLAN Filter	
9.	Security	
	Port Security	
	Port Security Global Settings	
	Port Security Port Settings	
	Port Security Address Entries	
	802.1X	
	802.1X Global Settings	
	802.1X Port Settings	
	Authentication Session Information	
	Authentication Session mornation	
	Authenticator Session Statistics	
	Authenticator Diagnostics	
	Addition Diagnostics	
	AAA Global Settings	
	Application Authentication Settings	
	Application Accounting Settings	
	Application Accounting Settings	
	Accounting Settings Server RADIUS Dynamic Author Settings	
	RADIUS	
	RADIUS Global Settings	
	RADIUS Slobal Settings	
	RADIUS Group Server Settings	
	RADIUS Statistic	
	TACACS+	
	TACACS+ Global Settings	
	TACACS+ Server Settings	
	TACACS+ Group Server Settings	
	TACACS+ Statistic	
	IMPB	
	IPv4	
	DHCPv4 Snooping	
	DHCP Snooping Global Settings	
	DHCP Snooping Port Settings	
	DHCP Snooping VLAN Settings	
	DHCP Snooping Database	
	DHCP Snooping Binding Entry	
	Dynamic ARP Inspection	
	ARP Access List	
	ARP Inspection Settings	
	ARP Inspection Port Settings	
	ARP Inspection VLAN	
	ARP Inspection Statistics	
	ARP Inspection Log	
	IP Source Guard	
	IP Source Guard Port Settings	
	IP Source Guard Binding	
	IP Source Guard HW Entry	

Advanced Settings	
IP-MAC-Port Binding Settings	
IP-MAC-Port Binding Blocked Entry	
IPv6	
IPv6 Snooping	
IPv6 ND Inspection	
IPv6 RA Guard	
IPv6 DHCP Guard	
IPv6 Source Guard	
IPv6 Source Guard Settings	
IPv6 Neighbor Binding	
DHCP Server Screening	
DHCP Server Screening Global Settings	
DHCP Server Screening Port Settings	
ARP Spoofing Prevention	
BPDU Attack Protection	
MAC Authentication	
Web-based Access Control	
Web Authentication	
WAC Port Settings	
WAC Customize Page	
Japanese Web-based Access Control	
JWAC Global Settings	
JWAC Port Settings	
JWAC Customize Page Language	
JWAC Customize Page	
Network Access Authentication	
Guest VLAN	
Network Access Authentication Global Settings	
Network Access Authentication Port Settings	
Network Access Authentication Sessions Information	
Safeguard Engine	
Safeguard Engine Settings	
CPU Protect Counters	
CPU Protect Sub-Interface	
CPU Protect Type	
Trusted Host	
Traffic Segmentation Settings	
Storm Control Settings	
DoS Attack Prevention Settings	
SSH	
SSH Global Settings	
Host Key	
SSH Server Connection	
SSH User Settings	
SSL	
SSL Global Settings	
Crypto PKI Trustpoint	
SSL Service Policy	
Network Protocol Port Protection Settings	
OAM	
Cable Diagnostics	

	DDM	357
	DDM Settings	358
	DDM Temperature Threshold Settings	359
	DDM Voltage Threshold Settings	359
	DDM Bias Current Threshold Settings	360
	DDM TX Power Threshold Settings	361
	DDM RX Power Threshold Settings	
	DDM Status Table	362
11.	Monitoring	363
	Utilization	363
	Port Utilization	363
	Statistics	364
	Port	364
	Port Counters	366
	Counters	367
	Mirror Settings	368
	sFlow	370
	sFlow Agent Information	370
	sFlow Receiver Settings	371
	sFlow Sampler Settings	372
	sFlow Poller Settings	373
	Device Environment	373
12.	Green	374
	Power Saving	374
	EEE	
13	Toolbar	
	Save	
	Save Configuration	
	Firmware Upgrade & Backup	
	Firmware Upgrade from HTTP	
	Firmware Upgrade from TFTP	
	Firmware Backup to HTTP	
	Firmware Backup to TFTP	
	Configuration Restore & Backup	
	Configuration Restore from HTTP	
	Configuration Restore from TFTP	
	Configuration Backup to HTTP	
	Configuration Backup to TFTP	
	Log Backup	
	Log Backup to HTTP	
	Log Backup to TFTP	
	Ping	384
	Trace Route	386
	Language Management	388
	Reset	
	Reboot System	389
	Wizard	389
	Online Help	389
	D-Link Support Site	389
	User Guide	389

	Surveillance Mode	
	Logout	
14.	Surveillance Mode	
	Surveillance Overview	
	Surveillance Topology	
	Device Information	
	Port Information	
	Group Details	
	IP-Camera Information	
	NVR Information	
	PoE Information	
	PoE Scheduling	
	Management	403
	File System	403
	Time	
	Clock Settings	
	SNTP Settings	
	Surveillance Settings	
	Surveillance Log	
	Health Diagnostic	
	Toolbar	
	Wizard	
	Tools	
	Firmware Upgrade & Backup	
	Firmware Upgrade from HTTP	
	Firmware Backup to HTTP	
	Configuration Restore & Backup	
	Configuration Restore from HTTP	
	Configuration Backup to HTTP	
	Language Management	
	Reset	
	Reboot System	
	Save	
	Save Configuration	
	Online Help D-Link Support Site	
	User Guide	
	Standard Mode	
	Logout	
•		
	pendix A - System Log Entries	
• •	pendix B - Trap Entries	
	pendix C - RADIUS Attributes Assignment	
	pendix D - IETF RADIUS Attributes Support	
Ар	pendix E - ERPS Information	

1. Introduction

Audience

This reference manual is intended for network administrators and other IT networking professionals responsible for managing the switch by using the Web User Interface (Web UI). The Web UI is the secondary management interface to the DGS-1510 Series switch, which will be generally be referred to simply as the 'Switch' within this manual. This manual is written in a way that assumes that you already have the experience and knowledge of Ethernet and modern networking principles for Local Area Networks.

Other Documentation

The documents below are a further source of information in regards to configuring and troubleshooting the switch. All the documents are available either from the CD, bundled with this switch, or from the D-Link website. Other documents related to this switch are:

- DGS-1510 Series Gigabit Ethernet SmartPro Switch Hardware Installation Guide
- DGS-1510 Series Gigabit Ethernet SmartPro Switch CLI Reference Guide

Conventions

Convention	Description
Boldface Font	This indicates a button, a toolbar icon, menu, or menu item. For example, Open the File menu and choose Cancel . Used for emphasis. This 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.
Initial capital letter	This indicates a window name. Names of keys on the keyboard have initial capitals. For example, click Enter.
Menu Name > Menu Option	This 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.

Notes, Notices, and Cautions

Below are examples of the three types of indicators used in this manual. When administering your switch using the information in this document, you should pay special attention to these indicators. Each example below provides an explanatory remark regarding each type of indicator.



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



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



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

2. Web-based Switch Configuration

Management Options Connecting using the Web Logging onto the Web Smart Wizard Web User Interface (Web UI)

Management Options

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

Web User Interface (Web UI)

The Switch can be managed through any of the RJ4/SFP/SFP+ ports on the front panel of the Switch by means of an HTTP/HTTPS connection using a Web browser like Microsoft[®] Internet Explorer, Mozilla Firefox, Safari, or Google Chrome.

Command Line Interface (CLI)

The Switch can be managed, Out-Of-Band (OOB), through the RJ45 Console port on the front panel of the Switch. Alternatively, the Switch can also be managed, in-band, through any of the RJ4/SFP/SFP+ ports on the front panel of the Switch by means of a Telnet connection. The command line interface provides complete access to all switch management features.

SNMP-based Management

The Switch can be managed with an SNMP-compatible console program. The Switch supports SNMPv1, SNMPv2c, and SNMPv3. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

Connecting using the Web UI

Most software functions of the DGS-1510 Series switches can be managed, configured, and monitored through the Web UI. Manage the Switch from remote stations anywhere on the network through a standard web browser. The web browser acts as a universal access tool and can communicate directly with the Switch using the HTTP or HTTPS protocol.



NOTE: The Command Line Interface (CLI) provides the functionality of managing, configuring, and monitoring **all** of the software features that are available on the Switch.

Logging onto the Web UI

To access the Web UI, simply open a standard web browser on the management PC, and enter the Switch's default IP address into the address bar of the browser and press the **Enter** key.

- 1	

NOTE: The default IP address of this switch is **10.90.90.90**, with a subnet mask of **255.0.0**.

🗿 http://t0.90.90/j 0 + 2 + × 10.90.90.90 Figure 2-1 IP address in Internet Explorer



NOTE: By default, one user account is already configured on the Switch. Both the username and password for this account is **admin**.



NOTE: After upgrading the firmware on the Switch and no user accounts were created, the default **admin** user account will automatically be created after rebooting the Switch with the new boot-up configuration file.



NOTE: After upgrading the firmware on the Switch and user accounts were created, the default **admin** user account will not be created automatically. Only after a factory reset was performed on the Switch will the default **admin** user account be created.

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

90,90,90
L.
admin

English
Login Reset

Figure 2-2 User Authentication Window

Enter the **User Name** and **Password** in the corresponding fields and click **Login**. This will open the Web UI. Management features available in the Web UI of the Switch are explained below.

Smart Wizard

After successfully connecting to the Web UI for the first time, the **Smart Wizard** embedded Web utility will be launched. This wizard will guide the user through basic configuration steps that is essential for first time connection to the Switch.

Step 1 - Web Mode

The Switch supports two Web Modes: **Standard Mode** and **Surveillance Mode**. The Standard Mode is used to configure, manage, and monitor most of the software features on the Switch. The Surveillance Mode is an additional web mode specifically designed to assist the user with surveillance features supported by the Switch.



NOTE: The **Web Mode** can only be changed when one user session is connected to the Web UI of the Switch.

	Smart Wizard The woord will guide you to do basic configurations on 4 steps for the Web Node. IP Information User Account and SNMP. If you are not changing the settings, click on "Exil" to politick to the main page.
0	Step 1 of 4: Choose the web interface mode.
	Web Mode
08	Standard Mode SumeRecentWode:
-	mans the waterd more time took Next
1.12	Hore the waterd herd time
())	

Figure 2-3 Web Mode

The fields that can be configured are described below:

Parameter	Description
Standard Mode	Select this option to access the Standard Mode after the Smart Wizard was completed.
Surveillance Mode	Select this option to access the Surveillance Mode after the Smart Wizard was completed.

Tick the **Ignore the wizard next time** option to skip the Smart Wizard on the next login.

Click the **Exit** button to discard the changes made, exit the Smart Wizard, and continue to the Web UI.

Click the **Next** button to accept the changes made and continue to the next step.

Step 2 - System IP Information

In this step, we can configure System IP Information.



NOTE: The Switch will probe for surveillance devices every 30 seconds. If a surveillance device is not in the same subnet as the switch, it will not be discovered automatically. Place the Switch management IP in the same subnet as the surveillance devices for ONVIF cameras to be added to the Surveillance Mode Web UI automatically.

System P Infor	ration			
• State	DHC8	*3		
IP ADDRESS	10	90 90	90	
Netmask	8 (255.0	0.01	4	
Outowin	0	0 0	0	

Figure 2-4 System IP Information

Parameter	Description
Static	Select this option to manually assign and configure the IP address settings for the Switch.
DHCP	Select this option to obtain IP address settings automatically from a DHCP server for the Switch.
IP Address	After selecting the Static option, manually enter the IP address of the Switch here.
Netmask	After selecting the Static option, manually select the Netmask option here.

The fields that can be configured are described below:

Parameter	Description
Gateway	After selecting the Static option, manually enter the IP address of the default gateway here.

Tick the **Ignore the wizard next time** option to skip the Smart Wizard on the next login.

Click the **Exit** button to discard the changes made, exit the Smart Wizard, and continue to the Web UI.

Click the **Next** button to accept the changes made and continue to the next step.

Step 3 - User Accounts Settings

In this step, we can configure the user account settings. This step can only be modified by a user account with the privilege level of 15.

liner Accounts Se		_	_	
QuarMania.	admin			
Purnweid Type	None	(*		
Pasawatti		3		

Figure 2-5 User Account Settings

The fields that can be configured are described below:

Parameter	Description
User Name	Select the user name of the administrator level account with the privilege level of 15.
Password Type	 Select the password type here. Options to choose from are: None - Specifies that no password will be configured for this user account. Plain Text - Specifies that the password for this user account will be in the plain text form. Encrypted-SHA1 - Specifies that the password for this user account will be in the encrypted form using the SHA1 encryption method.

Parameter	Description		
	• Encrypted-MD5 - Specifies that the password for this user account will be in the encrypted form using the MD5 encryption method.		
Password	Enter the password for the user account either in the plain text format or the encrypted format here based on the previous selection made.		
	In the encrypted format, the password will not be encrypted from plain text to the encrypted format. Instead, the encrypted password must be entered. To encrypt the password from plain text to the encrypted format, refer to the Password Encryption window.		

Tick the Ignore the wizard next time option to skip the Smart Wizard on the next login.

Click the **Exit** button to discard the changes made, exit the Smart Wizard, and continue to the Web UI.

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

Click the Apply button to accept the changes made and continue to the Web UI.

Step 4 - SNMP Settings

In this step, we can enable or disable the SNMP feature.

Welcome to Smart Wizard	munagement
SHMP	
SYANIF • Enshied	Deuteri
tgeore the willing next time	Exè Back Apply & Save

Figure 2-6 SNMP Window

The fields that can be configured are described below:

Parameter	Description
SNMP	Select the Enabled option to enable the SNMP feature. Select the Disabled option to disable the SNMP feature.

Tick the **Ignore the wizard next time** option to skip the Smart Wizard on the next login.

Click the **Exit** button to discard the changes made, exit the Smart Wizard, and continue to the Web UI.

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

Click the Apply & Save button to accept the changes made and continue to the Web UI.

Web User Interface (Web UI)

Areas of the User Interface

The Web UI on the Switch can be divided into distinct **Areas**. Different areas in the Web UI provide different manageability options to simplify configuration and feature monitoring.

Standard Mode

After accessing the Web UI in the **Standard Mode**, the following will be displayed:

D-Link				
Land State Man	a destruites et a discrimina	and the state of the	AREA 2	forming A space 20
matheway	Serie bismidat			
- 2024, Hellowie - 2024, Hell	Encode Million management Descusar Trans- contente for an ingeneration of the an- ingeneration of the an- the instances Trans-Million and Trans- ment of the an-	not, s > to car é	With white In Adaption International California Taranti Taranti Taranti Taranti	Ser Televist soles 1 Sub-Transfer Televist all mark # We That Televist Regulations
AREA 3	1 - 40 - 11 1996 - P			AREA 4
	200 - 100 - 100 200 - 100 - 100 200 - 100 - 100 200 - 100			AREA 4
		L		

Figure 2-7 Web UI (Standard Mode)

The following **Areas** can be observed in the above window.

Area Number	Description
AREA 1	In this area, a graphical near real-time image of the front panel of the Switch is displayed with ports and expansion modules. Port activity is displayed, depending on the specified mode. Some management functions like port monitoring are also accessible here.
	Click the D-Link logo to go to the D-Link website.
AREA 2	In this area is a toolbar used to access functions like Save , Tools , the Wizard , Online Help , accessing the Web UI in the Surveillance Mode , customized Language preference, and a Logout option.
	Click the Surveillance Mode option to change the switch mode from Standard Mode to Surveillance Mode.
	The user account and IP address currently logged into the Web UI will also be displayed in this toolbar.

Area Number	Description
AREA 3	In this area, the software features available in the Web UI of the Switch are grouped into folders containing hyperlinks that will open window frames in area 4.
	There is also a search option in this area that can be used to search for specific feature keywords in the Web UI to easily find the link to the set of features.
AREA 4	In this area, configuration and monitoring window frames are available based on the selections made in area 3.

Surveillance Mode

After accessing the Web UI in the **Surveillance Mode**, the following will be displayed:

				Surveillance Mad
ne) skoel	Ener () a di territori L'una lince Catalane	Crances Data VI	AREA 1	Files and some set-15
AND IN COLUMN		AND A RECTOR		
or advanced to Construction of Antonional Antonional Alt Antonional Alt Antonional Antonio Antonio	*** 1 ×	9x3 93	£_x0 ₿ x*	1 🔺 x 0 🐟 x 1
n Na an Araga Manazara Na Kasara	P P P			
10				
REA 2	DCmA			AREA 3
	CIRCURS.	009 0090 09		
				1000
				<u> </u>

Figure 2-8 Web UI (Surveillance Mode)

The following Areas can be observed in the above window.

Area Number	Description
AREA 1	In this area is a toolbar used to access functions like the Wizard , Tools , Save , Help , Online Help , accessing the Web UI in the Standard Mode , customized Language preference, and a Logout option. Click the Standard Mode option to change the switch mode from
	Surveillance Mode to Standard Mode.
	The user account and IP address currently logged into the Web UI will also be displayed in this toolbar.
AREA 2	In this area, the software features available in the Web UI of the Switch are grouped into folders containing hyperlinks that will open window frames in area 3.

Area Number	Description
	There is also a search option in this area that can be used to search for specific feature keywords in the Web UI to find the link to the set of features.
AREA 3	In this area, configuration and monitoring window frames are available based on the selections made in Area 2.
	The status of devices, IP cameras, and NVRs discovered on the switch will also be displayed in this area.



NOTE: For more information about the Surveillance Mode, refer to **Surveillance Mode** on page 391.

3. System

```
Device Information
System Information Settings
Peripheral Settings
Port Configuration
Interface Description
PoE
System Log
Time and SNTP
Time Range
```

Device Information

In this window, the Device Information, CPU, and Used status are displayed. It appears automatically when you log in the Switch. To return to the Device Information window after viewing other windows, click the **DGS-1510-28XMP** link.



Figure 3-1 Device Information Window

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 > System Information Settings**, as shown below:

Scillings		
us .		
1002	1	
Ahilat		
20.5 4 4		Apd +
	n Andra Distan	A ANY ANY ANY ANY ANY ANY ANY ANY ANY AN

Figure 3-2 System Information Settings Window

The fields that can be configured are described below:

Parameter	Description
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. This string can be up to 255 characters long.
System Contact	Enter a contact name for the Switch, if so desired. This string can be up to 255 characters long.

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

Peripheral Settings

This window is used to configure the environment trap settings and environment temperature threshold settings.

To view the following window, click **System > Peripheral Settings**, as shown below:

Paripharal Sattings		
- Homeshand Loop acting s		
Fin Toy	Condition representation	
Privet Licap	Central Control Control	
Temperature hop	Céntier (Contra	Apple
- Environment Temperature Three to	ét Sintinga.	
Unit	1 v	
Thanal	1	
High Threshold 3-100-2008	20 🔟 Övluri.	
Low Three IoN (-100-200)	li ⊴Dviui.	App (a



The fields that can be configured are described below:

Parameter	Description
	Click to enable or disable the fan trap state for waning fan event (fan failed or fan recover).

Parameter	Description
Power Trap	Click to enable or disable the power trap state for waning power event (power failed or power recover).
Temperature Trap	Click to enable or disable the temperature trap state for waning temperature event (temperature exceeds the thresholds or temperature recover).
Unit	Select the switch unit that will be used for this configuration here.
Thermal	Select the thermal sensor ID.
High Threshold	Enter the high threshold value of the warning temperature setting. The range is from -100 to 200 degree Celsius. Tick the Default check box to return to the default value.
Low Threshold	Enter the low threshold value of the warning temperature setting. The range is from -100 to 200 degree Celsius. Tick the Default check box to return to the default value.

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

Port Configuration

Port Settings

This window is used to view and configure the Switch's port settings.

et Setil ega —									
	train Pol	(Por	(4.4)	H	21.48	Achi How		4 m	
1	d anan	 Minut 	z Ent	10 101	Nuc	2 Dantes	10 M 100	14	
ague 👘	Speed	.33360.	ACTIVITIES		Owner or or	seats November	Sec. Sec.		
4ula 🛛 🕅		V V 1001	2 1004 (v/1000	4	Ritter		11		1620
Lan Salange									
1				Harel	and the second			A.8.5	
1998	I PE FORM	NTAN C	A LEX	Same	No.	the second	Species	the second states	terreture.
atriài	La .	Cracked	Auto-MC =	OF	CF.	Anope	Adoremed	Diss ded	
10.92	Covia	Cashie .	44.401	ST .	OF.	Macale	Record	2 m. Al	
1010165	1 lines -	24.36.6	A.6. 682.25	1.00	1.00	Activity	Roborcourse I.	See 43	
2002/001	11.000	- C.016	210 million	100	10.00	24/00/02/01	5.00 COORT.	-isona	
(environ)	083	Protoso (A 10-102 1	or	(er :	Acces	A 20-7 549 5	C RUT SHITS	
487526	Carlon	270.040	AND ADD A	34	. de	Aberga	Adorapeed	Captied	
vii 107	Covit	Cashe	ALCHOLD	OF	00	Haras	Publication .	Dia.mit	
ALC: NO.	10.64	takt.	AAND	3.04	100	Academica	Adda Calcod	C.a.a.d	
official and	1.083	• 1, 10(1)		1 1 1	14 6	Zant ang tal	2.40 Garden	1.04000	
antein).	1.580	-10046	ALC: NO.	- 5	1.80	Altre ipm	N BOADDARD	ACTIME	
ent néris	Q253	Spaces	ALIO-HELL	Of .	OF .	Abega	Auto-speed	Clear pied	
88:10:12	Cont	Capito	和此中国人	Storight	040	Abeas	Advised	Club, dv J	
1210012	Orya	Easter	Auto MIZE	-37	- CF	Acces	- benerika	Six Al	
CALIFORNIA S	11000	1. A. M. M. M.	ALC: UNK DECK	1.94	0.000	All and the second	Sector of the	E14 (C)	
OT DET	1.060	+ 12,060	(9.45-H10.2		11 Admit	And pass	E MORANDE E	Excreme 1	
amongal.	0965	Dracks	A.R625	OF.	C.	AD-CAR	Part s-stars	Castored	
8311017	Covin	Chicket	Add Albert	Of	(COR)	ALC: CARE	Autospend	Classified	
\$2,16912	10064	Same.	Advertise	38	100	Aberta	Nakolaka -	Jacks	
+ 1/10/11	1200	- 10 A	A.6.68232		1. A.M. (fee said	Advertisely	14.44	
120001	i i she	-12000	0.000000		1.00	And the second	Nilo canon	42.963	
with minder	0353	Stored	ALC: HELL		0.	42424	A An-Apart	S 40 1945	
421002	Cont	Chaded	AV82448	28	CM.	Absga	Adoveced.	Checkled	

To view the following window, click **System > Port Configuration > Port Settings**, as shown below:

Figure 3-4 Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable the physical port here.
MDIX	 Select the Medium Dependent Interface Crossover (MDIX) option here. Options to choose from are: Auto - Select this option for auto-sensing of the optimal type of cabling. Normal - Select this option for normal cabling. If this option is selected, the port is in the MDIX mode and can be connected to a PC's NIC using a straight-through cable or a port (in the MDIX mode) on another switch through a crossover cable. Cross - Select this option for cross cabling. If this option is selected, the port is in the MDI mode and can be connected to a port (in the MDIX mode) on another switch through a crossover cable.
Auto Downgrade	Select this option to enable or disable automatically downgrading advertised speed in case a link cannot be established at the available speed.
Flow Control	Select to turn flow control On or Off here. 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.
Duplex	Select the duplex mode used here. Options to choose from are Auto , Half , and Full .
Speed	Select the port speed option here. This option will manually force the connection on the selected port to connect at the speed specified here. Options to choose from are Auto , 10M , 100M , 1000M , 1000M Master , 1000M Slave , and 10G . The Switch allows users to configure two types of gigabit connections; 1000M Master and 1000M Slave , which refer to connections running a 1000BASE-T cable for connection between the Switch port and another device capable of a gigabit connection. The master setting (1000M Master) 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 (1000M Slave) uses loop timing, where the timing comes from a data stream received from the master. If one connection must be set for 1000M Slave. Any other configuration will result in a link down status for both ports.
Capability Advertised	When the Speed is set to Auto , these capabilities are advertised during auto-negotiation.
Description	Tick the check box to enter a 64 characters description for the corresponding port here.

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

Port Status

This window is used to view the Switch's physical port status and settings.

To view the following window, click **System > Port Configuration > Port Status**, as shown below:

NUL .								
	1							
1 Settings.							10.	
100	en c	NAL CONTRACT	HAM	eren arte Artes	nutaonno anaice	INPES	steat	1995
diri (Kristi	Contracted	20-10-6-xx-80-01	(01	21	24450	Asp-1004	UNUDASC-T
1202	Condict	13-13-14-14-1-10		01	45	Sec. 1	AU > 1004	1000345547
01/90	Messences.	2010/04/02/05/02		01	1 21	144	Auto	10002351-1
0.5764	Mul Saturday al	30 m (1 %) (1 64 64	1. 11	0.1	6.0	140	24 M	10.433811
difference in	 Mel Calacterization 	SC THE REPORT OF A	(1)	116	353	244.4	5.87	13 04544 1
Witzing	Here plantariat	$-30 \gg 0.13140.40$		00	372	6.005	20 W	18 0434+ 1
- 10 CB	Here Concerned	SIDDERS STREET		07	61 .01	905	204	120405-0
ile più a	Hos Canadariad	20-545856640	-	01	Ć1	i on	A.M.	T-TEADING?
1109 C	No5-Connected	20-02-02-02-02-02		07	108	Age	Adde	thoughadd-t
catis/12	Hostin metal	20-1D-04-A1-09-04	-	01	101	443	Ack	10002ASS-T

Figure 3-5 Port Status Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.

Port GBIC

This window is used to view active GBIC information found on each applicable physical port of this Switch.

To view the following window, click **System > Port Configuration > Port GBIC**, as shown below:

Part GBIC		~
Peri CDIC		
av. 1 🗹		
Unit 1 Sytunyo		
Interface Type	100023257	
eth1702		
Intertase Type	10008-8.0697	
white:		
Tales lace Type	10003255611	
36104		
Interface Type	10003A56/T	
eh105		
Intertase Espe	$(0,0) \in \mathcal{A}((0,-))$	
orb106		
Infection and Theory	1000233261	
ald00		
Interface Type	18003A56/T	

Figure 3-6 Port GBIC Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.

Port Auto Negotiation

This window is used to view detailed port auto-negotiation information.

To view the following window, click **System > Port Configuration > Port Auto Negotiation**, as shown below:

CARLO MAD	1000							
1) 	Constraint and the					1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1		
CIE (onesaulta Po Aadal-z Basha	s Diverse Stelle v Diverse Diverse	ing CS. Carlle 544 No.s Tailt (Kiroliya	na da seria di katika Na NER Sanok i	realition of Capab Teal Paratral	en verense bez		
k i Setting	Filescence							
Hal	1	К.Я	166	124.	110-5	1341K	10-6	INH
sal'ini -	Dis(6.)	×1.5111	Constantial Sec.	DM Hole 1	202 (Ball a	1041043.5	0.000	
1002	12410.0		Unable	DIMENSI.	30.84	1.60 -00		
60.01	H-10.000		000000000000000000000000000000000000000	I DIN ROLL	00,84			
eanse -	Hoppena		icongaine-	Instance.	1942,040			
2.010	Riterand	1.1	Contemporter.	104_101	107_108			+3
entat -	Cristine	1.1	Configuration	104_001	109_0 at	1 E		+17
ent%7	Crabled	24	Calibraty	ingial .	W.B.M.		40	40
ED3rh	Callson .		Cabas	DIM HAL .	200 Dall			-
ditter 🗌	24.0.5		Califa	IN HELL	202.8.4			
11111	Provide St.		it is the set of the	Ind Act.	202.00			

Figure 3-7 Port Auto Negotiation Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.

Error Disable Settings

This window is used to configure the sending of SNMP notifications for error disable state.

To view the following window, click **System > Port Configuration > Error Disable Settings**, as shown below:

arbeit .	Sector 4	15					
Sec.	a system in	- 10 10					
attanena pitait							10.00
ran Disclore Decovery Ledings							
end mere Grade 🕅	9	39.9	C and ex	- 21	mana: 346-62	ini i	100
	Di Dinaki Caron	_	-		1kk	Internal Original	
	Port Overarbe				Dimenteri	X0	
	Sector (scherk)				LINE COMPANY	(im)	
	BPRI 5 -				(magles)	10 A	
	Dytar: AR.				Decolec	202	
	HOP STORES				(M21601	30) (
	LACENES B. I.				Double)	5.000	

Figure 3-8 Error Disable Settings Window

The fields that can be configured for Error Disable Trap Settings are described below:

Parameter	Description
Asserted	Select this option to enable or disable the notifications when entering into the error disabled state.
Cleared	Select this option to enable or disable the notifications when exiting from the error disabled state.
Notification Rate	Enter the number of traps per minute. The packets that exceed the rate will be dropped. The value is between 0 and 1000.

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

The fields that can be configured for **Error Disable Recovery Settings** are described below:

Parameter	Description
ErrDisable Cause	Select the error disable causes here. Options to choose from are All, Port Security, Storm Control, BPDU Attack Protection, Dynamic ARP Inspection, DHCP Snooping, and Loopback Detect.
State	Select this option to enable or disable the auto-recovery for an error port caused by the specified cause.
Interval	Enter the time between 5 and 86400 seconds to recover the port.

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

Jumbo Frame

This window is used to view and configure the Jumbo Frame size and settings. The Switch supports jumbo frames. Jumbo frames are Ethernet frames with more than 1518 bytes of payload. The Switch supports jumbo frames with a maximum frame size of up to 9216 bytes.

es.	From Fort	To Part	Untraine Receive	Fore Sec (44.11)	
i 💽	00522	obtion in	1520	a) an	400
nii 1 Setilopt				M	
	(that)		14.0	nana Karata Kana Zantigini	
	(4.6%)			7828 1944	
	18.000			Tea.	
	APA NO.			25-di	
	1675 B.1			1534	
at:125				3021	
	1.525			1828	3
	0.036			2958	
	dening a			26.98	
	ANO ARE			15.4	
- 110; Se				1636	
	40.0011			102	
	APOR -			15.4	
	cated).			19-a	
	entrette.			rt.st	
	49:005			1526	

To view the following window, click **System > Port Configuration > Jumbo Frame**, as shown below:

Figure 3-9 Jumbo Frame Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Maximum Receive Frame Size	Enter the maximum receive frame size value here. This value must be between 64 and 9216 bytes. By default, this value is 1536 bytes.

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

Interface Description

This window is used to display the status, administrative status, and description of each port on the Switch.

To view the following window, click System > Interface Description, as shown below:

 			
hinkse	Shite	Administrative	Cenatake
49106	13 14	eraped.	
a@1002	ų.	e'adec	
48500	Kelva .	endet	
10.004	Vesa	6.8.364	H I
<1108	 Altrian 	0.8.39.10	
citizes	(Jenni	(c) a link w	
002204	(1994)	012/3010	
Attraction ((inci	entare	
ett 100	6753 6753	encore	
conterto.	50% B	a ju Det	1

Figure 3-10 Interface Description Window

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

PoE (PoE Switches Only)

The **DGS-1510-28P**, **DGS-1510-28XMP**, and **DGS-1510-52XMP** switches support Power over Ethernet (PoE) as defined by the IEEE 802.3af and 802.3at.



NOTE: The Power over Ethernet (PoE) settings are only available on the DGS-1510-28P, DGS-1510-28XMP, and DGS-1510-52XMP.

All ports can support PoE up to 30W. Ports 1-24 can supply about 48 VDC power to Powered Devices (PDs) over Category 5 or Category 3 UTP Ethernet cables. The Switch follows the standard PSE (Power Sourcing Equipment) pin-out *Alternative A*, whereby power is sent out over pins 1, 2, 3 and 6. The Switches work with all D-Link 802.3af capable devices.

The Switch includes the following PoE features:

- Auto-discovery recognizes the connection of a PD and automatically sends power to it.
- The Auto-disable feature occur under two conditions: firstly, if the total power consumption exceeds the system power limit; and secondly, if the per port power consumption exceeds the per port power limit.
- Active circuit protection automatically disables the port if there is a short. Other ports will remain active.

Class	Maximum power used by the PD	Maximum power supplied by the Switch
0	12.95 Watts	15.4 Watts
1	3.84 Watts	4 Watts
2	6.49 Watts	7 Watts
3	12.95 Watts	15.4 Watts
4	25.5 Watts	30 Watts

Based on IEEE 802.3af/at, power is received and supplied according to the following classifications:

PoE System

This window is used to configure the PoE system, and display the detailed power information and PoE chip parameters for PoE modules.

To view the following window, click **System > PoE > PoE System**, as shown below:

4. C	We we Third	40.25	Addressed 1	The S.A.		
- F	1 6	1%	[figurates [V]]	Di Ladra 🗵		1.1.1.1.1.1.1
						0.00000
11 D	eliano 1004	Page Ha	1100 ·	Design the shall be	15 da y 15 annual	Sorg William

Figure 3-11 PoE System Window

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Usage Threshold	Enter the usage threshold to generate a log and send the corresponding standard notification. The range is from 1 to 99 percent.
Policy Preempt	Select to enable or disable the policy preempt function. When this function is Enabled , under the power shortage condition, power provisioned to PDs with lower priority will instead be provisioned to PDs with higher priority. When this function is Disabled , the power management mode will use the first in, first serviced method.
Trap State	Select this option to enable or disable the sending of PoE notifications.

The fields that can be configured are described below:

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

Click the **Show Detail** button to see the PoE system Parameters table at the bottom of the window.

After clicking the **Show Detail** button, the following table will appear.

- Pole system Parameters -			
U K	Mas. Party	Device (D	SWilliam
1	24	E(1)	47
1			

Figure 3-12 PoE System (Show Detail) Window

PoE Status

This window is used to configure the description, and display the PoE status of each port.

One of the following PoE port states will be displayed in the table:

- Disabled
- Searching (remote PD is not connected)
- **Requesting** (remote PD is inserted but no power is provided yet)
- **Delivering** (remote PD is inserted and power is provided)
- **Faulty** (maintain power signature absent, PD short, overloading, power denied, thermal shutdown, startup failure, or classification failure)

To view the following window, click **System > PoE > PoE Status**, as shown below:

w 0.000 w		Devo m.	34			
The second secon	-1901	27.80				46.97
on the second		Arrest a				
Pat	N.A.S	Case	Max.040	2.8x4 (W)	Casilite	
df.(1.1.*)	Also (Int.)	8 V.		005		Fair of Description
Service ?	ondrining	6.96	111	114		Park of Description
April 1	Searching	1646	1.1	0.0		District Description
egrade -	Geendary	8.96	41	6.6		Melene Medociation
49433	Searching	8.%	4.8	68		palete presidente y
e. (2.8	Seculary	8.%	13	02		Delete Case foting
3.077	State in a	8.9,	(12)	0.0		Deters Denerotien
4.014	Section (ж¥,	1.1	10		Dones Description

Figure 3-13 PoE Status Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Description	Enter the text that describes the PD connected to a PoE interface. The maximum length is 32 characters.

Click the **Delete Description** button to clear the setting in the corresponding Description field.

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

PoE Configuration

This window is used to configure the PoE port.

To view the following window, click **System > PoE > PoE Configuration**, as shown below:

Solligen Lien					
a lettere					
ninited .	(6)1	- I Contraction of the local division of the local division of the local division of the local division of the		(1.500) (1.60)	6
- Lonerce	- <u>10400000</u>		Add To		Accily.
a second					
.906	Advise.	E PERMIT	Lagacy Lapport	I I I I I I I I I I I I I I I I I I I	
16.1.26	1.4C	La	District		Union or Corp.
W11,055	0.00	1.3%	Dire sets		Table 7 Acres 100
10.11.12	1.61	1.85	TRACE I		Unless Tree See
4 1 14		Lin	FL + 4-1		Cribbon in Corpo
#1122	5.8	Los	Dire ded		The Transform
arrs. 10.	+,62	tok.	Long ter to		The second second
#(1,1)		E.is.	10 - + T		Lokes we were
:1-100	- A.	1,05	Dist. A. J.		United a set daily
#3636	- 44K	Las.	Dissied.		134 (CT+) 540
1011021	1.00	1.55	10123013		Chicken Tree Search
1010-1	7.6.62	E isi	Direction of		Junka ve den

Figure 3-14 PoE Configuration Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Priority	Select the priority for provisioning power to the port. Options to choose from are Critical , High and Low .
Legacy Support	Select this option to enable or disable the support of legacy PD.
Mode	Select the power management mode for the PoE ports. Options to choose from are Auto and Never .
Max Wattage	When selecting Auto in the Mode drop-down list, this option appears. Tick the check box and enter the maximum wattage of power that can be provisioned to the auto-detected PD. If the value is not entered, the class of the PD automatically determines the maximum wattage, which can be provisioned. The valid range for maximum wattage is between 1000 mW and 30000 mW.
Time Range	When selecting Auto in the Mode drop-down list, this option appears. Tick the check box and enter the name of the time range to determine the activation period.

Click the **Delete Time Range** button to clear the setting in the corresponding Time Range field. Click the **Apply** button to accept the changes made.

PD Alive

This window is used to configure the PD Alive function for PDs connected to the PoE ports. The ping function is used to check if PDs, connected to the PoE ports, are active or not. When PDs appear to be inactive, the specified action (Reset, Notify, or Both) will be taken.

To view the following window	click System > PoE > PD Alive	as shown below:
TO VIEW LITE IONOWING WINDOW,	CIICK System - FOE - FD Allve	, as shown below.

or A 1945 I Aliee Configuration Ind –	ke Verson ja Kat	FILM A NEX - P	ar sao's			
and the second se		Division o	and the second			
Pro a linde com grad-una			ang Sara papang 👘 Ara	See Section 1.		
2	06. S		ors Da	n 🕑		- Reply
nik i Sattinga			15			
din .	PERSONA MARK	192 B ¹ Markets	. Induktion	Boby Canad	Modey fam	de Join 1
Maria 1	Examine	1111		1.	80	990
Series 7	Grades	6613	4	3.	80	3:45
dai%2	E realed	1119	24	1. A.	90.	Sah
eta1359	Created	1229	2	z	20	3 3 1)
22.035	Contest	0.000	3	1	30	3.41
6.638	C version in	100.00	28	I.	50	3.41
840°02	0.0000	1111	3 3	2	30	3.001
6.199.20	0.40	11.53			¥.	
1000	117-224-14	1.010	(a)	60	10	26303
-man-	117-030	1000	14	11 - W	#1	Sec.

Figure 3-15 PD Alive Window

The fields that can be configured are described below:

Parameter	Description			
Unit	Select the switch unit that will be used for this configuration here.			
From Port / To Port	Select the appropriate port range used for the configuration here.			
PD Alive State	Select to enable or disable the PD Alive function on the specified port(s).			
PD IP Address	Enter the IP address of the PD here.			
Poll Interval	Enter the poll interval here. This is the interval between ping messages from the system to PDs connected to the PoE port(s). The range is from 10 to 300 seconds.			
Retry Count	Enter the retry count here. This is the amount of ping messages that will be sent (at each interval) when PDs are not responding. The range is from 0 to 5.			
Waiting Time	Enter the waiting time here. This is how long the system will wait before sending ping messages to the PD connected to the PoE po after a 'Reset' action was taken. The range is from 30 to 300 seconds.			
Action	 Select the action that will be taken here. Options to choose from are: Reset - Specifies to reset the PoE port state (turn PoE off and on). Notify - Specifies to send logs and traps to notify the administrator. Both - Specifies to send logs and traps to notify the administrator and to reset the PoE port state (turn PoE off and on). 			

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

PoE Statistics

This window is used to display the PoE statistics.

To view the following window, click **System > PoE > PoE Statistics**, as shown below:

T.						
- 1570 -	N					
Southego .						
						dear a l
Pat .	NF5Abasi.	Dredout	368 K	Power Overent	Binalid Statestary	Street and
10110	- (j)	A		1	184 F	1 25-
10112.9	6		31	4	1980	1 13 w
MY12.3	0	9	- Y	<i>k</i> .	41	1 344
65123	14 - C	8.: 20	. 2	4	15	. Jea
did2.5	<u> (</u>		- 3	1 k	. 35	Qia-
8513.7	()	00	10	0	15	Oct 1
361777	(h)	(1)	ġ.	3		0ar
00000	(j)	1	í í	1	(H)	- 3w
wara i	36	4	1	20	5 m /	1.25
18.2.318	16		- 11	4	100	1 1 2 2

Figure 3-16 PoE Statistics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.

The fields that are displayed in the table are described below:

Parameter	Description	
MPS Absent	This field is incremented when the PD's Maintain Power Signature (MPS) is absent.	
Overload	This field is incremented when the power demand exceeds the maximum output power supplied.	
Short	This field is incremented when the internal circuit of the PD shorted out.	
Power Denied	This field is incremented when power was denied to the PD by the system.	
Invalid Signature	This field is incremented when an invalid PD signature was detected by the system.	

Click the Clear All button to clear PoE statistics for all ports.

Click the **Clear** button to clear the PoE statistics for the corresponding port.

PoE Measurement

This window is used to display the PoE measurement.

To view the following window, click **System > PoE > PoE Measurement**, as shown below:

Sinaka meneriti katak					
I M	6				
S - 194					
rising)					
POR	weinige (n)	tanna pag	tangente o go	theorem (MI)	
- eff. (24)	12%	68	16.%	36.4	
58 992	636	N.W.	8%	.404	
48.505	505	K.V.	62	360	
4.8 1/284	676	15.9.	H.v.	56.0	
(41)(4)	8.9.	82.	H.a.	MAY	
2012/01	r.y.	NW.	H.=	8.4	
0.08503	646	12.W.	6.×.	36.0	
48:500	6.%	104.	HON.	16.4	
48.199	6/8	h.w.	WA.	.HA	
##10215	636	1.5	RA.	36.0	
#A0070	NN	10%	H ^M .	36.3	
11/18/212	6.9.	17.	16.4	2401	

Figure 3-17 PoE Measurement Window

The fields that can be configured are described below:

Parameter	Description	
Unit	Select the switch unit that will be used for this configuration here.	
PoE LLDP Classification

This window is used to display the PoE LLDP Classification.

To view the following window, click **System > PoE > PoE LLDP Classification**, as shown below:

Pat LLDP Classification	P
2 PRETTINE COMPLEXION TARM	
	ł
Parked ACMI PPP 12 Discovery	
Note	
ninn diw ban 70	
Bion?	
Fartehild 2	
ANA DI Martanan	
Kone Internation from PC	
NUMBER OF THE OWNER	
Falshi 35	
PRE Discharten	
binan .	
nternalize ben 170	
Hone	
Parket MDA	
ever 12 and maximum	
Bine -	
htmale han 70	
- Hone	

Figure 3-18 PoE LLDP Classification Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.

System Log

System Log Settings

This window is used to view and configure the system's log settings.

To view the following window, click **System > System Log > System Log Settings**, as shown below:

System Log Settings		
DALLAR STATE		
Grants & Avriace State	Plottet V	
Tax	(1 A) V (0 (1-0))	- a.dy.
Harbert og Samlega		
Dullin Log Child	Traded	
Send.	(Warninge) v	
Division and the set	15 dias	
Willy Duby (D-85535)	200 six. The diale	1.9%
Conto a Log Service		
CARCESSE	utatisi v	
Secto	4Varent/ x	
Ovolatinik: New	15 d w	A 3D AV
Not sort og Arinings		
Heatin Lie State	[Bastled [v]]	
ann.	4(Auraja) [V]	
Donak Sas	BURN	×204

Figure 3-19 System Log Settings Window

The fields that can be configured for **Global State** are described below:

Parameter	Description
Source Interface State	Select this option to enable or disable the source interface's global state.
Туре	Select the type of interface that will be used. Option to choose from is VLAN .
VID	Enter the VLAN ID used here. The value is between 1 and 4094.

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

The fields that can be configured for **Buffer Log Settings** are described below:

Parameter	Description
Buffer Log State	Select whether the enable or disable the buffer log's global state here. Options to choose from are Enable , Disabled , and Default . When selecting the Default option, the buffer log's global state will follow the default behavior.
Severity	Select the severity value of the type of information that will be logged. Options to choose from are 0 (Emergencies), 1 (Alerts), 2 (Critical), 3 (Errors), 4 (Warnings), 5 (Notifications), 6 (Informational), and 7 (Debugging).
Discriminator Name	Enter the discriminator name used here. This name can be up to 15 characters long.

Parameter	Description
	Enter the interval for periodic writing of the logging buffer to FLASH. This value must be between 0 and 65535 seconds. By default, this value is 300 seconds. Tick the Infinite option, to disable the write delay feature.

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

The fields that can be configured for **Console Log Settings** are described below:

Parameter	Description
Console Log State	Select to globally enable or disable the state of the console log here.
Severity	Select the severity value of the type of information that will be logged. Options to choose from are 0 (Emergencies), 1 (Alerts), 2 (Critical), 3 (Errors), 4 (Warnings), 5 (Notifications), 6 (Informational), and 7 (Debugging).
Discriminator Name	Enter the discriminator name used here. This name can be up to 15 characters long.

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

The fields that can be configured for **Monitor Log Settings** are described below:

Parameter	Description
Monitor Log State	Select to globally enable or disable the state of the monitor log here.
Severity	Select the severity value of the type of information that will be logged. Options to choose from are 0 (Emergencies), 1 (Alerts), 2 (Critical), 3 (Errors), 4 (Warnings), 5 (Notifications), 6 (Informational), and 7 (Debugging).
Discriminator Name	Enter the discriminator name used here. This name can be up to 15 characters long.

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

System Log Discriminator Settings

This window is used to view and configure the system log's discriminator settings.

To view the following window, click **System > System Log > System Log Discriminator Settings**, as shown below:

Action Urgan P Seventy: Urgan	Severity Standarder Profit Unit Unit Unit	Seedy. Base STACKED POINT POINT State at Point Point Point Point Point Point Point	Device	☐058 ☐05935 ☐06935 ☐06935]0-02 _]0+02 _]W05	n n m Dimor	Tens Tans	E suster al	
Servedto - Brope	Savefit, Dispa 🔽 Standyschni Walth (206.55) (200.56) Affred Savefit (206.55) (200.56) Affred Savefit (200.56) (200.56) 	Severito 🛛 🖓 🖂 🔽		. nee	jaanoowen .	lekterik NAVC	liptee Tiktikve-m tigrou_rec.	L STORALOT. L 1998 H Mail H 400	
	Deal Dealers II	_addressdischoolsdischooldischool		e i		204.01	(Vab)	XCe expected	innt,

Figure 3-20 System Log Discriminator Settings Window

The fields that can be configured are described below:

Parameter	Description
Discriminator Name	Enter the discriminator name here. This name can be up to 15 characters long.
Action	Select the facility's behavior option and the type of facility that will be associated with the selected behavior here. Behavior options to choose from are Drops and Includes .
Severity	Select the severity behavior option and the value of the type of information that will be logged. Behavior options to choose from are Drops and Includes . Severity value options to choose from are 0 (Emergencies), 1 (Alerts), 2 (Critical), 3 (Errors), 4 (Warnings), 5 (Notifications), 6 (Informational), and 7 (Debugging).

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

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

System Log Server Settings

This window is used to view and configure system log's server settings.

To view the following window, click **System > System Log > System Log Server Settings**, as shown below:

ent est atoms	1	Oranievi Adore	10271		
C-Pol DEX 5921	54	39. m. #r.	4(Warmen)	-	
¥-9	25	to sugar sector provide	U trux.		-
					i na ka
ALCONTRACT.					



The fields that can be configured are described below:

Parameter	Description
Host IPv4 Address	Enter the system log server's IPv4 address here.
Host IPv6 Address	Enter the system log server's IPv6 address here.
UDP Port	Enter the system log server's UDP port number here. This value must be 514 or between 1024 and 65535. By default, this value is 514.
Severity	Select the severity value of the type of information that will be logged. Options to choose from are 0 (Emergencies), 1 (Alerts), 2 (Critical), 3 (Errors), 4 (Warnings), 5 (Notifications), 6 (Informational), and 7 (Debugging).
Facility	Select the facility value here. Options to choose from are 0 to 23.
Discriminator Name	Enter the discriminator name here. This name can be up to 15 characters long.

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

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

System Log

This window is used to view and clear the system log.

To view the following window, click System > System Log > System Log, as shown below:

01.06			
			Constant in the second s
a production of the			
i Costile 2		*****	Potentia Sector Sector Inc.
i Cettles 2 1715 M	Tin+	1761	log Destription
		that is a second se	ing Description Station in station

Figure 3-22 System Log Window

Click the **Clear Log** button to clear the system log entries displayed in the table.

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

System Attack Log

This window is used to view and clear the system attack log.

To view the following window, click System > System Log > System Attack Log, as shown below:

System Altack Log				
1158 <u>1</u> 🗸				Clean Attack Lag
Fotal Balaxies 0				
index.	Time	Level	Log Cesotytion	

Figure 3-23 System Attack Log Window

The fields that can be configured are described below:

Parameter	Description	
Unit	Select the switch unit that will be used for this configuration here.	

Click the **Clear Attack Log** button to clear the system attack log entries displayed in the table.

Time and SNTP

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 in each participant.

Clock Settings

This window is used to configure the time settings for the Switch.

To view the following window, click System > Time and SNTP > Clock Settings, as shown below:

Clock Settings		
- Report Setting 5		
Time (1113HPL95)	005454	
Date (DD / HM (11111))	01/01/2000	
		Ande



The fields that can be configured are described below:

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

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

Time Zone Settings

This window is used to configure time zones and Daylight Savings Time settings for SNTP.

To view the following window, click **System > Time and SNTP > Time Zone Settings**, as shown below:

I me dana Settinga		
Sec. 2. 1. 1. 10. 10.	Leased 3	
ters men	••• • • • •	
Recordina Selána		
From Week of the Michin	1	
Dom Die of Ballfaile	Gas:	
From Health	284	
From the possible	(K)+ ((-)	
To meet of the Vorth	1	
To Direct Av Your	Sat:	
In Vall.	248 C	
In one we was	[14] + [[13 -]	
0.8.4	(B)	
Our Selen		
From the transmission	- (c)	
From Henry	Les -	
Figure 1990	1	
Committee 1110460	(riv n -	
fo Bale Le Valle	01 **	
u vow	200	
To Year		
To Time (0) MVI	M T D + F	
ICRON.		[]

Figure 3-25 Time Zone Settings Window

The fields that can be configured are described below:

Parameter	Description
Summer Time State	 Select the summer time setting. Options to choose from are: Disabled - Select to disable the summer time setting. Recurring Setting - Select to configure the summer time that should start and end on the specified weekday of the specified month. Date Setting - Select to configure the summer time that should start and end on the specified date of the specified month.
Time Zone	Select to specify the offset of the local time zone from the Coordinated Universal Time (UTC).

The fields that can be configured for **Recurring Setting** are described below:

Parameter	Description
From: Week of the Month	Select week of the month that summer time will start.

DGS-1510 Series Gigabit Ethernet SmartPro Switch Web UI Reference Guide

Parameter	Description	
From: Day of the Week	Select the day of the week that summer time will start.	
From: Month	Select the month that summer time will start.	
From: Time (HH:MM)	Select the time of the day that summer time will start.	
To: Week of the Month	Select week of the month that summer time will end.	
To: Day of the Week	Select the day of the week that summer time will end.	
To: Month	Select the month that summer time will end.	
To: Time (HH:MM)	Select the time of the day that summer time will end.	
Offset	Enter the number of minutes to add during summer time. The default value is 60. The range of this offset is 30, 60, 90 and 120.	

The fields that can be configured for **Date Setting** are described below:

Parameter	Description	
From: Date of the Month	Select date of the month that summer time will start.	
From: Month	Select the month that summer time will start.	
From: Year	Enter the year that the summer time will start.	
From: Time (HH:MM)	Select the time of the day that summer time will start.	
To: Date of the Month	Select date of the month that summer time will end.	
To: Month	Select the month that summer time will end.	
To: Year	Enter the year that the summer time will end.	
To: Time (HH:MM)	Select the time of the day that summer time will end.	
Offset	Enter the number of minutes to add during summer time. The default value is 60. The range of this offset is 30, 60, 90 and 120.	

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

SNTP Settings

This window is used to configure the time settings for the Switch.

To view the following window, click System > Time and SNTP > SNTP Settings, as shown below:

N D' Settings				
HTP Clobel dekleps				
Current Three Sources	Dyniam Clópe			
XNUE OTS	Linstein V			
Ph 6 A 940 (2018) 201	22 NR			. Apohy
SMTP Server Setting				
Antext Same	St	(1) Petrovinies	init:	
	01 23			(84)
Late Ferrie 1				
SHITSawa	Water	Londkame	1	
(1.90 80.)			Deb	ti l

Figure 3-26 SNTP Settings Window

The fields that can be configured for **SNTP Global Settings** are described below:

Parameter	Description	
SNTP State	Select this option to enable or disable SNTP.	
Poll Interval	Enter the synchronizing interval in seconds. The value is from 30 to 99999 seconds. The default interval is 720 seconds.	

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

The fields that can be configured for SNTP Server Setting are described below:

Parameter	Description
IPv4 Address	Enter the IP address of the SNTP server, which provides the clock synchronization.
IPv6 Address	Enter the IPv6 address of the SNTP server, which provides the clock synchronization.

Click the Add button to add the SNTP server.

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

Time Range

This window is used to view and configure the time range settings.

To view the following window, click **System > Time Range**, as shown below:

n Koly.	and the second second					
here the s	22 ymm Sein	-1046 N	IC MARK	5 n	M L same are	
ione Time (HEMA)	0 9 0		To Tera Sililades	0 9 0	<u>N</u>	
	proven.					$ -\infty $
ortal Frankes t						
Case How	Skal Weeks	Skilling	BalWateka	End Tonic	100 (Da	-
Week da ya	¥isa -	.08.30	74	23.55	Territy Press In	2 Print Pr

Figure 3-27 Time Range Window

Parameter	Description
Range Name	Enter the name of the time range. This name can be up to 32 characters long.
From Week / To Week	Select the starting and ending days of the week that will be used for this time range. Tick the Daily option to use this time range for every day of the week. Tick the End Week Day option to use this time range from the starting day of the week until the end of the week, which is Sunday.
From Time / To Time	Select the starting and ending time of the day that will be used for this time range. The first drop-down menu selects the hour and the second drop-down menu selects the minute.

The fields that can be configured are described below:

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 **Delete Periodic** button to delete the periodic entry.

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

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

4. Management

User Account Settings
Password Encryption
Login Method
SNMP
RMON
Telnet/Web
Session Timeout
DHCP
DNS
NTP
IP Source Interface
File System
Physical Stacking
Virtual Stacking (SIM)
D-Link Discovery Protocol

User Account Settings

This window is used to create and configure the user accounts. The active user account sessions can be viewed.

There are several configuration options available in the Web User Interface (Web UI). The set of configuration options available to the user depends on the account's **Privilege Level**. A user account created with a higher privilege level will be given access to configure more features than a user account created with a lower privilege level.

The pre-defined privilege levels for user accounts are:

- **Basic User (Privilege Level 1)** This user account level has the lowest priority of the user accounts. The purpose of this type of user account level is for basic system checking.
- **Operator (Privilege Level 12)** This user account level is used to grant system configuration rights for users who need to change or monitor system configuration, except for security related information such as user accounts and SNMP account settings.
- Administrator (Privilege Level 15) This administrator user account level can monitor all system information and change any of the system configuration settings expressed in this guide.

To view the following window, click **Management > User Account Settings**, as shown below:

User Management Settings	Seauker. To bie		
CRAD COLLEGE	Hereing (CDA)		
second Tras . More	Carves		Ann
orbhs t			
liser Mann	l'haing -	- Deposite I	
1000	15	3014	in the second

Figure 4-1 User Management Settings Window

The fields that can be configured are described below:

Parameter	Description
User Name	Enter the user account name here. This name can be up to 32 characters long.

Parameter	Description
Privilege	Enter the privilege level for this account here. This value must be between 1 and 15.
Password Type	Select the password type for this user account here. Options to choose from are None , Plain Text , Encrypted-SHA1 , and Encrypted-MD5 . When selecting Encrypted-SHA1 or Encrypted-MD5 , the password will not be encrypted from the plain-text format to the encrypted format. Instead, the encrypted password must be entered. To encrypt the password from the plain-text format to the encrypted format, refer to the Password Encryption window.
Password	After selecting Plain Text , Encrypted-SHA1 , or Encrypted-MD5 as the Password Type , enter the password for this user account here.

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

Click the **Delete** button to remove the specified user account entry.

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

si Naspines	Settings	Seastor Table			
HUSK	18				
1910	Chief Holes	Deve de ign	Lines (mail	U. Little in the second s	
Longato -	0.000000000	1/	0.0 515		ter deletera
25.11	All	17	Luca .	1000000	Lát:

After clicking the **Session Table** tab, the following page will appear.

Figure 4-2 Session Table Window

A list of active user account session will be displayed.

Click the Edit button to access and configure the User Privilege settings.

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

After selecting the **Edit** button, the following page will appear.

ACENHAL CODUCTO	
15 1	
az ebens	opply und

Figure 4-3 User Privilege Window

The fields that can be configured are described below:

Parameter	Description	
Action	Select to enable or disable user level security.	
Privilege	Select the privilege level here. The range is from 1 to 15.	
Password	Enter the password here. This can be up to 32 characters long.	

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

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

Password Encryption

This window is used to configure whether to save the encryption of the password in the configuration file.

To view the following window, click **Management > Password Encryption**, as shown below:

Password Encryption		
Personal Disputer Settings		
Passevora Encryption State	() Franke og filmened	
NONIMARY IN M	Distance Station	6 m. 6.

Figure 4-4 Password Encryption Window

The fields that can be configured are described below:

Parameter	Description
Password Encryption State	Select this option to enable or disable the encryption of the password before stored in the configuration file.
Password Type	After the Password Encryption State is Enabled , this filed will be available. Options to choose from are Encrypted-SHA1 and Encrypted-MD5 .

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

Login Method

This window is used to configure the login method for each management interface that this Switch supports.

To view the following window, click **Management > Login Method**, as shown below:

and 15 V	Puttient Type Pain Tett		
pa wasat		All and a second se	
Applester		Local Holins	
Corece		Login Local	F B
Tvivi		Logisticat	1.4
155-		Lopitord	1.31
pa Pavezora			
colonitor Correals with	Passon for Phila Teat	Torevoid	
ectation Controls w	Pasyot Nex Pin Tra	Normal Annual Income	- 34

Figure 4-5 Login Method Window

The fields that can be configured for **Enable Password** settings are described below:

Parameter	Description
Level	Select the password level here. This value must be between 1 and 15.
Password Type	Select the password type here. Options to choose from are Plain Text , Encrypted-SHA1 , and Encrypted-MD5 . When selecting Encrypted-SHA1 or Encrypted-MD5 , the password will not be encrypted from the plain-text format to the encrypted format. Instead, the encrypted password must be entered. To encrypt the password from the plain-text format to the encrypted format, refer to the Password Encryption window.
Password	After selecting Plain Text , Encrypted-SHA1 , or Encrypted-MD5 as the Password Type , enter the password for this user account here.

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

The **Login Method** section will only be available when Authentication, Authorization, and Accounting (AAA) feature is disabled. The fields that can be configured for **Login Method** settings are described below:

Parameter	Description
Login Method	After clicking the Edit button, this parameter can be configured. Select the login method for the specified application here. Options to choose from are No Login , Login , and Login Local . No Login , as the name implies, requires no login authentication to access the specified application. Login will require the user to enter a password when trying to access the application specified. Login Local requires the user to enter a username and a password to access the specified application.

Click the **Edit** button to modify the corresponding login method.

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

The fields that can be configured for Login Password settings are described below:

Parameter	Description		
Application	Select the application that will be configured here. Options to choose from are Console , Telnet and SSH .		
Password Type	Select the password encryption type that will be used here. Options to choose from are Plain Text , Encrypted-SHA1 , and Encrypted-MD5 .		
Password	Enter the password for the selected application here. This password will be used when the Login Method for the specified application is set as Login .		

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

Click the **Delete** button to remove the password from the specified application.

SNMP

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 SNMPv1 and SNMPv2c, 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 SNMPv1 and SNMPv2c 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.

<u>Traps</u>

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 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

This window is used to configure the SNMP global settings and trap settings.

To view the following window, click **Management > SNMP > SNMP Global Settings**, as shown below:

SNMP Global Settings	
SHMP Globall Svidnige	
SHINIP Girkeri Stale	C Ender To Dubled
SIMP Response Transist Request	C Ender
SHMP UDP Fort (1-05005)	181
Trap Source Interface	Kat. Spedified
Hole: It somet into tase is not specified. The cores	s. If a deflue to address will be climate as the particity scales. If address,
Trap Settings	
Unp Metal District	 Evaluation of Distances
SMMP Authentication Trep	
E Fart Link Up	
E FailLieb.Down	
E constant	
E wantwar	4.oolv

Figure 4-6 SNMP Global Settings Window

Parameter	Description		
SNMP Global State	Select this option to enable or disable the SNMP feature.		
SNMP Response Broadcast Request	Select this option to enable or disable the server to response to broadcast SNMP GetRequest packets.		
SNMP UDP Port	Enter the SNMP UDP port number. The range is from 1 to 65535.		
Trap Source Interface	Enter the interface whose IP address will be used as the source address for sending the SNMP trap packet.		

The fields that can be configured for **SNMP Global Settings** are described below:

The fields that can be configured for Trap Settings are described below:

Parameter	Description
Trap Global State	Select this option to enable or disable the sending of all or specific SNMP notifications.
SNMP Authentication Trap	Tick this option to control the sending of SNMP authentication failure notifications. An authenticationFailuretrap is generated when the device receives an SNMP message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2c, authentication failure occurs if packets are formed with an incorrect community string. For SNMPv3, authentication failure occurs if packets are formed with an incorrect SHA/MD5 authentication key.

Parameter	Description
Port Link Up	Tick this option to control the sending of port link up notifications. A linkup trap is generated when the device recognizes that one of the communication links has come up.
Port Link Down	Tick this option to control the sending of port link down notifications. A linkDown trap is generated when the device recognizes a failure in one of the communication links.
Coldstart	Tick this option to control the sending of SNMP coldStart notifications.
Warmstart	Tick this option to control the sending of SNMP warmStart notifications.

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

SNMP Linkchange Trap Settings

This window is used to configure the SNMP Linkchange trap settings.

To view the following window, click **Management > SNMP > SNMP Linkchange Trap Settings**, as shown below:

eit :	Fran Eve	To Part	True Sealary	Top Some		
	- Marcan	0.102	Unabled T	Distance -		ishi
	Fan		Trua Serving		Trop Sawa	
	arata/1		- Vare		-10.000	
	em 02	1	Euper		Endplied	
	sta110/2 .		Cradet.		Indet	
	#A1834		18.947		Cashd.	
	= x13/5		23.00.0		= a d d	
	101119-0		e Care			
	Carning 22		6 U.SAC		in so series	
	101.02		Crucier:		Charles	
	10.157		Creative		Cashd	
	2.675 0		E n.M.T		Card.d.	
	4 (1257) 1		+ 6.00 P		- u de 1	
	Modeland:		- 1/ B/AL		-22.06/0	
	Series .		C SA SAC		Shares -	
	sin(27)4		Trailer -		Carlled.	
	d (17215)		C N SVE		2 million	



The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Trap Sending	Select this option to enable or disable the sending of the SNMP notification traps that is generated by the system.
Trap State	Select this option to enable or disable the SNMP link change trap.

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

SNMP View Table Settings

This window is used to 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.

To view the following window, click **Management > SNMP > SNMP View Table Settings**, as shown below:

HIRT & WA WITTIGH				
Vera sole	TO DE A	- 2		
Samana di ka	AND HOLES			
Vev Inc	Included			
Print and A state	Constantial B	auff		- Set
Fotal Entitles 4	20-0			
Veri		Sabter CID	Man Dype	
3.571	60	1.2.4 (2.2.5)	- m salad	
	(9)	47442 111	0.007	Delsta
1003		3265523221	Brazenia	Tel de
19475 (APR)	C1941 -	1.9 (199) 199 199 1		
		120533420	91.4085	Sec. 4
evers Fact				the second se
evers Fact	ced cal	120533(12)	stiges.	Tel de
ours sant sant	cut cut cuthur	110533412)	nciated nciated	teratur. Secolar

Figure 4-8 SNMP View Table Settings Window

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 the view type here. Options to choose from are: Included - Select to include this object in the list of objects that an SNMP manager can access. Excluded - Select to exclude this object from the list of objects that an SNMP manager can access.

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

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

SNMP Community Table Settings

This window is used to 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.

To view the following window, click **Management > SNMP > SNMP Community Table Settings**, as shown below:

Construction of the second					
XI TAUE	Fisin Text	-			
on municipi name	po viniti da				
ev Name	Storage	15			
and Regim	Found Only	-			
Amobilities	N char				
12010-200300000	536460r				- A.M.
dal Fallers S					
Contraction in Contraction of the		No. Alarah	An less logiti	Planess test Repair	
fine second.		the second s			 Events I content on The
23.48		Community Service	19. 19.		Teldy

Figure 4-9 SNMP Community Table Settings Window

The fields that can be configured are described below:

Parameter	Description
Кеу Туре	Select the key type for the SNMP community. Options to choose from are Plain Text , and Encrypted .
Community Name	Enter 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	Enter 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	 Select the access right here. Options to choose from are: Read Only - SNMP community members using the community string created can only read the contents of the MIBs on the Switch. Read Write - SNMP community members using the community string created can read from, and write to the contents of the MIBs on the Switch.
IP Access-List Name	Enter the name of the standard access list to control the user to use this community string to access to the SNMP agent.

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

Click the **Delete** button to remove the specified 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.

To view the following window, click **Management > SNMP > SNMP Group Table Settings**, as shown below:

HINP Group Sec	1,0							
Destances (2000)		- 1.0 eV	evision -	e part	Ĩ.			
		Weight an Armer		C rime -				
area ana ana		The Automation	$dm = \overline{M}$	Same y	N 1011	e dav	1	
P.A. Barris L.A.S.	and a second	22.800						
Station Tal	4 - P							144
four training S								
loar Critica B Bloom Honin	live/Mex	No. of Concession, Name	Web Very Berry	Robin View Varmi	Sauce Pake	Samular	Passodal Sam	
	the second s	Hann 👘	the state of the s			Second Level		Ibie e
Box Ban	Board Marso	Nan N	the state of the s	Reple View Variat	Sounds Madel	Second Level	PArchelant	Hole e Dale s
Stor Hote Stor Stor Stor Hall	Head Mins Constant	ritan Mi	the state of the s	Ne bie Wese Name Letter ange	Social Robot Str. Sylar Sylar	Second Level	PArchelant	
3.07	Head Mos Constant Constant	нан М Ф 45	the state of the s	Repaired And Languages Canverty	No. or in Maded St. Alta	Scoules	PArchelant	Univer-

Figure 4-10 SNMP Group Table Settings Window

The fields that can be configured are described below:

Parameter	Description
Group Name	Enter the group name of a maximum of 32 characters. The syntax is general string that does not allow space.
User-based Security Model	Select the security model here. Options to choose from are:
	 SNMPv1 - Select to allow the group user to use the SNMPv1 security model. SNMPv2c - Select to allow the group user to use the SNMPv2c security model. SNMPv3 - Select to allow the group user to use the SNMPv3
	security model.
Security Level	When selecting SNMPv3 in the User-based Security Model drop- down list, this option is available.
	 NoAuthNoPriv - Specify that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. AuthNoPriv - Specify that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. AuthPriv - Specify that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.
IP Access-List Name	Enter the standard IP access control list (ACL) to associate with the group.
Read View Name	Enter the read view name that the group user can access.
Write View Name	Enter the write view name that the group user can access.
Notify View Name	Enter a write view name that the group user can access. The notify view describes the object that can be reported its status via trap packets to the group user.

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

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

SNMP Engine ID Local Settings

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

To view the following window, click **Management > SNMP > SNMP Engine ID Local Settings**, as shown below:

Network and	ar samp.	
wheeld -	BODODEL/PCCE, PCAR ESPCOR	2 mm - 4 mm

Figure 4-11 SNMP Engine ID Local Settings Window

The fields that can be configured are described below:

Parameter	Description
Engine ID	Enter the engine ID string with the maximum of 24 characters.

Click the **Default** button to revert the engine ID to the default.

Click the Apply button to accept the changes made.

SNMP User Table Settings

This window is used to configure and display the SNMP users that are currently configured on the Switch.

To view the following window, click **Management > SNMP > SNMP User Table Settings**, as shown below:

SNMP Liver Table Setti	nga						
SHIMP Lave Seldings							
TEACHARA	Che Char						
Group Banna -	1 com						
Steal Print and a	Jyr.						
been a substance	hold-	- W					
Aub Polyes for Page at	606	- 12	Proceed ()		1		
Post in the Except	hose	- X -	Plan concert of	eninea 📗			
NUTHER DESCRIPTION	HOT.		vaya 6 da	n) 🔚			
Prio Teocal de Ke	ham	2	Kiry (32 cha				
The Response is the second	et enter						
And and sold and							
LOD HERE 1							
Internation from party	a ang ang Mis	¥1) 74	Restance Provid	Никасу колосия	Hagina Ha	PARMETERS	
1.2 1.6.	12		Bata	No.es	0000004600		04 ate

Figure 4-12 SNMP User Table Settings Window

The fields that can be configured are described below:

Parameter	Description
	Enter an alphanumeric string of up to 32 characters. This is used to identify the SNMP users.

Parameter	Description
Group Name	Enter the SNMP group name to which the user belongs. The syntax is general string that does not allow spaces.
SNMP Version	Select the SNMP version. Options to choose from are v1, v2c, and v3.
SNMP V3 Encryption	After selecting v3 in the SNMP Version drop-down list, this option is available. Options to choose from are None , Password , and Key .
Auth-Protocol	After selecting v3 in the SNMP Version drop-down list, and selecting either Password or Key in the SNMP V3 Encryption drop-down list, this option is available. Select the authentication level. Options to choose from are:
	 MD5 - Select to use the HMAC-MD5-96 authentication level. This field will require the user to enter a password or a key. SHA - Specify that the HMAC-SHA authentication protocol will be used. This field will require the user to enter a password or a key.
Priv-Protocol	After selecting v3 in the SNMP Version drop-down list, and selecting either Password or Key in the SNMP V3 Encryption drop-down list, this option is available. Select the private protocol. Options to choose from are:
	 None - Specify that no authorization protocol is in use. DES56 - Specify that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field will require the user to enter a password or a key.
IP Access-List Name	Enter the standard IP access control list (ACL) to associate with the user.

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

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

SNMP Host Table Settings

This window is used to configure and display the recipient of the SNMP notification.

To view the following window, click Management > SNMP > SNMP Host Table Settings, a	as shown
below:	

MNAP Tisos Selating a				
* HATTER AND A				
CHORE P.G. Askense		1		
Here Lie as Strands Martin	SNM	(V)		
Second And	READS	chie M		
utered a reset	192			
One of the Party State of the				#de
Taul Dillion: 1				
Ika.IP Asterna	SHAP was se	UDP Pat	Community Skins / SHIPTYS Text Home	
12 11 12 12	- 13	112	p #1/1	California -

Figure 4-13 SNMP Host Table Settings

The fields that can be configured are described below:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the SNMP notification host.
Host IPv6 Address	Enter the IPv6 address of the SNMP notification host.
User-based Security Model	 Select the security model here. Options to choose from are: SNMPv1 - Select to allow the group user to use the SNMPv1 security model. SNMPv2c - Select to allow the group user to use the SNMPv2c security model. SNMPv3 - Select to allow the group user to use the SNMPv3 security model.
Security Level	 When selecting SNMPv3 in the User-based Security Model drop- down list, this option is available. NoAuthNoPriv - Specify that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. AuthNoPriv - Specify that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. AuthPriv - Specify that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.
UDP Port	Enter the UDP port number. The default UDP port number of the trap is 162. The range of UDP port numbers is from 1 to 65535. Some port numbers may conflict with other protocols.
Community String / SNMPv3 User Name	Enter the community string to be sent with the notification packet.

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

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

RMON

RMON Global Settings

This window is used to enable or disable remote monitoring (RMON) for the rising and falling alarm trap feature for the SNMP function on the Switch.

To view the following window, click **Management > RMON > RMON Global Settings**, as shown below:

RMON Global Sattings			
- RNOH Global Setlings			
NMON Rising Alarm Trap	g: Enabled	© Coulder	
RMON Failing Alarm Trap	🙊 Drabled	Combine .	At the

Figure 4-14 RMON Global Settings Window

The fields that can be configured are described below:

Parameter	Description
RMON Rising Alarm Trap	Select this option to enable or disable the RMON Rising Alarm Trap Feature.

Parameter	Description
RMON Falling Alarm Trap	Select this option to enable or disable the RMON Falling Alarm Trap Feature.

Click the Apply button to accept the changes made.

RMON Statistics Settings

This window is used to configure and display the RMON statistics on the specified port.

To view the following window, click **Management > RMON > RMON Statistics Settings**, as shown below:

tan ammunika san	ings			
a For		nolae (1-62,525)	Contract	
a johod	11 T		127700	2.8
	10000	Sec.		
F.CK.	1976	Line I		

Figure 4-15 RMON Statistics Settings Window

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Port	Select to choose the port.
Index	Enter the RMON table index. The value is from 1 to 65535
Owner	Enter the owner string. The string can be up to 127 characters.

The fields that can be configured are described below:

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

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

Click the **Show Detail** button to see the detail information of the specific port.

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

After clicking the **Show Detail** button, the following window will appear.

WC H	Sathlie	a Talake																
ud na	Dele Source	Rey. Coura	000000	Draskan RKTa	Mali puet Piktu	Underslag Picto	9 versilae Picta	FIREBUI	Jate	cne Olisi	dh847	Disc Diad			tai ass Conta	236 CH Octobe	602 1622 50 mili	1124 1311
20	4412	200412	2002	177	201	0	0 (3	0.0	3	E	22	2077	.79	- 35 -	142	22	0

Figure 4-16 RMON Statistics Table Window

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

RMON History Settings

This window is used to configure and display RMON MIB history statistics gathering on the specified port.

To view the following window, click **Management > RMON > RMON History Settings**, as shown below:

IN H R	noy sounds						
	Pot .	1000(1-0557)	folgaet sumber th	-123(2)	amarya (1-3630)		Overan
	obditic z	1	3 3 - 1		1000	482	127 Gam
nà r	Pat	Decks in Decayale I	Sectors General	in and	CWAI		
	40.0	X	30	100	DHC Relatory		United Stock Letter



The fields that can be configured are described below:

Parameter	Description					
Unit	Select the switch unit that will be used for this configuration here.					
Port	Select to choose the port.					
Index	Enter the index value here. The value is from 1 to 65535.					
Bucket Number	Enter Specifies the number of buckets specified for the RMON collection history group of statistics. The range is from 1 to 65535. The default value is 50.					
Interval	Enter the time in seconds in each polling cycle. The range is from 1 to 3600.					
Owner	Enter the owner string. The string can be up to 127 characters.					

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

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

Click the **Show Detail** button to see the detail information of the specific port.

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

After clicking the Show Detail button, the following window will appear.

RMCN History Table	
PRICE History Table	
Individualing in the restrict Here. For the Heredesian Forter Millingson Forter Transition Forter Forter Forter Control of the Forter Party of the	
	Undk

Figure 4-18 RMON History Table Window

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

RMON Alarm Settings

This window is used to configure and display alarm entries to monitor an interface.

To view the following window, click **Management > RMON > RMON Alarm Settings**, as shown below:

noner () 42558)	1	10	many/(1-0147282647	h-		e.	
Andres	H.N.N.N		Taw	71,000	12 N		
Lalog Theories (1-24) 2-161(42)	C. C		Falling Thirsenold (Skin	PH 625-21	0		
ong-one taxane periodi	1 Laurence	10	- Andre g + Anne sa ar ann	praessi			
www.	1.120 charters						
						40	1. AL
tal Primer 1 Countries (Inter Lost	Wite Rains This shot	allen Devsiedelt sie	Enal Huteland Coal	Vo. Satas Ha	n veri	

Figure 4-19 RMON Alarm Settings Window

The fields that can be configured are described below:

Parameter	Description
Index	Enter the alarm index. The range is from 1 to 65535.
Interval	Enter the interval in seconds for the sampling of the variable and checking against the threshold. The valid range is from 1 to 2147483647 seconds.
Variable	Enter the object identifier of the variable to be sampled.
Туре	Select the monitoring type. Options to choose from are Absolute and Delta .
Rising Threshold	Enter the rising threshold value between 0 and 2147483647.
Falling Threshold	Enter the falling threshold value between 0 and 2147483647.
Rising Event Number	Enter the index of the event entry that is used to notify the rising threshold-crossing event. The valid range is from 1 to 65535. If not specified, no action is taken while crossing the ringing threshold.
Falling Event Number	Enter the index of the event entry that is used to notify the falling threshold-crossing event. The valid range is from 1 to 65535. If not specified, no action is taken while crossing the falling threshold.
Owner	Enter the owner string up to 127 characters.

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

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

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

RMON Event Settings

This window is used to configure and display event entries.

To view the following window, click **Management > RMON > RMON Event Settings**, as shown below:

nas even senegs					
escretten	1.42	A.R.			
n.;	None	12			
	1.124	20,00			
	100 C	(1.11)			
). 				i
GERRA 1			2001 0		
ad Dabka 1 Nilay Dayka 2004			Gam	yes These Terr	

Figure 4-20 RMON Event Settings Window

The fields that can be configured are described below:

Parameter	Description	
Index	Enter the index of the alarm entry between 1 and 65535.	
Description	Enter a description for the RMON event entry. The string is up to 127 characters long.	
Туре	Select the RMON event entry type. Options to choose from are None , Log , Trap , and Log and Trap .	
Community	Enter the community string. The string can be up to 127 characters	
Owner	Enter the owner string. The string can be up to 127 characters.	

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

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

Click the View Logs button to see the detail information of the specific port.

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

After clicking the **View Logs** button, the following window will appear.

Event Loga Table			
Event Logit Table			
Event index: 1	Event index: 1		
Total Entries: 0			
Log Index	top time	Lag Bis ng hai	
		- He A	



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

Telnet/Web

This window is used to configure Telnet and Web settings on the Switch.

To view the following window, click **Management > Telnet/Web**, as shown below:

Leines Veels		
Telear Seringe		
0.0.18.45	a material in position	
Port (+8525)	20	(4 #r
Weitz Belling p.		
Web State	w Endet in Dockd	
Port (~85828)	<u>a</u>	

Figure 4-22 Telnet/Web Window

The fields that can be configured for **Telnet Settings** are described below:

Parameter	Description	
Telnet StateSelect this option to enable or disable the configuration Telnet.		
Port	Enter the TCP port number used for Telnet management of the Switch. The default TCP port for the Telnet protocol is 23.	

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

The fields that can be configured for **Web Setting** are described below:

Parameter	Description
Web State	Select this option to enable or disable the configuration through the web.
Port	Enter the TCP port number used for Web-based management of the Switch. The "well-known" TCP port for the Web-based protocol is 80.

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

Session Timeout

This window is used to display and configure the session timeout settings. The outgoing session timeout values are used for Console/Telnet/SSH connections through the CLI of the Switch to the Telnet interface of another switch.

To view the following window, click **Management > Session Timeout**, as shown below:

Season limeout			
ansaon brinner			
Web Sevelor Timercal (63-35000)	100	sec (7 Defeuil	
Convelle Svervien Timeout (3-1439)	2	min 😥 Dehalt	
Culgoing Convola Seavion Timeout (3-1432)	0	min 🔀 Debalt	
Teined Secolori Timeset (2-1939)	2	min 🔽 Pelsali	
Cutgoing Teinet Section Timeost (3-1439)	0	min 17 Debuit	
OSLI Service Timesul (0-1409))	min 17 Default	
Outgoing 9311 Sevelor Timeout (0-1403)	0	min (2 Default	R aj de



The fields that can be configured are described below:

Parameter	Description
Web Session Timeout	Enter the web session timeout value here. The range is from 60 to 36000 seconds. The default value is 180 seconds.
	Select the Default option to use the default value.
Console Session Timeout	Enter the console session timeout value here. The range is from 0 to 1439 minutes. Enter 0 to disable the timeout. The default value is 3 minutes.
	Select the Default option to use the default value.
Outgoing Console Session Timeout	Enter the outgoing console session timeout value here. The range is from 0 to 1439 minutes. Enter 0 to disable the timeout. The default value is 0.
	Select the Default option to use the default value.
Telnet Session Timeout	Enter the Telnet session timeout value here. The range is from 0 to 1439 minutes. Enter 0 to disable the timeout. The default value is 3 minutes.
	Select the Default option to use the default value.
Outgoing Telnet Session Timeout	Enter the outgoing Telnet session timeout value here. The range is from 0 to 1439 minutes. Enter 0 to disable the timeout. The default value is 0.
	Select the Default option to use the default value.
SSH Session Timeout	Enter the SSH session timeout value here. The range is from 0 to 1439 minutes. Enter 0 to disable the timeout. The default value is 3 minutes.
	Select the Default option to use the default value.
Outgoing SSH Session Timeout	Enter the outgoing SSH session timeout value here. The range is from 0 to 1439 minutes. Enter 0 to disable the timeout. The default value is 0.
	Select the Default option to use the default value.

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

DHCP

Service DHCP

This window is used to configure the DHCP relay service on the Switch.

To view the following window, click **Management > DHCP > Service DHCP**, as shown below:

Service DID ¹		
Service Durch		
Centre DI OP Sara	(¿ Classifier 7) Cristian	Lada and a second s
Same Pict 2002		
Seven Hol DEPS.4:	W Claim Classic	i seate i

Figure 4-24 Service DHCP Window

The fields that can be configured for Service DHCP are described below:

Parameter	Description
Service DHCP State	Select this option to enable or disable the DHCP relay service.

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

The fields that can be configured for Service IPv6 DHCP are described below:

Parameter	Description
Service IPv6 DHCP State	Select this option to enable or disable the IPv6 DHCP relay service.

Click the Apply button to accept the changes made.

DHCP Class Settings

This window is used to configure and display the DHCP class and the DHCP option matching pattern for the DCHP class.

To view the following window, click **Management > DHCP > Service DHCP**, as shown below:

DHO*Class Settings		
- 1000 01 C10 G4 SP1010		
Dill OP Live Chars Shile	Disabled 💌	Asple
- Dec P. Class. Serrings		
Chara Humin	32 chary	Apple
Inital Enlances 1		
	Cloux Name	
	G.z.	Bolk De ste



The fields that can be configured for DHCP Class State are described below:

Parameter	Description
DHCP Use Class State	Select to enable or disable the DHCP class function here.

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

The fields that can be configured for **DHCP Class Settings** are described below:

Parameter	Description
Class Name	Enter the DHCP class name with a maximum of 32 characters.

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

Click the **Edit** button to modify the DHCP option-matching pattern for the corresponding DCHP class.

Click the **Delete** button to remove the specified 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 window will appear.

I ICP Cleve Optice deltings —			
filser Stree Caller († 42-1) Het	54052800		
Dirmul	0		- Azobi
lon Forder 1			
Opean	STER.	TREAM	
1.1	10.54		De etc
			1 488



The fields that can be configured are described below:

Parameter	Description	
Option	Enter the DHCP option number. The range is from 1 to 254.	
Hex	Enter the hex pattern of the specified DHCP option. Tick the check box not to match the remaining bits of the option.	
Bitmask	Enter the hex bit mask for masking of the pattern. The masked pattern bits will be matched. If not specified, all bits entered in Hex will be checked.	

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

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

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

DHCP Server

The Dynamic Host Configuration Protocol (DHCP) allows the Switch to designate 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 will allocate an IP address to the client. The DHCP client may be then utilize the IP address allocated by the DHCP server as its local configuration.

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 allocated IP address, the range of IP addresses that will be allowed in its DHCP pool, the ability to exclude various IP addresses within the range 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 assign the same IP addresses to important devices.

DHCP Server Global Settings

This window is used to display and configure the global DHCP server parameters.

To view the following window, click **Management > DHCP > DHCP Server > DHCP Server Global Settings**, as shown below:

DHCP Server Global Settings		
DITCP Use Class State		
Deciritian caracteria	CHARME SHORE	Apply
DIICP Server Settings		
Decirienți Panar (C.14)	y	
DECREMAND Frank (10) 10(0)	101 IV.	d g ds



The fields that can be configured in DHCP Use Class State are described below:

Parameter	Description
DHCP Use Class State	Select to enable or disable the DHCP Use Class State here. When enabled, the DHCP server will use DHCP classes for address allocation.

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

The fields that can be configured in DHCP Server Settings are described below:

Parameter	Description		
DHCP Ping Packet	Enter the number of ping packets that the Switch will send out or 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. A value of 0 means there is no ping test. The range is from 0 to 10. The default value is 2.		
DHCP Ping Timeout	Enter the amount of time the DHCP server must wait before timing out a ping packet. The range is from 100 to 10000 milliseconds. The default value is 500 milliseconds.		

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

DHCP Server Pool Settings

This window is used to display and configure the DHCP server pool settings.

To view the following window, click **Management > DHCP > DHCP Server > DHCP Server Pool Settings**, as shown below:

DUICH Server Post	Settings	
DITCP Server Post		
Post Vietna	(v out	4.90A
TYPE FERRE T		
	(N. 18 a	Ph Car Bill Spin Galger andr
1		

Figure 4-28 DHCP Server Pool Settings Window

The fields that can be configured are described below:

Parameter	Description
Pool Name	Enter the DHCP server pool name here. This name can be up to 32 characters long.

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

Click the Edit Class button to configure the DHCP class.

Click the **Edit Option** button to configure the DHCP server pool option settings.

Click the **Configure** button to configure the DHCP server pool settings.

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

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

After clicking the Edit Class button, the following page will appear.

A ICH Server Poel Class S	editari ppa		
DITCP Server Pool Clane Sadings			
Post Same	305		
Chara Ricela	Press Saled		
She Astron	1		
DJAKwa			- Azak
Total Delike: 1			
Chus Huns	Start Address	End Address	
10.2		5100100500	Det die by Roma Det die sy Arbiers
1.000			Jude.

Figure 4-29 DHCP Server Pool Class Settings Window

The fields that can be configured are described below:

Parameter	Description	
Class Name	Select an existing DHCP class name here that will be associated with this DHCP pool.	
Start Address	Enter the starting IPv4 address that will be associated with the DHCP class in the DHCP pool here.	
End Address	Enter the ending IPv4 address that will be associated with the DHCP class in the DHCP pool here.	

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

Click the **Delete by Name** button to remove the DHCP class association by name.

Click the **Delete by Address** button to remove the DHCP class association by address.

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

After clicking the Edit Option button, the following page will appear.

DHCP Server Pool	Option Settings		
DITCP Server Pool Op8	vn Svitinga		
Post Same	peol		
Option (1-254)			
Tgar	46.01	x	
			Apply
Option	Туру	Yalav	
200	a contra de la con	zitrą.	Telete.
			Zade

Figure 4-30 DHCP Server Pool Option Settings Window

The fields that can be configured are described below:

Parameter	Description
Option	Enter the DHCP option number here. The range is from 1 to 254.
Туре	 Select the DHCP option type here. Options to choose from are: ASCII - Enter the ASCII string in the space provided. This string can be up to 255 characters long. Hex - Enter the hexadecimal string in the space provided. This string can be up to 254 characters long. Select the None option to specify a zero-length hexadecimal string. IP - Enter the IPv4 address(es) in the space(s) provided. Up to 8 IPv4 addresses can be entered.

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

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

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

After clicking the **Configure** button, the following page will appear.

to al Samuel	ava					
cal flie .	Bichin					
anah Mana	Bichn					
visorus (1994auto	6.1.1.0.6	0 0 0 0	8			
ed Soley I	0 + 1 + 0 = 0					
Aud. Hoates		1.000	1.00	- 425 F		
	and the second sec	a second second	1.1			
3.9,9,4			1			
0.99990		a contraction of the	1.1.1		the second s	
49103 N. a. a. 30 mm	and the second	1.125			and the second second	
	Low second State	1				
NRCS Same your	Panor árdara 👘 ⊻					

Figure 4-31 DHCP Server Pool Configure Window

The fields that can be configured are described below:

Parameter	Description
Boot File	Enter the boot file name here. This can be up to 64 characters long.
Domain Name	Enter the domain name for the DHCP client here. This can be up to 64 characters long.
Network (IP/Mask)	Enter the network IPv4 address and subnet mask for the DHCP client here.
Next Server	Enter the next server IPv4 address here. The boot image file is stored on this server and can be retrieved by DHCP clients using this IP address. The server is typically a TFTP server. Only one next server IP address can be specified.
Default Router	Enter the IPv4 address of the default router for the DHCP client here. Up to 8 IPv4 addresses can be entered here. The IP address of the router should be on the same subnet as the client's subnet. Routers are listed in the order of preference. If default routers are already configured, the default routers configured later will be added to the default interface list.
DNS Server	Enter the IPv4 address to be used by the DHCP client as the DNS server here. Up to 8 IPv4 addresses can be entered here. Servers are listed in the order of preference. If DNS servers are already configured, the DNS servers configured later will be added to the DNS server list.
NetBIOS Name Server	Enter the WINS name server IPv4 address for the DHCP client here. Up to 8 IPv4 addresses can be entered here. Servers are listed in the order of preference. If name servers are already configured, the name server configured later will be added to the default interface list.
NetBIOS Node Type	 Select the NetBIOS node type for Microsoft DHCP clients here. The node type determines the method that NetBIOS uses to register and resolve names. Options to choose from are: Broadcast - This system uses broadcasts. Peer To Peer - This system (p-node) uses only point-to-point name queries to a name server (WINS). Mixed - This system (m-node) broadcasts first, and then
	 queries the name server. Hybrid - This system (h-node) queries the name server first, and then broadcasts. This is the recommended type.
Lease	Enter and select the lease time for an IPv4 address that is assigned from the address pool here. Enter the Days in the range from 0 to 365. Select the Hours and Minutes from the drop-down menus. Alternatively, the Infinite option can be selected to specify that the lease time is unlimited.

Click the Apply button to accept the changes made.

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

DHCP Server Exclude Address

This window is used to view and exclude a range of IPv4 addresses from being allocated to the DHCP client. The DHCP server automatically allocates addresses in DHCP address pools to DHCP clients. All the addresses except the interface's IP address on the router and the excluded address(es) specified here are available for allocation. Multiple ranges of addresses can be excluded. To remove

a range of excluded addresses, administrators must specify the exact range of addresses previously configured.

To view the following window, click **Management > DHCP > DHCP Server > DHCP Server Exclude Address**, as shown below:

0 ICH Server Loclade Address		
DITCP Server Cacksia Actively		
for gin Accord.		
Frankwe		- Apply
Toma Fatelea: 1		
Fingle Adds. to a	Enlätten	
152,163,712	\$2,168,70,100	C Calebra

Figure 4-32 DHCP Server Exclude Address Window

The fields that can be configured are described below:

Parameter	Description
Begin Address	Enter the first IPv4 address of a range of addresses to be excluded here.
End Address	Enter the last IPv4 address of a range of addresses to be excluded here.

Click the Apply button to accept the changes made.

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

DHCP Server Manual Binding

This window is used to display and configure the DHCP server manual binding settings. With a manual binding entry, the IP address can be bound with a client-identifier or bound with the hardware address of the host.

To view the following window, click **Management > DHCP > DHCP Server > DHCP Server Manual Binding**, as shown below:

Posta Salane Hente 🛞 – Handovana Adoreska 🔿 – Dillera Beentler	Coroscander.	V.at			8 m.ds.
PostMarie	Hort.	88.0	Hardwine Adomes	Caret service	

Figure 4-33 DHCP Server Manual Binding Window

Parameter	Description
Pool Name	Enter the DHCP server pool name here. This name can be up to 32 characters long.
Host	Enter the DHCP host IPv4 address here.
Mask	Enter the DHCP host network subnet mask here.
Hardware Address	Enter the DHCP host MAC address here.

The fields that can be configured are described below:
Parameter	Description
Client Identifier	Enter the DHCP host identifier in hexadecimal notation here. The client identifier is formatted by the media type and the MAC address.

Click the Apply button to accept the changes made.

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

DHCP Server Dynamic Binding

This window is used to view and clear the DHCP server dynamic binding entries.

To view the following window, click **Management > DHCP > DHCP Server > DHCP Server Dynamic Binding**, as shown below:

DHCP Server Dynamic I	Linding .			
DITCP: Server Dynamic Dinding	,			
P Address				Fed
Pool Serie	12 charv	78		
IP Advisor				du
Total Entries: 0				
1º 668 Des		Labor Labort warn Audress	Laaso Espiration	574

Figure 4-34 DHCP Server Dynamic Binding Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the binding entry IPv4 address here.
Pool Name	Enter the DHCP server pool name here. This name can be up to 32 characters long. Select the All option to clear the binding entries for all pools.

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

Click the **Clear** button to clear the entries based on the information specified.

DHCP Server IP Conflict

This window is used to view and clear the DHCP conflict entries from the DHCP server database.

To view the following window, click **Management > DHCP > DHCP Server > DHCP Server IP Conflict**, as shown below:

DHCP Server IP Config	:1			
DHCP Server IP Conflict.				
IF KARAWA				Ped
Post Serve	32 chary	7.4		
IP Address				dar
Total Entrive: 0				
LP ARE INC.		Detection Method	Destructions from the	

Figure 4-35 DHCP Server IP Conflict Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the IPv4 address of the conflict entry to be located or cleared.
Pool Name	Enter the DHCP server pool name here. This name can be up to 32 characters long. Select the All option to clear the conflict entries for all pools.

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

Click the **Clear** button to clear the entries based on the information specified.

DHCP Server Statistic

This window is used to display DHCP server statistics.

To view the following window, click **Management > DHCP > DHCP Server > DHCP Server Statistic**, as shown below:

DHCP Server Statistics		
		den
	LENDY NAMES AND ALL AND	
Addresse Poel a	l .	
Automatic Dindinas	0	
Manual Bindings	I	
Haltanner, Horsagos	9	
Renew Dessegus	0	
макада жағанас		
poornaquest	0	
CHOPC SCOVER	0	
19-00-99 - 080-991	ii .	
0-040-03 MH	0	
CHOPROLISAGE	0	
CERPINEDEM	0	
Verage Seri		
BOOTHERLY	0	
0-00406-6-6	н	
0-099638	0	
CHOPHAK .	0	

Figure 4-36 DHCP Server Statistic Window

Click the Clear button to clear the statistics information displayed here.

DHCPv6 Server

DHCPv6 Server Pool Settings

This window is used to display and configure the DHCPv6 server pool settings.

To view the following window, click **Management > DHCP > DHCPv6 Server > DHCPv6 Server Pool Settings**, as shown below:

10 10 % Server Pool Settings	
DITCPAS Survey Post	
era vane	4204.
TYR HEINE T	
DelSan.	
in a statistica de la constatistica de la constatistica de la constatistica de la constatistica de la constatis	Charges 2 Dieles

Figure 4-37 DHCPv6 Server Pool Settings Window

The fields that can be configured are described below:

Parameter	Description
Pool Name	Enter the DHCPv6 server pool name here. This name can be up to 12 characters long.

Click the Apply button to accept the changes made.

Click the **Configure** button to configure the DHCPv6 server pool settings.

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

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

After clicking the **Configure** button, the following page will appear.

CLIC: VS Server Post Contigue	ii					
DITCPSS Serve Pool Cardinary						
Post Same C Admini Tarlis & Phale Cologadian Tas Vicis John #14266002201 Phale ad Johan #2-42262012251	Face 200 copicit and 12 cmm	18				4.00%
1948 Stream 1958 Stream 1958 Stream	2018 1					
Note Diskes						
 Static Dir dings Address Chem Du D Varid "Belleve (KG-120-K)(T220) Fond En Meet K 	poorcone d Schen Plazaol	8+5	() Sano Girainga Prets 18 D Preterset Liveine (SC-12)(KCT2X	2014 6308 639-	ant .	Rgsh

Figure 4-38 DHCPv6 Server Pool Configure Window

The fields that can be configured in DHCPv6 Server Pool Configure are described below:

Parameter	Description
Address Prefix	Select and enter the DHCPv6 server pool IPv6 network address and prefix length here. For example, 2015::0/64.
Prefix Delegation Pool	Select and enter the DHCPv6 server pool prefix delegation name here. This name can be up to 12 characters long.
Valid Lifetime	Enter the valid lifetime value here. The range is from 60 to 4294967295 seconds. The valid lifetime should be greater than preferred lifetime. If this value is not specified, then the default valid lifetime will be 2592000 seconds (30 days).
Preferred Lifetime	Enter the preferred lifetime value here. The range is from 60 to 4294967295 seconds. If this value is not specified, the preferred lifetime will be 604800 seconds (7 days).
DNS Server	Enter the DNS server IPv6 address to be assigned to requesting DHCPv6 clients here.
Domain Name	Enter the domain name to be assigned to requesting DHCPv6 clients here.

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

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

The fields that can be configured in **Static Bindings** are described below:

Parameter	Description
Static Bindings Address	Enter the static binding IPv6 address assign to the specific client here.
Static Bindings Prefix	Enter the static binding IPv6 network address and prefix length here.
Client DUID	Enter the client DHCP Unique Identifier (DUID) here. This string can be up to 28 characters long.
IAID	Enter the Identity Association Identifier (IAID) here. The IAID here uniquely identifies a collection of non-temporary addresses (IANA) assigned on the client.
Valid Lifetime	Enter the valid lifetime value here. The valid lifetime should be greater than the preferred lifetime. The range is from 60 to 4294967295 seconds. By default, this value is 2592000 seconds (30 days).
Preferred Lifetime	Enter the preferred lifetime value here. The range is from 60 to 4294967295 seconds. By default, this value is 604800 seconds (7 days).

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

DHCPv6 Server Local Pool Settings

This window is used to display and configure the DHCPv6 server local pool settings.

To view the following window, click **Management > DHCP > DHCPv6 Server > DHCPv6 Server** Local Pool Settings, as shown below:

ULTOS Serves Los	1.1					
DITEPSS Serve Local Po						
PCR VIEW		1222/08				
ING ADDALE FIND LARC		CRAMER'S ST				
darignari tengra						100
Dod Serve		Izenn				(Fight
Total Californi I						10.00
HYNR SAME	6448.C	AND DRAFT STORE	- Fried-	IF COM		
HQI.	1.6.1.0.0				Line: Depit Del pro	



The fields that can be configured are described below:

Parameter	Description
Pool Name	Enter the DHCPv6 server pool name here. This name can be up to 12 characters long.
IPv6 Address / Prefix Length	Enter the IPv6 prefix address and prefix length of the local pool here.
Assigned Length	Enter the prefix length to be delegated to the user from the pool here. The value of the assigned length cannot be less than the value of the prefix length.

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 **User Detail** button to view the user information displayed in the lower table.

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

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

DHCPv6 Server Exclude Address

This window is used to specify IPv6 addresses that a DHCPv6 server should not assign to DHCPv6 clients. The DHCPv6 server assumes that all addresses (excluding the Switch's IPv6 address) can be

assigned to clients. Use this window to exclude a single IPv6 address or a range of IPv6 addresses. The excluded addresses are only applied to the pool(s) for address assignment.

To view the following window, click **Management > DHCP > DHCPv6 Server > DHCPv6 Server = Exclude Address**, as shown below:

LT ILL'Y & Server Exclude	e Palalman K		
DITCPSS Synwy Eaclash Astern			
The second	init 1		
High Evi-Acades	(and the second		a sph-
Tom Entries: 1			
Test	Les Defâbless	High Dis S. Adda. yo	E
1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -	2020.153	2525, 120	Code les
			and the second

Figure 4-40 DHCPv6 Server Exclude Address Window

The fields that can be configured are described below:

Parameter	Description
Low IPv6 Address	Enter the excluded IPv6 address or first IPv6 address in the excluded address range here.
High IPv6 Address	Enter the last IPv6 address in the excluded address range here (optional).

Click the Apply button to accept the changes made.

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

DHCPv6 Server Binding

This window is used to view and clear the DHCPv6 server binding entries.

To view the following window, click **Management > DHCP > DHCPv6 Server > DHCPv6 Server Binding**, as shown below:

uteranger om der der HCPvS Sveweitigt av	011			
PVI ATOM	ior			Pet Oar
Fara Finhais II		200		
0.01000		Il eS Adda o	Enderson Laboration	Value Latera en

Figure 4-41 DHCPv6 Server Binding Window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address	Enter the binding entry IPv6 address to be displayed or cleared here. Select the All option to display or clear all DHCPv6 client prefix bindings in or from the binding table.

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

Click the **Clear** button to clear the entries based on the information specified.

DHCPv6 Server Interface Settings

This window is used to display and configure the DHCPv6 server interface settings.

To view the following window, click **Management > DHCP > DHCPv6 Server > DHCPv6 Server Interface Settings**, as shown below:

ICPSS Steve Industries St	20.0				
Mensory with the		PostNarw	proven	A	
Apitonal	Classied	V DAMAGE		1.000	New York
	0.5-03-007-01-0	NG COMPANY			45.04
rde flace blame	- Kard	-0			- (Pa 1
				8	101
formi Californi I					
form Ericlen, (Substance) was	Peablicea	Rep & Controls	Believen 2	Had Freedbard	

Figure 4-42 DHCPv6 Server Interface Settings Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID here. The range is from 1 to 4094.
Pool Name	Enter the DHCPv6 server pool name here. This name can be up to 12 characters long.
Rapid Commit	Select to enable or disable two-message exchange here. By default, two-message exchange is not allowed.
Preference	Enter the preference value here. The range is from 0 to 255. Select the Default option to use the default value. Select the Allow Hint option to allow hints.
Interface Name	Enter the interface name here.

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 **Delete** button to remove the specified entry.

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

DHCPv6 Server Operational Information

This window is used to display the DHCPv6 server operational information.

To view the following window, click **Management > DHCP > DHCPv6 Server > DHCPv6 Server Operational Information**, as shown below:



Figure 4-43 DHCPv6 Server Operational Information Window

DHCP Relay

DHCP Relay Global Settings

This window is used to configure the smart relay feature of the DHCP relay agent.

To view the following window, click **Management > DHCP > DHCP Relay > DHCP Relay Global Settings**, as shown below:

DHCP Retay Global Settings		
- THCP Relay Signal Settings		
UP OF Street Holes Nate	ig: Detailed i ig: Enabled	100 k
	States Creat	

Figure 4-44 DHCP Relay Global Settings Window

The fields that can be configured are described below:

Parameter	Description
DCHP Smart Relay State	Select this option to enable or disable the DHCP smart relay.

Click the Apply button to accept the changes made.

DHCP Relay Pool Settings

This window is used to configure and display the DHCP relay pool on a DHCP relay agent.

To view the following window, click **Management > DHCP > DHCP Relay > DHCP Relay Pool Settings**, as shown below:

To the state of the second of					
an Anne	9.6.0				
AN FRANKS TO					
	Fool Han a	See	Developation	Class	
	5HCPacel	THE R LOW D	84	A 1	6.9.1



The fields that can be configured are described below:

Parameter	Description
Pool Name	Enter the address pool name with a maximum of 32 characters.

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

Click the Edit button to modify the corresponding information of the specific DHCP pool.

Click the **Delete** button to remove the specified 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 under Source, the following window will appear.

FIC: tealing freed	Source Settings			
HE PROMETER SPACE	a senega			
Prosidiame	DestRacal			
Searce IP Address		Dub wei Mach		
Fotal Estimates of				
	Name Planters		Parane 1 Month	
	10.238.3.11		195001	Life and a
				2. 4

Figure 4-46 DHCP Relay Pool Source Settings Window

The fields that can be configured are described below:

Parameter	Description
Source IP Address	Enter the source subnet of client packets.
Subnet Mask	Enter the network mask of the source subnet.

Click the Apply button to accept the changes made.

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

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

After clicking the Edit button under Destination, the following window will appear.

на с наму константа	Andonalaan Sellinge 2010 Antoin	
Posiciane Relev Destructori	CasePiped	
Coal Existen it		
	Testector	
	30.35.(210	
		2.4

Figure 4-47 DHCP Relay Pool Destination Settings Window

The fields that can be configured are described below:

Parameter	Description
Relay Destination	Enter the IP address of the relay destination DHCP server here.

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

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

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

After clicking the Edit button under Class, the following window will appear.

C.P. HANG FEET LOW C		
Positivanie	B+3Ppxc)	
Class Natio	Please Soloca 👘	- A47
Focal Existen et		
Harr.		
	287 EST	Caleto



The fields that can be configured are described below:

Parameter	Description
Class Name	Select the DHCP class name.

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

Click the Edit button to edit more information.

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

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

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

a ithir feating fraction	Dene Odit Settinge	
ны намунальная с	11742.04	
Posiciane	II-OPped	
Chara Shenz	DI OPCIan	
Phile Taind		704 p.
NACES IN CONTRACT		
	Tang, Addiew	
	10 1 21	Le sta
		Marak.

Figure 4-49 DHCP Relay Pool Class Edit Settings Window

The fields that can be configured are described below:

Parameter	Description
	Enter the DHCP relay target for relaying packets that matches the value pattern of the option defined in the DHCP class.

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

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

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

DHCP Relay Information Settings

This window is used to configure and display the DHCP relay information.

To view the following window, click **Management > DHCP > DHCP Relay > DHCP Relay Information Settings**, as shown below:

No TRUE OF ANY ANY	Obstad		managed street	Paral and		
	In the second second second	1		E aublec 👘		S
nationalism House	Replace	74	Extended operation	Li aubiec 🖉 🖛		kee v
HCTP FL-base in the state is the state.						
HCTPH-for induced in a						
		_				
CCR.4a blanchar Mai Debits 1 Inter24	Inext	e	ere states	i-any	lighter form	



The fields that can be configured are described below:

Parameter	Description
Information Trust All	Select this option to enable or disable the DHCP relay agent to trust the IP DHCP relay information for all interfaces.
Information Check	Select this option to enable or disable the DHCP relay agent to validate and remove the relay agent information option in the received DHCP reply packet.
Information Policy	 Select the Option 82 re-forwarding policy for the DHCP relay agent. Options to choose from are: Keep - Select to discard the packet that already has the
	 Neep - Select to discard the packet that already has the relay option. Drop - Select that the DHCP request packet that already has the relay option is left unchanged and directly relayed to the DHCP server. Replace - Select that the DHCP request packet that already has the relay option will be replaced by a new option.
Information Option	Select this option to enable or disable the insertion of relay agent information (Option 82) during the relay of DHCP request packets.

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

Click the **Edit** button to modify the corresponding interface.

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

DHCP Relay Information Option Format Settings

This window is used to configure and display the DHCP information format.

To view the following window, click **Management > DHCP > DHCP Relay > DHCP Relay Information Option Format Settings**, as shown below:

PRODUC	n Forter Benard D	Octout	Ŧ			
inierosta	an Fernar Gintuit (9	Cedad	-			1 Acres
let trais	a himika topico	norm top				
0.1	Dot DA	to fixe	form)	(16A)	26.06	
1	(<u>*)</u> at 109	🖂 eta 5321	🔄 🖂 Vendord 🔄	🗻 (Burealt). 🖂	Q. (7.4),	Ann
ind 3.84	diage.					
10000	State State	heread	a Marine a	DWIN.	- Entr	et to Webee
	8515.5					
	2650(2)					
	6.417./2					
	1100.2					
	2013/0					
	etti 5.3					
	da PON					
	ADDING:	13				
	351325					

Figure 4-51 DHCP Relay Information Option Format Settings Window

The fields that can be configured for **DHCP Relay Information Option Format Global** are described below:

Parameter	Description		
Information Format Remote	Select the DHCP information remote ID sub-option. Options to choose from are:		
	 Default - Select to use the Switch's system MAC address as the remote ID. User Define - Select to use a user-defined remote ID. Enter the user-defined string with the maximum of 32 characters in the text box. Vendor2 - Select to use vender 2 as the remote ID. Vendor3 - Select to use vender 3 as the remote ID. Export UDF - Select to use the expert UDF remote ID. Select the Standalone Unit Format after this selection here. 		
Information Format Circuit ID	Select the DHCP information circuit ID sub-option. Options to choose from are:		
	 Default - Select to use the default circuit ID sub-option. User Define - Select to use a user-defined circuit ID. Enter the user-defined string with the maximum of 32 characters in the text box. 		
	 Vendor1 - Select to use vender 1 as the circuit ID. Vendor2 - Select to use vender 2 as the circuit ID. 		
	 Vendor3 - Select to use vender 3 as the circuit ID. Vendor4 - Select to use vender 4 as the circuit ID. 		
	 Vendor5 - Select to use vender 5 as the circuit ID. Vendor6 - Select to use vender 6 as the circuit ID. 		
	 Export UDF - Select to use the expert UDF circuit ID. Select the Standalone Unit Format after this selection here. 		

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

The fields that can be configured for **DHCP Relay Information Option Format Type** are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Format Select the DHCP information circuit ID format. Options to che from are Vendor3 and Expert UDF.	
Туре	Select the DHCP information circuit ID format typ. Options to choose from are Remote ID and Circuit ID .
Value	Enter the vendor-defined string.

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

DHCP Relay Information Profile Settings

This window is used to display and configure the DHCP relay information profile settings.

To view the following window, click **Management > DHCP > DHCP Relay > DHCP Relay Information Profile Settings**, as shown below:

DI ICP Relay Information	i thuile Seiteige		_			
DICP fieles hiteration Option						
1064 Deleter	Umausa 🕑 Reas 🕑					
Human	109-102 (18-00-				112	420%
DECP Rates Information Profile						
Parameter	2**M/M		1	19.8	11	test 1
FOR FERNELL						
- Internation	**	Formal string				
Fig. 16			1.144.1	15:		LN 105
1			N I	11110		

Figure 4-52 DHCP Relay Information Profile Settings Window

Parameter	Description	
Case	Select the case that will be used here. Options to choose from are:	
	 Lowercase - Specifies that when using the lowercase format, the Option 82 MAC address for the user-defined profile will be formatted as: aa-bb-cc-dd-ee-ff. Uppercase - Specifies that when using the uppercase format, the Option 82 MAC address for the user-defined profile username will be formatted as: AA-BB-CC-DD-EE-FF. 	
Delimiter	Select the delimiter that will be used here. Options to choose from are:	
	Hyphen - Specifies that the format will be AA-BB-CC-DD-EE- FF.	
	 Colon - Specifies that the format will be AA:BB:CC:DD:EE:FF. 	
	 Dot - Specifies that the format will be AA.BB.CC.DD.EE.FF. None - Specifies that when not using any delimiter, the format will be AABBCCDDEEFF. 	

The fields that can be configured in **DHCP Relay Information Option MAC Format** are described below:

Parameter	Description
Delimiter Number	 Select the delimiter number here. Options to choose from are: 1 - Single delimiter, the format is: AABBCC.DDEEFF. 2 - Double delimiters, the format is: AABB.CCDD.EEFF. 5 - Multiple delimiters, the format is: AA.BB.CC.DD.EE.FF.

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

The fields that can be configured in **DHCP Relay Information Profile Settings** are described below:

Parameter	Description		
Profile Name	Enter the Option 82 profile name here. The profile can be used to define the flexible, user-defined Option 82 entry.		
	 Enter the Option 82 profile name here. The profile can be used to define the flexible, user-defined Option 82 entry. After clicking the Edit button, enter the user-defined DHCP Option 82 format string here. This string can be up to 251 characters long. The following rules need to be considered: This string can be a hexadecimal value, an ASCII string, or any combination of hexadecimal values and ASCII characters. An ASCII string needs to be enclosed with quotation marks ("") like "Ethernet". Any ASCII characters outside of the quotation marks will be interpreted as hexadecimal values. A formatted key string is a string that should be translated before being encapsulated in the packet. A formatted key string can be contained both ASCII strings and hexadecimal values. For example, "%" + "\$"+"1~32"+ "keyword"+ ":": % - Indicates that the string that follows this character is a formatted key string. "\$" or "0" - (Optional) Indicates a fill indicator. This option specifies how to fill the formatted key string to meet the length option. This option can be either "\$" or "0", and cannot be specified as both at the same time. "\$" - Indicates to fill the leading space (0x20). "0" - Indicates to fill the leading 0. The fill the 		
	 leading 0 (0) is the default setting. 1~32 - (Optional) Indicates a length option. This specifies how many characters or bytes the translated key string should occupy. If the actual length of the translated key string is less than the length specified by this option, a fill indicator will be used to fill it. Otherwise, this length option and fill indicator will be ignored and the actual string will be used directly. 		
	 keyword - Indicates that the keyword will be translated based on the actual value of the system. The following keyword definitions specifies that a command will be refused if an unknown or unsupported keyword is detected: 		
	 devtype - The model name of the device. Only an ASCII string is allowed. 		
	 sysname - Indicates the System name of the Switch. Only an ASCII string is allowed. 		
	 ifdescr - Derived from <i>ifDescr</i> (IF-MIB). Only an ASCII string is allowed. 		
	 portmac - Indicates the MAC address of a port. This can be either an ASCII string or a hexadecimal value. When in the format of an ASCII string, the MAC address format can be customized using special CLI commands. When in the format of a hexadecimal value, the MAC 		

Parameter	Description
	address will be encapsulated in order in hexadecimal.
	 sysmac - Indicates the system MAC address. This can be either an ASCII string or a hexadecimal value. In the ASCII string format, the MAC address format can be customized using special CLI commands. In the hexadecimal format, the MAC address will be encapsulated in order in hexadecimal.
	 unit - Indicates the unit ID. This can be either an ASCII string or a hexadecimal value. For a standalone device, the unit ID is 0.
	 module - Indicates the module ID number. This can be either an ASCII string or a hexadecimal value.
	 port - Indicates the local port number. This can be either an ASCII string or a hexadecimal value.
	 svlan - Indicates the outer VLAN ID. This can be either an ASCII string or a hexadecimal value.
	 cvlan - Indicates the inner VLAN ID. This can be either an ASCII string or a hexadecimal value.
	 : - Indicates the end of the formatted key sting. If a formatted key string is the last parameter of the command, its ending character (":") can be ignored. The space (0x20) between "%" and ":" will be ignored. Other spaces will be encapsulated.
	 ASCII strings can be any combination of formatted key strings and 0~9, a~z, A~Z, !@#\$%^&*()_+ -=\[]{}::"/?.,<>`, and space characters. "\" is the escape character. The special character after "\" is the character itself, for example, "\%" is "%" itself, not the start indicator of a formatted key string. Spaces not in the formatted key string will also be encapsulated. Hexadecimal values can be any combination of formatted key strings and 0~9, A~F, a~f, and space characters. The formatted key strings only support keywords that support hexadecimal values. Spaces not in the formatted key string will be ignored.

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

Click the **Delete** button to delete the specified entry.

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

DHCP Local Relay VLAN

This window is used to configure local relay on a VLAN or a group of VLANs.

To view the following window, click **Management > DHCP > DHCP Relay > DHCP Local Relay VLAN**, as shown below:

Diffic Local Hanry VLAP	80				
THE ALL GEAL WHAT WE CAN SAFER	85-1				
DECKS PALADA AND INC.	111	E ADDIASE	20.10	Costed	600.0
DECPLANERUS VIDUM	34 				

Figure 4-53 DHCP Local Relay VLAN Window

The fields that can be configured are described below:

Parameter	Description
DHCP Local Relay VID List	Enter the VLAN ID for DHCP local relay. Tick the All VLANs check box to select all VLANs.
State	Select this option to enable or disable the DHCP local relay on the specific VLAN(s).

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

DHCPv6 Relay

DHCPv6 Relay Global Settings

This window is used to configure the DHCPv6 relay remote ID.

To view the following window, click **Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Global Settings**, as shown below:

DERCEVE Relay Ginted Settings			
DHCPv5 Galay Global Sebbigs			
Period in the House Disard	Default in	<u>[x]</u>	
Pestid-Children Dynamic D UDP	14.01	See Like a se	
Pestillion fails five all Diraky	Keep		
Pv6 DHCP Relay Renate ID Option	Disabled		- 49. dy

Figure 4-54 DHCPv6 Relay Global Settings Window

The fields that can be configured are described below:

Parameter	Description
IPv6 DHCP Relay Remote ID Format	Select to choose the sub-type of the remote ID. Options to choose from are Default , CID With User Define , and User Define .
IPv6 DHCP Relay Remote ID UDF	Select to choose the User Define Field (UDF) for remote ID. Options to choose from are:
	 ASCII - Select to enter the ASCII string with a maximum of 128 characters in the text box. HEX - Select to enter the hexadecimal string with a maximum of 256 characters in the text box.
IPv6 DHCP Relay Remote ID Policy	Select to choose Option 37 forwarding policy for the DHCPv6 relay agent. Options to choose from are:

Parameter	Description		
	 Keep - Select to discard the packet that already has the relay agent Remote-ID Option 37. Drop - Select that the DHCPv6 request packet that already has the relay agent Remote-ID option is left unchanged and directly relayed to the DHCPv6 server. 		
IPv6 DHCP Relay Remote ID Option	Select this option to enable or disable the insertion of the relay agent remote ID Option 37 during the relay of DHCP for IPv6 request packets.		

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

DHCPv6 Relay Interface Settings

This window is used to configure and display the DHCPv6 relay interface settings.

To view the following window, click **Management > DHCP > DHCPv6 Relay > DHCPv6 Relay** Interface Settings, as shown below:

E Jan Linday Interdana Antonga				
(FILE) AN AN AN AN AN AN		1		
Manatan i Kalikan kaninar	14.44			
Experimentation of AM (1-1 (H))				28.9
a tao WARDHXO	34	H.		Constanting
otal English 4			117	10
e Velopi		The strengthene in the Avenueses	Despertmentary	i
14.41		012 11	Z	

Figure 4-55 DHCPv6 Relay Interface Settings Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the VLAN from 1 to 4094 for DHCPv6 relay.
Destination IPv6 Address	Enter the DHCPv6 relay destination address.
Output Interface VLAN	Enter the output interface for the relay destination.

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 **Delete** button to remove the specified entry.

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

DHCP Auto Configuration

This window is used to configure the DHCP auto-configuration function.

To view the following window, click **Management > DHCP > DHCP Auto Configuration**, as shown below:



Figure 4-56 DHCP Auto Configuration Window

The fields that can be configured are described below:

Parameter	Description
Auto Configuration State	Select this option to enable or disable the auto-configuration function.

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

DNS

Computer users usually prefer to use text names for computers for which they may want to open a connection. Computers themselves, require 32-bit IP addresses. Somewhere, a database of network devices' text names and their corresponding IP addresses must be maintained.

The Domain Name System (DNS) is used to map names to IP addresses throughout the Internet and has been adapted for use within intranets. For two DNS servers to communicate across different subnets, the DNS Relay of the Switch must be used. The DNS servers are identified by IP addresses.

Mapping Domain Names to Addresses

Name-to-address translation is performed by a program called a Name server. The client program is called a Name resolver. A Name resolver may need to contact several Name servers to translate a name to an address.

The Domain Name System (DNS) servers are organized in a somewhat hierarchical fashion. A single server often holds names for a single network, which is connected to a root DNS server - usually maintained by an ISP.

Domain Name Resolution

The domain name system can be used by contacting the name servers one at a time, or by asking the domain name system to do the complete name translation. The client makes a query containing the name, the type of answer required, and a code specifying whether the domain name system should do the entire name translation, or simply return the address of the next DNS server if the server receiving the query cannot resolve the name.

When a DNS server receives a query, it checks to see if the name is in its sub domain. If it is, the server translates the name and appends the answer to the query, and sends it back to the client. If the DNS server cannot translate the name, it determines what type of name resolution the client requested. A complete translation is called recursive resolution. This requires the server to contact

other DNS servers until the name is resolved. Iterative resolution specifies that if the DNS server cannot supply an answer, it will return the address of the next DNS server the client contacted.

Each client must be able to contact at least one DNS server, and each DNS server must be able to contact at least one root server.

The address of the machine that supplies domain name service is often supplied by a DHCP or BOOTP server, or can be entered manually and configured into the operating system at startup.

DNS Global Settings

This window is used to configure the DNS global settings.

To view the following window, click Management > DNS > DNS Global Settings, as shown below:

8 m/s.

Figure 4-57 DNS Global Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Domain Lookup	Select this option to enable or disable the DNS to carry out the domain name resolution.
IP Name Server Timeout Enter the maximum time to wait for a response from a spec name server. This value is between 1 and 60 seconds.	

Click the Apply button to accept the changes made.

DNS Name Server Settings

This window is used to configure and display the IP address of a domain name server.

To view the following window, click **Management > DNS > DNS Name Server Settings**, as shown below:

348 Name Server Selange			
IRIN RAIPA SISTAN AVENUE -			
k status service level			
n same sector ave	2.40.0		ke v
Lines Ferring 2			
Hend Sana			
100,130,5 101		Di sir	
5101.5.2		die wie	

Figure 4-58 DNS Name Server Settings Window

The fields that can be configured are described below:

Parameter	Description
Name Server IPv4	Select and enter the IPv4 address of the DNS server.
Name Server IPv6	Select and enter the IPv6 address of the DNS server.

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

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

DNS Host Settings

This window is used to configure the static mapping entry for the host name and the IP address in the host table.

To view the following window, click **Management > DNS > DNS Host Settings**, as shown below:

dang Host somegi				
ena salan Reference Reference	(35) w.e. [2040.1			
	Illion banas	ProProvidence	AgingTime	1
filolo: Toloi finance: 1 Dysamie: Totol Energie: 5	2007 Annas 2007 Annas	275.2760.1319.00 175.197.6.700	Ag og Tires Bisto	

Figure 4-59 DNS Host Settings Window

The fields that can be configured are described below:

Parameter	Description
Host Name	Enter the host name of the equipment.
IP Address	Select and enter the IPv4 address of the equipment.
IPv6 Address	Select and enter the IPv6 address of the equipment.

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

NTP

NTP Global Settings

This window is used to view and configure the Network Time Protocol (NTP) global settings.

To view the following window, click **Management > NTP > NTP Global Settings**, as shown below:

NTP-Sachel Settinge		
NTP lease NTT Glale	Danked & Dealers	Apply
NTF Authoritoution State An Principals days State Nutrification January	S-Franked COmmen	<u> 60%</u>
ATT Upper Orientes	Danks @ Date:	1
ATP Schema N + Marko Schema 1 (n) N + Marko Schema (r 14)	ad 100000	

Figure 4-60 NTP Global Settings Window

The fields that can be configured for NTP State are described below:

Parameter	Description
NTP State	Select the NTP feature's global state here. Options to choose from are Enabled and Disabled .

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

The fields that can be configured for NTP Authentication State are described below:

Parameter	Description
NTP Authentication State	Select the NTP feature's authentication state here. Options to choose from are Enabled and Disabled .

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

The fields that can be configured for **NTP Update Calendar** are described below:

Parameter	Description
NTP Update Calendar	Select the NTP feature's update calendar state here. Options to choose from are Enabled and Disabled .

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

The fields that can be configured for NTP Settings are described below:

Parameter	Description
NTP Master Stratum	Enter the NTP master stratum value here. This value must be between 1 and 15. Select the Default option to use the default value.
NTP Max Associations	Enter the NTP maximum amount of associations here. This value must be between 1 and 64.

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

NTP Server Settings

This window is used to view and configure the NTP server's settings.

To view the following window, click **Management > NTP > NTP Server Settings**, as shown below:

(IP Server Settings						
a) H avinar swang k						
j e Fieldoma		()PRActor	227	a 📃		
HARON (P-1)	· 1	NO MICTION				
Mar Pratics (19)	- F	$\hat{\mathbf{k}} = 2\pi i (\mathbf{k}, \mathbf{k})$	115			
Taria.	[Div. 7]					1 1 1 m 1 m 1 m
ICHER WITH A						
HTP Server	antika	40 <u>4</u> D	нин	MIN PO I	Mark Pér I	
10:00:00.122	+	10 00	F.da.	1.45	- 60 L	1.50 00.000
					33	

Figure 4-61 NTP Server Settings Window

Parameter	Description
IP Address	Select and enter the NTP server's IPv4 address here.
IPv6 Address	Select and enter the NTP server's IPv6 address here.
Version	Enter the NTP server's version number here. This value must be between 1 and 4.
Key ID	Enter the authentication key ID here. This ID must be between 1 and 255.
Min Poll	Enter the minimum poll intervals for NTP messages here. This value must be between 3 and 16 seconds.
Max Poll	Enter the maximum poll intervals for NTP messages here. This value must be between 4 and 17 seconds.
Prefer	Select whether this server is the preferred server in the list or not. Options to choose from are True and False .

The fields that can be configured are described below:

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

NTP Peer Settings

This window is used to view and configure the NTP peer settings.

To view the following window, click **Management > NTP > NTP Peer Settings**, as shown below:

n waaroomoge						
e Trédeline .		0.0644	ethi	2215.3		
MARCH (P-1)		No Meri	5. E			
a salat in	- 1 A	ine setu	17)	<u></u>		
*'8	Dive 7	5 1970.003 1				0.549
COLUMN TAX		•				
ale Her	Varie of	Nay at	Prime	lato Pos	Later Ave	1
000.002		10	Taby	6	- 19	1.50 0.500

Figure 4-62 NTP Peer Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Select and enter the NTP peer's IPv4 address here.
IPv6 Address	Select and enter the NTP peer's IPv6 address here.
Version	Enter the NTP peer's version number here. This value must be between 1 and 4.
Key ID	Enter the authentication key ID here. This ID must be between 1 and 255.
Min Poll	Enter the minimum poll intervals for NTP messages here. This value must be between 3 and 16 seconds.
Max Poll	Enter the maximum poll intervals for NTP messages here. This value must be between 4 and 17 seconds.
Prefer	Select whether this peer is the preferred peer in the list or not. Options to choose from are True and False .

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

NTP Access Group Settings

This window is used to view and configure the NTP access group settings.

To view the following window, click **Management > NTP > NTP Access Group Settings**, as shown below:

NII ⁴ Access Group Settings		
non av row out to country		
(a Colori		
Qie Akkes	Holy A	
Othe outers 200 I	Philippine -	
Ligina Lindow LikeTest Liverka Libera		- 20%
Some Franke: 1		
NIT OCCURATION	+ 40	Harrison and the second
344	the Mostly Sectory	
1		



Parameter Description Default Select this option to specify that a default entry (address 0.0.0.0, mask 0.0.0.0) will always be included and is the lowest priority in the list. **IP Address** Select and enter the IPv4 address of the host or network here. Netmask Select and enter the IPv4 network mask of the host or network here. **IPv6 Address** Select and enter the IPv6 address of the host or network here. IPv6 Mask Select and enter the IPv6 network mask of the host or network here. lanore Select this option to ignore all NTP related packets. No Serve Select this option to deny all NTP related packets, except for NTP control queries. No Trust Select this option to deny all NTP related packets that are not cryptographically authenticated. Version Select this option to deny all NTP related packets that don't match the current NTP version. No Peer Select this option to deny all NTP related packets that might mobilize an association unless authenticated. Select this option to deny all NTP control queries. No Query No Modify Select this option to deny NTP control gueries that attempted to modify the state of the server.

The fields that can be configured are described below:

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

NTP Key Settings

This window is used to view and configure the NTP key settings.

To view the following window, click **Management > NTP > NTP Key Settings**, as shown below:

111: Key Settinge				_
ATP Control Key				
5 1 (0 x 9 d Ser 0 255)		all set		4pphy.
ете наурная кор				
STP Recard Key (1-255)		-dhara		yeqs
O'Res Stors				
Sec. 6 (1925)				
NCS	2 den			1. 66.66
Texa Farries: 1				
Traulesi Key	· Ken Ki	Kay Type	Value	
	1	M05	ANALYSKATA ALARMATIKA ALARMATIKA	Caldo
			33	

Figure 4-64 NTP Key Settings Window

The fields that can be configured for NTP Control Key are described below:

Parameter	Description
NTP Control Key	Enter the NTP control key here. This key must be between 1 and 255. Select the None option not to use an NTP control key.

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

The fields that can be configured for NTP Request Key are described below:

Parameter	Description
NTP Request Key	Enter the NTP request key here. This key must be between 1 and 255. Select the None option not to use an NTP request key.

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

The fields that can be configured for NTP Key Settings are described below:

Parameter	Description
Key ID	Enter the NTP key number here. This authentication key number must be between 1 and 255.
MD5	Enter the MD5 NTP key here. This key can be up to 32 characters long.

Click the Apply button to accept the changes made.

NTP Interface Settings

This window is used to view and configure the NTP interface settings.

To view the following window, click **Management > NTP > NTP Interface Settings**, as shown below:

TP Interface Settings		
ITP interface Settings		
Total Fundas: 1		
index texter blande	NUP State	
40411	FIND M	F.E.

Figure 4-65 NTP Interface Settings Window

The fields that can be configured are described below:

Parameter	Description
NTP State	After click the Edit button, select the NTP feature's state on the interface specified. Options to choose from are Enabled and Disabled .

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

NTP Associations

This window is used to view a list of NTP associations.

To view the following window, click **Management > NTP > NTP Associations**, as shown below:

0.5.7								
Real Province	linet	and a state of the second	191	Bejert	K. deg (t den t	Regission	
29110-10-76m	11(n)	. N.	10	1	(0.00.0)	0.00.000	110.0	Control 1
10000	2()E ((64)	1.1	(D, Θ, Ω)	I G G ((1010)	1.473
						111	10	Г

Figure 4-66 NTP Associations Window

Click the **Detail** button, next to the specified entry, to view more information about the NTP association, as shown below:

A Harscardoni			
adhar			
Renote	-0.80.605	Liss	6.8.00
N THE .	(April 2 march	Parameter	(rapie)
58,811		Certaky.	£
ung .	71	forms.	1900
Planting and a	1 = 4	No. With the radius	1.2.2.1
7Tal	×	lins -	
e e contra de la c	36.5	(Welling)	19 Acc.
ting Ba	B156	Prior.	696.
Lander	-4	Cour.	0-S1A
100	# 10.90 Z A	100 C	C= ()
Saliverse The	REDCORDE DECEMBER THAT FROM THE	Orbitale Theodores	CONDECIDE REPORTED THE THE T
Harrison Long song	2.8.8.6.8.6.8.10(-201)	Include the territory	LEGRER ER AL MET
Harrier Inersone Mille Della	Electronic - o posicial - il relicent -	From d.Sa	é écenne le sécelle, inclinair
Ene Doer	2, 2, 3, 4, 2, 2, 1, 4	Officer	C SCIECK
(integra	2 · # · # ·	False Parisa	1881
Tita Dia	100000		

Figure 4-67 NTP Associations (Detail) Window

NTP Status

This window is used to view NTP status information.

To view the following window, click **Management > NTP > NTP Status**, as shown below:

	HTP SUID.
La ep Indicator	Unavyrichte siz wei
Statum	11
Frectsion	4
Red Distance	v C0000.0
Roof Disperation	τ C0000.0
Reference D	(STCP)
Surface and There	00000000.000000000 The FW9 7 2006 6 23 16:00000
System Dugy	Henter HTP Kennel State
.lw	0.0003006 a
Slavelley	0.000 ppm
Auth Deby	0.000000 3

Figure 4-68 NTP Status Window

IP Source Interface

This window is used to configure the IP source interface settings.

To view the following window, click **Management > IP Source Interface**, as shown below:

and the second			
·	VID (2-4054)	1	
		00 1 V0.2-4040	VI 1 VID21424

Figure 4-69 IP Source Interface Window

The fields that can be configured are described below:

Parameter	Description
Source Interface State	Select to Enable or Disable the source interface feature's global state here.
Interface Type	After enabling the Source Interface State option, select the interface type here. The only option available is VLAN .
VID (1-4094)	After selecting the VLAN as the Interface Type , enter the VLAN ID used here. This value must be between 1 and 4094.

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

File System

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 (FFS) 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.

File System				
1158	:			
Partit	6			Ce (
Cape	l			
Dries	Madia Type	Sim (MI)	File System Type	Label
10. 10.	Piede -	27	PPS	

To view this window, click **Management > File System** as shown below:

Figure 4-70 File System Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Path	Enter the path string

Click the **Go** button to navigate to the path entered.

Click the <u>c:</u> hyperlink to navigate the C: drive.

After clicking the c: hyperlink, the following window will appear:

•• <u>•</u> ∧•• <u>∧</u>							<u> </u>	
1.19	-	Seeda	throay T	2425				
1.00	k fe	Alt	5 a intel	Lipówe Times	Han	120 11		
	D-H	-	826030	Jan Et 2000 00000 22	Fauri 70.00 heri	dass op-	MAGE	200 Mile 1
2	30571	175	0252404	Jun 11 2000 10008 00	Panel 70 000 had	2001 op	NUMBER	241303
2	0007	100	1534	Aur 11 2800 10/12/06	chill, a fa	Joes Vp	Kenere .	04.035
		14	1	A # 12 2000 P000 82	mAn.		- Selete	

Figure 4-71 File System - Search for Drive Window

Click the **Previous** button to return to the previous window.

Click the Create Directory button 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 **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.

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

eut.	<u>i</u>	9			
98	e.			<u></u>	
den min					
an and the	9 11 1-1-1-1	startup coning in a	1520071		
entorus II		nen ny-saris	Brook of L	E Sapara	

Figure 4-72 File System - Copy Window

When copying a file to the file system of this switch, the user must enter the **Source** and **Destination** path. Tick the **Replace** check box to replace the current running configuration with the indicated configuration file.

Click the **Apply** button to initiate the copy.

Click the Cancel button the discard the process.

Physical Stacking

The Switch supports switch stacking, where a set of six switches can be combined and managed by one IP address through Telnet, the Web UI, the RJ45 console port, or through SNMP. Each switch of this series has two stacking ports located at the front of the device, which can be used to connect other devices and make them stack together. After adding these stacking ports, the user may connect

these ports together using fiber cables or Direct Attach Cables (DAC) in one of two possible topologies.

- **Duplex Chain** -The Duplex Chain topology stacks switches together in a chain-link format. Using this method, data transfer is only possible in one direction and if there is a break in the chain, then data transfer will obviously be affected.
- **Duplex Ring** -The Duplex Ring stacks switches in a ring or circle format where data can be transferred in two directions. This topology is very resilient because if there is a break in the ring, data can still be transferred through the stacking cables between switches in the stack.

Figure 4-73 Switches stacked in a Duplex Chain



Figure 4-74 Switches stacked in a Duplex Ring

Within each of these topologies, each switch plays a role in the Switch stack. These roles can be set by the user per individual Switch, or if desired, can be automatically determined by the Switch stack. Three possible roles exist when stacking with the Switch.

Primary Master - The Primary Master is the leader of the stack. It will maintain normal operations, monitor operations and the running topology of the Stack. This switch will also assign Stack Unit IDs, synchronize configurations, and transmit commands to remaining switches in the switch stack. The Primary Master can be configured manually by assigning the Switch the highest priority (a lower number denotes a higher priority) before physically assembling the stack or it can be determined automatically, by the stack, through an election process which determines the lowest MAC address and will assign that switch as the Primary Master, if all priorities are the same. The Primary master are physically displayed by the seven segment LED to the far right on the front panel of the switch where this LED will flash between its given Box ID and 'H'.

Backup Master - The Backup Master is the backup to the Primary Master, and will take over the functions of the Primary Master if the Primary Master fails or is removed from the Stack. It also monitors the status of neighboring switches in the stack, will perform commands assigned to it by the Primary Master and will monitor the running status of the Primary Master. The Backup Master can be set by the user by assigning this Switch the second highest priority before physically assembling the stack, or it can be determined automatically by the stack through an election process that determines the second lowest MAC address and then will assign that switch as the Backup Master, if all priorities are the same. The Backup master are physically displayed by the seven segment LED to the far right on the front panel of the switch where this LED will flash between its given Box ID and 'h'.

Slave - Slave switches constitute the rest of the switch stack and although not Primary or Backup Masters, they can be placed into these roles when these other two roles fail or are removed from the stack. Slave switches perform operations requested by the master, monitor the status of neighbor switches in the stack and the stack topology, and adhere to the Backup Master's commands once it becomes a Primary Master. Slave switches will do a self-check to determine if it is to become the Backup Master if the Backup Master is promoted to the Primary Master, or if the Backup Master fails or is removed from the switch stack. If both Primary and Backup masters fail, or are removed from the Switch stack, it will determine if it is to become the Primary Master. These roles will be determined, first by priority and if the priority is the same, the lowest MAC address.

Once switches have been assembled in the topology desired by the user and powered on, the stack will undergo three processes until it reaches a functioning state.

Initialization State - This is the first state of the stack, where the runtime codes are set and initialized and the system conducts a peripheral diagnosis to determine each individual switch is functioning properly.

Master Election State - Once the codes are loaded and initialized, the stack will undergo the Master Election State where it will discover the type of topology used, elect a Primary Master and then a Backup Master.

Synchronization State - Once the Primary Master and the Backup Master have been established, the Primary Master will assign Stacking Unit IDs to switches in the stack, synchronize configurations for all switches and then transmit commands to the rest of the switches based on the users configurations of the Primary Master.

Once these steps have been completed, the switch stack will enter a normal operating mode.

Stack Switch Swapping

The stacking feature of the Switch supports "hot swapping" of switches in and out of the running stack. Users may remove or add switches to the stack without powering down or largely affecting the transfer of data between switches in the stack, with a few minor provisions.

When switches are "hot inserted" into the running stack, the new switch may take on the Primary Master, Backup Master or Slave role, depending on configurations set on the newly added switch, such as configured priority or MAC address. Yet, if adding two stacks together that have both previously undergone the election process, and therefore both have a Primary Master and a Backup master, a new Primary Master will be elected from one of the already existing Primary Masters, based on priority or MAC address. This Primary Master will take over all of the Primary Master's roles for all new switches that were hot inserted. This process is done using discovery packets that circulate through the switch stack every 1.5 seconds until the discovery process has been completed.

The "hot remove" action means removing a device from the stack while the stack is still running. The hot removal is detected by the stack when it fails to receive heartbeat packets during its specified interval from a device, or when one of the stacking ports links is down. Once the device has been removed, the remaining switches will update their stacking topology database to reflect the change. Any one of the three roles, Primary Master, Backup Master, or Slave, may be removed from the stack, yet different processes occur for each specific device removal.

If a Slave device has been removed, the Primary Master will inform other switches of the hot remove of this device through the use of unit leave messages. Switches in the stack will clear the configurations of the unit removed. Dynamically learned databases, such as ARP, will also be cleared.

If the Backup Master has been hot removed, a new Backup Master will be chosen through the election process previously described. Switches in the stack will clear the configurations of the unit removed. Dynamically learned databases, such as ARP, will also be cleared. Then the Backup Master will begin backing up the Primary Master when the database synchronization has been completed by the stack.

If the Primary Master is removed, the Backup Master will assume the Primary Master's role and a new Backup Master will be chosen using the election process. Switches in the stack will clear the configurations of the unit removed. Dynamically learned databases, such as ARP, will also be cleared. The new Primary Master will inherit the MAC and IP address of the previous Primary Master to avoid conflict within the stack and the network itself.

If both the Primary Master and the Backup Master are removed, the election process is immediately processed, and a new Primary Master and Backup Master are determined. Switches in the stack will clear the configurations of the units removed, and dynamically learned databases, such as ARP, will be cleared as well. Static switch configurations still remain in the database of the remaining switches in the stack and those functions will not be affected.



NOTE: If there is a Box ID conflict when the stack is in the discovery phase, the device will enter a special standalone topology mode. Users can only get device information, configure Box IDs, save and reboot. All stacking ports will be disabled and an error message will be produced on the local console port of each device in the stack. Users must reconfigure Box IDs and reboot the stack.

	enen							
Shudking M	K.N.	g, Hand	Store .	4 90				300k
stantin.	id .	ig reach		8				*20 ⁴
Ing Stat		$\{(\cdot,\cdot)\} \in \mathcal{H}(\mathcal{A}(\mathbb{R}))$	30 12 (A)	8				
ere al la companya								
darent ile	nd I		Nes For		Auta 🐱	Priority (1-52)	1	0.45
Texe again International Tex		Duglys_01#1			Mr Dex (D) 3 et generation Dr			
Den Court	E:	i			1995-1990-1990-1990-1990-1990-1990-1990-			
Rein	110.04	, the local black of	harst	during.	100	Petrolesee	the second state and the second state of the s	HWA WARRAN
	Nuby.	1006 1510 DEPAH	and the	32	76 TE 64 A1 82 80	300,018	1 20.095	. A.
10		2011 +2031	7,4		Accession and a second	100 000 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	100000	
		6.91, 62.83	38					
12		N91_F2(8)	30.					
N.								
1000	Diam's I	1001_1001	24. 39			1. A	2	

Figure 4-75 Physical Stacking Window

The fields that can be configured for **Physical Stacking** are described below:

Parameter	Description
Stacking Mode	Select this option to enable or disable the stacking mode.
Stack Preempt	Select this option to enable or disable preemption of the master role to come into play when a unit with a better priority is added to the Switch later.
Trap State	Select this option to enable or disable sending of stacking related traps.

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

I he fields that can be	configured for Stack ID	are described below:

Parameter	Description
Current Unit ID	Select the unit ID of the switch in the stack.
New Box ID	Select the new box ID for the switch that is selected in the Current Unit ID . The user may choose any number between 1 and 6 to identify the switch in the switch stack. Auto will automatically assign a box number to the switch in the switch stack.
Priority	Enter the priority of the Switch stacking unit. The range is from 1 to 63.

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

Virtual Stacking (SIM)

D-Link Single IP Management (SIM) is a concept that will stack switches together over Ethernet instead of using stacking ports or modules. There are some advantages in implementing the Single IP Management feature:

- SIM can simplify management of small workgroups or wiring closets while scaling the network to handle increased bandwidth demand.
- SIM can reduce the number of IP address needed in your network.

• SIM can eliminate any specialized cables for stacking connectivity and remove the distance barriers that typically limit your topology options when using other stacking technology.

Switches using D-Link Single IP Management (labeled here as SIM) must conform to the following rules:

- SIM is an optional feature on the Switch and can easily be enabled or disabled through the Command Line Interface or Web Interface. SIM grouping has no effect on the normal operation of the Switch in the user's network.
- There are three classifications for switches using SIM. The Commander Switch (CS), which is the master switch of the group, Member Switch (MS), which is a switch that is recognized by the CS a member of a SIM group, and a Candidate Switch (CaS), which is a Switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.
- A SIM group can only have one Commander Switch (CS).
- A SIM group accepts up to 32 switches (numbered 1-32), not including the Commander Switch (numbered 0).
- Members of a SIM group cannot cross a router.
- There is no limit to the number of SIM groups in the same IP subnet (broadcast domain); however, a single switch can only belong to one group.
- If multiple VLANs are configured, the SIM group will only utilize the management VLAN on any switch.
- SIM allows intermediate devices that do not support SIM. This enables the user to manage switches that are more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. The Switch may take on three different roles:

- **Commander Switch (CS)** This is a switch that has been manually configured as the controlling device for a group, and takes on the following characteristics:
 - It has an IP Address.
 - It is not a command switch or member switch of another Single IP group.
 - It is connected to the member switches through its management VLAN.
- **Member Switch (MS)** This is a switch that has joined a single IP group and is accessible from the CS, and it takes on the following characteristics:
 - It is not a CS or MS of another IP group.
 - It is connected to the CS through the CS management VLAN.
- **Candidate Switch (CaS)** This is a switch that is ready to join a SIM group but is not yet a member of the SIM group. The Candidate Switch may join the SIM group of the Switch by manually configuring it to be a MS of a SIM group. A switch configured as a CaS is not a member of a SIM group and will take on the following characteristics:
 - It is not a CS or MS of another Single IP group.
 - It is connected to the CS through the CS management VLAN

The following rules also apply to the above roles:

- Each device begins in a Candidate state.
- A CS must change its role to CaS and then to MS, to become a MS of a SIM group. Thus, the CS cannot directly be converted to a MS.
- The user can manually configure a CS to become a CaS.
- A MS can become a CaS by:
 - Being configured as a CaS through the CS.
 - If report packets from the CS to the MS time out.
- The user can manually configure a CaS to become a CS
- The CaS can be configured through the CS to become a MS.

After configuring one switch to operate as the CS of a SIM group, additional DGS-1510 Series switches may join the group by manually configuring the Switch to be a MS. The CS will then serve as the in band entry point for access to the MS. The CS's IP address will become the path to all MS's of the group and the CS's Administrator's password, and/or authentication will control access to all MS's of the SIM group.

With SIM enabled, the applications in the CS will redirect the packet instead of executing the packets. The applications will decode the packet from the administrator, modify some data, and then send it to the MS. After execution, the CS may receive a response packet from the MS, which it will encode and send it back to the administrator.

When a CaS becomes a MS, it automatically becomes a member of the first SNMP community (includes read/write and read only) to which the CS belongs. However, if a MS has its own IP address, it can belong to SNMP communities to which other switches in the group, including the CS, do not belong.

Upgrade to Version 1.61

To better improve SIM management, the DGS-1510 Series switches have been upgraded to version 1.61 in this release. Many improvements have been made, including the Commander Switch (CS) now having the capability to automatically rediscover member switches that have left the SIM group, either through a reboot or web malfunction. This is accomplished through the use of Discover packets and Maintenance packets that previously configured SIM members will send and receive after a reboot. Once a MS has had its MAC address and password saved to the CS's database, if a reboot occurs in the MS, the CS will keep this MS information in its database and when a MS has been rediscovered, it will add the MS back into the SIM tree automatically. No configuration will be necessary to rediscover these switches.

There are some instances where pre-saved MS Switches cannot be rediscovered. For example, if the Switch is still powered down, if it has become the member of another group, or if it has been configured to be a Commander Switch, the rediscovery process cannot occur.

The topology map now includes new features for connections that are a member of a port trunking group. It will display the speed and number of Ethernet connections creating this port trunk group.

- Firmware The switch now supports MS firmware downloads from a TFTP server.
- **Configuration Files** This switch now supports downloading and uploading of configuration files both to (for configuration restoration) and from (for configuration backup) MS's, using a TFTP server.
- Log The Switch now supports uploading MS log files to a TFTP server.

The user may zoom in and zoom out when utilizing the topology window to get a better, more defined view of the configurations.

Single IP Settings

This window is used to configure the SIM settings. The Switch is set as a Candidate (CaS) as the factory default configuration and Single IP Management is disabled.

To view the following window, click **Management > Virtual Stacking (SIM) > Single IP Settings**, as shown below:

Single IP Settings		
SIN Such Configure		
Sec entry	Lasted <u>in</u>	Apole
99 hale Challana		
Pole Core	Credites 💌	
Crosp Harra	josz.	ngoh.
an wengi		
The Sala	Capted TV	
14.5.4(3)/RI	30 Vet	
Hold (1997) 00 2501	lot un	
Paralactics, SILPHOL 49,41		. Apply

Figure 4-76 Single IP Settings Window

The fields that can be configured for SIM State Configure are described below:

Parameter	Description
SIM State	Select this option to enable or disable the SIM state on the Switch. Select Disabled to render all SIM functions on the Switch inoperable.

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

Parameter	Description
Role State	Select to change the SIM role of the Switch. Options to choose from are:
	 Candidate - A Candidate Switch (CaS) is not the member of a SIM group but is connected to a Commander Switch. This is the default setting for the SIM role of the Switch. Commander - Select to make the Switch a Commander Switch (CS). The user may join other switches to this Switch, over Ethernet, to be part of its SIM group. Choosing this option will also enable the Switch to be configured for SIM.
Group Name	Enter a group name. This is optional. This name is used to segment switches into different SIM groups.

The fields that can be configured for **SIM Role Configure** are described below:

Click the $\ensuremath{\textbf{Apply}}$ button to accept the changes made.

The fields that can be configured for **SIM Settings** are described below:

Parameter	Description
Traps State	Select to enable or disable the SIM trap state.
Interval	Enter the interval in seconds. The range is from 30 to 90.
Hold Time	Enter the hold-time in seconds. The range is from 100 to255.
Parameter	Description
-----------------	---
Management VLAN	Enter the single IP management message VLAN ID.

After enabling the Switch to be a Commander Switch (CS), the **Single IP Management** folder will then contain four added links to aid the user in configuring SIM through the web, including **Topology**, **Firmware Upgrade**, **Configuration Backup/Restore**, and **Upload Log File**.

Topology

This window is used to configure and manage the Switch within the SIM group.

To view the following window, click **Management > Virtual Stacking (SIM) > Topology**, as shown below:

Claster I	Cevice Manee	Local Port	Speed	Remote Port	MAC: Address	Nodel Name
	Ratio	-	-		IS PERALITIES	DOS-1810/2004
👙 seen	Mandah	w.	Objected Frail	2	00 16 04 62 10 FO	LOUIS TO TO ACCOUNT
Syraen Syraen	SWEET	2	segara e i an	3	0-70-10-10-001-0	LIGIS NOT BEACH
Anna 1						
Carlower a						

Figure 4-77 Topology Window

There is a menu bar at the top of the window containing File, Group, Device, View, and Help.

File

Print Topology

On the **File** menu, select **Print Topology** to print the SIM topology map to any of the printers configured on the PC accessing the Web UI.

Preference

On the File menu, select Preference to configure the display properties for the SIM topology map.

	1 and 1	
Interval (10-300)	20	
Show All	O Show !	lember Only
	UK.	Cancel

Figure 4-78 Preference

The fields that can be configured are described below:

Parameter	Description
Interval	Enter the SIM topology display refresh interval value here. The range is from 10 to 300.
Show All	Select this option to display all available SIM devices in the topology.
Show Member Only	Select this option to only display SIM member devices in the topology.

Click the \mathbf{OK} button to accept the changes made.

Click the **Cancel** button to discard the changes made.

Group

Add to Group

Select a Candidate Switch (CaS) from the list and then select **Add to Group** on the **Group** menu to add the selected CaS to the SIM group. Password authentication is required when a CaS is added to the SIM group.

assword			
and and a second	-		
	Apply	Cancel	

Figure 4-79 Add to Group (Input Password)

The fields that can be configured are described below:

Parameter	Description
Password	Enter the password of the CaS.

Click the **Apply** button to add the CaS to the SIM group.

Click the **Cancel** button to discard the addition and return to the Topology window.

Remove from Group

Select a Member Switch (MS) from the list and then select **Remove from Group** on the **Group** menu to remove the selected MS from the SIM group.

Device

Configure

Select a device from the list and then select **Configure** on the **Device** menu to connect to the Web User Interface (if available) on the selected device.

View

Refresh

On the View menu, select Fresh to refresh the items displayed in the page.

Topology

On the View menu, select Topology to view the following:



Figure 4-80 Topology Window

Click the **Zoom In** button enlarge the size of the displayed items. Click the **Zoom Out** button reduce the size of the displayed items. Click the **Save** button to save the display. Click the **Back** button to return to the previous window. This window will display how the devices within the SIM Group connect to other groups and devices. Possible icons on this window are as follows:

lcon	Description	lcon	Description
$\langle\!\!\!\!$	Group	*	Layer 3 Member Switch
۲	Layer 2 Commander Switch	87	Member Switch of other group
٢	Layer 3 Commander Switch	١	Layer 2 Candidate Switch
۲	Commander Switch of other group		Layer 3 Candidate Switch
٩	Layer 2 Member Switch	-	Unknown device
\bigcirc	Non-SIM devices		·

<u>Tool Tips</u>

In the Topology view window, the mouse plays an important role in configuration and in viewing device information. Point to a specific device in the Topology window to display more information about the device

Name	Switch	<u> </u>	Name:	Switch	
Concerning and the second s		ywitch			5wi
Model:	DGS-1610-28XMP	a service a	Model:	DGS-1510-52XMP	
MAC.	3C-1E-04-A1-CC-00		MAC:	3C-1E-04-52-10-E0	
Local Port			Local Port:	2	
Remote Por	t		Remote Por	t2	
Port Speed.			Port Speed:	Gigabit-Full	

Figure 4-81 Device Information Utilizing the Tool Tip

Point to a line between two devices to display the connection speed between the two devices.



Figure 4-82 Port Speed Utilizing the Tool Tip

Righ-Click

Right-click a device to allow the user to perform various functions, depending on the role of the Switch in the SIM group and the icon associated with it.

Group	Commander Switch	Member Switch	Candidate Switch
Sel Property	54 Property	Remove from Group Configure Property	Sk: Add to Group Property

The fields that can be configured are described below:

Parameter	Description
Property	Specifies to display more information about the device.
Configure	(Member Switch Only) Specifies to connect to the Web User Interface (if available) on the selected device.
Add to Group	(Candidate Switch Only) Specifies to add the selected CaS to the SIM group. Password authentication is required when a CaS is added to the SIM group.
Remove from Group	(Member Switch Only) Specifies to remove the selected MS from the SIM group.

coperty.		Property		
are:	Switt	Name	Swat	
9787 980:	1759 (a) (Min M	PORCHECTIC CONTRACT	
446	08-(E-04-4/1-06-30	MAC:	00-4E-04-44-00-80	
00.000011		L BORT POR		
La de Ref		Rende Pot.	-	
VelSovel.		Port Speed	-	

Figure 4-83 Group Property

Figure 4-84 Commander Switch Property

Harmen Montoff	Xeedalla DOOS 1991D 900 MP	N ACTION	Swith Look Skite was	
MR2:	30-10-04-52-13-00	NAC:	ro-55-15-5-52-ro	
Local Post:	2	DAMEST.		
Kenera Port	2	RaideRet 1	2.000 C	
Port Speed:	Olgabo Full	Pel Spect	Classifi 7.4	

Figure 4-85 Member Switch Property

Figure 4-86 Candidate Switch Property

The fields displayed are described below:

Parameter	Description
Name	Displays the Device Name of the Switches in the SIM group configured. If the device is not configured with a name, it will be given the name default and tagged with the last six digits of the MAC address to identify it.

DGS-1510 Series Gigabit Ethernet SmartPro Switch Web UI Reference Guide

Parameter	Description
Model	Displays the model name of the Switch.
MAC	Displays the MAC address of the Switch.
Local Port	Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field.
Remote Port	Displays the number of the physical port on the MS or CaS that the CS is connected to. The CS will have no entry in this field.
Port Speed	Displays the connection speed between the CS and the MS or CaS.

Help

About

On the Help menu, select About to display the SIM Copyright information and release date.



Figure 4-87 About Window

Firmware Upgrade

This window is used to upgrade firmware from the Commander Switch to the Member Switch. Member Switches will be listed in the table.

To view the following window, click **Management > Virtual Stacking (SIM) > Firmware Upgrade**, as shown below:

ravan Vigna						
tti Savar P		Selvilleonea				- Condord
and Parkdon 1		19				1/2/4 /1/2/3
na Cristen I	Margarit .	MVC Address	Platform	Hole Time	Plannyas ne Verselars	Device Name

Figure 4-88 Firmware Upgrade Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address.
Path\Filename	Enter the path and file name.

Click the **Download** button to update the firmware.

To specify a certain Switch for firmware download, tick its corresponding check box.

Configuration File Backup/Restore

This window is used to upgrade configuration files from the Commander Switch to the Member Switch using a TFTP server. Member Switches will be listed in the table.

To view the following window, click **Management > Virtual Stacking (SIM) > Configuration File Backup/Restore**, as shown below:

ABARBAR IN	Deckap Tenten					
TE Saver IP		Servicile cons				
					No Done	
al Cristen: I	- 10					
	Manton IC	MVC Address	Fielfara	Liciti Time-	Damys te Versian	Device Name
the second s			100000010-22560	83	140034	

Figure 4-89 Configuration File Backup/Restore Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address.
Path\Filename	Enter the path and file name.

Click the **Restore** button to update the configuration from a TFTP server to the member switch.

Click the **Backup** button to back up the configuration file to a TFTP server.

Upload Log File

This window is used to upload log files from SIM member switches to a specified PC.

To view the following window, click **Management > Virtual Stacking (SIM) > Upload Log File**, as shown below:

kud Log Tim						
nië Server IP	2	Severa and the second				
						Upload
zai Cebien: i	K 11					
	Mantper 10	MVC Address	Platform	tion Time	Dannes te Version	Device Name
10		20/16/04/52 11:01	1006-00°D-022640	31	1.10000年11	Sales
		20 TE 32 42 H EF	1036.1610.62364	33	1.00004	18.0

Figure 4-90 Upload Log File Window

ParameterDescriptionTFTP Server IPEnter the TFTP server IP address.Path\FilenameEnter the path and file name.

The fields that can be configured are described below:

Click the **Upload** button to initiate the file transfer.

D-Link Discovery Protocol

This window is used to configure and display D-Link Discovery Protocol (DDP).

To view the following window, click **Management > D-Link Discovery Protocol**, as shown below:

LE US DATABAN PERSON NGCHERALAN DISC					
la la la Concerna Pratocolità Region Taman	W	анл] ж			
OP Part Settings		MARKER.			
64]) 🔄	hanta, <mark>anist e</mark>	forthe address	161 W	a and a second of	()
Led to Settings	10 6.0				1
	- that			Mark 1	
	10.01			Deutox	
1	10,710	1		114.1	
	(#148)			FACE OF	
	10.000			k noti se	
	e# 100			Enstead	
	42.00			Enders	
	1.8 1007			India	
	14.2008	1		te d'a	
	101110			+ 9/40 ⁻¹ 41	
	FUIC91			Endere.	
	REPORT.			Cristiet	
	161012	1		Dubix	8
	10000 C			takin .	
	1.109/06			10.010	
	mana the			FRADE	

Figure 4-91 D-Link Discovery Protocol Window

The fields that can be configured for **D-Link Discovery Protocol** are described below:

Parameter	Description
D-Link Discovery Protocol State	Select this option to enable or disable DDP global state.
Report Timer	Select the interval in seconds between two consecutive DDP report messages. Options to choose from are 30 , 60 , 90 , 120 , and Never .

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

The fields that can be configured for **DDP Port Settings** are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable DDP port state.

5. Layer 2 Features

FDB VLAN STP ERPS (G.8032) Loopback Detection Link Aggregation L2 Multicast Control LLDP

FDB

Static FDB

Unicast Static FDB

This window is used to view and configure the static unicast forwarding settings on the Switch.

To view the following window, click **L2 Features > FDB > Static FDB > Unicast Static FDB**, as shown below:

san Serie (MB 191 - Al - 194) - AMIG(1	141 VOITANN	MICANNA PERFORMAN	(4.4)
nateriorias: 1		Contraction Contraction Contraction	De ste 48
-11	MINE MATERIAL	197	
14	00-01-07-00-00-00	101.05	2135

Figure 5-1 Unicast Static FDB Window

The fields that can be configured are described below:

Parameter	Description
Port / Drop	Allows the selection of the port number on which the MAC address entered resides. This option could also drop the MAC address from the unicast static FDB. When selecting Port , select the switch unit and port number.
Unit Number	Select the switch unit that will be used for this configuration here, when Port is selected in the previous drop-down list.
Port Number	Select the port number used here, when Port is selected in the previous drop-down list.
VID	Enter the VLAN ID on which the associated unicast MAC address resides.
MAC Address	Enter the MAC address to which packets will be statically forwarded or dropped. This must be a unicast MAC address.

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

Click the **Delete All** button to delete all the entries found in the display table.

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

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

Multicast Static FDB

This window is used to view and configure the multicast static FDB settings.

To view the following window, click L2 Features > FDB > Static FDB > Multicast Static FDB, as shown below:

ikie nao Sirane 700			
ne normi 1 jej jednovi jej	la Mat Alfred Le		rçah.
oral Granies: 1		Luca.	n He All
	M24.5459463	ligner Byre	1 4 C 2 B

Figure 5-2 Multicast Static FDB Window

The fields that can be configured are described below:

Parameter	Description		
Unit	Select the switch unit that will be used for this configuration here.		
From Port / To Port Select the appropriate port range used for the configuration he			
VID Enter the VLAN ID of the VLAN the corresponding MAC add belongs to.			
MAC AddressEnter the static destination MAC address of the multicate This must be a multicast MAC address. The destination address should start with 01. For example, 01-00-00-00			

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

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

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.

MAC Address Table Settings

This window is used to view and configure the MAC address table's global settings.

To view the following window, click L2 Features > FDB > MAC Address Table Settings, as shown below:

MAG Atkiness Lable Settin	H.	
Silonal Sertings	WW. Annual Learning	
Aging Time (0, 10-1000000)	[200 DB	
Agent exercisioner	(reading) schools	Apply

Figure 5-3 MAC Address Table Settings (Global Settings) Window

The fields that can be configured are described below:

Parameter	Description
Aging Time	Enter the MAC address table's aging time value here. This value must be between 10 and 1000000 seconds. Entering 0 will disable MAC address aging. By default, this value is 300 seconds.
Aging Destination Hit	Select to enable or disable the aging destination hit function.

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

After clicking the **MAC Address Learning** tab, at the top of the page, the following page will be available.

Giodol Settinga	MAXC diskinent Lectring	
N KNCKAL	loan en Jonar 🔄 Jacoba 🖂	
in taviage.	0.000	
	IVA	200
	10 G	Dete
	24+ P.	India
	10.000	Paul a
	(W/LB)	+0.6.5
	wski	for sc
	18.00	I tat er
	VE-537	End a
	10.000	Ext.A.
	(Writing)	P1.41 X
	emiesti	+CVLV
	attrainth.	Englise
	s±1042 -	Erst in:
	431040	DAA.
	e le terrete	79.411
	collector -	+1307F

Figure 5-4 MAC Address Table Settings (MAC Address Learning) Window

The fields that can be configured are described below:

Parameter	Description			
Unit Select the switch unit that will be used for this configuration h				
From Port / To Port Select the range of ports that will be used for this cor here.				
State	Select to enable or disable the MAC address learning function on the ports specified here.			

MAC Address Table

This window is used to view the entries listed in the MAC address table.

To view the following window, click L2 Features > FDB > MAC Address Table, as shown below:

1	in abita in		Con Deserve to Park	n w
off-metric			Con Control diss (324)	Rec.
AS PROVIDE	TESS WORLD IN		Okar Synamic by MMC	Pix:
La taba s 4			Cica 4	Sec.4.
ta heles 4 - Mite	MRC Address	ine:		Sev.4.
Conception and the second	MACABANYA Construction	2010		Cev A
Conception and the second		andr. Dylania		Cey A
ta Indus 4 San T I I	24-5-04-50	2010		Cera A



The fields that can be configured are described below:

Parameter	Description	
Port	Select the switch unit and the port that will be used for this configuration here.	
VID	Enter the VLAN ID that will be used for this configuration here.	
MAC Address	Enter the MAC address that will be used for this configuration here.	

Click the **Clear Dynamic by Port** button to clear the dynamic MAC address listed on the corresponding port.

Click the **Clear Dynamic by VLAN** button to clear the dynamic MAC address listed on the corresponding VLAN.

Click the Clear Dynamic by MAC button to clear the dynamic MAC address entered.

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

Click the Clear All button to clear all dynamic MAC addresses.

Click the View All button to display all the MAC addresses recorded in the MAC address table.

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

MAC Notification

This window is used to view and configure MAC notification.

To view the following window, click **L2 Features > FDB > MAC Notification**, as shown below:

NVC Hodification Sector;	200 Soffwater Heavy	
NVC Resiliantion Clobel Ser	131	
MAGA Jerra Neutralia	trd a grante	
66 State 24400 (42)		
He was the print of	1	
NOC Validation TraceStates	Test & glasset	
int through	Jawat Shire Lag	et an diran
1.A. 20100 A	dima: [e] [Unrest]e	d Learniel and
Sector Sector Sector		
artenay	Rad of Logo	Waterward Loop
dhiX4	Canada 2	Ended
2.016.1	Law!	Doubl
10107	Care	11.041
distant.	Trainer.	IT SHEET.
63155	11/2 (6/4	HANNER.
entres.	Canded	Elevent
eni 67	Classified	Dieded
0.076.0	0.4.41	Caki
r star	Com.	D of a l
WARM'S	Tity and	11/3/01
-Mosta+1	United	(Lines)
entro;	Tapted	(Directed)
diff.":	Strended -	Drechd
345704-	0.443	Cashi
6,121.2	Higher.	Of Jone 9

Figure 5-6 MAC Notification (MAC Notification Settings) Window

The fields that can be configured are described below:

Parameter	Description	
MAC Address Notification	Select to enable or disable MAC notification globally on the Switch.	
Interval	Enter the time value between notifications. This value must be between 1 and 2147483647 seconds. By default, this value is 1 second.	
History Size Enter the maximum number of entries listed in the history lo for notification. This value must be between 0 and 500. By o this value is 1.		
MAC Notification Trap State	Select this option to enable or disable the MAC notification trap state.	
Unit	Select the switch unit that will be used for this configuration here.	
From Port / To Port	Select the range of ports that will be used for this configuration here.	
Added Trap	Select this option to enable or disable the added trap for the port(s) selected.	
Removed Trap	Select this option to enable or disable the removed trap for the port(s) selected.	

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

After clicking the MAC Notification History tab, the following page will be available.

MAC Notification			
NAC Notification Settings	MAC Notification Illatory	L	
Total Enhies (0			
History Italies		MAC Discoger Message	

Figure 5-7 MAC Notification (MAC Notification History) Window

A list of MAC notification messages will be displayed.

VLAN

VLAN Configuration Wizard

This window is used to start the VLAN configuration wizard.

Create/Configure VLAN

To view the following window, click **L2 Features > VLAN > VLAN Configuration Wizard**, as shown below:

VLA	4 Configuretion V	fizerd			
PM-08	Configuration Waters				
*	Canada VI AN				
0	VID (1-1094) Overfigure VLAM				
	VID (1-4094)				
					And

Figure 5-8 VLAN Configuration Wizard (Step 1) Window

The fields that can be configured are described below:

Parameter	Description
Create VLAN	Select this option to create a new VLAN.
	• VID - Enter the VLAN ID here. The range is from 1 to 4094.
Configure VLAN	Select this option to configure an existing VLAN.
	• VID - Enter the VLAN ID here. The range is from 1 to 4094.

Click the **Next** button to continue to the next step.

Create VLAN

After selecting the Create VLAN option and clicking the Next button, the following window will appear.

50	3																						
A ANITIME .	7LAN0002																						
ui -																							
ikt.	14021-0	300		180	191		1.53	. 19	520	1	1.1	13	11	1.1		7. 18	150	- 30	30.	$\langle k^{2}\rangle$	3.0	26	- 1
Tagad			0.0	200		0.0	10	Û.		÷.	0		3	Č.			80	0	0	3		1	
100.000	- 24		195	252		3.5	$2, \Omega$		\mathbb{C}		$\mathbb{Q}_{\mathbb{Q}}$	(0, 0)	Ξ.	Ç.	C (Ð	Q.,	2	0.	$\mathbb{C}_{\mathbb{C}}$	$\mathfrak{T}_{\mathcal{T}}$
Heri Historian		*	90 Q	0.00	1	9 - 9	÷ +	÷.	*	*	÷.,	*)	e -	Ť.,	9 Q	• •			.	1	1	۰.	4
Hale SEALTHER	-44		115	11.1			10.0							<u>_</u>			90						
M Philippin		H.,	H	0.00	1	H 1	е н.	H		H	H	H	Ħ	Ħ	14. A					1		H.	
Webcons, Millippi d; TATILIDK																							
win The selected member set	(a) will be transition	e dor filles	e. h.	Weed	1.0	i.																	
www.with.in Through will be a	n a dan yada wataya	机制造制制																					



The fields that can be configured are described below:

Parameter	Description
VLAN Name	Enter the name for the VLAN here.
Tagged	Select the switch ports that are tagged members of this VLAN here.
Untagged	Select the switch ports that are untagged members of this VLAN here.
Not Member	Select the switch ports that are not members of this VLAN here.
Native VLAN (PVID)	Select the switch ports that support the native VLAN here.

Click the View Allowed VLAN button view the allowed VLAN settings.

Click the **Back** button to return to the previous step.

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

After clicking the View Allowed VLAN button, the following window will appear.

Rat	VLAS MUST	Hora, MIAM	University VLAN	Instant MLAN
6417	19 , 000	1		2.497-0011
eogus	- Ang		¥1	
0.0111	e.,000		82	
6073.9	Hyrod	1		
ana ta ta	(synan	-1	t :	
633.5	-gran	- 1	X -	
and de la	synan	.1	1	
ontin -	eyran	10	*	
ndal 9	Hymin.	1	1	
rajari	Hyperic		1. N.	
hsart.	Hypoth	- 1	*	
62.62.24	-pitelet	1		

Figure 5-10 Allowed VLAN Window

Configure VLAN

After selecting the **Configure VLAN** option and clicking the **Next** button, the following window will appear.

Configure VLAN																											
eic -	2.																										
VLANITIANS		KI 92																									
wit :	1	191																									
1.664		39823.86	1.5	2.	1		310	101	NER.		10		10	512	5.08	115	10 H	12	10		8	275	\mathbf{v}_{i}		EIS)	20	
Test		4		2.49		$\mathcal{O}_{\mathcal{O}_{\mathcal{O}}}$	2.0		0	Ċ.,			Ċ.			1	1	6	\mathbf{O}	0	$\mathcal{O}_{\mathcal{O}}$	$\langle 0 \rangle$				1	
245 CY 4		- 20	$-\infty$	\mathbf{C}_{i}	Ο.	06		60	$\langle Q \rangle$	\mathbb{C}^{*}	$\overline{\Omega}_{i}$		$\mathbb{O}_{\mathbb{P}}$	\mathbb{O}^{1}	(Ω)	\mathcal{C}^{*}	\mathbf{C}_{i}	\mathbb{Q}_{2}	0		0	10	O		\mathbb{O}^{1}	\mathcal{D}_{i}	5
Ret Hentber		4	- 18. L	Ψ.,	9 .	10.0	6.19			۰.	8	9	۰.	*	۰.	$\Phi_{\rm el}$	9 .	8	\mathbf{g}_{i}	(\mathbf{r})	$(\underline{\mathbf{n}})$	۰.	${\mathfrak P}^{*}$		8	${\cal A}_{i}$	
Main SEAL PRES		- 48		1	m			10		17	1		0	-		10	C)										1
ST # Million de la			- H (H	14	100	4 H	- 11	H	H	H	H	4	H	H	+	10	10		-	100	and a	1	14	H	H	H
A Access Hillight & T-Truck																											
Mas Alkard Alka																					:0	ester.		1	124	ple.	

Figure 5-11 VLAN Configuration Wizard (Configure VLAN) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Enter the name for the VLAN here.
Tagged	Select the switch ports that are tagged members of this VLAN here.
Untagged	Select the switch ports that are untagged members of this VLAN here.
Not Member	Select the switch ports that are not members of this VLAN here.
Native VLAN (PVID)	Select the switch ports that support the native VLAN here.

Click the View Allowed VLAN button view the allowed VLAN settings.

Click the **Back** button to return to the previous step.

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

After clicking the View Allowed VLAN button, the following window will appear.

Dat	MLAN Mode	Haber VLAN	Uniopate VLAN	Tease of MLAN
dealers.	8,000	1		7043035311
997097	9,09	1 () () () () () () () () () (N	
(WALC)	1007	0.9	*:	
2011/20	eyton	10		
10120	ispect	(a	1	
1030	eyród	1	10	
2001/1/2	september 1	1	1.1	
WILLIE .	14 M W	17	1	
analan -	eyroy)	1	1	
APRIL 19	eyron.		*	183
WARE	1470-147	5.8	*** 1	
0000016	$=_{\gamma} (r_{\gamma})^{-1}$	0		1.20
einaktik (Hypert .	0	9-3	
68-72-11 C	estint		* C	

Figure 5-12 Allowed VLAN Window

802.1Q VLAN

This window is used to view and configure the VLAN settings on this switch.

To view the following window, click L2 Features > VLAN > 802.1Q VLAN, as shown below:

8245 YUAN						
waa w	Service de la			L	sach	24 103
nin Vena						
VID (14054)	(C				fird	386 A.I
Ten Freisert -						
	teana teazipatan	Taggeriner or Aven	lanningen warnen kome	M KR Tge		
000 VI M					the second s	

Figure 5-13 802.1Q VLAN Window

The fields that can be configured for 802.1Q VLAN are described below:

Parameter	Description
VID List	Enter the VLAN ID list that will be created here.

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

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

The fields that can be configured for Find VLAN are described below:

Parameter	Description
VID	Enter the VLAN ID that will be displayed here.

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

Click the View All button to locate all the 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.

VLAN Interface

VLAN Interface Settings

This window is used to view and configure VLAN interface settings.

To view the following window, click L2 Features > VLAN > VLAN Interface, as shown below:

VDAH name	a Sedagi	Poel Summary			
	1 - 2				
1201834 1931	at A to Develo	Equivalence by	Analytick borns from	3.0000000000	
eh Da	lişbe d	English	As the state	show pecality	udt:
- applied	ible i	DAM'N.	64546.44	Show Deted.	Cdr.
0.046	Holand	Ha dia n	Cal	Show Brind	
off which it	-epoint	-3/8/9/	Autor Ja	Direction of the	**
APSOS .	lighted.	LODA :	Alchef-Ull	bloas Helal	+1.
aH355	(jobed	Disbiet:	April-Al	stor end	ud:
1010	this)	Example:	CALCULAR CAL	Shok Detel	C dec
0.0018	Here a	- FS 41 S	Called 200	Clicks Derivel	P.4-
or Activity	Hjórit	+1/8/90	Nation Vie	Shee Deskut	
10.000	Hereit	20092	Astronych	Mars Delait	

Figure 5-14 VLAN Interface Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
	•

Click the **Show Detail** button to view detailed information about the VLAN on the specific interface. Click the **Edit** button to re-configure the specific entry.

AN REALIST CONTRACTS		
-wt	PROV.	
dire train	Read	
lative VLAN		
- All a thight a risk	Y.	
Mail/Telacol/VLAM		
Dynamic Tagged VLAt		
ngrine terminang	Pr mort	
unversitie Clarky True	Alt AL	

After clicking the VLAN Detail button, the following page will appear.

Figure 5-15 VLAN Interface Information Window

On this page, detailed information about the VLAN of the specific interface is displayed. Click the **Back** button to return to the previous page. After click the **Edit** button, the following window will appear. This is a dynamic window that will change when a different **VLAN Mode** was selected. When **Access** was selected as the **VLAN Mode**, the following page will appear.

Configure VL/M Interloop						
Pet .	90.37		Citizee.			
C.MARKA	eccess .	- U	(81) I	the fail	75721	
Geografic Exerc	A Smit A&	100	1 >		1.1.57.0	142
handa Cecele a	$\mathcal{L} \in \mathcal{L} \cup \mathcal{L} \cup \mathcal{L}$					
securitaria;	<u>b</u> :					
					- Karan	69.04

Figure 5-16 Configure VLAN Interface - Access Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , and Trunk .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select this option to enable or disable the ingress checking function.
VID	Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
Clone	Tick this option to apply the configuration to the specified ports.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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

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

When Hybrid was selected as the VLAN Mode, the following page will appear.

Configure VLAN Intertece						
Configure VLAH Interface						
Ten-	40.27	A.4.5%	C Clone			
SLEMER,A.	Heter		QH-1	Pays Tail	75 751	
Car spatial Exercit	Distrikt 248	1.1	$ 1 \times $	anian x	1570	1943
harco Capiton	CONTRACTOR	men -				
Ballio V. NI	🔽 BOBANI AB					
A42.0 - 1090	h					
10.1	2.12	1				
Activities	(Channel) (I	upost -				
WE WITH AN ADDRESS						
rainini -yever conggeniti. Aki -ange						
Oumanit lighted Taggied YLAN (Tange						
and the second s					6023	4.50%



The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , and Trunk .

Parameter	Description
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select the check box to enable or disable the ingress checking function.
Native VLAN	Tick this option to enable the native VLAN function.
VID	After ticking the Native VLAN check box, this option will be available. Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
Action	Select the action that will be taken here. Options to choose from are Add , Remove , Tagged , and Untagged .
Add Mode	Select whether to add an Untagged or Tagged parameters.
Allowed VLAN Range	Enter the allowed VLAN range information here.
Clone	Tick this option to apply the configuration to the specified ports.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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

When Trunk was selected as the VLAN Mode, the following page will appear.

Configure VLAN Interfece						
Configure VLAH Interloce						
Prit.	40.31		Cicco.	1		
ALMINA .	LINDK		10-1	Pays To I	To Pail U	
сиприлюкуют	A sinit Ail	1.0	1 >	and y	1.1.570	142
hands Caulon	or Fandric Erfor			Contraction of the		
Haller VLAN	(Zhatney viria) Vic Brausian (L. 17	and the				
An in most	þ	Chinese .				
40.3	hore	2				
Adound to All Range	17	1				
Current Allower MLAN Film ge-		76				
					Mar.A.	P. g. dis

Figure 5-18 Configure VLAN Interface - Trunk Window

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , and Trunk .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	After selecting Trunk as the VLAN Mode the following parameter will be available. Select to enable or disable the ingress checking function.
Native VLAN	Tick the check box to enable the native VLAN function. Select if this VLAN supports Untagged or Tagged frames.
VID	After ticking the Native VLAN check box, this option will be available. Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.

The fields that can be configured are described below:

Parameter	Description
Action	Select the action that will be taken here. Options to choose from are All , Add , Remove , Except , and Replace .
Allowed VLAN Range	Enter the allowed VLAN range information here.
Clone	Tick this option to apply the configuration to the specified ports.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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

Port Summary

After selecting the **Port Summary** tab, the following page will be available.

VLAN Interfect Settings		opi Poet Summary			
• () • 1 2013 ()	1				
	M OR MORE	HALLOO VE AR	Haragen at the	Neget MAN	IN BACK, LABOR MEAN
walsel.	High W			1445	
nA102.	Hyb.M.		17		
100.002	- 19 year at	12.	1-11-		
10000	2010		11		
Print 1	Hr, brie		1		
matrix.	15,648		(
63807	Hybrid		1		
THORNE IN	10,0-0			()).	
TUNA .	ie juni		•		
MALINE	H, DIC		£		

Figure 5-19 VLAN Interface Port Summary Window

802.1v Protocol VLAN

Protocol VLAN Profile

This window is used to view and configure the Protocol VLAN profile.

To view the following window, click L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile, as shown below:

талона намения талона	anne Type Enemes	8	1
es Durer: 1 - State	Tiura Rype	 EtherType	

Figure 5-20 9 Protocol VLAN Profile Window

The fields that can be configured are described below:

Parameter	Description
Profile ID	Enter the profile ID that will be created here.

Parameter	Description
Frame Type	Select the frame type here. Options to choose from are Ethernet2 , SNAP and LLC .
Ether Type	Enter the Ethernet type in hexadecimal form.

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

Protocol VLAN Profile Interface

This window is used to view and configure the Protocol VLAN profile interface.

To view the following window, click L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile Interface, as shown below:

de New Process VLAN is include					
an <u>🕑</u> anna	🧕 emeri (t 🕑	- MOR-407 [i enants (u	9	4256
od 18-dap	Excels 10	No. Store	Priority		
Porc					

Figure 5-21 Protocol VLAN Profile Interface Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the switch unit and the port that will be used for this configuration here.
Profile ID	Select the ID of the protocol group.
VID	Enter the VLAN ID of the Protocol VLAN.
Priority	Select the priority of the Protocol VLAN.

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

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

GVRP

GVRP Global

This window is used to view and configure the GARP VLAN Registration Protocol (GVRP) global settings.

To view the following window, click L2 Features > VLAN > GVRP > GVRP Global, as shown below:

GVRP Globel	_	_	
RURP GIMM			
Clubal SVNF Skile	CENSER	s plitabled	
Dynamic VLAN Crystian	(CERTADAD	@Okabilet	
			Ace /

Figure 5-22 GVRP Global Window

The fields that can be configured are described below:

Parameter	Description
Global GVRP State	Select this option to enable or disable the global GVRP state here.
-	Select this option to enable or disable the dynamic VLAN creation function here.

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

GVRP Port

This window is used to view and configure the GVRP port settings.

To view the following window, click L2 Features > VLAN > GVRP > GVRP Port, as shown below:

Vier Pink				
WITP Port				
un - Frankra	Ta Pen	GNRS SIME IN 100	(0) (10-(0)00)	10-10000)
191 (#0529 (P)	#1100 St.	U antiest × 30	orderson and state	contention in 1000 contention in
New		10 S		10 Arr
The Leave Time should be r				
Lawy XI Timi should by ge	ADDE THEY SHARE THE .			
Uniti Settinga				111
Port	GARE SIMUL	Join Time	terve Time	L COVIE CALIFORNIA
68:331	Olaidiati	22	(M)	1000
631/32	Otection	35	82	1636
ed isos	Olinda ext	32	80	1600
42.024	Ound av	22	8	1600
421/05	Olardi et	22	50	1630
48.005	Starking.		<u>50</u>	1000
TOTAL	Clevel inc	30	50	1000
43.500	Otati et	22	20	:1039
K#1/9/2	Obubliev.	20	50	1000
2510213	Clind A	33. 	20	1000
164090	Oud A	25	20	(00)

Figure 5-23 GVRP Port Window

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
GVRP Status	Select this option to enable or disable the GVRP port status. This enables the port to dynamically become a member of a VLAN. By default, this option is disabled.
Join Time	Enter the Join Time value in centiseconds. This value must be between 10 and 10000 centiseconds. By default, this value is 20 centiseconds.
Leave Time	Enter the Leave Time value in centiseconds. This value must be between 10 and 10000 centiseconds. By default, this value is 60 centiseconds.
Leave All Time	Enter the Leave All Time value in centiseconds. This value must be between 10 and 10000 centiseconds. By default, this value is 1000 centiseconds.

The fields that can be configured are described below:

GVRP Advertise VLAN

This window is used to view and configure the GVRP advertised VLAN settings.

To view the following window, click **L2 Features > VLAN > GVRP > GVRP Advertise VLAN**, as shown below:

GVRP Advertise VLAN					
RVSP Advanties 31 AN					
	To Pot	Ador Add 🔤	Adeetsa VID List 13 or 245	I	
ULLI SMIRZ					
Port	_		10	entise VI AR	
C31321					
ATTE 19 (2)					
With 1905					
eth1104					
s04180%					
6.578/6					
100 C 8 C					
2011/05					
eth1105					
ath (72/10					
Bh (70/11					
81.070772					
MITTAUTS.					
strift.hr					
et+1/2/15					

Figure 5-24 GVRP Advertise VLAN Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Action	Select the advertised VLAN to port mapping action that will be taken here. Options to choose from are All , Add , Remove , and Replace . When selecting All , all the advertised VLANs will be used.
Advertise VID List	Enter the advertised VLAN ID list here.

GVRP Forbidden VLAN

This window is used to view and configure the GVRP forbidden VLAN settings.

To view the following window, click **L2 Features > VLAN > GVRP > GVRP Forbidden VLAN**, as shown below:

GV8P Forbidden VLAN				
SVRP Forbidder MINH				
Line From Part	To Port	Ador Add a	Forbidden VID Litt 2 or 2-5	Angly
ter i Serlige.				
Per		_	Foreigner villige	_
0.0	0			
67019	D.			
eth 10	a -			
eth 10	M			
6.610	e			
e(h18)	6			
010				
ere s				
eth (K	-			
at 175				
di Ut				
Shi Dh				
Mo1/4				
MTY1/C.				
et ni fil	45			

Figure 5-25 GVRP Forbidden VLAN Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Action	Select the forbidden VLAN to port mapping action that will be taken here. Options to choose from are AII , Add , Remove , and Replace . When selecting AII , all the forbidden VLANs will be used.
Forbidden VID List	Enter the forbidden VLAN ID list here.

GVRP Statistics Table

This window is used to display GVRP statistics information.

To view the following window, click **L2 Features > VLAN > GVRP > GVRP Statistics Table**, as shown below:

1.5			610/ F			0.8	0 Sa 1
			0.000.000			Stav A	Claim A
115xUitya						1.0 0.000 - 50	
-907			10000	I state typy	10000	ina sena	1497
2003202	N 6		, ú	10	1 .	1.5	. <u>I</u> I.
- 0000000	tic -				1	1.1	
2.5 (002)	fD.	B	é	6	1	E .	0
250.043	TX .	1		4	1		0
00332121	H.F.		<i>b</i>	4	1	1	Ø.
0000000	15:	1	i i i	10	T	1	ji ji
6.12.1	8.0	1.1	())	- 16 i	1	100	
8/102/4	TA	10	0.0	6	11	L.C.	<u>0</u>
	.ED	1	0	0	1	1.	0 0
10120	TX	1	8	0	1 13	1	÷.
	11.6	1		0	1.	1	.0.
Contraction of the second			- 11 million (11)	10		1.1	11
30110	110	1		112			
\$155 \$1057	18 HE				1	1.5	U.

Figure 5-26 GVRP Statistics Table Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Port	Select the port number of which GVRP statistic information will be displayed.

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

Click the **Clear** button to clear all the information for the specific port.

Click the View All button to view all GVRP statistic information.

Click the **Clear All** button to clear all the information in this table.

Asymmetric VLAN

This window is used to configure the asymmetric VLAN function.

To view the following window, click L2 Features > VLAN > Asymmetric VLAN, as shown below:

Asymmetric VLAN			
си условита на Ам Содина во УССИ Такт	(Friday)	gound)	

Figure 5-27 Asymmetric VLAN Window

The fields that can be configured are described below:

Parameter	Description
Asymmetric VLAN State	Select this option to enable or disable the asymmetric VLAN function

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

MAC VLAN

This window is used to view and configure MAC-based VLAN settings.

To view the following window, click L2 Features > VLAN > MAC VLAN, as shown below:

AC YUM				
WOARD TO ANY NOTICE	VID (1 4994)	No.h D	v 1	- spok
oni Hellos, 1				
MAL REPORT	-11	etitare .	NUM .	100
AA60-00-00-00-77	1		Jection .	aunierae

Figure 5-28 MAC VLAN Window

The fields that can be configured are described below:

Parameter	Description
MAC Address	Enter the MAC address that will be used for this configuration here.
VID	Enter the VLAN ID for the MAC-based VLAN.
Priority	Select the priority of the MAC-based VLAN.

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

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

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

L2VLAN Interface Description

This window is used to display and configure the Layer 2 VLAN interface description.

To view the following window, click L2 Features > VLAN > L2VLAN Interface Description, as shown below:

Trans L2VL/Al Interface Descript					
C NI KATAMINI	30.2 B Y				(p
	Essano -				· * 4.45
and LEVEA Vibrantaen Deveriptio	N				
LATSH SINGLY	n:				
ind L2V SAM Interface Description	1			[]	Sec 13
LATER Sector	n			[II See 11
i na kalendarina	500.0	Adm 1 prock 4	Description	[i ser ti

Figure 5-29 L2VLAN Interface Description Window

The fields that can be configured for Create L2VLAN Interface Description are described below:

Parameter	Description
L2VLAN Interface	Enter the ID of the Layer 2 VLAN interface here.
Description	Enter the description for the Layer 2 VLAN interface here.

Click the Apply button to accept the changes made.

The fields that can be configured for Find L2VLAN Interface Description are described below:

Parameter	Description
L2VLAN Interface	Enter the ID of the Layer 2 VLAN interface here.

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

Click the View All button to view all the entries.

Click the **Delete Description** button to remove the description from the specified Layer 2 VLAN.

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

Auto Surveillance VLAN

Auto Surveillance Properties

This window is used to configure the auto surveillance VLAN global settings and display the ports surveillance VLAN information.

The Switch regards a host as an NVR once it connects to the IPC via HTTP, HTTPS, or RTSP. The Switch will learn the NVR on this port and move it into the surveillance VLAN until the triggered aging mechanism age-out or the LAN cable is removed.

When the host sends an ARP request to an IPC, the Switch still regards the host as an NVR but only temporarily move it into the surveillance VLAN. The host will automatically be moved out of the surveillance VLAN after about 30 seconds if it is not recognized as an NVR anymore.



NOTE: The same PC, or PCs connected to the same LAN port on the Switch, cannot simultaneously manage the Switch and the IP cameras connected to the Switch.

To view the following window, click L2 Features > VLAN > Auto Surveillance VLAN > Auto Surveillance Properties, as shown below:

vuto Surveillario	e i 'i operitina			
Note: Settings				
Schellungs VLAV SI	á.	@Cardet COvered		
Surveillance vita vita	(2-1047)	þ		
SLOWBARD VLAVICE	a	(r 🖂		
en antima pi-a izan		(ca in a		
Internet and the second	ALCO ALCONOM	and a second sec		
Meaner Forts		100-000-02710051		
Operation Monitors Pro-	e	100.052.595	-1	anne
	AND and Voley VLAN ID can	22.22.2.2.2.		rigida .
NAME OF ADDRESS OF AD	ASH DIANG YORK VEARIND CHI	on ov tree state die		
AMT, GEODAL BURNEL				
Search and the search	Astalitett			
- Icensis Investes;		ы 0		
Hy COAvaled ONVI	t in the second s	9.		
ori Settings				
nar ^C aase	at teres	20.0		
🖂 amb				14.6
		and the second second		
and the burys	Pal		2976	
1	10.01		FOR 2	-
	onto ta 1		Februar	
	49.337		Ended	
	48.53.1		Enstad	
	48:03:3		Drabled	
	W.5M		Draked	
	30.07		DiAleJ	
	10.030		tabled	
	×0.010		trutin)	
	(BINK)		EQUIT:	

Figure 5-30 Auto Surveillance Properties Window

The fields that can be configured for **Global Settings** are described below:

Parameter	Description
Surveillance VLAN State	Select this option to enable or disable the surveillance VLAN state
Surveillance VLAN ID	Enter the surveillance VLAN ID. The range is from 2 to 4094.
Surveillance VLAN CoS	Select the priority of the surveillance VLAN from 0 to 7.
Aging Time	Enter the aging time of surveillance VLAN. The range is from 1 to 65535 minutes. The default value is 720 minutes. The aging time is used to remove a port from surveillance VLAN if the port is an automatic surveillance VLAN member. When the last surveillance device stops sending traffic and the MAC address of this surveillance device is aged out, the surveillance VLAN aging timer will be started. The port will be removed from the surveillance VLAN after expiration of surveillance VLAN aging timer. If the surveillance traffic resumes during the aging time, the aging timer will be reset and stop.
ONVIF Discover Port	Enter the TCP/UDP port number here. The range is either 554, or from 1025 to 65535. This is used to configure the TCP/UDP port number for RTSP stream snooping. ONVIF-capable IPC and ONVIF-capable NVR utilize WS-Discovery to find other devices. Once IPCs are discovered, the Switch can further discover NVRs

Parameter	Description
	by snooping RTSP, HTTP, and HTTPS packets between NVRs and IPCs. These packets cannot be snooped if the TCP/UDP port is not equal to the RTSP port number.

The fields that can be configured for **Port Settings** are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable the state of the port.

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

MAC Settings and Surveillance Device

This window is used to configure the user-defined surveillance device OUI and display the surveillance VLAN information.

To view the following window, click L2 Features > VLAN > Auto Surveillance VLAN > MAC Settings and Surveillance Device, as shown below:

Units defined M	AC Section As is Garage	inse VLAri Summary				
o accimicate devid Tel par est l'épot COL Actives	Cher (* Surveiller mit finden die	ster de l'es cui garator as artor la Device 👻	Lance (dec) Marci	in care		10.1
and service			175			
a Salara I.	Company AT (P	Real of the local division of the local divi		MAY Sciences		
	AND A LODGE A			MAC & Average 27 T 2 Average		Teles
	Company of Type	Real of the second		MAC & Real of	Maria	
	Compose of Type T2 81 Type	Constant of the second se		HAT Is been as	Navia 1949 1949 1951 10	Ter/AM

Figure 5-31 User -defined MAC Settings Window

The fields that can be configured are described below:

Parameter	Description
Component Type	Select the surveillance component type. Options to choose from are Video Management Server, VMS Client/Remote Viewer, Video Encoder, Network Storage, and Other IP Surveillance Device.
Description	Enter the description for the user-defined OUI with a maximum of 32 characters.
MAC Address	Enter the OUI MAC address.
Mask	Enter the OUI MAC address matching bitmask.

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

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

After clicking the Auto Surveillance VLAN Summary tab, the following page will appear.

Anto Somellance VLAB Some	"		
ини Тура	Description	MAC Address	Start Time
	anwari Tyrpa	onveri Type Deversityatise	anwer Type Owerselpeise MWC Addresse

Figure 5-32 Auto Surveillance VLAN Summary Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.

ONVIF IP-Camera Information

This window is used to display ONVIF IP camera information.

To view the following window, click L2 Features > VLAN > Auto Surveillance VLAN > ONVIF IP-Camera Information, as shown below:

WARE BASIC	annora fittoreadar	813						
1.00								
tat.								
inte see	ings.							
au Dai	es Discovered: 3							
						Trough per		
Pat	IP Address	WVC Address	Note	Vanalactore	Chica St	Description III est		
	1111881112	WHICH STREET, SALES	138093.209	1003.51513	250000	L :	Means Decade	
1043		and the second	1123131313181	HURSON AND	+123206	1.5	Mana Sec. 4	
1004.1 1004.0	The later	Add a state of a defective of	time district for					

Figure 5-33 ONVIF IP-Camera Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used in the display here.

Click the IP Address hyperlink to connect to the Web Interface of the IP camera.

Click the More Detail button to view detailed ONVIF IP camera information.

Click the Edit button to configure the state and description of the IP camera.

After click the More Detail button, the following window will appear.

MAN AN TRANSPORT	34882/I	
Aver Street Barrier	20 () ()	
Aparen	RE 120037	
44C Address	ni/10-30-00-04-00	
жн.	DOMEAN	
dere bestere	E 07-51231	
2.61	Dest	
la:see		
ll contra	(101.e.	
40.00	CHA-	
ender som engende	0.1/23/82/0	
ne Na rege	li entre	
PAR SPACE	estimation of the second se	

Figure 5-34 ONVIF IP-Camera Information (More Detail) Window

After click the Edit button, the following window will appear.

CINAL EStamore Selfa	i i i i i i i i i i i i i i i i i i i	
DMM+103 among Settings		
Post. References	exition For the E.Z.	
ever namen F-Cometa State	early walds (2003) Traced	
Lakapana		
		<u>5.4</u> 5.6

Figure 5-35 ONVIF IP-Camera Information (Edit) Window

The fields that can be configured are described below:

Parameter Description	
IP-Camera State	Select to enable or disable the IP camera state here.
Description	Enter the description for this IP camera here.

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

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

ONVIF NVR Information

This window is used to display ONVIF Network Video Recorder (NVR) information.

To view the following window, click L2 Features > VLAN > Auto Surveillance VLAN > ONVIF NVR Information, as shown below:

ALC: NO. DOL: NO.	red of							
	1							
ent Anthrop								
disting it uses I	and a second							
				and the second se				
2.41		NALY Julies of	Former Landser	Thomas in a second	Corine	D an Antin		
STREET, STREET, STREET, ST		NLC Internet	Frank Lander	Thorques (Mages)	Series 1	D webste	PSe na bil	

Figure 5-36 ONVIF NVR Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used in the display here.

Click the IP Address hyperlink to connect to the Web Interface of the NVR.

Click the **IP-Camera List** button to view the list of IP cameras that are connected to the NVR.

Click the Edit button to configure the description of the NVR.

After click the **IP-Camera List** button, the following window will appear.

PER-Lamona Uni				
Seat.	17.5 alchest	INC. Action 14	George	Less r plans
100100	10.000	2362/1420-2446	2	

Figure 5-37 ONVIF NVR Information (IP-Camera List) Window

Click the IP Address hyperlink to connect to the Web Interface of the IP camera. Click the **Back** button to return to the previous window.

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

	10000							
	1 ×							
d all had been d	an an an air 2							
and inclusion of	Fasters	No. Like a	Frence Laster	Through	(ana)	Dartes		
STREET, SQUARE,	CONTRACTOR OF THE OWNER.	NAC A NEW IN	Prices Laster	and the second se	(Qray) 	n where	(PSe no bil)	200

Figure 5-38 ONVIF NVR Information (Edit) Window

The additional fields that can be configured are described below:

Parameter	Description
Description	Enter the description for this NVR here.

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

Voice VLAN

Voice VLAN Global

Voice VLAN is a VLAN used to carry voice traffic from IP phone. Because the sound quality of an IP phone call will be deteriorated if the data is unevenly sent, the quality of service (QoS) for voice traffic shall be configured to ensure the transmission priority of voice packet is higher than normal traffic.

The switches determine whether a received packet is a voice packet by checking its source MAC address. If the source MAC addresses of packets comply with the organizationally unique identifier (OUI) addresses configured by the system, the packets are determined as voice packets and transmitted in voice VLAN.

To view the following window, click L2 Features > VLAN > Voice VLAN > Voice VLAN Global, as shown below:

Voica VLAB Global		
Volca st.AN Granet		
NEW VERY DISA	Constant and and	2007 - 1200
WANDON COS	(16) <u>-</u>	
Vignes time (14 a robo	[24] [24]	i fedro i

Figure 5-39 Voice VLAN Global Window

The fields that can be configured are described below:

Parameter	Description		
Voice VLAN State	Select this option to enable or disable the voice VLAN.		
Voice VLAN ID	Enter the voice VLAN ID. The value is range from 2 to 4094.		
Voice VLAN CoSSelect the priority of the voice VLAN from 0 to 7.			
Aging Time	Enter the aging time of surveillance VLAN. The range is from 1 to 65535 minutes. The default value is 720 minutes. The aging time is used to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of voice VLAN aging timer. If the voice traffic resumes during the aging time, the aging timer will be reset and stop.		

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

Voice VLAN Port

This window is used to show the ports voice VLAN information.

To view the following window, click L2 Features > VLAN > Voice VLAN > Voice VLAN Port, as shown below:

unit Exerect 1	To Pot State To Pot Distance Distance A		Sec. 1
antin Section	<i>II</i> == 0.		
1941	East.		
x10500	Dr. al.ord	(a.e.b.a)	
CONTRACT	the street.	(Antonio)	
A DE TAR AS	11/10/101	Autoritation (
10.00	Division of	Arating	
10.00	Disbad	Arabay	
AB 105	Divident.	(LANDA)	2
(8300)	Me, d. les L	, Vaca(16,4)	
(01 ° a (8)	10.0007	Valuetaria	
Am 1/100	112-12-10	Annu may	
enti CPD	Disebied	Arminter	
1518/1	Dhabled	Arabitar	
1.00012	Dr. al. inst	ALLAND .	8
0.000405	The dead	Astanta .	
amin.202	117 (0) (17	6475.0876	
#21045	Dia shi e t	Arasmo.	
4011010	Disub-lead	Araling.	
12010217	Distant	le alle av	

Figure 5-40 Voice VLAN Port Window

The fields that can be configured are described below:

Parameter	Description	
Unit	Select the switch unit that will be used for this configuration here.	
From Port / To Port	Select the appropriate port range used for the configuration here.	
State	Select this option to enable or disable the state of the port.	
Mode	Select the mode of the port. Options to choose from are Auto Untagged , Auto Tagged , and Manual .	

Voice VLAN OUI

This window is used to configure the user-defined voice traffic's OUI. The OUI is used to identify the voice traffic. There are a number of pre-defined OUIs. The user can further define the user-defined OUIs if needed. The user-defined OUI cannot be the same as the pre-defined OUI.

To view the following window, click L2 Features > VLAN > Voice VLAN > Voice VLAN OUI, as shown below:

(Add Sector	Aus	Description	
0140301002	THE REPORT	[12 chay	N
N FRIDE 2 -			
UNI Administ	and the second se	Lauchene	10-
\$3-\$1-\$3-\$0-65-65	FT-FT-FT-96-60-80	Out as	1.16.46
(0.15-SE X (4.0)	FF FF OF 3C CS 80	CONA	- 040.000
11214-01031	EKEE SE SE TETTE	Ca ji	-141.93
11:00-2010.001	68.68.66.8118.01	- Cart F. Da	. Dit 200
1040484-00468	FF-FF-FF-10-C0-00	HERE'S PORT	(De 111
35-03-10-03-00-00	FF4T4T40640400	Prov	1200
(0.0079-00-00-00	FF.(F-(T-00-00-00	Viz.641	1001000
Republic and the second	11111-14 (K.1918)	2104 C	1. 14 mile

Figure 5-41 Voice VLAN OUI Window

The fields that can be configured are described below:

Parameter	Description		
OUI Address Enter the OUI MAC address.			
Mask Enter the OUI MAC address matching bitmask.			
Description Enter the description for the user-defined OUI with a magical sectors.			

Click the Apply button to accept the changes made.

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

Voice VLAN Device

This window is used to show voice devices that are connected to the ports. The start time is the time when the device is detected on this port, the activate time is the latest time saw the device sending the traffic.

To view the following window, click L2 Features > VLAN > Voice VLAN > Voice VLAN Device, as shown below:

Voice VLAN Device			
Voice VLAH Device Table			
Uni i m			
Tomi Endes:0			
Port	West Integration	STATE LICEN	NUS R

Figure 5-42 Voice VLAN Device Window
The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.

Voice VLAN LLDP-MED Device

This window displays the voice VLAN LLDP-MED voice devices connected to the Switch.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN LLDP-MED Device**, as shown below:

Voice VLAN LLDP-MED Device						
Voice VLAH LLOP ME	- Voka VLAH LLDP MED Device Table					
Total Enhiese 0						
Inder Park	Chavala ID Sabigov	Chunata ID	Port ID Subtype	PollD	Croute Time	Evenue Tenv (avc)
	Character and Sho	C BALAN D	Post in analysis	PSHIP	110404	

Figure 5-43 Voice VLAN LLDP-MED Device Window

STP

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 D-Link 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, 802.1D-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:

- 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).
- A configuration revision number (named here as a Revision Level and found in the **MST Configuration Identification** window) and;

• 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:

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

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

STP Global Settings

This window is used to view and configure the STP global settings.

To view the following window, click L2 Features > STP > STP Global Settings, as shown below:

	(EXCERT				Linear and
Spinorsania - ((Hellow)				
States (Costed				
1851 *	10				4367
270	<u>.</u>				License.
78.1	1.00	Daily 160-70 (12)	122		
15	100	The line Court (1-10)	<u>k</u>)	2014	
18.	feat.fea	1110030000000	352		1000
	ini terrativa ini terrativa (1851 * (1976) 19 19 19 19 19 19		initia marta (Jestiano) initia di Constanti initia di Constanti init	Granmant (Jackand ∰Dhaddad ()Dhaddad 051 * ∞ 3****** 3****** 3****** 3***** 3***** 3****** 3****** 3****** 3********	Antonian Creation A Dualled Control ISST

Figure 5-44 STP Global Settings Window

The field that can be configured for **Spanning Tree State** is described below:

Parameter	Description
Spanning Tree State	Select this option to enable or disable the STP global state here.

Click the Apply button to accept the changes made.

The fields that can be configured for **STP Traps** are described below:

Parameter	Description
STP New Root Trap	Select this option to enable or disable the STP new root trap option here.
STP Topology Change Trap	Select this option to enable or disable the STP topology change trap option here.

Click the Apply button to accept the changes made.

The fields that can be configured for **STP Mode** are described below:

Parameter	Description
STP Mode	Select the STP mode used here. Options to choose from are MSTP , RSTP , and STP .

Click the Apply button to accept the changes made.

The fields that can be configured for **Spanning Tree Priority** are described below:

Parameter	Description
Priority	Select the STP priority value here. This value is between 0 and 61440. By default, this value is 32768. The lower the value, the higher the priority.

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

The fields that can be configured for **Spanning Tree Configuration** are described below:

Parameter	Description
Bridge Max Age	Enter the bridge's maximum age value here. This value must be between 6 and 40 seconds. By default, this value is 20 seconds. The maximum age value 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.
Bridge Hello Time	After selecting RSTP/STP as the STP Mode , this parameter will be available. Enter the bridge's hello time value here. This value must be between 1 and 2 seconds. By default, this value is 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.
Bridge Forward Time	Enter the bridge's forwarding time value here. This value must be between 4 and 30 seconds. By default, this value is 15 seconds. Any port on the Switch spends this time in the listening state while moving from the blocking state to the forwarding state.

Parameter	Description
TX Hold Count	Enter the transmit hold count value here. This value must be between 1 and 10 times. By default, this value is 6 times. This value is used to set the maximum number of Hello packets transmitted per interval.
Max Hops	Enter the maximum number of hops that are allowed. This value must be between 6 and 40 hops. By default, this value is 20 hops. This value is 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 BDPU packet and the information held for the port will age out.

STP Port Settings

This window is used to view and configure the STP port settings.

To view the following window, click L2 Features > STP > STP Port Settings, as shown below:

IP Port Setting											
6 C		Ŷ		man nat	1110		in Post	ent/12	w.		
2000/01-2000000	X4/49.03		-1	800	cracked	10	Court Sect.	Charled	~		
Jik Type		Auto	1	Patrixet	Network		TONER	Ubicted	\mathbf{x}		
1700 Estyute	ŝ	Disabled	2	Frienty	123	1	$0.000 \ {\rm Time} \ (-3)$			142	- 09E 7
nd 1 softings											
1 99	State	Cost	- 00	ad Bad	Lind line -		Duttest	OTH Faller		BUUManan	(Viente
mun	With the -	0.2.000		exerni -	- And State		-djó.sza-sign	linine's		1612060	128
#101.5		61300	1.1	e/n w	A Provide		-nja ven +age	HERMAN		income.	01
anns v	40.00	81801		640 M	ADDATE		Haya Man Faon	TRANSFE .		Disabed.	124
. ITTERN	- DAD W	8/10(0)	10	ichten -	A BANK P	115	HILLING HILL	Branks.		Contracted.	2.36
and the second	Finitian.	16.16.20100	10	entra .	A MARKE	1 12	Fighten Figh	termént.		fananies.	281
more	- East an	0.00000	0	and an	A \$100.29	12	Fright was Flight	filandes.		families.	(91
marce.	First wa	3/19/09	2.3	italitan 👘	3.84628	133	Fapa teo Faja	literated.		TO MARKET	251
muse.	Tables	6212000	30	instruction in the	A \$16779		Edge ten Fage	lines.		filmed.	di.
mice	THE W	0.253000	1.0	and an	A8472		Fégnines-Fégn	Distance di		fit while a	:28
MYLL'SS	Teta	30703000	- 5	instrum	A. 800 28	1 2	Edge Van Espe	Division of		Distanted.	QIT

Figure 5-45 STP Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Cost	Enter the cost value here. This value must be between 1 and 200000000. This value 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. The lower the number, the greater the probability the port will be chosen to forward packets.
State	Select to enable or disable the STP port state.

Parameter	Description
Guard Root	Select to enable or disable the guard root function.
Link Type	Select the link type option here. Options to choose from are Auto , P2P , and Shared . A full-duplex port is considered to have a point- to-point (P2P) connection. On the opposite, a half-duplex port is considered to have a Shared connection. The port cannot transit into the forwarding state rapidly by setting the link type to Shared . By default, this option is Auto .
Port Fast	Select the port fast option here. Options to choose from are:
	 Network - The port remains in the non-port-fast state for three seconds. The port will change to the port-fast state if no BPDU is received and changes to the forwarding state. If the port received the BPDU later, it will change to the non-port-fast state. Disabled - The port is always in the non-port-fast state. It will always wait for the forward-time delay to change to the forwarding state. Edge - The port directly changes to the spanning-tree forwarding state when a link-up occurs without waiting for the forward-time delay. If the interface receives a BPDU later, its operation state changes to the non-port-fast state. This is the default option.
TCN Filter	Select to enable or disable the TCN filter option. Enabling TC filtering on a port is useful for an ISP to prevent the external bridge to a core region of the network, causing address flushing in that region, possibly, because those bridges are not under the full control of the administrator. When a port is set to the TCN filter mode, the TC event received by the port will be ignored. By default, this option is Disabled .
BPDU Forward	Select to enable or disable BPDU forwarding. If enabled, the received STP BPDU will be forwarded to all VLAN member ports in the untagged form. By default, this option is Disabled .
Priority	Select the priority value here. Options to choose from are 0 to 240 . By default, this option is 128 . A lower value has higher priority.
Hello Time	Enter the hello time value here. This value must be between 1 and 2 seconds. This value specifies the interval that a designated port will wait between the periodic transmissions of each configuration message.

MST Configuration Identification

This window is used to view and configure the MST configuration identification settings. 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.

To view the following window, click **L2 Features > STP > MST Configuration Identification**, as shown below:

Astream group march	nice Marti	
NULLARY REPORT OF THE SECOND		
Conference Spece	2010 M A100 00	
Paratos Lateria A. Arto;	1	
David	AND THE PARTY PROPERTY ACTIVATION OF	- eg.
ada a di Adago		17 13
MENDER (FRA.		
	Амур 🔛	
X D Uni	1032	100 MAR
Test Extent 1	100 March 100	
nakasa).	yu un	
0 er	1184	The Advantage of Advances of A

Figure 5-46 MST Configuration Identification Window

The fields that can be configured for MST Configuration Identification are described below:

Parameter	Description
Configuration Name	Enter the MST 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	Enter the revision level value here. This value must be between 0 and 65535. By default, this value is 0. This value, along with the Configuration Name, identifies the MSTP region configured on the Switch.

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

The fields that can be configured for	Instance ID Settings are described below:
The herde that early be conligated for	

Parameter	Description
Instance ID	Enter the instance ID here. This value must be between 1 and 16.
Action	Select the action that will be taken here. Options to choose from are Add VID and Remove VID.
VID List	Enter the VID list value here. This field is used to specify the VID range from configured VLANs set on the Switch.

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

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.

STP Instance

This window is used to view and configure the STP instance settings.

To view the following window, click **L2 Features > STP > STP Instance**, as shown below:

The statice	tintasca State	catance Plinity	
3481	200.00.0	12769-1798 ov. 4-1	(.a.)
			10
ance CIST			utintojinote RSTPj
	and Distance in		
Bally-Null tru			102.03.04.08
Discrete evaluation of the law of the second		. B (B	NUMBER OF THE TRANSPORT
110	gana, Krat Kengh Antowas (Polada)		é korendari
Č.	an grief an Einige Administratification	80-30	K3-90-96-K3. E

Figure 5-47 STP Instance Window

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.

MSTP Port Information

This window is used to view and configure the MSTP port information settings.

To view the following window, click L2 Features > STP > MSTP Port Information, as shown below:

	1.000.000.000.000.000				
	PVI 921724	-			Ales oreast natural and
HOH Seldings					
feistende Bb	e e d	thready	elabel -	10 e	
6457	200,000	120	Tavaslas	No Sa	1 B

Figure 5-48 MSTP Port Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Port	Select the port number that will be cleared here.

Click the Clear Detected Protocol button to clear the detected protocol settings for the port selected.

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

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.

ERPS (G.8032)

For more information, refer to Appendix E - ERPS Information.

ERPS

This window is used to view and configure Ethernet Ring Protection Switching (ERPS) settings.

To view the following window, click L2 Features > ERPS (G.8032) > ERPS, as shown below:

TRIS		
Othernel Sing C.0652		
Anakan: be	un	dgsky
Total Cables: 1		
HIVEN BAL	astance at	<u> </u>
Dex.	1	mitting with national Standards . Direct

Figure 5-49 ERPS Window

The fields that can be configured are described below:

Parameter	Description
Ring Name	Enter the Ethernet Ring Protection (ERP) instance's name here. This name can be up to 32 characters long.

Click the Apply button to create an ITU-T G.8032 ERP physical ring.

Click the **Edit Ring** button to modify an ITU-T G.8032 ERP physical ring.

Click the Edit Instance button to configure the ERP instance.

Click the Show Status button to view the ITU-T G.8032 ERP physical ring's status information.

Click the **Delete** button to delete the specified ITU-T G.8032 ERP physical ring.

After click the Edit Ring button, the following window will appear.

zəl Lithernet Köny Stamat Sing Sadəya			
- 1000 (2000) (2000)	Hist.		
ar Marco (971 22)	and an	The second states and	
St. How How a	N. Saint	Charles State	
tat.	2 54 60500	V TOVER Starve	
with	NS PAR	The strength	
			Arab faithe

Figure 5-50 ERPS (Edit Ring) Window

The fields that can be configured are described below:

Parameter	Description
Instance ID	Select the checkbox and enter the ERP instance number here. This value must be between 1 and 32. Select the Specify radio button to configure this parameter as per normal. Select the None radio button to revert this parameter to the default setting.
Sub Ring Name	Select the checkbox and enter the physical ring's sub-ring name here. This name can be up to 32 characters long. Select the Specify radio button to configure this parameter as per normal.

Parameter	Description
	Select the None radio button to revert this parameter to the default setting.
Port0	Select the checkbox and then select the switch's unit ID and the port number that will be the first ring port of the physical ring. Select the Specify radio button to configure this parameter as per normal. Select the None radio button to revert this parameter to the default setting.
Port1	Select the checkbox and then select the switch's unit ID and the port number that will be the second ring port of the physical ring. Select the None option, from the drop-down menu, specifies that the inter-connected node is a local node endpoint of an open ring. Select the Specify radio button to configure this parameter as per normal. Select the None radio button to revert this parameter to the default setting.

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

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

After click the **Edit Instance** button, the following window will appear.





Parameter	Description
Description	Select the checkbox and enter the ERP instance's description here. This description can be up to 64 characters long. Select the Specify radio button to configure this parameter as per normal. Select the None radio button to revert this parameter to the default setting.
R-APS Channel VLAN	Select the checkbox and enter the R-APS channel VLAN's ID for the ERP instance here. The APS channel VLAN of a sub-ring instance is also the virtual channel of the sub-ring. This value must be between 1 and 4094. Select the Specify radio button to configure this parameter as per normal. Select the None radio button to revert this parameter to the default setting.
Inclusion VLAN List	Select the checkbox and enter the inclusion VLAN list here. A range is identified when a hyphen (-) is used. For example, VLANs 1 to 5 can be entered as 1-5. A list is identified when commas (,) are used. For example, use VLANs 1,3,5. The VLANs specified here will be protected by the ERP mechanism. Select the Specify radio button to configure this parameter as per normal. Select the None radio button to revert this parameter to the default setting.

The fields that can be configured are described below:

Parameter	Description
MEL	Select the checkbox and enter the ring MEL value of the ERP instance here. This value must be between 0 and 7. The configured MEL value of all ring nodes that participate in the same ERP instance should be identical. Select the Specify radio button to configure this parameter as per normal. Select the None radio button to revert this parameter to the default setting.
Profile Name	Select the checkbox and enter the G.8032 profile's name here that will be associated with this ERP instance. Multiple ERP instances can be associated with the same G.8032 profile. The instances associated with the same profile protect the same set of VLANs, or the VLANs protected by one instance are a subset of LANs protected by another instance. This name can be up to 32 characters long. Select the Specify radio button to configure this parameter as per normal. Select the None radio button to revert this parameter to the default setting.
RPL Port	Select the checkbox and then select the RPL port option here. Options to choose from are Port0 and Port1 . The option selected will be configured as the RPL port.
RPL Owner	Select the checkbox and then select whether this node is the RPL owner or neighbor. Options to choose from are Enabled and Disabled . Enabling this option will specify this RPL as an owner.
Activate	Select the checkbox and then select whether or not to active this ERP instance. Options to choose from are Enabled and Disabled . Enabling this option will active this ERP instance.

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

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

After click the Show Status button, the following window will appear.

ERPS Status		
n allumma'ni waluk 2980		
HINGTH HILL	xed.	
Instance ID	,	
Description		
HEL		
R-APS Chan el	realist aux dat	
Modes I ST MERS		
POLI 1		
Guassi Timer	Sti na	
Hold-C 1 Timer) m	
WIRLING .	Simi-	
Here of we	Provide a local de la construcción de la construcci	
Instance state	Handverse	
Acat a GPL	·	
Operational FIPL	•	
Podo Stala	Purve dire	
Poltatata	Kunsadan	
ACIE DIRET, EDIT		
Operational RPL Port	·	
		K ale

Figure 5-52 ERPS (Show Status) Window

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

ERPS Profile

This window is used to view and configure the Ethernet Ring G.8032 profile settings.

To view the following window, click L2 Features > ERPS (G.8032) > ERPS Profile, as shown below:

thannel Ring C.0653 Prol				
- cite Han e	te cher	1		Angle Delex
Tokal Calarka: 1				
V MARKAD	10 CON	en s	Part State	
Porte		ward at the	PERAPOSE (IPL)	L HEREI
PORT		*********	P1860001	Carlot a starting

Figure 5-53 ERPS Profile Window

The fields that can be configured are described below:

Parameter	Description
Profile Name	Enter the G.8032 profile's name here. This name can be up to 32 characters long. Multiple ERP instances can be associated with the same G.8032 profile. The instances associated with the same profile protect the same set of VLANs, or the VLANs protected by one instance are a subset of LANs protected by another instance.

Click the **Apply** button to associate the G.8032 profile with the ERP instance created.

Click the **Delete** button to disassociate the G.8032 profile based on the **Profile Name** entered.

Click the Edit button to modify the specified G.8032 profile.

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

E St Libernet Prohie		
Citizativei Frantis Sectional		
How Have	P116	
D. Mercula de C.	District (M)	
- Healthe	(Fielder) [M]]	
Contine (K-25X)	policie de la companya de la compa	
1 (d-01Timer (0-1000)	i a j	
WTR Timer (1-(2)	r te	
		But I State

Figure 5-54 ERPS Profile (Edit) Window

The fields that can be configured are described below:

Parameter	Description
TCN Propagation	Select the checkbox and then select the TCN propagation state. Options to choose from are Enable and Disabled . This function is used to enable the propagation of the topology change notifications from the sub-ERP instance to the major instance.
Revertive	Select the checkbox and then select the revertive state. Options to choose from are Enable and Disabled . This function is used to revert back to the working transport entity, for example, when the RPL was blocked.

Parameter	Description
Guard Timer	Select the checkbox and enter the guard timer value here. This value must be between 10 and 2000 milliseconds. By default, this value is 500 milliseconds.
Hold-Off Timer	Select the checkbox and enter hold-off timer value here. This value must be between 0 and 10000 milliseconds. By default, this value is 0 milliseconds.
WTR Timer	Select the checkbox and enter the WTR timer value here. This value must be between 1 and 12 minutes. By default, this value is 5 minutes.

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

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

Loopback Detection

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 function can be implemented on a range of ports at a time. The user may enable or disable this function using the drop-down menu.

To view the following window, click **L2 Features > Loopback Detection**, as shown below:

shace Matchion & Sharp 5.4	01			
obadi Colocilei Olma	Crasled S	Her.P	Per-based R	
ON A AMERICAN	- WA	ana paraz	16 Jac	
et de la	Disepter ⊻	14 m	Studern 👱	
train Type	Variation 🔍	Canalis a Versilari	₩.Ø	La contrate de
nación de la compañía	20.			
nestenan rereite	us Danist <u>(desx</u>)	2 B.M	ANEN N Sale	Tereford mode
	- Fanist <u>(dt.)</u>			· · · · · · · · · · · · · · · · · · ·
<u>* 8</u>	Tanist (#133			100.000
<u>1 8</u>	Tanitat <u>(2003)</u> Denosio	dergraft aller	WW1	na anges
1 1 <u>1 19</u> (111) (111) (111)	Tenrot jørste Derover Der Der	(MCCUN) ALLAN alkad	Kital Farm Farm Karn	in o ys
2000 (0.00) (0.00) (0.00) (0.00)	Tonitet <u>(2003)</u> Deniesti De Pr 	ferigner aller alles agent	Arel Fam Fam Fam Fam	NSD.
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Tentet (/#53) Detector De Content De De Content De De De Content D	feriting aller alled alled aller	Notal Form Form Vota	in o ys

Figure 5-55 Loopback Detection Window

The fields that can be configured for Loopback Detection Global Settings are described below:

Parameter	Description
Loopback Detection State	Select to enable or disable loopback detection. The default is Disabled .
Mode	Select the loopback detection mode. Options to choose from are Port-based and VLAN-based .
Enable VLAN ID List	Enter the VLAN ID for loop detection. This only takes effect when the VLAN-based is selected in the Mode drop-down list.

Parameter	Description
Interval	Enter the interval in seconds that the device will transmit all the CTP (Configuration Test Protocol) packets to detect a loop-back event. The valid range is from 1 to 32767 seconds. The default setting is 10 seconds.
Traps State	Select to enable or disable the loopback detection trap state.
Action	 Select the action that will be taken here. Options to choose from are: Shutdown - Specifies that when a loop was detected, the port will be shut down (disabled) in the port-based mode. Traffic will be blocked on the specific VLAN in the VLAN-based mode. None - Specifies that when a loop was detected, the port will not be disabled in the port-based mode. Traffic will not be block on the specific VLAN in the VLAN-based mode. Only log and trap messages will be sent.
Address Type	 Select the address type here. This is used to configure the destination address type in LBD packets for loopback detection. Options to choose from are: Multicast - Specifies that only multicast LBD packet will be sent. The destination address is CF-00-00-00-00. Broadcast - Specifies that only broadcast LBD packet will be sent. The destination address is FF-FF-FF-FF-FF.

The fields that can be configured for Loopback Detection Port Settings are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable the state of the port.

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

Link Aggregation

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 32 port trunk groups with 1 to 8 ports in each group.



Figure 5-56 Example of Port Trunk Group

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 32 link aggregation groups, each group consisting of 1 to 8 links (ports). Each port 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 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.

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.

This window is used to view and configure the link aggregation settings.

To view the following window, click L2 Features > Link Aggregation, as shown below:

Ink Appropria	ñ				
Normal Printpolitik 1 Juli - Status Kapa Normal II	n de g Tele	t nis Source Destination S Source destination S	61		7304 8304
Covered Strary Inte	netari —				
Contraction and the second	40746 54701 - 91	Taffail (en: 3/11)(P)	Girada (D.(1-02)	989 [00	rad (Merservale Par)
	and the second	a para none per			
Data English: 1					
Charles and Berrie p	PROVAL	NAC FORM	MARA STREET	Manager Ports	
Patistran e	Shik	8		1040-0210	Cales Channel, Channel Level 1
and the second second second					

Figure 5-57 Link Aggregation Window

The fields that can be configured for Link Aggregation are described below:

Parameter	Description
System Priority	Enter the system's priority value used here. This value must be between 1 and 65535. By default, this value is 32768. The system priority determines which ports can join a port-channel and which ports are put in the stand-alone mode. The lower value has a higher priority. If two or more ports have the same priority, the port number determines the priority.
Load Balance Algorithm	Select the load-balancing algorithm that will be used here. Options to choose from are Source MAC, Destination MAC, Source Destination MAC, Source IP, Destination IP, and Source Destination IP. By default, this option is Source MAC.

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

The fields that can be configured for **Channel Group Information** are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Group ID	Enter the channel group number here. This value must be between 1 and 32. The system will automatically create the port-channel when a physical port first joins a channel group. An interface can only join one channel-group.
Mode	Select the mode option here. Options to choose from are On , Active , and Passive . If the mode On is specified, the channel

Parameter	Description
	group type is static. If the mode Active or Passive is specified, the channel group type is LACP. A channel group can only consist of either static members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group.

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

Click the **Delete Member Port** button to remove the specific member port.

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

Click the **Channel Detail** button to view detailed information about the channel.

After clicking the **Channel Detail** button, the following page will be available.

al Chanal Groot	Alte .					
NiCland	1					
O exception	and shares					- 4000c
For	318	24	ANTERSTREES	(escription		
Pel-daniti	du.		u nost			Deleter Clust 1 other
100 Charlos II Anio						
Evil Sharmyl	11					
Matheat	20. de 1					
Vel Channel Octain	foresto.		10 1. A 200 A 44			
795.	LACP Ten pai	Weeking No.	k LACE star	Part Princh	Post Van Ser	_8
-0.03739	Man	P.R.F.	(8)	Hart	Qui e	COLUMN STATE
ana ta	. New	1001	C63.	Holen	inere .	100 B.M.
W10.2.72	5000	(SAC) -	(060)	Hotes	1,000	7.8
676323	1010	hare .	(20	Hom	1000	1.8
Vel Channel Heidda	u hlandar					
Dat .	la wa Siska 10	Pates Pollo	Partavi GACP Teresal	Park a Workking	Rede Fr	tan Post Pokely
and the second second	R.w.s	2.40	(6) (a)	HOLT		8.00
armannah	and a second sec	1940	incises -	NOP 5		HWA
amikei)	11.51.0	(Asia)	HARDA.	John S.		11.57.6
#30.6045	tione.	223	Horse	Hore		2000
Now:						. 24di
CALL ADD.						
	k an aggingern and ba					
		ten netzen en zoiten ten				
Intoise Detivities	2.0 a 3.4 visits					

Figure 5-58 Port Channel Window

The fields that can be configured for **Port Channel Description** are described below:

Parameter	Description
Description	Enter the description for the port channel here. This can be up to 64 characters long.

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

Click the **Delete Description** button to clear the setting in the corresponding Description field.

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

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

L2 Multicast Control

IGMP Snooping

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.

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.

To view the following window, click L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings, as shown below:

GMI1 Shooping Settings			
HOSH HATEIGE			
	CHARM BORN		less is
NAR SIAN SUBJECT			
VIC 0-1690	id find er i∳Dtadet		k, e
owe service of the			
VIC 11-0094			Line and A
INFINIS 1			
101	AT KHI NA WY	tter c	
1	1.15	In Alter	Starte Data Edit

Figure 5-59 IGMP Snooping Settings Window

The field that can be configured for **Global Settings** is described below:

Parameter	Description
Global State	Select this option to enable or disable IGMP snooping global state.

Click the Apply button to accept the changes made.

The fields that can be configured for **VLAN Status Settings** are described below:

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094, and select to enable or disable IGMP snooping on the VLAN.

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

The fields that can be configured for IGMP Snooping Table are described below:

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094.

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

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

Click the Show Detail button to see the detail information of the specific VLAN.

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 Show Detail button, the following window will appear.

2014 Shooping VLAN Parameter	9	
A25	±.	
Tait #	Finalised	
4 Timum Vorgion	41	
Cast Laws	Desblad (histored)	
Resold Suppression	Disabled	
toppesse out time	'O associate	
busher@tate	Disables	
Dura y Merson	a	
ium Interval	125 decords	
tal Respective Time	10 seconda	
Roductionen Value	0	
aat Nambar Coary Arterval	t awourder	
Provi Reporting	Fileshied Source address (20.010)	

Figure 5-60 IGMP Snooping VLAN Parameters Window

The window displays the detail information about IGMP snooping VLAN. Click the **Modify** button to edit the information in the following window.

After clicking the **Modify** or **Edit** button in IGMP Snooping Settings window, the following window will appear.

UNIV Secoperg VLAN Settings		
VID (1.4004)	1	
8whit	*Erablen Ocablen	
Himemyatan	1 •	
FastLaske	GEFANCE & DISANCE	
Record Supposes on	(Draties offersides	
Suppress on Time (1 801)	10	
Queter State	(Fotbled in Peabled	
Query Version	2 *	
Guary Internal (1-34744)	125 000	
Nav Record on Title (1925)	10	
Hornaultrau Value (%-11	2	
Last Memoer Query Werkel (* 25)	1 000	
Prog Reporting	Ecoblect in Cleanbert Sound Address	
	· · · · · · · · · · · · · · · · · · ·	doole.

Figure 5-61 IGMP Snooping VLAN Settings Window

The fields that can be configured are described below:

Parameter	Description
Minimum Version	Select the minimum version of IGMP hosts that is allowed on the VLAN.
Fast Leave	Select this option to enable or disable the IGMP snooping fast leave function. If enabled, the membership is immediately removed when the system receive the IGMP leave message.
Report Suppression	Select this option to enable or disable the report suppression. The report suppression function only works for IGMPv1 and IGMPv2 traffic. When report suppression is enabled, the Switch suppresses the duplicate reports sent by hosts. The suppression for the same group report or leave will continue until the suppression time expired. For report or leave messages to the same group, only one report or leave message is forwarded. The remaining report and leave messages are suppressed.
Suppression Time	Enter the interval of suppressing duplicate IGMP reports or leaves. The range is from 1 to 300.
Querier State	Select this option to enable or disable the querier state.
Query Version	Select the general query packet version sent by the IGMP snooping querier. Options to choose from are 1 , 2 , and 3 .
Query Interval	Enter the interval at which the IGMP snooping querier sends IGMP general query messages periodically.
Max Response Time	Enter the maximum response time, in seconds, advertised in IGMP snooping queries. The range is 1 to 25.
Robustness Value	Enter the robustness variable used in IGMP snooping.
Last Member Query Interval	Enter the interval at which the IGMP snooping querier sends IGMP group-specific or group-source-specific (channel) query messages.
Proxy Reporting	Select this option to enable or disable the proxy-reporting function.
Source Address	Enter the source IP of proxy reporting. This is available when Enabled is selected in Proxy Reporting .

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

IGMP Snooping Groups Settings

This window is used to configure and view the IGMP snooping static group, and view IGMP snooping group.

To view the following window, click L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Groups Settings, as shown below:

IN NEWSDORING MADE									
VICT-9680	Seallip Advised	3240		free too		Te Peri	-	100000000000000000000000000000000000000	
		1.11	N.	No.02	1.1	onid9		- April April - Comp	- Orderlander
to ne state	Cess;	1.4.2014.0							
1	- 1 es							L Barris	
AN FORME 1									
Wi I	11		òrea	ANY NA					uni
14			, t	11.2.1.2					
							13	u lered 🚺 🗄	
Richard State									
ang way		1.000							
d.	1. 1.4.1		-					. Dec	
distance to									
SW052	Usep Address	100	_	Seate 644			14	Franker	Pus

Figure 5-62 IGMP Snooping Groups Settings

The fields that can be configured for **IGMP Snooping Static Groups Settings** are described below:

Parameter	Description
VID	Enter a VLAN ID of the multicast group.
Group Address	Enter an IP multicast group address.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
VID	Click the radio button and enter a VLAN ID of the multicast group.
Group Address	Click the radio button and enter an IP multicast group address.

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

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

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

Click the Find All button to view all the entries.

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

The fields that can be configured or displayed for **IGMP Snooping Groups Table** are described below:

Parameter	Description
VID	Click the radio button and enter a VLAN ID of the multicast group.
Group Address	Click the radio button and enter an IP multicast group address.
FM	Displays the filter mode. The value of the filter mode can be either IN (Include) or EX (Exclude).
	IN (Include) - The filter mode is Include.

Parameter	Description
	EX (Exclude) - The filter mode is Exclude.
Exp (sec)	Display the time left in seconds before the entry expires.

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

Click the Find All button to view all the entries.

IGMP Snooping Mrouter Settings

This window is used to configure the specified interface(s) as the multicast router ports or as forbidden to be multicast router ports on the Switch.

To view the following window, click L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Mrouter Settings, as shown below:

ACC 1: 40901	Cortgination		11.0		Frank Frank	and the second second	10.207			
	Pret	1	1	x.	49124	12	111100	E.	1 Antro	Seide
10.01-4094	-								26.8	ind of
AC D. HOHO										
				_		Perm		_		

Figure 5-63 IGMP Snooping Mrouter Settings Window

The fields that can be configured for IGMP Snooping Mrouter Settings are described below:

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094.
Configuration	Select the port configuration. Options to choose from are:
	 Port - Select to have the configured ports to be static multicast router ports. Forbidden Port - Select to have the configured ports not to be multicast router ports.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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

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

The fields that can be configured for IGMP Snooping Mrouter Table are described below:

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094.

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

Click the Find All button to view all the entries.

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

IGMP Snooping Statistics Settings

This window is used to clear and display the IGMP snooping related statistics.

To view the following window, click L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings, as shown below:



Figure 5-64 IGMP Snooping Statistics Settings Window

The fields that can be configured for IGMP Snooping Statistics Settings are described below:

Parameter	Description
Statistics	Select the interface here. Options to choose from are AII , VLAN , and Port .
VID	Enter a VLAN ID between 1 and 4094. This is available when VLAN is selected in the Statistics drop-down list.
Unit	Select the switch unit that will be used for this configuration here. This is available when Port is selected in the Statistics drop-down list.
From Port / To Port	Select the appropriate port range used for the configuration here. This is available when Port is selected in the Statistics drop-down list.

Click the **Clear** button to clear the IGMP snooping related statistics.

The fields that can be configured for IGMP Snooping Statistics Table are described below:

Parameter	Description
Find Type	Select the interface type. Options to choose from are VLAN, and Port.
VID	Enter a VLAN ID between 1 and 4094. This is available when VLAN is selected in the Find Type drop-down list.
Unit	Select the switch unit that will be used for this configuration here. This is available when Port is selected in the Find Type drop-down list.
From Port / To Port	Select the appropriate port range used for the configuration here. This is available when Port is selected in the Find Type drop-down list.

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

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

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

MLD Snooping

Multicast Listener Discovery (MLD) Snooping is an IPv6 function used similarly to IGMP snooping in IPv4. It is used to discover ports on a VLAN that are requesting multicast data. Instead of flooding all ports on a selected VLAN with multicast traffic, MLD snooping will only forward multicast data to ports that wish to receive this data through the use of queries and reports produced by the requesting ports and the source of the multicast traffic.

MLD snooping is accomplished through the examination of the layer 3 part of an MLD control packet transferred between end nodes and a MLD router. When the Switch discovers that this route is requesting multicast traffic, it adds the port directly attached to it into the correct IPv6 multicast table, and begins the process of forwarding multicast traffic to that port. This entry in the multicast routing table records the port, the VLAN ID, and the associated multicast IPv6 multicast group address, and then considers this port to be an active listening port. The active listening ports are the only ones to receive multicast group data.

MLD Control Messages

Three types of messages are transferred between devices using MLD snooping. These three messages are all defined by four ICMPv6 packet headers, labeled 130, 131, 132, and 143.

- **Multicast Listener Query** Similar to the IGMPv2 Host Membership Query for IPv4, and labeled as 130 in the ICMPv6 packet header, this message is sent by the router to ask if any link is requesting multicast data. There are two types of MLD query messages emitted by the router. The General Query is used to advertise all multicast addresses that are ready to send multicast data to all listening ports, and the Multicast Specific query, which advertises a specific multicast address that is also ready. These two types of messages are distinguished by a multicast destination address located in the IPv6 header and a multicast address in the Multicast Listener Query Message.
- Multicast Listener Report, Version 1 Comparable to the Host Membership Report in IGMPv2, and labeled as 131 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.
- **Multicast Listener Done** Akin to the Leave Group Message in IGMPv2, and labeled as 132 in the ICMPv6 packet header, this message is sent by the multicast listening port stating that it is no longer interested in receiving multicast data from a specific multicast group address, therefore stating that it is "done" with the multicast data from this address. Once this message is received by the Switch, it will no longer forward multicast traffic from a specific multicast group address to this listening port.
- **Multicast Listener Report**, **Version 2** Comparable to the Host Membership Report in IGMPv3, and labeled as 143 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.

MLD Snooping Settings

This window is used to configure the MLD snooping settings.

To view the following window, click L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Settings, as shown below:

VED 0-4690 Centre: @Checked Construction VED 0-4690 Centre: @Checked VED 0-4690 Centre: @Checked Centre: @Ch	
A AM Selve Schem VE 10-KSHO / Endter @Classed VE 10-KSHO /	100 V
VERSIONER LENGT	
90.11-6090 L	
Index Filmes 1	
AND AT AN AS AN	
t the brand Sector	140

Figure 5-65 MLD Snooping Settings Window

The field that can be configured for **Global Settings** is described below:

Parameter	Description
Global State	Select this option to enable or disable MLD snooping global state.

Click the Apply button to accept the changes made.

The fields that can be configured for VLAN Status Settings are described below:

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094, and select to enable or disable MLD snooping on the VLAN.

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

The fields that can be configured for **MLD Snooping Table** are described below:

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094.

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

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

Click the Show Detail button to see the detail information of the specific VLAN.

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 Show Detail button, the following window will appear.

LD Brooping VLAN Pa		
LD Shooping VLAR Parameter	ř.	
ve:	±1	
Plaisa -	Frahled	
Hintimum Aproxim	41	
Decil away	Disabled (histored)	
Report Suppression	Disables	
Expressed on Tartes	1) assessed	
Prog Reporting	Disabled: Source Address (c)	
Home Protocomy	Eralded	
Guener State	Disables	
Query Mession	2	
Gurs Interal	125 seconds	
Has Responsed inter	10 seconda	
Robushase Value	2	
Lastic status Guary Internal	t accents	
ACCESS/ACCESSION		Maadiy

Figure 5-66 MLD Snooping VLAN Parameters Window

The window displays the detail information about MLD snooping VLAN. Click the **Modify** button to edit the information in the following window.

After clicking the **Modify** or **Edit** button in MLD Snooping Settings window, the following window will appear.

ILD Snooping VLAN Soldr	ige.		
NED Shooping VEAN Solange			
VID (1.4004)	ić.		
Subir	+ Etablet - Ois	abiten 🚬	
Honsmessen	1		
FastLizzie	CErabio (O)s	Mice .	
Recutfuppession	ODestine (Con	difest	
Suppress on Time (1933)	10		
Hibe Hapothip	C Problem (g Pre Courte Address	Ant	
Hivoter Porticitaring	BERING OUS	010	
Ocenter State	C:Pophlattin/Se	dd+m	
Query Version	2		
Guery Interval (1-94744)	125	166	
No. Response Time (1925)	10		
Robushead Value (1-71	2		
LassUplener Quen Interval (* 253	1	504	
		15149	Apply

Figure 5-67 MLD Snooping VLAN Settings Window

The fields that can be configured are described below:

Parameter	Description
Minimum Version	Select the minimum version of MLD hosts that is allowed on the VLAN.
Fast Leave	Select this option to enable or disable the MLD snooping fast leave function. If enabled, the membership is immediately removed when the system receive the MLD leave message.

Parameter	Description
Report Suppression	Select this option to enable or disable the report suppression.
Suppression Time	Enter the interval of suppressing duplicate MLD reports or leaves. The range is from 1 to 300.
Proxy Reporting	Select this option to enable or disable the proxy-reporting function.
Source Address	Enter the source IPv6 of proxy reporting. This is available when Enabled is selected in Proxy Reporting .
Mrouter Port Learning	Select this option to enable or disable Mrouter port learning.
Querier State	Select this option to enable or disable the querier state.
Query Version	Select the general query packet version sent by the MLD snooping querier. Options to choose from are 1 , and 2 .
Query Interval	Enter the interval at which the MLD snooping querier sends MLD general query messages periodically.
Max Response Time	Enter the maximum response time, in seconds, advertised in MLD snooping queries. The range is 1 to 25.
Robustness Value	Enter the robustness variable used in MLD snooping.
Last Listener Query Interval	Enter the interval at which the MLD snooping querier sends MLD group-specific or group-source-specific (channel) query messages.

MLD Snooping Groups Settings

This window is used to configure and view the MLD snooping static group, and view MLD snooping group.

To view the following window, click L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Groups Settings, as shown below:



Figure 5-68 MLD Snooping Group Settings Window

The fields that can be configured for MLD Snooping Static Groups Settings are described below:

Parameter	Description
VID	Enter a VLAN ID of the multicast group.
Group Address	Enter an IPv6 multicast group address.

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
VID	Click the radio button and enter a VLAN ID of the multicast group.
Group Address	Click the radio button and enter an IP multicast group address.

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

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

Click the Find All button to view all the entries.

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

The fields that can be configured or displayed for **MLD Snooping Groups Table** are described below:

Parameter	Description
VID	Click the radio button and enter a VLAN ID of the multicast group.
Group Address	Click the radio button and enter an IPv6 multicast group address.
FM	Display the filter mode. The value of the filter mode can be either IN or EX .
	 IN (Include) - The filter mode is Include. EX (Exclude) - The filter mode is Exclude.
Exp (sec)	Display the time left in seconds before the entry expires.

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

Click the Find All button to view all the entries.

MLD Snooping Mrouter Settings

This window is used to configure the specified interface(s) as the router ports or forbidden to be IPv6 multicast router ports on the VLAN interface on the Switch.

To view the following window, click L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Mrouter Settings, as shown below:

0.011080	Config Italiae	100		Front Fort	To Port			
	Port	 1	-	V1124	D rttre	नि	L Artes	Tel da
to since any more	NF (1945						().	
10 (1.4094)	ine taxin						1	- Sided
10 (1.4094) 019 FRIDKS 1	0			_	ANTA		<u></u>	i aadaa

Figure 5-69 MLD Snooping Mrouter Settings Window

The fields that can be configured for MLD Snooping Mrouter Settings are described below:

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094.
Configuration	 Select the port configuration. Options to choose from are: Port - Select to have the configured ports as being connected to multicast-enabled routers. Forbidden Port - Select to have the configured ports as being not connected to multicast-enabled routers. Learn pimv6 - Select to enable dynamic learning of multicast router port.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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

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

The fields that can be configured for MLD Snooping Mrouter Table are described below:

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094.

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

Click the Find All button to view all the entries.

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

MLD Snooping Statistics Settings

This window is used to clear and display the MLD snooping related statistics.

To view the following window, click L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Statistics Settings, as shown below:

Contraction of the second s	100000 20000		10.0	19626	2.22 C	To Port		
artor F	MD(14661)	-	104.	- 500 - 17	And the second se	CONTRACTOR OF STREET	- 19 C	du.
	11 12			and then	in the	The second	100	
sisting and she she	A faile a							
d free	0.M002#845	the second second second		tere ter	o the first of			
00520		1.1.		11101	- Pinney		- 192	Dos Al
LAN E		and the second se						
						1.20	1.00	1. 10000
N. FINOS 1							1.12	1 1.8.4
					Vic.			
N FORK 1	100		et D				IX	TX
		PL.			Vic.	wa		1 252.00

Figure 5-70 MLD Snooping Statistics Settings Window

The fields that can be configured for MLD Snooping Statistics Settings are described below:

Parameter	Description
Statistics	Select the interface here. Options to choose from are AII , VLAN , and Port .

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094. This is available when VLAN is selected in the Statistics drop-down list.
Unit	Select the switch unit that will be used for this configuration here. This is available when Port is selected in the Statistics drop-down list.
From Port / To Port	Select the appropriate port range used for the configuration here. This is available when Port is selected in the Statistics drop-down list.

Click the Clear button to clear the MLD snooping related statistics.

The fields that can be configured for MLD Snooping Statistics Table are described below:

Parameter	Description
Find Type	Select the interface type. Options to choose from are VLAN, and Port.
VID	Enter a VLAN ID between 1 and 4094. This is available when VLAN is selected in the Find Type drop-down list.
Unit	Select the switch unit that will be used for this configuration here. This is available when Port is selected in the Find Type drop-down list.
From Port / To Port	Select the appropriate port range used for the configuration here. This is available when Port is selected in the Find Type drop-down list.

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

Click the Find All button to view all the entries.

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

Multicast Filtering

This window is used to view and configure the Layer 2 multicast filtering settings.

To view the following window, click L2 Features > L2 Multicast Control > Multicast Filtering, as shown below:

Anteon Trees				
меси	<u>paret 1</u>	NA STORA PEA	Forward Uning started In	- (6 <i>4)</i>
Corte Entrine: 1				
	distantion of the second se			
	a ke		NUMBER OF STREET	
	yilan debat	_	na arviant e are inser- Decensi Using Marine Cro	



The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list that will be used for this configuration here.
Multicast Filter Mode	Select the multicast filter mode here. Options to choose from are:

Parameter	Description
	 Forward Unregistered - Specifies that registered multicast packets will be forwarded based on the forwarding table and all unregistered multicast packets will be flooded based on the VLAN domain. Forward AII - Specifies that all multicast packets will be
	flooded based on the VLAN domain.
	 Filter Unregistered - Specifies that registered packets will be forwarded based on the forwarding table and all unregistered multicast packets will be filtered.

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

LLDP

LLDP Global Settings

This window is used to configure the LLDP global settings.

To view the following window, click L2 Features > LLDP > LLDP Global Settings, as shown below:

LLUP Global Settings		
LLDP Cicital Settingy		
1107.9979	⊖Enabled ⊕Citabled	
1.10F Force of State	CEnders - @Clarked	
LL0P Truc State	CEnders @Diversed	
LLDP-MED Tray Galv	Canabiesi @Clivebied	Assiv
TTTPSMH012000g002000		
First Glad Ryperd Count (1-10)	4 Ja 10.	Apply
LLDP Configurations		
Mercurya IX Interval (* 2748)	xe on	
Mercury: 12 How Malphot (2.13)	4 205	
Real Decay of the	2 23	
(2.15687) (2-318-7	×945	-2(4)2
LEDP Ayation Information		
Disc & R.Adappe	MACO FAILURY	
Church ID	30546-64-641489-61	
System Nerre	Grauth	
Nychen Execution	Aspalat Historial Aspacisio Astro-	
Sectors Capabilities Salavelad	Byzanier, Bedev	
Styring Constanting + March -	Hope and Horge	
UDDMSD System Information		
Derive Class	Network Connectivity Device	
Handester Brein an	A1	
Financial Review	1.03.015	
2010-2010 Hitel Auto	171007	· · · · · · · · · · · · · · · · · · ·
Seria Humber	R25V1P1000011	

Figure 5-72 LLDP Global Settings Window

The fields that can be configured for LLDP Global Settings are described below:

Parameter	Description
LLDP State	Select this option to enable or disable the LLDP feature

Parameter	Description
LLDP Forward State	Select this option to enable or disable LLDP forward state. When the LLDP State is disabled and LLDP Forward Sate is enabled, the received LLDPDU packet will be forwarded.
LLDP Trap State	Select this option to enable or disable the LLDP trap state.
LLDP-MED Trap State	Select this option to enable or disable the LLDP-MED trap state.

The fields that can be configured for LLDP-MED Configuration are described below:

Parameter	Description
Fast Start Repeat Count	Enter the LLDP-MED fast start repeat count value. This value must be between 1 and 10.

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

The fields that can be configured for LLDP Configurations are described below:

Parameter	Description
Message TX Interval	Enter the interval between consecutive transmissions of LLDP advertisements on each physical interface. The range is from 5 to 32768 seconds.
Message TX Hold Multiplier	Enter the multiplier on the LLDPDUs transmission interval that used to compute the TTL value of an LLDPDU. This value must be between 2 and 10.
Relnit Delay	Enter the delay value for LLDP initialization on an interface. This value must be between 1 and 10 seconds.
TX Delay	Enter the delay value for sending successive LLDPDUs on an interface. The valid values are from 1 to 8192 seconds and should not be greater than one-fourth of the transmission interval timer.

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

LLDP Port Settings

This window is used to configure the LLDP port settings.

To view the following window	, click L2 Features > LLDP > LLDP Port Settings	a abour bolow:
	, CIICK LZ Features > LLDF > LLDF Fort Settings	, as shown below.

PPstSelan				
i Crimière	To fast institute	iny dalitype	Admin State (17 Salaty)	a action Acquires
v mbille v	an 124 w Dash	ere lars	Tx and BX	V Brrow V
IN THE DESIGNATION OF ST	d to the Gelder's secret.		2011a	and the state of t
COMPANY.				181 - 1819/ - J
Part	All the set of	9.644.0	Action Alters	LAND-DALLARS.
enter.	Diant est	Lon .	74 mm FX	
41022	Did w	(Lies)	TARK TX	
4033	Deut ev-	1.00	100.00	
4/0/64	(BC)(Ca)	204	124.46	
Analasia	(anne let)	1002	n me Ka	
en122	Titusk wr.	1003	The sec \$2	
dit127	Disat ed	Loca 1	73 are 52	
411/2/2	Drukou	1001	TANK MARK	
10731	Or ever	0042	Care MS	
Verty bits	10(90.00)	1102	102.82	
Advections	filmst en	1001	The mar Ref.	
48/10/12	Disc at	Lices	TA WE THE	
V8.4012	Dridini	Ucti	The state	
10.000	(they do not)	30mF	Epie MC	
You have	decembring.	17622	t the Ma	
10/2/016	Discover.	1103	To pre 400	
40:40:17	Dist ed	Local	The area fixe	
10010	Disat po	Lon.	TABLE IX	
0.079.035	Ur, d (n)	3004	18 p. 0. 197	
(Artshire)	conclusion in	114	Data etc	
ARX/0.5	tana se	1103	t the KK	
C/C/296	District	1263	Think RC	
	Diret wi	Lives	72.000.723	
48.3324	Ur, duration	inst.	TR p. 6. 112	

Figure 5-73 LLDP Port Settings Window

The fields that can be configured are described below:

Parameter	Description		
Unit	Select the switch unit that will be used for this configuration here.		
From Port / To Port	Select the appropriate port range used for the configuration here.		
Notification	Select this option to enable or disable the sending of LLDP notifications.		
Subtype	Select the subtype of LLDP TLV(s). Options to choose from are MAC Address , and Local .		
Admin State	Select the local LLDP agent and allow it to send and receive LLDP frames on the port. Options to choose from are:		
	 TX - The local LLDP agent can only transmit LLDP frames. RX - The local LLDP agent can only receive LLDP frames. TX and RX - The local LLDP agent can both transmit and receive LLDP frames. This is the default option. Disabled - The local LLDP agent can neither transmit nor receive LLDP frames. 		
IP Subtype	Select the type of the IP address information to be sent. Options to choose from are Default , IPv4 , and IPv6 .		

Parameter	Description
Action	Select the action that will be taken here. Options to choose from are Remove and Add .
Address	Enter the IP address that will be sent.



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

LLDP Management Address List

This window is used to view the LLDP management address list.

To view the following window, click L2 Features > LLDP > LLDP Management Address List, as shown below:

-				
No. of Concession, Name	2000000		1176	
errite	And the second s	IF-1996		Activitiang Parts



The fields that can be configured are described below:

Parameter	Description	
All/IPv4/IPv6	Select the subtype. Options to choose from are AII , IPv4 , and IPv6 .	

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

LLDP Basic TLVs Settings

Type-length-value (TLV) 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.

To view the following window, click **L2 Features > LLDP > LLDP Basic TLVs Settings**, as shown below:

i For Pet	ToPort	Per Description	ilydan Bana	Eystern Costription	Bytten Capacities	i
 obdive z 	anan 🔺	Disabled a	Neaked 2	Distant 2	Near of St.	250.5
i t Sitilaipi					ng 20070	21. S.114
that	Paid Changeloin	9,00	en Marine	Spikeralization		Apple a Copietale est
which the	Decition.	C.	abid (Displace.		Drawed
COLUMN .	100/4/10	10	i 6 1	10.54 M (00.00-1
Although a	190AbAd		anen -	11/dhiek		isoner .
de la	Database	6	ursed	E sobiet		(Louisied
48/105	Directive	0	ni olivid	Exposed		Divebled
10.335	Devition	0	n fed	Danks		Divational
01.027	Desider	0	6.6.5	0.4060		(Materia)
100/0168	100/01/0		1.9.1	0.500.0		0.000
ARCO 89	(HEADAR)	- (P	urană	(Crimeri		(adapted)
atb/10/10	Dissbiler	0.	orbed	Disbled		Encessed
wh14015	Denabli vil.	0	acted 1	Divisional		Dirabilid
130032	06.04	0.0	atal i	C.A.A.D		thuside)
CARDING	Strade et	0	2 H F	17.00.1		Brothil
STREET,	1003036	- 6	uner)	11/19/3		(17/men)
40010005	Tim Mp Avi	0	to set d	ELLANES.		Octable 5

Figure 5-75 LLDP Basic TLVs Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Port Description	Select this option to enable or disable the Port Description option.
System Name	Select this option to enable or disable the System Name option.
System Description	Select this option to enable or disable the System Description option.
System Capabilities	Select this option to 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.

To view the following window, click L2 Features > LLDP > LLDP Dot1 TLVs Settings, as shown below:

(10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000) (10.000)	i inchi 2 inthi	i 🔄 jaman ja	Partician Protocolism District - Production	V. AR Now	Brahamideniny Brahamideniny Brahamideniny Market Andrea
NEWLIN NEWLIN	LI Selley				
Normal Normal	Pori	Part VLAH D	Enabled Portland Protocol VIC	Disabled VLAS North	Crasted Protocol Idealty
eP (2a) Data or	on the second	Jacob et al.			
eff (24) Dinit effective eff (24) Dinit effective eff (24) Dinit effective eff (24) Dinit effective eff (24) Dinit effective val (24) Dinit eff	OR SUB-	HEADAY.			
vill 1028 Divid vs (# 1024 - 000 to c 000 to c 000 to c 000 Divid vs 000 Divid vs 000 Divid vs 000 Divid vs	APSON	Database			
i Balani - Balani - Constani - Co	alt 10 a				
AR VER VIEW AR VER VIEW AR VER VIEW AR VER VIEW AR VER VIEW AR VER VIEW AR VER VIEW	vili 1/2(8-)	Dividing			
an San Angelan An San Angelan An Old Data an An Old Data an	(B. 16 Bel)	and the second			
e#1532 Disk:ec ch.0013 Disk:ex ch.0014 Disk.ex	olitika k	16020 (m)			
an 1913 - Dhah ay 1919 - Dhah a	ARS(3)	File Active			
dener (non a	48.532	Otake set			
	0.00 %	Divit w			
101410 101410 -	1999	Dutin			
	110012	105300			
TOPHI DESEN	anteria:	1903030			
	DE	tabled			



The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Port VLAN	Select this option to enable or disable the port VLAN ID TLV to send. The Port VLAN ID TLV is an optional fixed length TLV that allows a VLAN bridge port to advertise the port's VLAN identifier (PVID) that will be associated with untagged or priority tagged frames.
Protocol VLAN	Select this option to enable or disable Port and Protocol VLAN ID (PPVID) TLV to send, and enter the VLAN ID in PPVID TLV.
VLAN Name	Select this option to enable or disable the VLAN name TLV to send, and enter the ID of the VLAN in the VLAN name TLV.
Protocol Identity	Select this option to enable or disable the Protocol Identity TLV to send, and the protocol name. Options for protocol name to choose from are None , EAPOL , LACP , GVRP , STP , and 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.

To view the following window, click L2 Features > LLDP > LLDP Dot3 TLVs Settings, as shown below:

ant sea	o w. wings						
4 (5)	Danifys Ventum (a)	tetai <u>ottot ai</u>	USCOUP Letter and MARS Rotation	Lin fangelin <u>Dadke z</u>	Notine Tene Que Laborie J <u>al</u>	Pour Validi Diatha 🚊	epsit:
11.54			the second s	11.11.11.11.11.11.11.11.11.11.11.11.11.	40.00	122	21 202000
For		ASIAIY Configurali:	na Sileikun	DecAsgreation	Historian Fran	n Siby	Forest Vis VDI
1.11	9)	104400		26-000	i tha dir th		2014-000 d
e-114	w.	Union		1022/0	(HC/B/Ar		0.02.000
1010	a -	Dissident		Creatived	Disaster	÷	Encoded
(0)10	40	Dischlet		Dimited	District		Classified.
19303	e:	Disident		Diaded	Distance		Classifiert .
1.18	•	Diador.		(the short	(Ballot)	1	(Deck)
4703	0.5	1953606		19,200	300000		ter states a
(entre	1.	1400M		Distance	Dentine		(Otalaka
4210	K.	Disaties		Disapted	Dinish en		Clineded
adal S.	19. 19	Dischief		2 low that	Disablys.	-	Classified
2017.	90	Deamer		Deputient	Displayer		Could the
= 0.7	14	105300		14.06.0	10+44		2014 (de 16.1
1000.0	16	indana -		0524248	HICLE/IC		- include
and.	90	THE SHE		Designed	Disactor		Transfer
distant.	3	Descel		Classified	Directive)		Clearled

Figure 5-77 LLDP Dot3 TLVs Settings Window

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
MAC/PHY Configuration/Status	Select this option to enable or disable the MAC/PHY Configuration/Status TLV to send. The MAC/PHY Configuration/Status TLV is an optional TLV that identifies (1) the duplex and bit-rate capability of the sending IEEE 802.3 LAN node, and (2) the current duplex and bit-rate settings of the sending IEEE 802.3 LAN node.
Link Aggregation	Select this option to enable or disable the Link Aggregation TLV to send. The Link Aggregation TLV indicates contains the following information. Whether the link is capable of being aggregated, whether the link is currently in an aggregation, and the aggregated port channel ID of the port. If the port is not aggregated, then the ID is 0.
Maximum Frame Size	Select this option to enable or disable the Maximum Frame Size TLV to send. The Maximum Frame Size TLV indicates the maximum frame size capability of the implemented MAC and PHY.
Power Via MDI	Select this option to enable or disable the power via MDI TLV to send. Three IEEE 802.3 PMD implementations (10BASE-T, 100BASE-TX, and 1000BASE-T) allow power to be supplied over the link for connected non-powered systems. The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN station.

LLDP-MED Port Settings

This window is used to enable or disable transmitting LLDP-MED TLVs.

To view the following window, click **L2 Features > LLDP > LLDP-MED Port Settings**, as shown below:

DR MCI	D Port Selitopa —							
	Row Part Mitter 19	To Part set (Main Set	Sectoration Electrical or	Capabilities To unbit of Section	Roboto R	Nevers Policy Dischlor (*)	Politi (Neodiation)	A+7
nii 1 Se	ed agai							
10	Pat	Notification	Copeti		Investory	Network Fo	kγ.	PSE
- 9	+ () % * ()	The Art	15.4	40	(Waters)	Desident	Ċ.	the second
- 10	erace.v.	Service.	110.00	ant .	DOM: N	106,470	Ś.	THE ARMY
- 24	erviza i	Lo sed	THAT	24	OWNERS.	linte de		There is
	1111 .	Chuckyd	Enst	90	Disst ec	Diantres	E.	Ducted
- 14	6625	Clauded,	Dow	60	Divid-on.	Direct-is	l.	Darahu
1	40.24	20 A.F	Dr. A	(i)	Or de la	(mation	(i	17-16-1
- 20	erana a	$H^{1}(\omega)(0,0)$	Ale of	601	OK MARK	10.470	6	Heaters .
- 24	WILL &	12,004	10.7	91	00.00.00	1 MACHE		U.S. Market
	encan:	Castoled	Den	(ed)	Disabled:	Dead-er		Example 1
- 36	8 (0)(0)	Clearlyd	Chial,	leci 👘	Distant	Disati et		Diversion
-30	20011	CarAd	Dr.d.	(i)	Destina.	256433	ř.	Distant .
- 9	4/1.612	- 4.1	Lie al	(0. U)	On the set	100.000		11-140
- 77	etertit.	12.401	1974	din .	DOM: N	100,50,70	6	11/22/07
10	1.(chia)	C to sied	. Line	44	Diost est	TRACKS	C.	Distance of the
- 36	8 NO15	Canaka	Inst	ad	Divisit est	Dind of	ę	Encoded
- 33	1 (91)	200.003	Elect.	191.	Dr.d. a.	Durden	6	Division -
- 39	0.74,017	$= (a, \phi_i) I$	Livial.	(i)	Dé. d. al	(inside a	č.	All added
- 30	a ta ken	0.00	11/7	60	George	(MC/C/w	6	(Understood
1	e scenii :	C CO GMG	111.97	e)	Distant-Art	Titche ne	6	ERADAS
- 36	f. 1062	0.0004	0.000	ed	Dive oc	Disat-e	6	Display
- 34	8.19623	Country	Disal	ind in the second s	Dive es	Disponen	ř.	C velved
- 83	0.1002	Ca.4/1	Ded	10	Distant	Dividi Ve	8	D.W.M.J.
- 22	eta en e	102,001	The a	60	(ACM INT)	10.410	0	HOLE I
14	n ta kul	CONT.	1944	44	(97,97-97)	URADA:	6	1. Contract
	envolas.	Capited	ČD S	-94	Divid ed	Disan-w		Dicased
	8 (622)	Canter	Et al.	64	Diad et	Direct-re		English2

Figure 5-78 LLDP-MED Port Settings Window

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Notification	Select this option to enable or disable the sending of LLDP-MED notifications.
Capabilities	Select this option to enable or disable transmitting the LLDP-MED capabilities TLV.
Network Policy	Select this option to enable or disable transmitting the LLDP-MED network policy TLV.
PSE	Select this option to enable or disable transmitting the LLDP-MED extended power via MDI TLV, if the local device is PSE device or PD device.
Inventory	Select this option to enable or disable transmitting the LLDP-MED inventory management TLV.

LLDP Statistics Information

This window is used to view the neighbor detection activity, LLDP Statistics, and the settings for individual ports on the Switch.

To view the following window, click L2 Features > LLDP > LLDP Statistics Information, as shown below:

	aleză întermetico	2					
LDP Stellarb	en information						
La. Carac	THE .	000 896348					Chevilles for
Total Investo		5.3 C					
Granter des	6	- 50					
Term Despy							
Tetal Aprest	a l	्व					
LOP States	No. Company						
1158	1 🖂	-90	Binner,	÷ .		i con Counter	Clear 48
that I Selfie	12	20090	00000000				a nahara
Pet	Tele Tereniti	data data	Tub Lines	Total Bounda	UANTLA DESCRIPTION	Teld TLY Unit every	Total Accounts
	Contraction of the local division of the loc		CONTRACTOR OF THE OWNER.			term that is more than	- Contraction of the second second
enset.	01	×	ć.	τ¢	(C)	4	1
PARA SAIST	51 1	4 A	¢. ¢	70 3	e e	к Х	1
	- 21					<u>(</u>	(() (
22163	51 1	×		1	(c.)	к Х	1. 2.
20182 2002 20183 20183	91 1 1 1 1 1	4 1	t t	1	e e	* *	1 2 2
20182 2022 2023 2023 2025	31 1 1 1	8 9 0	2 6 1	2	e e	* *	2
80182 20003 20003 20032	51 3 7 4	8 6 6 1	5 5 7 7 8	2 3 1	с с г г	\$ \$ \$ 1 1	2
20182 2002 20183 20183 20185 20185	51 1 1 1 1 1 1 1 1	8 8 10 11	0 6 1 1	3 3 1 4 3	с с г г	5 5 7 1 1 1	1 2 3 4 4 3 3
20182 2002 10183 20185 20185 20185 20182	51 1 1 1 1 1 1 1 1	* * * * *	5 5 7 7 8	3 3 1 1 4 3	6 6 1 1 1 6	5 5 7 1 1 5	1 2 1 1 1

Figure 5-79 LLDP Statistics Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be displayed.
Port	Select the port number that will be displayed.

Click the **Clear Counter** button to clear the counter information for the statistics displayed.

Click the **Clear All** button to clear all the counter information displayed.

LLDP Local Port Information

This window is used to display the information on a per port basis currently available for populating outbound LLDP advertisements in the local port brief table shown below.

To view the following window, click L2 Features > LLDP > LLDP Local Port Information, as shown
below:

R Local Port Driel Tab	Tere .		
4		weater a	(rd) ones par
an bornage			
Fa C	Port ID Subhype	Poil ID	≓at Description
N7:09	2010	(11) N	The programme of the dates of
#1.64	. 5/9	#110N	The performance better the be-
1000	_N/M -	en: 02	B4. to Carptonic 9 DGC-IC-1938
wy Ka	incid.	etrifer	D-L n « Carptonic 1 06 0-1010-30.
67.08	Local	en 100	D-L reCorporation 060-1510-20.
#1 KK	LSCA	en 100	D-L + Corporator 200-15 (0-20.)
7.0160	send -	70 da	D-L + + Contraste + 062-75-70-20.
#11 CC	12.1	11.00	D-L + C = C = C = 1 0 000-15 10-200
0.000	UA.A	8.5.00	D-E-11 Careau (1065-1510-20)
#0,010	LA.I.	pulyin -	Difference and Contract (COS-1510-80)
ALCOPT		±1000	B Los Constantes DOS 15 W St.
4111212	140	e effetter	10 Los Caracines (30) 2230, 28.

Figure 5-80 LLDP Local Port Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be displayed.
Port	Select the port number that will be displayed.

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

Click the Show Detail button to view detailed information of the specific port.

DP Local Information Table		
Pet	attri 611	
Ped ID Sablyce	Local .	
MOLENCE CONTRACTOR OF A DECISION OF A DECISION OF A DECISION OF A DECISION OF A DECISION OF A DECISION OF A DECISION OF A DECISION OF A DECISION OF A DECISION OF A DECISION OF A DECISION OF A DECISION OF A DECISION OF A DECISION OF A DECISION OF A DECISION OF A DECISION OF A DECISIONO OF A DECISIONO OF A DECISIONO OF A DEC	2004	
Puil De Astalian	D-brik Corporation DOS-1918 23200P HWA1 the waity 1 20000 Post Ten Unit 1	
POR EVED	1	
Venegement Address Count	1	
PPAD Block	t de la construcción de la constru	
A SMINADA FIETAS COLIE	1	
Protocol Identity Eatings, Count	The second s	
WASH-Y Cartiguration Status	20 ov Ferni	
Power Via HIDI	Shee Deal	
Indu Aspendigu Land	Straw 16 fail	
Auxinum Frame Site	105	
TION MEDICOLOGICAL	20 av 16 tal	
televate Policy	Show Detail	
Dilas dest acessi via MOI	Star Dali	

After clicking the Show Detail button, the following window will appear.

Figure 5-81 LLDP Local Port Information - Show Detail Window

To view more details about, for example, the **MAC/PHY Configuration/Status**, click the <u>Show Detail</u> hyperlink.

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

After clicking the <u>Show Detail</u> hyperlink, a new section will appear at the bottom of the window.

LLUP Local Port Information	
LLDP Local Information Table	
Pet	atti 01
Post ID Sablyon	Local
MOCH.	/109/1
Post Dependence	D-brid Serporation DOS-1910-285MP HW A1 Innovativ 1,700007 Poil, 1 or (Unit 1
POT EVID	1
Management Address Count	1
1777 D Dallers	t de la constante de
M SMINADE FILTER Collin	1
Protocol Identity Entry, Count	L. C.
MACEHY Configuration Status	<u>200 PUL</u>
Power Via HDI	Star Debi
Link Appropriate	XI as the fail
Maximum Frame Site	155
ETTO- MED Copations	Million 16 (St)
Helwork Policy	2how Detail
Drive dwt ewewnyje MOI	9 m B al
	Lade
Missioner statings of the states	
Asta Merphalica Support	Surgers in the
Auto-Nepolisiton Employ	Enabled
As in Republic Miner Science of Capability	8.81(m)
Auto-Hegoliation Operational NAU Type	DHB/WC

Figure 5-82 LLDP Local Port Information - Show Detail Window

LLDP Neighbor Port Information

This window is used to display the information learned from the neighbors. The switch receives packets from a remote station but is able to store the information as local.

To view the following window, click L2 Features > LLDP > LLDP Neighbor Port Information, as shown below:

		and the second se	and the second se		·
et 11.	- 10 M	Pvt. rtd/06		144	dea
					Ch. e. 28
u Ditivi: 1					di desar

Figure 5-83 LLDP Neighbor Port Information Window

The fields that can be configured are described below:

Parameter	Description	
Unit	Select the switch unit that will be displayed.	
Port	Select the port number that will be displayed.	

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

Click the **Clear** button to clear the specific port information.

Click the **Clear All** button to clear all the port information displayed.

Click the **Show Detail** button to view detailed information of the specific port.

After clicking the **Show Detail** button, the following window will appear.

1922 Pagenes Internation Labe		
Bay C	1	
chorac II Contrepon	Missic Administra	
Chavels ID	FB-7D-6B-3B-36-00	
Port ID Salakov	Local	
Port ID	ach1040	
Port Devic letter		
Syntaine Manen		
System Description		
Cystein Celeidilles		
Venagement Address Entries:	<u>Sittaw Detail</u>	
MMDD B M	Show Data (
VEX IS an Editors	Street 16 Mill	
Protocol Rightly Entries	Sitter Terral	
MAG6711Y Configuration/Gistus	Of the De Mill	
Proven WA IND I	Sitter Detail	
Link Aggregation	Show Detail	
Macanon Pranie Sac	E CONTRACTOR OF CONTRACTOR OFO	
Hoknawn TLWs	Stree Terral	
LLCI7-MED Department	Show Detail	
Helivors Policy	Sites Terral	
Estanded Power Vis MDI	Show Detail	
inventory islanagement	Show Detail	

Figure 5-84 LLDP Neighbor Port Information - Show Detail Window

To view more details about, for example, the **LLDP-MED Capabilities**, click the <u>Show Detail</u> hyperlink.

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

After clicking the Show Detail hyperlink, a new section will appear at the bottom of the window.

LDP Neighber Pert Informatio	n	
LIN PORTOR DESTINATION LADA		
Er in Er	1	
Endose III sunghe	Missic Address	
Character D	FB-70-66-35-36-06	
Perl ID Sabiyon	Local	
Port ID	ath10410	
Port Deviciel as		
System Manes		
System Description		
Cystein Capabilities		
Management Address Eniries	Show Detail	
PPVDDéla	Show De M	
VEX.N. Same Fathers	Sillies 1640/1	
Protocol Identity Entries.	Sites Peter	
MAG/PEP Configuration/Status	Show De Mil	
Proven Via ND I	Sitos Detal	
Link Aggregation	Share De Mi	
Machinen France Size	t.	
Hokowa TLAX	Story Frend	
LLCP-MED Depaidlifies	Show Dedail	
Helson's Policy	Street Terral	
Estanded Prover Vis MDI	Of the Detail	
investory leta sagement	Ohos, Dedal J	R. e.h
LDIVMED Capabilities		
LLDP MCD Capabilities Crabled:		
LLOP MED Geologics	Not Separat	
Network Policy	Hol Support	
Location Residieshoe	Not Second	
Hannawa Kawar Walletti	is all support	
inventory.	Not Support	

Figure 5-85 LLDP Neighbor Port Information - Show Detail Window

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

6. Layer 3 Features

ARP Gratuitous ARP UDP Helper IPv4 Interface IPv4 Static/Default Route IPv4 Route Table IPv6 Interface IPv6 Neighbor IPv6 Static/Default Route IPv6 Route Table IPMC

ARP

ARP Aging Time

This window is used to view and configure the ARP aging time settings.

To view the following window, click **L3 Features > ARP > ARP Aging Time**, as shown below:

Timesul (min)	
2481	F-B-
	111 1 4 1 2 2 50

Figure 6-1 ARP Aging Time Window

The fields that can be configured are described below:

Parameter	Description
Timeout	Enter the ARP aging timeout value here.

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

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

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

Static ARP

This window is used to view and configure the static ARP settings.

To view the following window, click L3 Features > ARP > Static ARP, as shown below:

ALC: NOT					
raana 🗖	llats	an Addway 30-11-22-32-4	HAA		- a do.
Total Civilian: 1	0.075	ereneeren anderenee			
mandasi na mano	të Arteki k	Rainformir Arbitista	Agengi taren	No.	
		300 HE KA 67 KM KC	(Second)		Dir Doka
skat	33/00 93/00 -	200-10.444-0.1 CC.CU.	200000000000000000000000000000000000000		

Figure 6-2 Static ARP Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the IP address that will be associated with the MAC address here.
Hardware Address	Enter the MAC address that will be associated with the IP address here.

Click the Apply button to accept the changes made.

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.

Proxy ARP

This window is used to view and configure the proxy ARP settings. The Proxy ARP feature of the Switch will allow the Switch to reply to ARP requests destined for another device by faking its identity (IP and MAC Address) as the original ARP responder. Therefore, the Switch can then route packets to the intended destination without configuring static routing or a default gateway. The host, usually a Layer 3 switch, will respond to packets destined for another device.

Proxy ARP			
Procy ARP			
Total Enhiese 1			
Interface Home	Prvsy ARP Sluty	Local Provy ARP State	
wigen i	Disolited	Deablet	CC1
		10	S 1 2 3 95

To view the following window, click L3 Features > ARP > Proxy ARP, as shown below:

Figure 6-3 Proxy ARP Window

Parameter	Description
Proxy ARP State	Select to enable or disable the proxy ARP state here.

Parameter	Description
Local Proxy ARP State	Select to enable or disable the local proxy ARP state here. This local proxy ARP function allows the Switch to respond to the proxy ARP, if the source IP and destination IP are in the same interface.

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.

ARP Table

This window is used to view and configure the ARP table settings.

To view the following window, click L3 Features > ARP > ARP Table, as shown below:	:
--	---

e ostaton				
HARA Z RUAR DI REPU		dif Ashina	Not	
lladværddises	0.00048	o Tus 💦 👬 🔤 🔻	002%	[ts).
en Frankessa				(ba. 9)
Internation in which	di Antonia	HEYWAYE ALEENA	viaina ilinekonine	104
dett.	0.00.001	06-33-70-00-35-13	200	1.2.01
and .	10.3058.14	16 OF -41 OS 22 22	16	Oper
A.1	10 3 10 3	SCHEREN AV HER	. Facet	Sec

Figure 6-4 ARP Table Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Select and enter the interface's VLAN ID used here. This value must be between 1 and 4094 .
IP Address	Select and enter the IP address to display here.
Mask	After the IP Address option was selected, enter the mask address for the IP address here.
Hardware Address	Select and enter the MAC address to display here.
Туре	Select the type option here. Options to choose from are All and Dynamic .

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

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

Click the **Clear** button to clear the specific entry.

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

Gratuitous ARP

This window is used to view and configure the gratuitous ARP settings. A gratuitous ARP request packet is an ARP request packet where the source and the destination IP address are both set to the IP address of the sending device and the destination MAC address is the broadcast address.

Generally, a device use the gratuitous ARP request packet to discover whether the IP address is duplicated by other hosts or to preload or reconfigure the ARP cache entry of hosts connected to the interface.

To view the following window, click **L3 Features > Gratuitous ARP**, as shown below:

Contractor AND Clouds Settings				
e na e a she star	0.000	5-0-64		
CLERK ATTERSES	D AND	FUANT		
er bistalta Alfred Statistical englis SMa	difference.	and the second		
Calarian AMP Committed A	-8 Examples	O Cardet		1 (44)
CONTRACTOR AND SERVICE CONTRACTOR	101			
Total Ballione T				
in heliuse film we			Inishal Tervitavsi	
de al			38	

Figure 6-5 Gratuitous ARP Window

Parameter	Description
IP Gratuitous ARP State	Select option to enable or disable the transmission of gratuitous ARP request packets.
Gratuitous ARP Trap State	Select this option to enable or disable the ARP trap state.
IP Gratuitous ARP Dad-Reply State	Select this option to enable or disable the IP gratuitous ARP Dad-reply state.
Gratuitous ARP Learning State	Select this option to enable or disable the gratuitous ARP learning state. Normally, the system will only learn the ARP reply packet or a normal ARP request packet that asks for the MAC address that corresponds to the system's IP address. This option used to enable or disable the learning of ARP entries in the ARP cache based on the received gratuitous ARP packet. The gratuitous ARP packet is sent by a source IP address that is identical to the IP that the packet is queries for.

The fields that can be configured are described below:

Click the Apply button to accept the changes made.

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.

UDP Helper

IP Forward Protocol

This window is used to display and configure the IP forward protocol settings. This feature is used to enable the forwarding of a specific UDP service type of packets.

To view the following window, click L3 Features > UDP Helper > IP Forward Protocol, as shown below:

awas Picked		
envine environ alle end (terraria)		- Agoby
N FRANC I		
COP Fail	Ava.Ava.bys	[
2	Time Service	En la companya da companya
-7	EX-1 S Have Servey	Contraction of the local division of the loc
1. 24	1409.00	Listere
1.140	49	Dakes
66	TETE	F -h-h
100	140.05465	Reference 1
100	\$W30505	Colored Colored



The fields that can be configured are described below:

Parameter	Description
IP Forward Protocol UDP Port	Enter the destination port of the UDP service to be forwarded.

Click the Apply button to accept the changes made.

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

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

IP Helper Address

This window is used to add or remove a target address for the forwarding of UDP broadcast packets. This feature takes effect only when the received interface has an IP address assigned.

The system only forwards packets that satisfy the following restrictions:

- The destination MAC address must be a broadcast address.
- The destination IP address must be an all-one broadcast.
- The packets are IPv4 UDP packets.
- The IP TTL value must be greater than or equal to 2.

To view the following window, click L3 Features > UDP Helper > IP Helper Address, as shown below:

Helper Address		
P Telev Address		
Emphania (a Ref. art)		
el server serve		d gody.
Tora Ferrer 1		
in Arbent, Human	ETHALAN ARENDA	
4 A	0.5.5 10	De vie

Figure 6-7 IP Helper Address Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID used here. The range is from 1 to 4094.
IP Helper Address	Enter the target IPv4 address for the forwarding of the UDP broadcast packet here.

Click the Apply button to accept the changes made.

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

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

IPv4 Interface

This window is used to view and configure the IPv4 interface settings.

To view the following window, click L3 Features > IPv4 Interface, as shown below:

interiora —						
and Miles	K(94)	j)		1	in the second se	il de la companya de
	900 - El	2.0			- 33,000 - 54	e 1939.
a Distance						
a Ditie: I	4.61	Patters	Surrouting	t and blocker		

Figure 6-8 IPv4 Interface Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the interface's VLAN ID here. This value must be between 1 and 4094.

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 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.

After clicking the **Edit** button, the following window will be available.

IPső Intertece Contigure				
IPol mierkase Setärga	City Client			
Min Same	4 2 .			Look
series-				
Shik.	batt/ v			
Dest bio (Stday			Apph
Primory (P. Settings				
HEREN	<u>8176 y</u>			
le entroy	100000000000000000000000000000000000000			
1017	200 0 0 0 0			4(s), 0(s))
Securian P. Selimp				
PAAR				
Ne.				r aob
Secondary P Carry				
Tom Entries: 1				
IF Attrais		Hed U.s.	h a subty	
23.1.1.1	285.051	Mark W	*8	ve de
			321	

Figure 6-9 IPv4 Interface Configure Window

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

The field that can be configured for **Settings** is described below:

Parameter	Description
State	Select this option to enable or disable the IPv4 interface's global state.
Description	Enter the description for the IPv4 interface here. This can be up to 64 characters long.

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

The field that can be configured for **Primary IP Settings** is described below:

Parameter	Description	
Get IP From	 Select the get IP from option here. Options to choose from are: Static - Users can enter the IPv4 address of this interface manually in the fields provided. DHCP - This interface will obtain IPv4 information automatically from the DHCP server located on the local network. 	
IP Address	Enter the IPv4 address for this interface here.	
Mask	Enter the IPv4 subnet mask for this interface here.	

The fields that can be configured for **Secondary IP Settings** are described below:

Parameter	Description
IP Address	Enter the IPv4 address as the secondary interface here.
Mask	Enter the IPv4 subnet mask as the secondary interface here.

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

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.

After clicking the **DHCP Client** tab, the following page will appear.

Mas Intertene Corrigore		
Pvd interlace Settings	Olice Client	
0859 Classification (0.0 400)	4	
One Birkhon.	NAME THE	
Have Marine	(1) (10) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	
focu-	Dece (3-10000) 30 - House 30 - Blander	<u></u>

Figure 6-10 DHCP Client Window

The fields that can be configured are described below:

Parameter	Description
DHCP Client Client-ID	Enter the VLAN interface, whose hexadecimal MAC address will be used as the client ID to be sent with the discover message.
Class ID String	Enter the vendor class identifier with the maximum of 32 characters. Tick the Hex check box to have the class identifier in the hexadecimal form.
Host Name	Enter the host name. The maximum length is 64 characters. The host name must start with a letter, end with a letter or digit, and only with interior characters letters, digits, and hyphens.
Lease	Specify the preferred lease time for the IP address to request from the DHCP server. Enter the day duration of the lease, or select the hour and minute duration of the lease.

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

IPv4 Static/Default Route

This window is used to view and configure the IPv4 static and default route settings. The Switch supports static routing for IPv4 formatted addressing. Users can create up to 64 static route entries for IPv4. 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 request 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.

To view the following window, click L3 Features > IPv4 Static/Default Route, as shown below:

Pel Store Delas it Rossa				
Hours & Same	nar Solici 💽		igi0-dus-macx	, Andr
Total Britler: PANNON	NAS	UCONF.	BERKO Sarah	
2002	2.2:20	30.1.1.234	dial	De si a
			111 1 1 1 1 1	

Figure 6-11 IPv4 Static/Default Route Window

The fields that can be configured are described below:

Parameter	Description		
IP Address	Enter the IPv4 address for this route here. Tick the Default Route check box to use the default route as the IPv4 address.		
Mask	Enter the IPv4 network mask for this route here.		
Gateway	Enter the gateway address for this route here.		
Backup State	 Select the backup state option here. Options to choose from are: Primary - The route is used as the primary route to the destination. Backup - The route is used as the backup route to the destination. 		

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

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.

IPv4 Route Table

This window is used to view and configure the IPv4 route table settings.

To view the following window, click L3 Features > IPv4 Route Table, as shown below:

P MORES	Sec				
in anna an tha					
Description and Description					
a share the second second					
annala SHole	en Esperad				0.00
ninska (C. H. sta Dobka f					
	an Sarah	Ganady	Pavelica Rama	684	
Diaka 1			Prestica Naria Acat	6a0	

Figure 6-12 IPv4 Route Table Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Select and enter the single IPv4 address here.
Network Address	Select and enter the IPv4 network address here. In the first space enter the network prefix and in the second space enter the network mask.
Connected	Select this option to display only connected routes.
Hardware	Select this option to display only hardware routes. Hardware routes are routes that have been written into the hardware chip.
Summary	Display the brief information of the active routing entries.

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.

IPv6 Interface

This window is used to view and configure the IPv6 interface's settings.

To view the following window, click L3 Features > IPv6 Interface, as shown below:

Il's6 Interfece			
Pv6 interface			
N REPORT VIAN 11-40340			repole ind
Total Entries: 1			
lefettera	Division and the	Link Staties	
stari)	Enabled	Up	(Color)
			11 2 4 1 2 2 2

Figure 6-13 IPv6 Interface Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the VLAN interface's ID that will be associated with the IPv6 entry.

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 **Detail** button to view and configure detailed settings for the IPv6 interface entry.

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

After clicking the **Detail** button, the following page will be available.

end method brands	Interthick Pro 27/08/948	Height of Linksheet	010706-003	
nation NVC Calle	nat Dhebled - ❤			Led I have
na na katala na kata				
Nel + Inc.ex		[180.04] [1.56 million]		19 M
States Setting				
o interventi (B-DC DCDC)	P			NSP
0 Seltinas				
ep and (a-state	9	Calculate Tarte (2008-0000)	e Jer	
Las griffinds Kirg	3 0	The Calor Ha	01. <u>v</u>	
Windowen (1-136)	0 (M)	- 78 Stational (4: 00)	0	
KALMINE (HK.R)	37 186		16 da 3 (16	ly the



The fields that can be configured for Interface are described below:

Parameter	Description
IPv6 State	Select to enable or disable the IPv6 interface's global state here.

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

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

The fields that can be configured for Static IPv6 Address Settings are described below:

Parameter	Description
IPv6 Address	Enter the IPv6 address for this IPv6 interface here.
	Select the EUI-64 option to configure an IPv6 address on the interface using the EUI-64 interface ID.
	Select the Link Local option to configure a link-local address for the IPv6 interface.

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

The fields that can be configured for NS Interval Settings are described below:

Parameter	Description
NS Interval	Enter the NS interval between 0 and 3600000 milliseconds.

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

The fields that can be configured for ND Settings are described below:

Parameter	Description
Hop Limit	Enter the IPv6 hop limit value here. This is used to configure the hop limit to be advertised in RA messages. The IPv6 packet originated at the system will also use this value as the initial hop limit. To use the default value on this interface, configure this value as 0. The range is from 0 to 255.
Reachable Time	Enter the reachable time used in the ND protocol here. The configured time is used by the router on the interface and is also advertised in RA message. If the specified time is 0, the router will use 30 seconds on the interface and advertise 0 (unspecified) in RA message. The reachable time is used by the IPv6 node in

Parameter	Description
	determining the reachability of the neighboring nodes. The range is from 0 to 3600000 milliseconds in multiples of 1000 milliseconds.
Managed Config Flag	Select to turn the managed configure flag On or Off here. This is used to enable or disable the management configure flag in the advertised RA message. When the neighboring host receives the RA with an enabled flag, the host should use a stateful configuration protocol to obtain IPv6 addresses.
Other Config Flag	Select to turn the other configure flag On or Off here. This is used to enable or disable the other configure flag in the advertised RA message. When this feature is enabled, the router will instruct the connected hosts to use a stateful configuration protocol to obtain auto-configuration information other than IPv6 address.
RA Min Interval	Enter the minimum value of the interval between retransmission of RA messages here. The range is from 3 to 1350 seconds. This value must be smaller than 75% of the maximum value.
RA Max Interval	Enter the maximum value of the interval between retransmission of RA messages here. The range is from 4 to 1800 seconds.
RA Lifetime	Enter the RA lifetime value here. The range is from 0 to 9000 seconds. The lifetime value in RA informs the received host of the lifetime for taking the router as the default router.
RA Suppress	Select to enable or disable the sending of RA messages on the interface here. By default, this feature is enabled on a VLAN interface and disabled on a tunnel interface.

After clicking the **Interface IPv6 Address** tab, at the top of the page, the following page will be available.

vê înterlace				
Pvo interface tertings	interface (Ps 5 Address	Heighbor Discover	DHORVS Client	
tule i Endulesce f				
As Marson Type :		Period de la companya		
LIND LECK ABOM	L	Hele 22 - TENHE HEATING		Factories .
	L	HERE AN INCOME.		Twinter .

Figure 6-15 IPv6 Interface (Detail, Interface IPv6 Address) Window

Click the **Delete** button to delete the specified entry.

After clicking the **Neighbor Discover** tab, at the top of the page, the following page will be available.

19yd Interlace Sectings	Interface, Pró. Sadores	Heigh bar Ola swer		NCP/Claim	_	
Professional Lands	Infacelule Ten Ind	ended May Time Dess.	Link Day	hanna in the		
2010 201 0007 - 501	204000	2262630	Traded .	Cruested	1.041	100

Figure 6-16 IPv6 Interface (Detail, Neighbor Discover) Window

Click the Edit button to configure the following parameters:

		Discover	DIFCPr6 Class	
ne entract Del Parto Proto, Lenvis Parlane	and the second second	en en sen	. 100	0010

Figure 6-17 IPv6 Interface (Detail, Neighbor Discover, Edit) Window

The fields that can be configured are described below:

Parameter	Description
Preferred Life Time	Enter the preferred lifetime value here. The range is from 0 to 4294967295 seconds. The default value is 604800 seconds (7 days).
Valid Life Time	Enter the valid lifetime value here. The range is from 0 to 4294967295 seconds. The default value is 2592000 seconds (30 days).
Link Flag	Select to enable or disable the on-link flag here. The default option is Enabled .
Autoconfig Flag	Select to enable or disable the auto-configure flag here. The default option is Enabled .

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

After clicking the DHCPv6 Client tab, at the top of the page, the following page will be available.

Provinse take wettings	Interface the 27 citizette	Hergistismut (2004)	DECKNEC INT	
alcone clarp				2,000
 MCNICHISAND				

Figure 6-18 IPv6 Interface (Detail, DHCPv6 Client) Window

Click the Restart button to restart DHCPv6 client on an interface.

The fields that can be configured for DHCPv6 Client Settings are described below:

Parameter	Description
Client State	Select this option to enable or disable the DHCPv6 client state. Tick the Rapid Commit check box to proceed with two-message exchange for prefix delegation.

IPv6 Neighbor

This window is used to configure and view the IPv6 neighbor settings.

To view the following window, click L3 Features > IPv6 Neighbor, as shown below:

PvG Helphoo: Section						
n na an	ithe Active	70111	NGC Activity	11-12-03-19-00		(), e.e.
6 (6 Factor 2007) (1 -8004)	Potos	EST.				C. Sev.
ionii Pelowani						Close A
Da onres	ini	a nyaé dana s	Law root?	1,000	ana na	Sector a set of
3013 A. U	19-22	ANNAL T	78.91	20.02		The star

Figure 6-19 IPv6 Neighbor Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter an interface VLAN ID.
IPv6 Address	Enter the IPv6 address.
MAC Address	Enter the MAC address.

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 **Clear** button to clear all the information for the specific port.

Click the Clear All button to clear all the information in this table.

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.

IPv6 Static/Default Route

This window is used to view and configure the IPv6 static or default routes.

To view the following window, click L3 Features > IPv6 Static/Default Route, as shown below:

Pri Store Twins a Rouse					
Prélédéses Prélédéses Intérnéron Prélédés Net Roc Prélédéses Roma Xan	PP2-001 PP11 Pase celet	19 Dekal Bees			eely:
Total Entries: 9					
itel address	Bahal cugi	Red Mar	And Status Manual	(higher of	

Figure 6-20 IPv6 Static/Default Route Window

The fields that can be configured are described below:

Parameter	Description		
IPv6 Address/Prefix Length	Enter the IPv6 address and prefix length for this route here. Tick the Default Route option to use the default route as the IPv6 address.		
Interface VLAN	Enter the interface's VLAN ID that will be associated with this route here.		
Next Hop IPv6 Address	Enter the next hop IPv6 address here.		
Backup State	 Select the backup state option here. Options to choose from are: Primary - The route is specified as the primary route to the destination. Backup - The route is specified as the backup route to the destination. 		

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

IPv6 Route Table

This window is used to view and configure the IPv6 route table.

To view the following window, click L3 Features > IPv6 Route Table, as shown below:

n Roune Table			_	_
i Rouse Taku				
Putrakas 2007				
	Lana Palwy			
Interface VLAN 1 - 409-0				
Canadian Dinagraa Distataa				Test
Ad to have 0			14	1000
HWG ASSAMAGEWESI ASST	Alexa Helps	STRATES BATH	COP :	Province:

Figure 6-21 IPv6 Route Table Window

Parameter	Description
IPv6 Address	Select and enter the IPv6 address to display here.
IPv6 Address/Prefix Length	Select and enter the IPv6 address and prefix length to display here. Select the Longer Prefixes option to display IPv6 routes with prefixes greater than and equal to the prefix length.
Interface VLAN	Select and enter the interface's VLAN ID to display here.
Connected	Select this option to display only connected routes.
Database	Select to view all the related entries in the routing database instead of just the best route.
Hardware	Select this option to display only hardware routes. Hardware routes are routes that have been written into the hardware chip.
Summary	Display the brief information of the active routing entries.

The fields that can be configured are described below:

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

IPMC

IP Multicast Global Settings

This window is used to display and configure the global IP Multicast (IPMC) settings.

To view the following window, click L3 Features > IPMC > IP Multicast Global Settings, as shown below:

IP Multicent Global Settings			
P Multicest Table Lookup Mode —			
Тари новкар мали	⊛ 1 ^a	C MM	Apply

Figure 6-22 IP Multicast Global Settings Window

The fields that can be configured are described below:

Parameter	Description
Table Lookup Mode	Select the IP multicast forwarding lookup mode here. Options to choose from are:
	 IP - Specifies multicast forwarding lookup based on the IP address. MAC - Specifies multicast forwarding lookup based on the MAC address.

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

IP Multicast Forwarding Cache

This window is used to display the content of the IP multicast routing forwarding cache database.

To view the following window, click L3 Features > IPMC > IP Multicast Forwarding Cache, as shown below:

P Malikani Carwaning Talaka					
teresponentes I	30 P. P. A	rine))	194	Stored
tal talifs t					
Warmen Carls and	Parasite derite	and and provide a state		The legitime of the legitime in the	

Figure 6-23 IP Multicast Forwarding Cache Window

The fields that can be configured are described below:

Parameter	Description
Group Address	Enter the multicast group IP address here.
Source Address	Enter the source IP address here.

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

Click the **Show All** button to display all the entries.

7. Quality of Service (QoS)

Basic Settings Advanced Settings

Basic Settings

Port Default CoS

This window is used to view and configure the port's default CoS settings.

To view the following window, click **QoS > Basic Settings > Port Default CoS**, as shown below:

niterionite Remainstat					
¥1 1 जि}	form that	Te Pert	Contrast Cards at 10 March Cardson and	0.844	ee
nii ti Setiloga	2	and the second s	11. 2213		
	100		1040401558		100,0040
	2.01904	1	1		16.
	00100		1.		2,66,2
	COLUMN .		1		160
	40.004		1		He
	street.		1		lk.
	6.871046		1		18. 16. 164
	e de tatal Protoso		1		Max
	initials.				
	621104		1		16.
	strif230.		(I)		1R
	1000000		1 C		48.
	ain PC III				16
	0.01215	1	1		IN .
	inite no		1		. 440
	anit245		1		HA.

Figure 7-1 Port Default CoS Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Default CoS	Select the default CoS option for the port(s) specified here. Options to choose from are 0 to 7 .
	Click the Override check box to apply the port's default CoS to all packets (tagged or untagged) received by the port.
	Select the None option to use the default settings.

Port Scheduler Method

This window is used to view and configure the port scheduler method settings.

To view the following window, click **QoS > Basic Settings > Port Scheduler Method**, as shown below:

unit Prois Post		Area wineva		
1 8 2t184 3	00011 4	WRR .		
arii ti Setiloga	- 08			
Bat		A.A.	naar (Priss)	
tio:ex			MIL	(F
100 CM			1994	
007710			M0+	
42-64			Mit	
48-06			MD3	
861.87			MIT	2
00.00			All+	
200 ⁻¹ 2385			()))-	
4811(6)			MRF .	
em(040			MOS	
ani Qit			MDN	
1.600.02			MOL	1
1.419211	1		6254	

Figure 7-2 Port Scheduler Method Window

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Scheduler Method	Select the scheduler method that will be applied to the specified port(s). Options to choose from are Strict Priority (SP), Round-Robin (RR), Weighted Round-Robin (WRR), and Weighted Deficit Round-Robin (WDRR). By default, the output queue-scheduling algorithm is WRR .
	WDRR operates by serving an accumulated set of backlogged credits in the transmit queue in a round robin order. Initially, each queue sets its credit counter to a configurable quantum value. Every time a packet from a CoS queue is sent, the size of the packet is subtracted from the corresponding credit counter and the service right is turned over to the next lower CoS queue. When the credit counter drops below 0, the queue is no longer serviced until its credits are replenished. When the credit counters of all CoS queues reaches 0, the credit counters will be replenished at that time. All packets are serviced until their credit counter is zero or negative and the last packet is transmitted completely. When this condition happens, the credits are replenished. When the credits are replenished at to each CoS queue credit counter. The quantum for each CoS queue may be different based on the user configuration.
	must also be in the strict priority mode.
	WRR operates by transmitting permitted packets into the transmit queue in a round robin order. Initially, each queue sets its weight to a configurable weighting. Every time a packet from a higher priority CoS queue is sent, the corresponding weight is subtracted by 1

Parameter	Description
	and the packet in the next lower CoS queue will be serviced. When the weight of a CoS queue reaches zero, the queue will not be serviced until its weight is replenished. When weights of all CoS queues reach 0, the weights get replenished at a time.

Queue Settings

This window is used to view and configure the queue settings.

To view the following window, click **QoS > Basic Settings > Queue Settings**, as shown below:

ucue Beltings			
ana kohinga			
	To Ford Canvas D Canvas I II III III	W/77, Welgell (X-427)	WCRR duertern (3-127) Apply
hill 9.4 Birgs			
Prat	Operate 10	AND N HER	METER Spandown
	0	1	1
	1	1	1
	2		1
ell (3691	×	1	1
	-	1	1
	5	1	1
	9	1	1
	7	3	1
	0	H	4
		1	1
	2	1	1
aline/sz	2	1	1
	1	1	1
	5	1	1
	6	1	1
	1	1	1
	0	1	1
		1	1
		1	1
ethri-0/3	5	1	1
	4	1	1
			1
	5	1	1
	ĩ	2	1

Figure 7-3 Queue Settings Window

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Queue ID	Enter the queue ID value here. This value must be between 0 and 7 .
WRR Weight	Enter the WRR weight value here. This value must be between 0 and 127. To satisfy the behavior requirements of Expedited Forwarding (EF), the highest queue is always selected by the Per- hop Behavior (PHB) EF and the schedule mode of this queue should be strict priority scheduling. The weight of the last queue should be zero while the Differentiate Service is supported.
WDRR Quantum	Enter the WDRR quantum value here. This value must be between 0 and 127.

CoS to Queue Mapping

This window is used to view and configure the CoS-to-Queue mapping settings.

To view the following window, click **QoS > Basic Settings > CoS to Queue Mapping**, as shown below:

CoS to Queue Mapping	
CaS	Ourue (D
đ	2 💌
· · · · · · · · · · · · · · · · · · ·	0
2	· •
5) x
4	4
5	2 1
н	8 .
7	7 .
	CREAT CONTRACT



The fields that can be configured are described below:

Parameter	Description
Queue ID	Select the queue ID that will be mapped to the corresponding CoS value. Options to choose from are 0 to 7 .

Port Rate Limiting

This window is used to view and configure the port rate limiting settings.

To view the following window, click **QoS > Basic Settings > Port Rate Limiting**, as shown below:

Ta Pan Division Internet (20)	RAM 1 TE		
	 By Case dwidth (SF-1000000) Created (SF-10) Cyntaca 	Moa Duorikke S- Ne Duorikke S-	120300)
1	<u>.</u>	Cabe	
Rela	Durint	NA	Serve.
Ho L wit	Noting	Sie Linde	Holdman
(Holl and	No Ling.	20, D. el	HoLT .
Holen:	National	26.174	Hoter
Becch	to private in the	36 (i m	Hof a
H(51.001	1531-1010	Ski Lihat I	BALACT
661.85	insides.	100.010	Relation
No Limit	Nation	Vic Linili	No Limi
No. L. p. :	192 (A14)	See Lines.	Holes .
Holes .	Sec.and .	Sie Le ni	Rider
901.9C	fore whet	with	Hotor
Heli att	151.878	10100	Here and
Holing	National Commission	Seame	les Limit
No Engl	Nacimit -	Ve bint	- No Limit
BULF.	NACES	-Yes for set	HALT
	Harr No.L.m. No.L.m. No.L.m. No.L.m. No.L.m. No.L.m. No.L.m. No.L.m. No.L.m. No.L.m. No.L.m. No.L.m. No.L.m. No.L.m. No.L.m.	Hair Dorn Rair Dorn Rollint Nollint Rollint Nollint	Tate Date Cable Rate Date Date Date No.Let No.Let No.Let No.Let No.Let No.Let No.Let No.Let

Figure 7-5 Port Rate Limiting Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction option here. Options to choose from are:
	 Input - The rate limit for ingress packets is configured. Output - The rate limit for egress packets is configured.
Rate Limit	Select and enter the rate limit value here.
	When Bandwidth is selected, enter the input/output bandwidth value used in the space provided. This value must be between 64 and 10000000 kbps. Also, enter the Burst Size value in the space provided. This value must be between 0 and 128000 kilobytes.
	When Percent is selected, enter the input/output bandwidth percentage value used in the space provided. This value must be between 1 and 100 percent (%). Also, enter the Burst Size value in the space provided. This value must be between 0 and 128000 kilobytes.
	Select the None option to remove the rate limit on the specified port(s). The specified limitation cannot exceed the maximum speed of the specified interface. For the ingress bandwidth limitation, the ingress can trigger a pause frame or a flow control frame when the received traffic exceeds the limitation.

Queue Rate Limiting

This window is used to view and configure the queue rate limiting settings.

To view the following window, click **QoS > Basic Settings > Queue Rate Limiting**, as shown below:

गरा व	er fiel 1495e		ia Port ania (A.M.	Sec. 3	станан (с Г. ж		nds div (5 epert (3-13				1993	Cardwa Terond	14(04-100 14(02)	00000		Ntes No
n Cruis	Contraction of the local division of the loc		3.	uirt -	20	and i	Cer	un5	565	rat .	Ca.	un:	94	und.	94	
166	-	-	100	MLS		Mex	Min.	Piex.	Vir	Yas.		No.	Ve	-	Mit	14.0
		Rok	1941	Mate	Han	N/N	Hale	-	Role	100	Rafe	MARK	Kati	8.4hT	•m	Kelo
at:01	Rolf.	No U 🖓	Not -	(a.u.,	No.L.	1,2,4	No Li 🗸	by L.	lit U .	Roll	$[0,0,0]_{1}$	Hol_{-}	1.76	Re L	Re.d.	No E
68 (NG	Nala	No U.S.	$\{H_{\mathcal{T}}\}_{n=1}^{\infty}$	Stell .	Beller	10.4	$(0,1)_{\rm sc}$	Hall	- 16 B	No in	Section.	164-	Sec.	Mc E	HZGL.	36.2 -
1.9 100	BALL	20.0	Hill.	Stell	Med	10.0	30. I	RUL	the lat	Bola	Set U	Heit,	30.4	No. L	Note	$(36.1)_{\pm}$
in in t	$\mathbf{K}(t) = -$	56.0	Hat	20171	Me I	10.0	26.10	POLL	With .	(Mail)	Section	0.0	$(2\pi)^{-1} =$	90.	10.0° 0	dat to
10110	BALL	56.0	1655	240.01	1644	88.1	36.1	6001	3011	6011	A8.0	860	No. 1	No.1	105.1	30011
101100	Wall	50.0	Hole	Ra II.	Wet.	10.0	Sic.L.	15014	lant.	Nou	20.0	1601	1,211	No.L.	10061	Ne is
at off	Hold.	No B	$\{h_{i}\}_{i=1}^{n}$	$150\mathrm{H}_\odot$	No.	na d.	Hell -	No L	Ve II	Note	50.00	Hol	1.0.1	Bolt .	No.L	Sk U
12.19%	NALL	26.11	Hillin	296.44	Maker	The lat	16 L	Holds	4×11_	Nyth	24 U.S.	16.3.	104	Bellin .	Had	$\{0,1\}_{i=1}^{n}$
(81)(81)	$\mathbb{N}[t] =$	26.01	Hall	APR 11	96.4L	39.5	20.16	BOLL	Mr (r	Halle	Sec.	0.0	$\mathcal{M}(0)$	Mall	$\{0,0,1\}$	W.U
11111	800	54.31	- Hill I	-224 (1	B03	ash i	200	1932.1	March .	36010	Sten	not	2201	NOT-	90334	Burlie
ris (Chr.	8511	58.11	8610	A# 11	94.1	35.3	98.0	6511	100	BALL	50.0	H21	101.0	96-11	105(3)	396.0
en 1 (042	Kault	Se U.	Hålder	Status.	Red	List	Skills.	Natio	30 H	Roll.	56 U.S.	161	ites 1	Sto L	Red.	be U .
differo	NaLL	Re 11 .	Note:	Well .	No.	10.4	MODIE	Rott	Ma D	HOLE	$[N_{\rm T}, U_{\rm eff}]$	$\{0,1,\ldots,$	1,600	No Li	HEAL	No Li 🗉
e le ferre	N.C.L.	W. U.	Helen	SVell.	16.1.	NO.L.	14. L	HALL!	W.D.	Halle	NED.2	Holes.	No. L.	Beller	No CA	398 M
a far di s	6.11	No. 1	B. H.	20.611	Here	10.0	The second	Born	Main	Sec.	226.31	in a	(Aleter-	No.1	NEL	Marin .

Figure 7-6 Queue Rate Limiting Window

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Queue ID	Select the queue ID that will be configured here. Options to choose from are 0 to 7 .
Rate Limit	Select and enter the queue rate limit settings here. When the Min Bandwidth option is selected, enter the minimum bandwidth rate limit value in the space provided. This value must be between 64 and 10000000 kbps. Also, enter the maximum bandwidth (Max Bandwidth) rate limit in the space provided. This value must be between 64 and 10000000 kbps. The granularity is 64. When the minimal bandwidth is configured, the packet transmitted from the queue can be guaranteed. When the maximum bandwidth is configured, packets transmitted from the queue cannot exceed the maximum bandwidth even if the bandwidth is available. When configuring the minimal bandwidth, the aggregate of the
	When configuring the minimal bandwidth, the aggregate of the configured minimum bandwidth must be less than 75 percent of the interface bandwidth to make sure the configured minimal bandwidth can be guaranteed. It is not necessary to set the minimum guaranteed bandwidth for the highest strict priority queue. This is because the traffic in this queue will be serviced first if the minimal bandwidth of all queues is satisfied.
	The configuration of this command can only be attached to a physical port but not a port-channel. That is the minimum

Parameter	Description
	guaranteed bandwidth of one CoS cannot be used across physical ports.
	When the Min Percent option is selected, enter the minimum bandwidth percentage value in the space provided. This value must be between 1 and 100 percent (%). Also, enter the maximum percentage value (Max Percent) in the space provided. This value must be between 1 and 100 percent (%).

Advanced Settings

DSCP Mutation Map

This window is used to view and configure the Differentiated Services Code Point (DSCP) mutation map settings. When a packet is received by an interface, based on a DSCP mutation map, the incoming DSCP can be mutated to another DSCP immediately before any QoS operations. The DSCP mutation is helpful to integrate domains with different DSCP assignments. The DSCP-coS map and DSCP-color map will still be based on the packet's original DSCP. All the subsequent operations will base on the mutated DSCP.

To view the following window, click **QoS > Advanced Settings > DSCP Mutation Map**, as shown below:

The Instal Automotion and												
antor North Lago	CSOP Jun (Mar	C.spin D/GP	(646)									
(\$9.8 · · · · · · · · · · · · · · · · · · ·				1								Sec.
				- 61	_	_	Ingh	a ones				
-			TRANS.		-	-	i.	SCO.	¥.		120	
	- 12	7	1	2.2	- 2	<u>_</u>	5.0	1	7	.1	1 Y	
	16 RS	20 J	101	1	1.16	1.1423	115	10	17	1.30	12	
	199	10	273	52	19.5	74	23.	31	29	- 85	1.1	
that work	1044	24	201		.18	40	.2%	- 26	35	- 65	144	Delate
	-40	20 S	1.00	-6	- 44	41	125	14	315	48	-49	
	55		- 54	53	- 25	24	55	38	37	86	25	
	15	68	351	-82	11500							

Figure 7-7 DSCP Mutation Map Window

The fields that can be configured are described below:

Parameter	Description
Mutation Name	Enter the DSCP mutation map name here. This name can be up to 32 characters long.
Input DSCP List	Enter the input DSCP list value here. This value must be between 0 and 63.
Output DSCP	Enter the output DSCP value here. This value must be between 0 and 63.

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

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

Port Trust State and Mutation Binding

This window is used to view and configure port trust state and mutation binding settings.

To view the following window, click **QoS > Advanced Settings > Port Trust State and Mutation Binding**, as shown below:

en 1 (v)	Francisco Maria 11 - •	To Part To bar	Taxi Sora	CSOP MARTINSKO III. III. UNIV	O Bare	69.7
ellin Sectope		2 (1990) (P100)		Tistor Mana	100-100 C	
	(Sal)	Rest States	_	1147-1141		_
	6187	164565				
100 C	671762:	(4/12.4)				
34	latera international de la constante de la const	78.9732+				
	MAR.	Taut Lat				
24	6:123	240 hat				
	60.201	Titul Gell				
	04%7	to a Section				
	601/8.S	(6/415(4)				
	entra e	10.01 (325)				
4	estal E	74.4 245				
	EDH .	1x.d 0x5				
10	1.042	14.4545				
. (e	0.00	in a familie				
10	rivela.	18387614				
	e de la	18.01.027				



The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Trust State	Select the port trust state option here. Options to choose from are CoS and DSCP .
DSCP Mutation Map	Select and enter the DSCP mutation map name used here. This name can be up to 32 characters long.
	Select the None option to not allocate a DSCP mutation map to the port(s).

DSCP CoS Mapping

This window is used to view and configure the DSCP CoS mapping settings.

To view the following window, click **QoS > Advanced Settings > DSCP CoS Mapping**, as shown below:

Costant and			
Fran Fort	Te Pert Coll (865-110-10-01	
2 Mar.29	* [abid2] \$ 1 ¥		405
: Section			1.1 AM
1901	G.*	Heat and	
	1		
8		1.14	
	2	ALC: N	
30.001	3	29-01	
1.949.0003	10 C	15.0	
		40-47	
	(*) (*	4511	
1	1	- 11.0 °	
		. (61	
	3	5-01	
	-	6-12	
Contraction (2	24-7.1	
(217)216		r' 54	
	(A)	#150	
		858	
	7	8-43	
	1	Q.T.	
1	71	1.0	
	2	No. Chi	
10.00	1	11 da	
1.12.122		33-18	
	3	- K-47	
		40.55	

Figure 7-9 DSCP CoS Mapping Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
CoS	Select the CoS value. Options to choose from are 0 to 7 .
DSCP List	Enter the DSCP list value to map to the CoS value here. This value must be between 0 and 63.

CoS Color Mapping

This window is used to view and configure the CoS color mapping settings.

To view the following window, click **QoS > Advanced Settings > CoS Color Mapping**, as shown below:

na Distribution	Tarilor Cost in (47,	com.	
ni Doster 1 🗵 obiAt		Galer Grann A	
	ing states i	turne a	
a li n Sectopi			
	(and an	2348.1 ml	
	Sidut	3.2	
001975	70 m		
	+21		
	Gener	52	
#1127.	Ye an		
1.500355	Sec.		
	199.9	11	
#3037.0	W Inc.		
	Creat	3-7	
# 11%N	We are		
	a _c ,		
	(30.9 m)	17	
- 10703-04	100 APA		
	R41		
	Steele -	2.7	
21 (FM)	Ye 28.		
100478	-101		
	Selection of the select	17	
61112	16.06		

Figure 7-10 CoS Color Mapping Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
CoS List	Enter the CoS value that will be mapped to the color. This value must be between 0 and 7 .
Color	Select the color option. Options to choose from are Green , Yellow , and Red .

DSCP Color Mapping

This window is used to view and configure the DSCP color mapping settings.

To view the following window, click **QoS > Advanced Settings > DSCP Color Mapping**, as shown below:

ni Fan Fan	TR PRI DACPI M 343	Carl	
1 🔽 🔤 🖓	· [001021 [8]	aver a	405
nii ti Setiloga		-X. X. X	
1591	15star	in Real and	
	tion .	111	
CONTRACT 1	64.4		
	674		
1000000	Onest	0-63	
10.002	Yelse		
12022/25	But .		
	- 18 d.e.	111	
0.0159-025	1140		
	6245		
	Graec	040	
48.109	Velter		
1	15.0		
112200	26×0	111	
(#***#)	cars.		
01/26/00	Red		
	Grave	5-63	
10.226	Yeller	0.000	
	B.4		
	2630	(13)	

Figure 7-11 DSCP Color Mapping Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
DSCP List	Enter the DSCP list value here that will be mapped to a color. This value must be between 0 and 63.
Color	Select the color option that will be mapped to the DSCP value. Options to choose from are Green , Yellow , and Red .

Class Map

This window is used to view and configure the class map settings.

To view the following window, click **QoS > Advanced Settings > Class Map**, as shown below:

Chan Maritiana (1770)	Nutrice Visits Crisits Nimm Ave 18		
Form Entries: 2			
LANK Map risers	Multiple March Colours		
dura-mez	ivs≠ err	Bable	CONTRACTOR -
stor to ball	In d Arr	Paul .	Celota -

Figure 7-12 Class Map Window

The fields that can be configured are described below:

Parameter	Description
Class Map Name	Enter the class map name here. This name can be up to 32 characters long.
Multiple Match Criteria	Select the multiple match criteria option here. Options to choose from are Match All and Match Any .

Click the Apply button to accept the changes made.

Click the Match button to 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.

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

Class Usp Horn	C302-010		
No. C.			
- Hone 2 Sector			
6- Alt Bons	32.4 m a		
() 265 Lh1(5-2)	114		
DOCT UNICHES	125161	C Collecter	
🕐 Presidence (Jacob 7)	147	CT-A alt	
Ch Projects Harne	Refe 1	TT	
C: VID Lb.1 (4054)	111		
			Reb Apr.

Figure 7-13 Match Rule Window

Parameter	Description
None	Select this option to match nothing to this class map.
Specify	Select the option to match something to this class map.
ACL Name	Select and enter the access list name that will be matched with this class map here. This name can be up to 32 characters long.
CoS List	Select and enter the CoS list value that will be matched with this class map here. This value must be between 0 and 7.

Parameter	Description
DSCP List	Select and enter the DSCP list value that will be matched with this class map here. This value must be between 0 and 63.
	Tick the IPv4 only check box to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets.
Precedence List	Select and enter the precedence list value that will be matched with this class map here. This value must be between 0 and 7.
	Tick the IPv4 only check box to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets. For IPv6 packets, the precedence is most three significant bits of traffic class of IPv6 header.
Protocol Name	Select the protocol name that will be matched with the class map here. Options to choose from are None , ARP , BGP , DHCP , DNS , EGP , FTP , IPv4 , IPv6 , NetBIOS , NFS , NTP , OSPF , PPPOE , RIP , RTSP , SSH , Telnet , and TFTP .
VID List	Select and enter the VLAN list value that will be matched with the class map here. This value must be between 1 and 4094.

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

Aggregate Policer

This window is used to view and configure the aggregate policer settings.

To view the following window, click **QoS > Advanced Settings > Aggregate Policer**, as shown below:

Single Cara Serginge (e. g. a. a.) = de la Ser, e. () Han a. (Hale) = Ser (L. 1994)		0.ee.0	Two Films Sections						
				25 (2010) 25 (11) (11) (10) (11)		1.1	100 March 100 Ma		
			166		Manager And Strip (1994)		Ku, w		
the excite		Increase.	- (284P) (1	Provincian a		THE WORKS	Hannik . DOCH HAL		
Weider School		Nate .	A WELLAND	Case See		Titsebler -			
Vette		000000						1	
Barn	Annan Reis	Horeat Dury, Star	No. Deni Ster	ContarnActor	Econd Action	Walk Actor	Doke Aware	100	
A766	100	-114		Tracardi	Tomini		Direbled.	English	



Parameter	Description			
Aggregate Policer Name	Enter the aggregate policer's name here.			
Average Rate	Enter the average rate value here. This value must be between 0 and 10000000 kbps.			
Normal Burst Size	Enter the normal burst size value here. This value must be between 0 and 16384 Kbytes.			
Maximum Burst Size	Enter the maximum burst size value here. This value must be between 0 and 16384 Kbytes.			
Confirm Action	Select the confirm action here. The confirm action specifies the action to take on green color packets. If the confirm action is not specified, the default action is to Transmit . Options to choose from are:			

Parameter	Description	
	 Drop - Specifies that the packet will be dropped. Set-DSCP-Transmit - Enter the IP DSCP value in the space provided. This value sets the IP Differentiated Services Code Point (DSCP) value and transmits the packet with the new IP DSCP value. Set-1P-Transmit - Enter the 1P transmit value in the space provided. This value sets the IEEE 802.1p value and transmits the packet with the new value. Set-DSCP-1P - Enter the IP DSCP and 1P transmit values in the spaces provided. Transmit - Specifies that packets will be transmitted unaltered. 	
Exceed Action	 Select the exceed action here. The exceed action specifies the action to take on packets that exceed the rate limit. For a two rate policer, if the exceed action is not specified, the default action is Drop. Options to choose from are: Drop - Specifies that the packet will be dropped. Set-DSCP-Transmit - Enter the IP DSCP value in the space provided. This value sets the IP DSCP value and transmits 	
	 the packet with the new IP DSCP value. Set-1P-Transmit - Enter the 1P transmit value in the space provided. This value sets the IEEE 802.1p value and transmits the packet with the new value. Set-DSCP-1P - Enter the IP DSCP and 1P transmit values in the spaces provided. Transmit - Specifies that packets will be transmitted unaltered. 	
Violate Action	Select the violate action here. The violate action specifies the action to take on packets that violate the normal and maximum burst sizes for singe rate policing. It specifies the action to take for those packets that did not conform to both CIR and PIR. For a single rate policer, if the violate action is not specified, it will create a single-rate two-color policer. For a two-rate policer, if the violation action is not specified, the default action is equal to the exceed action. Options to choose from are:	
	 Drop - Specifies that the packet will be dropped. Set-DSCP-Transmit - Enter the IP DSCP value in the space provided. This value sets the IP DSCP value and transmits the packet with the new IP DSCP value. Set-1P-Transmit - Enter the 1P transmit value in the space provided. This value sets the IEEE 802.1p value and transmits the packet with the new value. Set-DSCP-1P - Enter the IP DSCP and 1P transmit values in the spaces provided. Transmit - Specifies that packets will be transmitted unaltered. 	
Color Aware	Select this option to enable or disable color aware option here. When color aware is not specified, the policer works in the colorblind mode. When color aware is enabled, the policer works in the color aware mode.	

Click the **Delete** button to remove the specific entry.
After clicking the Two Rate Setting tab, at the top of the page, the following page will be available.

Single Reta Settings	Two Taxe Settin					
		·				
a possi de de cella el d	1					
an a		line.	12.00 (19.00 (19.00))	44)	63 ye	ei.
an in the man of	(i)	light.	PERFECT DATE		KEVA	a
toman datar	tanet 👘 😓	And a state of the	Forest Materia	L'rep.	1.111	
New Joshiden	Dep +	ALC: NOTE OF	Doles Annals	Cleables	((e)	1410 - 210
Veranis ?-		1				-490
Nam CR Caller Da	e. Pft. DockSarol	Codon Adar	Crowned Action	Webse Addre	Color Awara	
AP162 100 100	01 21	There's	. 675	0.98	Divebled	The Set Set of

Figure 7-15 Two Rate Settings Window

Parameter	Description	
Aggregate Policer Name	Enter the aggregate policer's name here.	
CIR	Enter the Committed Information Rate (CIR) value here. This value must be between 0 and 10000000 kbps. The committed packet rate is the first token bucket for the two-rate metering.	
Confirm Burst	Enter the confirm burst value here. This value must be between 0 and 16384 Kbytes. The confirm burst value specifies the burst size for the first token bucket in kbps.	
PIR	Enter the Peak information Rate (PIR) value here. This value must be between 0 and 10000000 kbps. The peak information rate is the second token bucket for the two-rate metering.	
Peak Burst	Enter the peak burst value here. This value must be between 0 and 16384 Kbytes. The peak burst value is the burst size for the second token bucket in kilobytes.	
Confirm Action	 Select the confirm action here. The confirm action specifies the action to take on green color packets. If the confirm action is not specified, the default action is to Transmit. Options to choose from are: Drop - Specifies that the packet will be dropped. Set-DSCP-Transmit - Enter the IP DSCP value in the space provided. This value sets the IP DSCP value and transmits the packet with the new IP DSCP value. Set-1P-Transmit - Enter the 1P transmit value in the space provided. This value sets the IEEE 802.1p value and transmits the packet with the new value. Set-DSCP-1P - Enter the IP DSCP and 1P transmit values in the spaces provided. Transmit - Specifies that packets will be transmitted unaltered. 	
Exceed Action	 Select the exceed action here. The exceed action specifies the action to take on packets that exceed the rate limit. For a two rate policer, if the exceed action is not specified, the default action is Drop. Options to choose from are: Drop - Specifies that the packet will be dropped. Set-DSCP-Transmit - Enter the IP DSCP value in the space provided. This value sets the IP DSCP value and transmits the packet with the new IP DSCP value. Set-1P-Transmit - Enter the 1P transmit value in the space provided. This value sets the IEEE 802.1p value and transmits the packet with the new value. Set-DSCP-1P - Enter the IP DSCP and 1P transmit values in 	

Parameter	Description
	 Transmit - Specifies that packets will be transmitted unaltered.
Violate Action	Select the violate action here. The violate action specifies the action to take on packets that violate the normal and maximum burst sizes for singe rate policing. It specifies the action to take for those packets that did not conform to both CIR and PIR. For a single rate policer, if the violate action is not specified, it will create a single-rate two-color policer. For a two-rate policer, if the violation action is not specified, the default action is equal to the exceed action. Options to choose from are:
	 Drop - Specifies that the packet will be dropped. Set-DSCP-Transmit - Enter the IP DSCP value in the space provided. This value sets the IP DSCP value and transmits the packet with the new IP DSCP value. Set-IP-Transmit - Enter the 1P transmit value in the space provided. This value sets the IEEE 802.1p value and transmits the packet with the new value. Set-DSCP-1P - Enter the IP DSCP and 1P transmit values in the spaces provided. Transmit - Specifies that packets will be transmitted unaltered.
Color Aware	Select this option to enable or disable color aware option here. When color aware is not specified, the policer works in the colorblind mode. When color aware is enabled, the policer works in the color aware mode.

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

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

Policy Map

This window is used to view and configure the policy map settings.

To view the following window, click **QoS > Advanced Settings > Policy Map**, as shown below:

Policy Hap				
Create/Delete Policy Map				
Policy Map Name	Return			Apply
Taallis Policy				
Policy Mag Hame	12 share	Class Map Name	12 alson	Apply
Total Babbes: 1				
		Policy Map Name		
		Paticy-Map-1		Colette
				11 P P 1 5 4 G
Class Rates				
	Class	Alg Hame		

Figure 7-16 Policy Map Window

The fields that can be configured for Create/Delete Policy Map are described below:

Parameter	Description
Policy Map Name	Enter the policy map's name here that will be created or deleted. This name can be up to 32 characters long.

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

The fields that can be configured for **Traffic Policy** are described below:

Parameter	Description
Policy Map Name	Enter the policy map's name here. This name can be up to 32 characters long.
Class Map Name	Enter the class map's name here. This name can be up to 32 characters long.

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

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 view the rules of a specific policy map, click the policy map name in the table (the **Policy Map Name** will toggle to the bold font).

ламы англа кажулыр —				
не-сулаге хагал	[Pakas			kot v
Treffic Policy				
Million Market	<u>10000</u>	$\{X_i(y_i),y_j\} \in \{i,j\}$	22/2019	
Total English 1				
		Pulicy Max Hann		
		PARA ROLT.		
			1910	ana la ann Te
InterioNau-Uniter				
	Class Nep Harn			
	7.52/305.8		Set Actor Pai	eter 🕴 De ete
			100	THE REPORT OF

Figure 7-17 Policy Map (View Rules) Window

Click the **Set Action** button to configure the action for the policy map.

Click the **Policer** button to configure the policer action for the policy map.

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

Police Map Home	Party			
Class Map Harra	Obiza			
Set Active				
OHAN C				
e Openly				
Adlen Creodence (S-1)	Nom	😥 Theology		
(1946) 2007 (963)	Nem	🗽 🗇 eks wy		
(1044) 205 (0-5)	Month	<u>× (1</u>		
("New 2nd Queue (9-7)	Depart			

After clicking the Set Action button, the following window will appear.

Figure 7-18 Set Action Window

The fields that can be configured are described below:

Parameter	Description
None	Select this option to match nothing to this policy map.
Specify	Select the option to match something to this policy map.
New Precedence	Select a new precedence for the packet. This value must be between 0 and 7. Tick the IPv4 only to only mark IPv4 precedence. Setting the precedence will not affect the CoS queue selection.
New DSCP	Select a new DSCP for the packet. This value must be between 0 and 63. Tick the IPv4 only to only mark IPv4 precedence. Setting DSCP will not affect the CoS queue selection.
New CoS	Select a new CoS value for the packet. This value must be between 0 and 7. Setting CoS will not affect the CoS queue selection.
New CoS Queue	Select a new CoS queue for the packet. This value must be between 0 and 7. This overwrites the original CoS queue selection.

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

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

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



Figure 7-19 Police Action Window

Parameter Description None Select this option to match nothing to this policy map. Specify Select the option to match something to this policy map. Average Rate Enter the average rate in kilobits per second. **Normal Burst Size** Enter the normal burst size in kilobytes. **Maximum Burst Size** Enter the maximum burst in kilobytes. **Conform Action** Select the action to take on green color packets. Options to choose from are Drop, Set-DSCP-Transmit, Set-1P-Transmit, Transmit, and Set-DSCP-1P.

Parameter	Description
Exceed Action	Select the action to take on yellow color packets. Options to choose from are Drop , Set-DSCP-Transmit , Set-1P-Transmit , Transmit , and Set-DSCP-1P .
Violate Action	Select the action to take on red color packets. Options to choose from are None , Drop , Set-DSCP-Transmit , Set-1P-Transmit , Transmit , and Set-DSCP-1P .
Color Aware	Select this option to enable or disable color aware mode.

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

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

Policy Binding

This window is used to view and configure the policy binding settings.

To view the following window, click **QoS > Advanced Settings > Policy Binding**, as shown below:

and reacting writing					
ni PaniSa 1 (2) AniON A	To Fort	Director Reported	Policy Usp Hones at 12 die s	(See	L.see_J
nii ti Setiloga		WIN WAR	2010. 201		
all and a		2 December 1		This y Map Rate	
1.6969					
1.111-0					
191110					
entiste .					
800188					
12168	1				
(\$500					1
(9546)					
19:19					
e ni 1940					
#113231					
žava –					1
100000			1		
0003.71					
831575					-



The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction option here. Option to choose from is Input . Input represents Input specified ingress traffic.
Policy Map Name	Enter the policy map name here. This name can be up to 32 characters long. Select the None option to not tie a policy map to this entry.

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

8. Access Control List (ACL)

ACL Configuration Wizard ACL Access List ACL Interface Access Group ACL VLAN Access Map ACL VLAN Filter

ACL Configuration Wizard

This window is used to guide the user to create a new ACL access list or configure an existing ACL access list.

To view the following window, click ACL > ACL Configuration Wizard, as shown below:





ACL COMMON	kar Masari -		
an exterior	varianted version to her type wided a	al 550 Aprily Post	
Do you want to	create a new ACL access list or update a	e a dating spore a lini?	
CONCHE			
ACC MARK	A 8004		
g Speaks			
a Jacoba			5-51
2010/02/02	dunderst#C, nore reacts state		1 <u></u> 1
ana orașe de la competencia de la comp			1
<mark>ban Tin I</mark> ra		#EL 7534	Totalia MA

Figure 8-2 ACL Configuration Wizard (Access-List Assignment) - Update Window

The fields that can be configured are described below:

Parameter	Description
Create	Select and enter the ACL name with a maximum of 32 characters.
Update	Select to see a table below with the existing ACL access lists. Select the specific re-configure the entry.

Click the **Next** button to continue.

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

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



Figure 8-3 ACL Configuration Wizard (Select Packet Type) Window

The fields that can be configured are described below:

Parameter	Description
MAC	Select to be MAC ACL.
IPv4	Select to be IPv4 ACL.
IPv6	Select to be IPv6 ACL.

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

Click the Next button to continue.

After clicking the **MAC** radio button and the **Next** button, the following window will appear.

ea barge s seguerovnemmer og som Nord Exercit	TO CHART & DWATCH	1 cens	6		
o ka reje stjelje	12	1	CC		
	ChereiType	W210 VLAN			
and adverse					
※ 毎7		854			
Second Second	31.4092.02	ener. Statu	I THE ROLE AVER		
Cheve True	2146.97.6	Theo.	AT A PARTY AND A PARTY AND		
Weldow) 100	36.46 47.15	776.(s	of 1 the map areas		
e koord by pr					
Horse History (you	Proce Selec	<u> 19</u>			
when the set to be and		100			
-hourt type March Mit Re-	++(
SUATO VIOR					
O.S. Para coud					
and the second se					
-8 V D+ -400K					
CIRLAN Denve		1			
The Barge Doc	101				
Time Barge h2.c	10.00				

Figure 8-4 ACL Configuration Wizard (Add Rule for MAC ACL) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. Select Auto Assign to automatically generate an ACL rule number for this entry.
Source	 Select and enter the source information here. Options to choose from are: Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's MAC address here. MAC - The Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination	 Select and enter the destination information here. Options to choose from are: Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's MAC address here. MAC - The Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Specify Ethernet Type	Select the Ethernet type option here. Options to choose from are aarp, appletalk, decent-iv, etype-6000, etype-8042, lat, lavc-sca, mop-console, mop-dump, vines-echo, vines-ip, xns-idp, and arp.
Ethernet Type	Enter the Ethernet type hexadecimal value here. This value must be between 0x0 and 0xFFFF. When any Ethernet type profile is selected in the Specify Ethernet Type drop-down list, the appropriate hexadecimal value will automatically be entered.
Ethernet Type Mask	Enter the Ethernet type mask hexadecimal value here. This value must be between 0x0 and 0xFFFF. When any Ethernet type profile is selected in the Specify Ethernet Type drop-down list, the appropriate hexadecimal value will automatically be entered.
CoS	Select the CoS value used here. This value is between 0 and 7 .
VID	Enter the VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094.
VLAN Range	Enter the VLAN range here. Enter the minimum and maximum VLAN ID in the range here.
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .

Click the $\ensuremath{\textbf{Back}}$ button to return to the previous window.

Click the **Next** button to continue.

After clicking the **IPv4** radio button and the **Next** button, the following window will appear.

ecae valiga o supultos aura Guaixatos (4. 1185535)	bee to create a root rai	e. Literation	020		
mana layy	24	T		diam'	
Aven berrieben	1980	2015 		01009	
PréAkurr	Ext.	EN405CF	TCPTive		
Pv4Akaszi	For L	EN405CF	TCP Fixe		

Figure 8-5 ACL Configuration Wizard (Add Rule for IPv4 ACL) Window

This window has a dynamic section. Every selection made in the **Protocol Type** drop-down list will change the bottom part of this window.

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. Select Auto Assign to automatically generate an ACL rule number for this entry.
Protocol Type	Select the protocol type option here. Options to choose from are TCP, UDP, ICMP, EIGRP, ESP, GRE, IGMP, OSPF, PIM, VRRP, IP-in-IP, PCP, Protocol ID, and None.

After selecting the **TCP** option as the **Protocol Type**, the following section will appear.

sa na Glas Avalgana na 🕫 Sel		Add Rate ** Apply Part.			
nar salan a wasan salah	No la chias a aver	uk.			
5 Auto de 140 (178551)		Course			
aka Taz	5840	12	(0,235)	Electric 6	
seda ana mana					
Instations.	Car	20%0.0%12*	14 Pielap	1	
1			N		
the locates		264.545			
æler		2010		1	
Sears (illicit	1. 1.2.2.1	Deditation Control			
DF 🔲	1 11.1	annear Ob			
widtard 👘	-	With	and 🗍		
- Pol					
Searce Peril Please Se	144 V				
Please Se	And Poll	distance Place	ca Sninca 💌	(C1.96.0.0)	
through the start Physics St	test [w]				
-fixade By	sat bell	4 835255 1953	ar Salest 141	(E-5352.2)	
PM DSCP			and the second	a constant	
WP States Bases	and a table	AVA COLD			
0.0901/0-62 [fines 3					
1. 78 S. (25 S.)					
TCP Flag TCP Flagadv toor	1.1.14 L 1.4. 1.4.				
here Bang	 Applement 				

Figure 8-6 ACL Configuration Wizard (Add Rule for IPv4 ACL) TCP Window

Parameter	Description
Source	 Select and enter the source information here. Options to choose from are: Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IP address here. IP - The Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	 Select and enter the destination information here. Options to choose from are: Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IP address here. IP - The Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	 Select and enter the source port value here. Options to choose from are: = - The specific selected port number will be used. > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used.

Parameter	Description
	 ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	 Select and enter the destination port value here. Options to choose from are: = - The specific selected port number will be used. > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).
ToS	After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are ack , fin , psh , rst , syn , and urg .
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .

After selecting the **UDP** option as the **Protocol Type**, the following section will appear.

este staligns septembe aurik 5 Gegevort (4. 1962535) 1975 : Sov	0.9	- CARACAN		Pagmadu	
Avan den den	1.570	38	000		
PutAkinar	Part .	IP-40SCP			
In activit					
W. A.		$-i \phi = i \phi_{\mu \mu}$			
bean Diest		Column West			
bert is a		Exchanges (1949)			
We have a		(matrix)			
Pest.					
Source Field Rivery Sin	64.012				
1.308.50	ed in	(0.69558) 11 march 2044	6 K)	(0.895255	
Double Brit Please Se	ed in				
Paraz	-1	at the set of the set of the	1	11.144310	
0.6010.002					
in Philippedia and Phane.		une Select			
O 5089 (0421 - FRANK)	8 a				
Traffic form					
the cards					

Figure 8-7 ACL Configuration Wizard (Add Rule for IPv4 ACL) UDP Window

Parameter	Description
Source	 Select and enter the source information here. Options to choose from are: Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IP address here. IP - The Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	 Select and enter the destination information here. Options to choose from are: Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IP address here. IP - The Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	 Select and enter the source port value here. Options to choose from are: = - The specific selected port number will be used. > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used.

Parameter	Description
	• Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	 Select and enter the destination port value here. Options to choose from are: = - The specific selected port number will be used. > - All ports greater than the selected port, will be used.
	 < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).
ToS	After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .

After selecting the **ICMP** option as the **Protocol Type**, the following section will appear.

entrarial light	Address and the second second	The subscript costs and	
A2443 18100000	644 T	(3-325) 📋 Tragmente	
PriAkting 10	M7 Ph40SCP	-	
	Kued III Conecco		
Per Actional Re Cas	36 A.M.		
Sector Sector	THE R. LEWIS		
Sec.	Deleter D.P.		
		(in)	
1949 ¹			
BOATHENPREAMATER PAD	a Salec: •		
CRP (Hounge 7) 24 (2-322)	Herizogia Code (3-323)	ş	
194080			
or Photos Salad	 Col Plana Salact 		

Figure 8-8 ACL Configuration Wizard (Add Rule for IPv4 ACL) ICMP Window

Parameter	Description
Source	 Select and enter the source information here. Options to choose from are: Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IP address here. IP - The Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	 Select and enter the destination information here. Options to choose from are: Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IP address here. IP - The Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Specify ICMP Message Type	Select the ICMP message type used here.
ICMP Message Type	When the ICMP Message Type is not selected, enter the ICMP Message Type numerical value used here. When the ICMP Message Type is selected, this numerical value will automatically be entered.

Parameter	Description
Message Code	When the ICMP Message Type is not selected, enter the Message Code numerical value used here. When the ICMP Message Type is selected, this numerical value will automatically be entered.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).
ToS	After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .

After selecting the EIGRP, ESP, GRE, IGMP, OSPF, PIM, VRRP, IP-in-IP, PCP, or Protocol ID option as the Protocol Type, the following section will appear.

Benne sondgrun ondere in ausber 19 Seine eine 14, if 1825231		Contractor.		
anara iya	8369	- pr	(6-825) 📄 Trapheria	
Assign Information				
The second second				
Présidente	Pr4 DSCP			
Ever Accessed				
20.70		36.731		
Sec. 1		THE R	(
Stor. Ster		where a second		
		D.H.		
1.000 B (11)		(maxim)		
Predisor Protection Places S				
And M.S. Wang and Manager, "Manager, N.	okal 👘 Taŭ Pisa	n Selection T		
The strength strength	4.4 7			
ORAFORI AND				

Figure 8-9 ACL Configuration Wizard (Add Rule for IPv4 ACL) EIGRP Window

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are:
	 Any - Any source traffic will be evaluated according to the conditions of this rule.
	 Host - Enter the source host's IP address here. IP - The Wildcard option will also be available. Enter the
	group of source IP addresses by using a wildcard bitmap.

Parameter	Description
	The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	 Select and enter the destination information here. Options to choose from are: Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IP address here. IP - The Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).
ToS	After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .

After selecting the **None** option as the **Protocol Type**, the following section will appear.

<mark>Plesse vaniga standar konstanter k</mark> 19. Se aventer 14. († 165535)	ostalan a rew tale.	Conver		
entrarial light	No.2	· ·	(-465) E fragmente	
Politikarsz (************************************	FW DXP	Naca Seco Seco Mataa		
PADSCI # IT "Noncente Pieces See O DOCR D'121 Receiver The Range State Scher B. Carrol C		Solice -		

Figure 8-10 ACL Configuration Wizard (Add Rule for IPv4 ACL) None Window

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.

Parameter	Description
Source	 Select and enter the source information here. Options to choose from are: Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IP address here. IP - The Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	 Select and enter the destination information here. Options to choose from are: Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IP address here. IP - The Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).
ToS	After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .

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

Click the **Next** button to continue.

After clicking the IPv6 radio button and the Next button, the following window will appear.

ecter vanige op angeleiken dur: De gue van 14. († 169533)		nen Lietzenisch			
ental lige	224	T	(1425) L	Trapments	
Assign Electropics	0802	1010 D			
Ph@Adcauge	Fait	#%SDSCF	TCP/Leg	The label	

Figure 8-11 ACL Configuration Wizard (Add Rule for IPv6 ACL) Window

This window has a dynamic section. Every selection made in the **Protocol Type** drop-down list will change the bottom part of this window.

The **fixed** fields that can be configured are described below:

Parameter	Description	
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. Select Auto Assign to automatically generate an ACL rule number for this entry.	
Protocol Type	Select the protocol type option here. Options to choose from are TCP, UDP, ICMP, Protocol ID, ESP, PCP, SCTP, and None.	

After selecting the **TCP** option as the **Protocol Type**, the following section will appear.

Sauce et March (1995) Jaco Tear	100	ch. Connton	13-	(Transfe	
organia mensis	Part	35412422	1011min	Fire Land	
in a second second	THE.	And Darks	. In the second	Prov Calif	
Pris Learnes Sectors		Sec.			
entr Ottol	EUCT.		Contraction and Contraction of Co		
Search OP-8	2012.1	Donaka jury	5 2012.1		
Profestange		16	é-Lerga		
Put	-71				
Scale Pol. Please 5 Please 5	ees (v) des (v)	diame Pleasa	5490 PD	21840	
the structure when the set of	665 / 10 1 10				
Phase 9	454 (M)	4 88528 Phone	sasa (4)	(E \$3523)	
IP-R DSCP					
DSCHOLED HOMA OLA	e. 101				
TEP THE TEP THE DAY, DIVIDING	4 [104][256][266]				
FRUITIN					



Parameter	Description		
Source	Select and enter the source information here. Options to choose from are:		
	 Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IPv6 address here. 		
	 IPv6 - The Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided. 		
Destination	Select and enter the destination information here. Options to choose from are:		

Parameter	Description				
	 Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided. 				
Source Port	 Select and enter the source port value here. Options to choose from are: = - The specific selected port number will be used. > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. 				
Destination Port	 Select and enter the destination port value here. Options to choose from are: = - The specific selected port number will be used. > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. 				
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.				
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are ack , fin , psh , rst , syn , and urg .				
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.				
Time Range	Enter the name of the time range to associate with this ACL rule.				
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .				

After selecting the **UDP** option as the **Protocol Type**, the following section will appear.

- Cernigandase Wasers					
ca contiguration visuare					
aless ListAssays verd ~ 2	eets watered syperio				
влокахода конскител	Dento sneets a new	inuli.			
Characteria (1997)		0.0-46			
And yet	-0-	2	3.2.4	1782-118	
Autogenzame Groener					
Polationa	74	(20,0002	Baselater	1	
				4	
In Address					
8 Am		- 1911	n e		
Scena (Contra	E.F.	Destinative (C)	1 10000		
Source Class	2012	Low room	en de <mark>Puiete</mark>		
Professions			ló Lorca	191	
- Dec					
Source Part - Michigan Se	2.11.E				
		exercised - 1946 in	17 ×	energente.	
Legences for Anne An	Contraction and a second second				
Enviro	a 1	researce; Entries an	17. 1	(3/5869)	
Ind DOT					
192 J. BL PRAK DAY					
- Parking -	92 - Oğ	1.2			
An of the American States of the	1				
	5 V				
Tableman (2 cist	11				
Access Access	1.6.9 ±				
					. /a.d

Figure 8-13 ACL Configuration Wizard (Add Rule for IPv6 ACL) UDP Window

Parameter	Description
Source	Select and enter the source information here. Options to choose from are:
	 Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are:
	 Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Source Port	Select and enter the source port value here. Options to choose from are:
	 = - The specific selected port number will be used. > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s)

Parameter	Description
	provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	 Select and enter the destination port value here. Options to choose from are: = - The specific selected port number will be used. > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the
	drop-down list.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .

After selecting the ICMP option as the Protocol Type, the following section will appear.

KOLKINIZ (M. 1169535)	70.0	(1440-24)	en e		
nal lyw Mega hannanaw	1049 1	7.1	X-625)	🗁 Јартињ	
PASAkara	ICM2	PNSOSCP	Fire Label	1	
PROVIDE:					
20.744		- (A - A	ù.		
() Uzd Seato	- pattern	area MI	es line	-	
2011 (2011-04)	12/2 H	Contension de	4 MAR		
- PORY OF	94 		var nor i c		
CIM.					
Specify KINP Passage Te		-		-100	
Internation (Martin	AID.	Jan well as may as you?		99	
PHS D SC#					
1991 FRI SCI NAME OF	A1				
Rev Label					
Paul an of Second					

Figure 8-14 ACL Configuration Wizard (Add Rule for IPv6 ACL) ICMP Window

Parameter	Description
Source	Select and enter the source information here. Options to choose from are:
	 Any - Any source traffic will be evaluated according to the conditions of this rule.
	 Host - Enter the source host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are:
	 Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Specify ICMP Message Type	Select the ICMP message type used here.
ICMP Message Type	When the ICMP Message Type is selected, this numerical value will automatically be entered.
	When the ICMP Message Type is not selected, enter the ICMP Message Type numerical value used here.
Message Code	When the ICMP Message Type is selected, this numerical value will automatically be entered.
	When the ICMP Message Type is not selected, enter the Message Code numerical value used here.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .

After selecting the **Protocol ID**, **ESP**, **PCP**, or **SCTP** option as the **Protocol Type**, the following section will appear.

lesae kaniga sinaparka nu 9 Secuence (A. (1.69535)	mber to struke a rew rate	n Lighter			
entra lane	Pressed D	· · ·	y.425)	E Ingrada	
ascija Educebov	To and the	61 82153. -			
P\5Akmzi	Prepscp	Revised	-		
evinence.					
and the second second			άų.		
Stat	parent.	the second s	IN HER		
5000 1500s	12-2-11	3.8 miles (
PORV N	en [www.unor	12	
IPH6 D SCR					
1802-00 HJD Filence Co	iei -				
Row's she					
Towitation 10-10465151	i du				

Figure 8-15 ACL Configuration Wizard (Add Rule for IPv6 ACL) Protocol ID Window

Parameter	Description
Protocol	Enter the Protocol ID value used here. This value must be between 0 and 255.
Fragments	Select the Fragments option to include packet fragment filtering.
Source	 Select and enter the source information here. Options to choose from are: Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	 Select and enter the destination information here. Options to choose from are: Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63 .
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range to associate with this ACL rule.

Parameter	Description
	Select the action that this rule will take here. Options to choose from are Permit and Deny .

After selecting the **None** option as the **Protocol Type**, the following section will appear.

Colorence (A. 1189535)		(CAMOR)	a	
matal liye	Norg	(T)	(1425) 📄 Tapawis	
Alvert Herricelow				
P-5 Adapter	PreDSCP	Baylated		
PROCEEDED				
Record and Record		- A 1	40	
19 Uzd	pill-	ale come Mil	a per-	
Seat. 25156	12:2ml	3.44AA (10	A (1982	
HOLY	-		vertion 👘	
PHODSC#				
180200 HIG Fleme Ca	ed ····			
Revise:				
Toy Law (0-1048975)				

Figure 8-16 ACL Configuration Wizard (Add Rule for IPv6 ACL) None Window

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source	 Select and enter the source information here. Options to choose from are: Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	 Select and enter the destination information here. Options to choose from are: Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.

Parameter	Description
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .

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

Click the **Next** button to continue.

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

ACL CONTROL	skar (Waxa)				
Same	avianced via Science	and the second	and the Read of Long		
	a company of a party of	man of the second state	and solve the party of the second		
	(do you want to apply d		and a second second		
				i met an	



The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction here. Option to choose from is In.

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

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

ACL Access List

This window is used to view and configure the ACL access list settings.

To view the following window, click **ACL > ACL Access List**, as shown below:

ACL Aspend 3	99						
ACL Type	21.	- 44	(1-14295) L		U Albhama	<u>10070 1</u>	9.41
ara kanusa	9			10 I.U.		- MI	
u <i>u</i>	- BACKO	056.0890	STATE OF STREET	2.2400	COUNT 2000		34,888,63
						and one last over	All Col
Sector parts	ini Anton	511	Rule:	Time I	Range (Conver	

Figure 8-18 ACL Access List Window

Parameter	Description
ACL Type	Select the ACL profile type to find here. Options to choose from are AII, IP ACL, IPv6 ACL, MAC ACL, and Expert ACL.

Parameter	Description
ID	Enter the ACL ID here. The range is from 1 to 14999.
ACL Name	Enter the ACL name here. This name can be up to 32 characters long.

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

Click the **Add ACL** button to create a new ACL profile.

Click the Clear All Counter button to clear all the counter information displayed.

Click the **Clear Counter** button to clear the counter information for the rule displayed.

Click the Add Rule button to create an ACL rule for the ACL profile selected.

Standard IP ACL

After clicking the Add ACL button, users can create a new ACL profile, as shown below:

al na s	Standard IP AC: 1	
1(1-1999)		
O. 13 TO	17 0175	
	enadoer of AZI, more encluding a schemer	844.9



The fields that can be configured are described below:

Parameter	Description		
ACL Type	Select the ACL profile type here. Options to choose from are Standard IP ACL, Extended IP ACL, Standard IPv6 ACL, Extended IPv6 ACL, Extended MAC ACL, and Extended Expert ACL.		
ID	Enter the ACL ID from 1 to 1999.		
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.		

Click the **Apply** button to create the new ACL profile.

After creating a Standard IP ACL profile, the newly created Standard IP ACL profile will be displayed in the ACL profile display table, as shown below:

ACL Type		AL.	- i -	di (i-i-iandi)	- L		Allhama 🛄	ntin:	F	
ana enn				erer to cros		2			5	440.424
T inter	ita ta	10		(MAR)	start segmenter.	a sange	1/10/07/05/00	BAPAR.	14 H	
1	Sancar	te C	Careland .	рж.	<u>8</u>	11	Shalled :		5.4	Detel -
								(iii)		
								Design Content (a se Center []	
Seams	CONTRACTOR OF	4.8.00		TKK.		Ing Ison		Contra-		

Figure 8-20 Standard IP ACL (Main) Window

Click the **Edit** button to re-configure the specific ACL profile.

Click the **Delete** button to remove the specific ACL profile.

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

To add an ACL rule in the ACL profile, select it (the ACL profile will toggle to the bold font), and click the **Add Rule** button.

ACL Type	- 20	+		L	<u> </u>	Production of the second second	dir.	1	1.0
ani kan					1.11				411451
11			na isyan	Stort even you as	e a wrog 👘	Isonation Market	-	1000	
	Standard P	St.ar	savit2.x0L	10	90.	Dis ablest		5.0	Debela
							100	an in 💼 16	
	ar de Car	8					Over 41 Carton	Oxectante	
Column I	DO NA	1.4 mil	TR.K.	_	True Dama.		O.e.e.		

Figure 8-21 Standard IP ACL (Selected) Window

After selecting the ACL profile and clicking the **Add Rule** button, users can configure the new ACL rule, in the selected ACL profile, as shown below:

AND ALL THE			
	ii ii		
Page 1999 Page 1	at water at		
702, 1813	Mania MV22		
Second Hard-Hard		ender fin with the state of the party of the	
10.0	2 Mill Olin		
Neth PAthens			
40.200	*	464	
Sector Diad	Dadaaba 🤨	Lod Land	
Serve pitte	Ostanto (r laine	
Ve Savis		or even	
	dil tan	1	
Des Base	(Particular States)		

Figure 8-22 Standard IP ACL (Add Rule) Window

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535 . If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Source	 Select and enter the source information here. Options to choose from are: Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IP address here. IP - The Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap.

Parameter	Description
	The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are:
	 Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IP address here. IP - The Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Time Range	Enter the name of the time range to associate with this ACL rule.

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

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

To enable the **Counter State** option or to enter a **Remark** for the profile, click the **Edit** button, next to the specific ACL profile (found in the ACL profile table).

U.U. Servera U.U.						
Küllinge 🧳	a +	🤟 D (1-14995)	LE ACC	tata minut	- 4	
ani kanasit						Add Asia 1
REAL PROPERTY	2017 - 1870 -	Station press to	isan inanagat	en Konstat		
i Standardi?	Skedert PAC.	20	¹⁰ Divisit	-	E Lang	Gelde.
and a similar to a	laic.			Close 41 C	niere [. Casa Conta].	
Sourcetta	Adat	This:	ten tana	C.e.s.c		
211	MARKE.	12,309		1. S. 1975	100 C	Os ats

Figure 8-23 Standard IP ACL (Edit ACL) Window

The fields that can be configured are described below:

Parameter Description						
Start Sequence No.	Enter the start sequence number here.					
Step	Enter the sequence number increment here.					
Counter State	Select to enable or disable the counter state option here.					
Remark	Enter an optional remark that will be associated with this profile here.					

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

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

To view the list of rules, that are associated with an ACL profile, select the ACL profile (found in the ACL profile table). The rule of ACL rules, connected to the selected ACL profile, will be displayed in the ACL rule table, as shown below:

CL Acores Out								
al. Type 🛛 🗛	+	₩. D (1-14995)			ALLERS DIRE			
ani katilik t						· · · · ·	. 3	441-454
ee eta kare		B10.1590	хил менесала	a waga 👘	LOBIER AND	*****	12	
i Standardi?	5	understift ACL	10	10	Gradies		5.0	Debde
						THE T		
Aurila (Pribet) Raie	S				00	a de conser (c	l ve Centre	an Da
Science Na	A.A.e.s	1006		len lann.		Cuerte -		
1000 Aug 100	www.et	10,000				1.1.1.1.1.1.1.1.1.		Os ex

Figure 8-24 Standard IP ACL (Rule Display) Window

Click the **Delete** button to remove the specific ACL rule.

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

Extended IP ACL

After clicking the Add ACL button, users can create a new ACL profile, as shown below:

01.7.4%	Estanded IP ACL	
1(2000-9999)		
O, Namo	07 0975	
	ader of ACL right e musical sets before	.828.9

Figure 8-25 Extended IP ACL (Add Profile) Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL profile type here. Options to choose from are Standard IP ACL, Extended IP ACL, Standard IPv6 ACL, Extended IPv6 ACL, Extended MAC ACL, and Extended Expert ACL.
ID	Enter the ACL ID from 2000 to 3999.
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.

Click the **Apply** button to create the new ACL profile.

After creating an Extend IP ACL profile, the newly created Extend IP ACL profile will be displayed in the ACL profile display table, as shown below:

	411-924
	A11 421
Komans	
5.0	Richard e.
Incast of	10 state
	関门

Figure 8-26 Extended IP ACL (Main) Window

Click the Edit button to re-configure the specific ACL profile.

Click the **Delete** button to remove the specific ACL profile.

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

To add an ACL rule in the ACL profile, select it (the ACL profile will toggle to the bold font), and click the **Add Rule** button.

KCL Type	<u>si</u>	→ ⊕ D(1-1995)	1		ALLEATS TOTAL		5	
ATE FORM	ey.		w s				1	444.444
1.1	ALC: HORS	(44 STR	STATE ANE INCOME.	sag	Exercise States	носия	14 H	
	Canda di P	Standard 14CE	40 30	12	Chebind		5.4	Gelele.
2000	Edge P	Calvadia P.AC.	30	10.0	Dhashd		I water	C. Coleta
						181		

Figure 8-27 Extended IP ACL (Selected) Window

After selecting the ACL profile and clicking the **Add Rule** button, users can configure the new ACL rule, in the selected ACL profile, as shown below:

Add ALL IGIa		
Add Acts Bale Fill Not Travel NOT Travel Second His (SHE SOL Zolow Proped Type	Ann - court - court	
All II Professor Second Professor () P	Second or All	
Destruction (Destruction (De	artiteli Faer Store -	
in the second se	uks. 🔷 753 (Lana Salus 🖘	tex I ame

Figure 8-28 Extended IP ACL (Add Rule) Window

This is a dynamic page. Every selection made in the **Protocol Type** drop-down list will change the bottom part of this window.

Parameter	Description			
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.			
Action Select the action that this rule will take here. Options to ch from are Permit and Deny .				
Protocol Type	Select the protocol type option here. Options to choose from are TCP, UDP, ICMP, EIGRP, ESP, GRE, IGMP, OSPF, PIM, VRRP, IP-in-IP, PCP, Protocol ID, and None.			

After selecting the **TCP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Acd ALL Itels				
460.001.042				
en Marineren Marineren Meseren Her (H-1220) Meser Procest Type	R - 104 (11)			
- with Machine				
de Ary Access (*) (* a) (*) (* Wildow		e Ar, () Fol () F () F () F () Scare		
- AUT HIL				
Desceiver Description Description Description Description Description	WE T	[043341] <u>Face Step - *</u>	Jeans	
Enough the	and other	0-65535) Classification (0-55235	
TOP THE	Dei Fift Fine	e di naturitari iling		
ell sorg ell' <u>Phone</u>	sik= -	844: *		
Tex Banc	Part 1	-		 II ARY

Figure 8-29 Extended IP ACL (Add Rule) TCP Window

Parameter	Description
Source	 Select and enter the source information here. Options to choose from are: Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IP address here. IP - The Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	 Select and enter the destination information here. Options to choose from are: Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IP address here. IP - The Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	 Select and enter the source port value here. Options to choose from are: = - The specific selected port number will be used. > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port

Parameter	Description	
	number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.	
Destination Port	 Select and enter the destination port value here. Options to choose from are: = - The specific selected port number will be used. > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. 	
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are ack , fin , psh , rst , syn , and urg .	
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).	
ToS	After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.	
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.	
Time Range	Enter the name of the time range to associate with this ACL rule.	

After selecting the **UDP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Act ALL IGA					
AND SEE THE					
1	A44				
VID Transfe	-1907				
700, In 1	the same the se				
SHORE HE SHEETS		disentander de rekommenen	Research 1		
7d m	R. 1994	(1.10 m).			
Presci Type	L09		ATATA		
with Marine					
ik Ata		de AC.			
Secure Colored 🔝		0.000			
988.2% () IT	-	Owned of the	1		
W. dcare		Vi stare			
1.1.1.1			12		
and the second					
Dearbeillen in Nave dein	Partino del				
Philo Tan	(1.1.2)	(HCGRI) Francisson +	jaran j		
District Test Physics Sec.	a : •		100520-53		
Terris Sea		(0-65525) Canada Saleera -	(0-55535)		
		Pinna Sides:			
CLUBER 2 PRI Planets					
Ing Ban	10.014				
Institute.	3 200			Sack II	Asper
					14.30.00

Figure 8-30 Extended IP ACL (Add Rule) UDP Window

Parameter	Description	
Source	 Select and enter the source information here. Options to choose from are: Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IP address here. IP - The Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked. 	
Destination	 Select and enter the destination information here. Options to choose from are: Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IP address here. IP - The Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked. 	
Source Port	 Select and enter the source port value here. Options to choose from are: = - The specific selected port number will be used. > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. 	
Destination Port	 Select and enter the destination port value here. Options to choose from are: = - The specific selected port number will be used. > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. 	
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).	
ToS	After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.	
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.	

After selecting the **ICMP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Acd ALL Itale	
443301346	
Li Alb Avera Alb Avera Alb Avera Bio (H45522) Alba Proposi Topa - Avera Bio (H4552)	And
Serve (1) Food (1) Food (2) F (2) F (3) F (4) F	de Ary Demoid or Vil scient
are the -	
Specificitin Herseys Tran	Frankédal 👘
apakanyada davrasisi	hereign in the set
et in Providina (Seare) (y 1999-3, Vill (Provid	
Travelarge	Text Aspe

Figure 8-31 Extended IP ACL (Add Rule) ICMP Window

Parameter	Description	
Source	Select and enter the source information here. Options to choose from are:	
	 Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IP address here. IP - The Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked. 	
Destination	Select and enter the destination information here. Options to choose from are:	
	 Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IP address here. IP - The Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked. 	
Specify ICMP Message Type	Select the ICMP message type used here.	
ICMP Message Type	When the ICMP message type is selected in the Specify ICMP Message Type drop-down list, this numerical value will automatically be entered.	
	When the ICMP message type is not selected in the Specify ICMP Message Type drop-down list, enter the ICMP Message Type numerical value used here.	
Message Code	When the ICMP message type is selected in the Specify ICMP Message Type drop-down list, this numerical value will automatically be entered.	

Parameter	Description	
	When the ICMP message type is not selected in the Specify ICMP Message Type drop-down list, enter the Message Code numerical value used here.	
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).	
ToS	After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.	
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.	
Time Range	Enter the name of the time range to associate with this ACL rule.	

After selecting the **EIGRP**, **ESP**, **GRE**, **IGMP**, **OSPF**, **PIM**, **VRRP**, **IP-in-IP**, **PCP**, **Protocol ID**, or **None** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

	24.04	
D NUMB	-1.00	
0, In -	er en elle alt	
ACOMING HIS OFFICER		Tala entre de versioner d'a la canaci
den som som som en som en Den som en so	Responsible.	71.
reacti "yee	CKRP	- 2 Ditt: []Tranava
such Products		
ik Ar		ŵ Ăr;
X. 6140 🎼		ender Office Contraction
decree (1) In		dur dur
Mi deard		W stars (

Figure 8-32 Extended IP ACL (Add Rule) EIGRP Window

Parameter	Description			
Fragments	Select the Fragments option to include packet fragment filtering.			
Source	Select and enter the source information here. Options to choose from are:			
	 Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IP address here. IP - The Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked. 			
Destination	Select and enter the destination information here. Options to choose from are:			
	Any - Any destination traffic will be evaluated according to the conditions of this rule.			
Parameter	Description			
---------------	--	--	--	--
	 Host - Enter the destination host's IP address here. IP - The Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked. 			
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).			
ToS	After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.			
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.			
Time Range	Enter the name of the time range to associate with this ACL rule.			

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

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

To enable the **Counter State** option or to enter a **Remark** for the profile, click the **Edit** button, next to the specific ACL profile (found in the ACL profile table).

CL Type	24	+ 1	4) (D) (1-14095)		Alchers		1	2.41
ara kan	894 Y.						3	sui sui
11 6	un naime -	ACC 1804	Statt Sorganica Sa	210p	10000103200	Horito IX	1.22	SALVA CA
1.55	a sia sity	Conserve PACE	42	13	Dated		54	Detet
2000	Con a Pro-	Edgewall*ACL	9 .	10	Skotled		(Contract)	C. (Celete
						10	回該日前	
	0.2003.00					Des Millions	Res Casta	A6.946
Same.	1993	Alar	**	1.	n Bray	(bade)		10
10		(Intell	15.89		1. A 6 1.0		1	Course .

Figure 8-33 Extended IP ACL (Edit ACL) Window

The fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Step	Enter the sequence number increment here.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this profile here.

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

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

To view the list of rules, that are associated with an ACL profile, select the ACL profile (found in the ACL profile table). The rule of ACL rules, connected to the selected ACL profile, will be displayed in the ACL rule table, as shown below:

CLANDING	1044						
CL Trate	<u>, 1</u>	₩ D (1-14995)	31 <u> </u>	10.	ALLER		
ATRI FORM							
	ALC: 10074	644 STR	station groups and the	sinp	EN INCOME.	NYOVA.	
	Carica diff	Standard CACE	42 30	12	Chebind	500	Gebele
2000	LOCAP	Calesdie PAC.	30	10.0	Danks	(Second Co	C. Colete
							日間一つ
a yaa ahaan	2008 1002					· Al Canala Case Canala,	- Art. Pate
Samer	ter altern		- 1	na Keny		taan III	
10	BATS	15 88		1997 - 1995 1997 - 1995		Tister)	Tel star

Figure 8-34 Extended IP ACL (Rule Display) Window

Click the **Delete** button to remove the specific ACL rule.

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

Standard IPv6 ACL

After clicking the Add ACL button, users can create a new ACL profile, as shown below:

al nas	Standard PV6 ACLUS	
1 (44000-12999)		
Ol: Hame	19 00 20	
	den of ACL rights in call to scheder	Add y

Figure 8-35 Standard IPv6 ACL (Add Profile) Window

The fields that can be configured are described below:

Parameter	Description				
ACL Type	Select the ACL profile type here. Options to choose from are Standard IP ACL, Extended IP ACL, Standard IPv6 ACL, Extended IPv6 ACL, Extended MAC ACL, and Extended Expert ACL.				
ID	Enter the ACL ID from 11000 to 12999.				
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.				

Click the **Apply** button to create the new ACL profile.

After creating a Standard IPv6 ACL profile, the newly created Standard IPv6 ACL profile will be displayed in the ACL profile display table, as shown below:

AL Type	AL 7			and the second second	Williams			
ara kanaw	4					y.	. 5	- Ald Ald
	CAR HARDA	60, 60	200 20120100 55	NY .	classifier state.	Henara		
161	Constant?	Shedadi" #01	0 0	- 10	Crabled		1 80	Colds.
0000	CFAR.	CARENDOT HOL		- 10	Distinct		1	C. Celete
22022	Tarek Off	2 - 16 - 1896 - 123.	(0)	39	the stand		1	Links
		a				100 (L	HEI KR I	

Figure 8-36 Standard IPv6 ACL (Main) Window

Click the **Edit** button to re-configure the specific ACL profile.

Click the **Delete** button to remove the specific ACL profile.

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

To add an ACL rule in the ACL profile, select it (the ACL profile will toggle to the bold font), and click the **Add Rule** button.

CL Type	4		- El-	_	ALIANS DIMENSI			
ara karana				a		vit - 2	, 9	440454
Contraction of the	000-04000	(13 1 6 9)	STIT SOCIONESSING	stap ;	successory and	HOMAGE		
101	Gar tada"	Olerdad C KOL	17	36	Crubed		1.00	Cold e
0000	CAN'	Durack's TAGE.	at .	11	Cost of		1 40	10-ded e
20000	Samlardet	Santer/P/9201	(0)	- 10	DepOil (1 44	Delete
						100		1 3

Figure 8-37 Standard IPv6 ACL (Selected) Window

After selecting the ACL profile and clicking the **Add Rule** button, users can configure the new ACL rule, in the selected ACL profile, as shown below:

od ALL Itale					
443.0CL 9.42					
	+10.04				
12 1	Stational .				
ta In 1	Santrative Pta				
ACCENTER HIS PHOTOSOFT	1.0	and a solution for the	Distant College and		
d m	REAL PLAN	50.000 E200E8 C 03			
Reat For eddings					
44 200		8 S.T			
	and the second se	E HAT	23121		
Serve Other E	1wir	xiel E Pré	700,0		
and the second					
Pre'sLend		Tublaid			
Grae Gange	[Siden				
				 	1040
					And the local data



Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535 . If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Source	Select and enter the source information here. Options to choose from are:
	 Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are:
	 Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Time Range	Enter the name of the time range to associate with this ACL rule.

The fields that can be configured are described below:

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

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

To enable the **Counter State** option or to enter a **Remark** for the profile, click the **Edit** button, next to the specific ACL profile (found in the ACL profile table).

al Trp	é ai		bigi-riaasi 📋		Allhers	CHIN.	í.	
an en			antonina inf		1		5	441454
0	as ware	ALC: 1804	and support sa	. The	Lenotre state	HORAND	- 14 - H	- CANCER
	Carence?	Oler bed THOL	× 10	0	Eraties		5.8	Gelela.
209	Dile 1.87	Divide Page	10) (0)	10	Diativisi		I was a	Coleta
1100	Statistic	Standard Tob ARL	D	0	Doubled 1		ELSE ST	Dalais
						100 1	ales kr is	
			97.02			Shitt With Links and	dan thate	Adda Houles
Sin ala	nan e	when a	6.6	32	Man a	(Selen)	WALKS PARTY	Subsection.
	0 f	and the	tro est			111515253	1	to and the

Figure 8-39 Standard IPv6 ACL (Edit ACL) Window

The fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Step	Enter the sequence number increment here.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this profile here.

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

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

To view the list of rules, that are associated with an ACL profile, select the ACL profile (found in the ACL profile table). The rule of ACL rules, connected to the selected ACL profile, will be displayed in the ACL rule table, as shown below:

CL Asoma (M							
CL Trpe	<u>a</u> +		1	104	ALMATA MINUTE			*.el
ara karnasi	i.			u.		10 V	. 8	444.454
a second	0.1.0.000	112 - 14Pa	CT TROUBLE ARE	ostop ;	The state of the second s	SHOW		
101	Gir tud"	Olerdard Trick	10	31 31 31	Cruck ed			Debela
080	CAN'	Danker Tich.	(0)	110	Cat of		1	Colete
20080	Same dis	SamariP-58ACL	(E)	- 30	the block		1 8.44	Delete
						303 2		
on an com p	s Theory Male				(inclusion)	With the state of the	San Chailes	
Second com		16.6r		Канар		reda i	and the second	an orderen
- 90	Paral	in wy	6463	1963 and 196	37	E nackata)	1	Second



Click the **Delete** button to remove the specific ACL rule.

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

Extended IPv6 ACL

After clicking the Add ACL button, users can create a new ACL profile, as shown below:

CL They	Extended (N5 ACL 1	
199900-11999 <u>1</u>		
C. Hame	11 (01)	
	eder of ACL rome must be a better	Rady

Figure 8-41 Extended IPv6 ACL (Add Profile) Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL profile type here. Options to choose from are Standard IP ACL, Extended IP ACL, Standard IPv6 ACL, Extended IPv6 ACL, Extended MAC ACL, and Extended Expert ACL.
ID	Enter the ACL ID from 13000 to 14999.
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.

Click the **Apply** button to create the new ACL profile.

After creating an Extend IPv6 ACL profile, the newly created Extend IPv6 ACL profile will be displayed in the ACL profile display table, as shown below:

CL Type	4		31	100	OLNers mov	- 1	1
ani karina	12.1					WI .	airea.
THE R	864.5899	251100	2040.0000.000	NY 8	Non Internation	Homans.	and the second s
121	Simple*	Carrier PAGE	10 10	- 10	Crosted	50	Debel 4
0000	Extender.	Distantive Place.		10	District	1	Contraction of the second s
22030	Statistics.	Savat Revolu	10) 	30	(enters)	1.54	Colline 1
2000-011		61X 8 X 8 4 5 5		11		1	Lakers .
							l si i
					-2.12		

Figure 8-42 Extended IPv6 ACL (Main) Window

Click the Edit button to re-configure the specific ACL profile.

Click the **Delete** button to remove the specific ACL profile.

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

To add an ACL rule in the ACL profile, select it (the ACL profile will toggle to the bold font), and click the **Add Rule** button.

Adu Type	<u>si</u>	 ⇒ ⊕ D (1-1498) 	<u></u>		CLEARS MINIST		ſ	
ara karaas	40 J							ALL ALL
1. 11.	SLI SAVA	60, 100	Tart shown on the	200	1040004500	Honara	52 S	
161	Shurene"	She field \$61	0	0 30	Draties		5.0	Debite.
0000	LARGE	Counter of the Co		00	District		1 10	C. Celete
11000	the hills	the role of PAR AND	17	76	Dis No.		1 Section 1	Delete
28.81	had stratight	Edward (Pyl 11)	11	16	10-54 (m)		1 20	Valere
						100 (19		1313
	11110816					oll Course I de		Add Houles
ANTINE A	None Contraction	10.65	Une	Range		ALL CALCULAR	ar causer .	

Figure 8-43 Extended IPv6 ACL (Selected) Window

After selecting the ACL profile and clicking the **Add Rule** button, users can configure the new ACL rule, in the selected ACL profile, as shown below:

od ALL Idule		
AND ALL THEY		
n Alt Frank Alt Frank Sheanna Rh (14220) Alt Fr	Total - Const - Con	r.
head free	TCP - 03255 (Prantyra	
North Press		
Neuronau Diens Se Dermanifiet Jean Se Dermanifiet Jean Se	n e de la constance de la const	
Horana Estimologi Palalan Kiti Habbara Anarahanga	Ban Eri Evi Evi Ban Bin Phan Scat + La 200	

Figure 8-44 Extended IPv6 ACL (Add Rule) Window

This is a dynamic page. Every selection made in the **Protocol Type** option will change the bottom part of this window.

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.

Parameter	Description
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Protocol Type	Select the protocol type option here. Options to choose from are TCP, UDP, ICMP, Protocol ID, ESP, PCP, SCTP, and None.

After selecting the **TCP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

od ALL Ifula	
AAAACLINA:	
1	720.00
WD NAME	-real-
20. Inc.	er sale (1946-03)
SHOW SHE SHOULD BE	disedución de extrementationeral
Adam	Remark (1.11.4)
Presce Type	10.9 ·
de Ata	2.52
	(AF (())
90075	1012 - MARCEN - PA 2013 1
Prefix Length	Tails Length
Heat Test	
REPORT Plana Se	
B-13	-1 7 (1989) FD4 7 (1993)
bermanent han te	ad the second
State Te	na - Justice Fair Dire - Jonato
10 million	Too Etc. Fort For Fig. Too
ESCH (CR3)	
	Plan Scott +
PROFILE TO ASSOCIO	
нальнора.	(Cares)
	Ass I Age

Figure 8-45 Extended IPv6 ACL (Add Rule) TCP Window

Parameter	Description
Source	 Select and enter the source information here. Options to choose from are: Any - Any source traffic will be evaluated according to the
	 Host - Enter the source host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are:
	 Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Source Port	Select and enter the source port value here. Options to choose from are:
	 = - The specific selected port number will be used.

Parameter	Description
	 > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	Select and enter the destination port value here. Options to choose from are:
	 = - The specific selected port number will be used. > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are ack , fin , psh , rst , syn , and urg .
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range to associate with this ACL rule.

After selecting the **UDP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Acd ACL Incle			
444.0CL Bak			
en Viz Korre Viz, Fills	toole en sale dev		
SHORT OF BALLAND	1	direct acciently relation to a feature of	
7d m	R. Maria	151179674	
Presci Nee	A DR	0.255Darwa	
- REAL PROFILE CO.			
de At i		8.57	
80075	1 10-02	Exercise 2 = ex = 1001 1	
PrefixLength	E	Pails Length	
Heat Dut Sciencification Plaque Set	wa ite i		
Et a state	-1 *	at excess Providence of the	* 1v
beening and the bases be-	ed in		
EKIN Tr		at you Familiar - Die	4.4.4
DSCP (Classi	Picer Sel-	4	
PROCESS IN MARINE	1		
ICONSER.	Satara		
22	- 02		Ann I Ann

Figure 8-46 Extended IPv6 ACL (Add Rule) UDP Window

Parameter	Description
Source	 Select and enter the source information here. Options to choose from are: Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	 Select and enter the destination information here. Options to choose from are: Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Source Port	 Select and enter the source port value here. Options to choose from are: = - The specific selected port number will be used. > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	 Select and enter the destination port value here. Options to choose from are: = - The specific selected port number will be used. > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range to associate with this ACL rule.

After selecting the **ICMP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Acd ALL Itule					
Add ACL Rate Fill Vite Exercisi Vite Exercisi Vite Exercisi Silverant State (Self-State)	122-84] di nel acche de		namat .	
(Add on	Reference (1910)	Ч			
Presci Tyse	CMR 2	•	loss: _in	ARANA	
- 3030.006.7103.01			<u> 1999</u>		
Seconds.	He can	R AN C Aler C Aler C Aler C Aler C Aler C Aler C Aler	2002 1 2002 1		
No.3-4509					
sheeting as enverte the					
KINPMEASIK TOM (1929)]%	1.0012 (31.0.17 2226)			
ELEP 340 Florestel 3-100575 Jan Hann	Preve Select		10		
					tea ana

Figure 8-47 Extended IPv6 ACL (Add Rule) ICMP Window

Parameter	Description
Source	Select and enter the source information here. Options to choose from are:
	 Any - Any source traffic will be evaluated according to the conditions of this rule.
	 Host - Enter the source host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are:
	• Any - Any destination traffic will be evaluated according to the conditions of this rule.
	 Host - Enter the destination host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Specify ICMP Message Type	Select the ICMP message type used here.
ICMP Message Type	When the ICMP Message Type is selected in the Specify ICMP Message Type drop-down list, this numerical value will automatically be entered.
	When the ICMP Message Type is not selected in the Specify ICMP Message Type drop-down list, enter the ICMP Message Type numerical value used here.
Message Code	When the ICMP Message Type is selected in the Specify ICMP Message Type drop-down list, this numerical value will automatically be entered.
	When the ICMP Message Type is not selected in the Specify ICMP Message Type drop-down list, enter the Message Code numerical value used here.

Parameter	Description
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range to associate with this ACL rule.

After selecting the **Protocol ID**, **ESP**, **PCP**, **SCTP**, or **None** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

ed Alli, Hole				_
443.0CL 345				
	150.01			
AD Description	-rouse			
W. Inc.	21 20 - D-070			
SHORE HE WHEN THE REPORT		The end as she with real subscription must be		
Adam.	Remain of the	anna a' chuir ann an t-chuir ann an t-chuir ann an t-chuir ann ann ann ann ann ann ann ann ann an		
Presci Tyse	Protoco 10	DOSS DAMAG		
ile Ata		8.5°C		
1916-191		2 Av 800 1		
SAME AND A		- PA 2010 1		
PretsLeight		Create Langth		
	51 (1)			
CSOP 3. 651	Please Salars 17			
NAME AND DESCRIPTION OF	1			
True Dange	(C drata			
1000-107	Westing and	And the second se	and a	i aye

Figure 8-48 Extended IPv6 ACL (Add Rule) Protocol ID Window

Parameter	Description
Protocol	Enter the Protocol ID value used here. This value must be between 0 and 255.
Fragments	Select the Fragments option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are:
	 Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are:
	 Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IPv6 address here. IPv6 - The Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.

Parameter	Description
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range to associate with this ACL rule.

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

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

To enable the **Counter State** option or to enter a **Remark** for the profile, click the **Edit** button, next to the specific ACL profile (found in the ACL profile table).

kal Tep	e ar	÷0 🚸	D (1- 4995)		All Hans	and the second s	F	
ára e a				л	07		. 5	ALC: NO
. 11	act same	841 (V)PA	etti Tixoqineçon Ho.		Contra and	HORATE	100	a succession of the second
1	Margad?	Danderst PAC.	n¢.	0	Eraties		1 100	Detel a.
2000	Dinith.	DIN CASPAC.	it it	10	DiaMo		I was I	Coleta
11001	26.44.46	Standard Bye MCL	19) 19)	0.5	tracks.		1 48	Malain .
(anar	Set and	Second and the case of	0	12	Unable		Lierant	Letter .
						101	1111 III III	<u>s</u> e
	00000008					stee of course [)	dear courses .	
Process.		ian i	10.61	U.S.	e Kange	1746-0481	and an other states	a characteristic
1	ų – į	Scot	10.00					Sec.

Figure 8-49 Extended IPv6 ACL (Counter State Enabled) Window

The fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Stop	Enter the stop sequence number here.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this profile here.

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

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

To view the list of rules, that are associated with an ACL profile, select the ACL profile (found in the ACL profile table). The rule of ACL rules, connected to the selected ACL profile, will be displayed in the ACL rule table, as shown below:

UL Asomo	50. ₁₀ .				sector sector		
Vill Type	A 7			- U A	ALHers MINUT	- 19	
ani kani ka			12				esta esta
n TI	811.58760	60 APA	THE SHORE CRIME	200	Jacobio antes	Konara	
151	Shirese *	Shadad17.401	10	0	Dradec	5.0	Debde.
20030	LANGE	CARRIED TO CL	(D)	- 30	District	En sellerer	Colorine -
22022	Sha hade	the set of \$500 state.	12	-20	$\mathbf{D} \in [0,\infty]$	1.54	Lobin
2881	had so all off	Edward (A) EAD	u.	16	Parallelist	20	, Volere
							131)
	111080	M				off Courser Clear Courser	Add Kulle
MORNEN	es aven	10.64	, in the second s	e Kalage		veas.	
. 19	Paul	10.00			31	Lawler [Chiefe

Figure 8-50 Extended IPv6 ACL (Rule Display) Window

Click the **Delete** button to remove the specific ACL rule.

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

Extended MAC ACL

After clicking the **Add ACL** button, users can create a new ACL profile, as shown below:

21. 7.g.s	Extended MAC ACL	
(1000-7899)		
a, Namo		
	action of ACC, many a multiple to believe	622 Y

Figure 8-51 Extended MAC ACL (Add Profile) Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL profile type here. Options to choose from are Standard IP ACL, Extended IP ACL, Standard IPv6 ACL, Extended IPv6 ACL, Extended MAC ACL, and Extended Expert ACL.
ID	Enter the ACL ID from 6000 to 7999.
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.

Click the **Apply** button to create the new ACL profile.

After creating an Extend MAC ACL profile, the newly created Extend MAC ACL profile will be displayed in the ACL profile display table, as shown below:

		+ + D(1-1995)		1.1.1.1.1.1	CLEARS CONTRACT			A al.
an ean e								-
	BLL SHOP	2011 - 1600	Intern wedgen de Ro.	2000	provide and the	Homers		
1	Sim sad"	Shedard17 #01	10	.0 .10 .70	Dradec		5.4	Gelde.
0000	Edwardt"	Edit A C PATE	- D)	00	Diades		- 44	- Coleta -
16230	date in the	EARLANDS ALL	17 11	26	Caster		1.84	Delete
	Stational.	-1 wa years /33		- 20	H estation		20	Colors
582.00	- Antonios	Antipologica (Maria)	ti	- 39g -	HORSEN.		200	Dickets
						101 101		
elen Sizar	Service and		11	90 - 14		higi ati	20	

Figure 8-52 Extended MAC ACL (Main) Window

Click the Edit button to re-configure the specific ACL profile.

Click the **Delete** button to remove the specific ACL profile.

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

To add an ACL rule in the ACL profile, select it (the ACL profile will toggle to the bold font), and click the **Add Rule** button.

		12		ALMana Contraction			(* +1
					10		444.454
GER HANN	2011 1804)	NAME AND POINT OF	269	He wing street	SECTION		and the second
CandardP	Olyr Sed T KOL	4	32	Craties		5.4	Colda-
Diked?	DAVIDE PACE	19. 19.	D	DIANE			Colora -
Bare MAD	Edit des BACACE	(1)	- 10	Deschied.		1 Section 1	L'adaire :
a de la compañía de las	- M. 46 10090100	N	110-	******		1 20	Linkers
FOR STREET	+00.0000-406.000	71	213	ALCONT.		20	Dekts
					he he		
	CandandP Edwardt Maria Mari Carlanat	Canada ANP Shard and TACL Dalar ANP Dalar Back PACC Norm MAC Dalar Ann PACC An analysis State Ann PACC AND An analysis State Ann Ann Ann	Carebrad P Sherbad (* 401.) (Dahadi * Dahada P 801,) (* Marebiat Dahada MAC Art.) (* Marebiat Na, ski menada * (*	Carebool? Standard? *CL C H Date Start Date Start P SD, S D Date Start P SD, S D D Start MAC Date Start P SD, S D Start P SD, S S S D	Cardword Standard (* 42L) K 10 Endoles Extended Extended (* 42L) K 10 Extended Extended Extended (* 42L) K 10 Extended (* 42L) Extended Extended (* 42L) K 10 Extended (* 42L) Extended Extended (* 42L) K 10 Extended (* 42L) Extended Extended (* 42L) K 10 Extended (* 42L)	Construct® Standard * 40L C 10 Drashed Data dir Data dir # 60L C D Drashed Data dir Data dir # 60L C D Drashed Data dir Data dir # 60L C D Drashed Data dir Data dir # 60L C D Drashed Data dir Data dir # 60L C D Drashed Data dir Data dir # 60L C D Drashed Data dir # 60L D D Drashed D Data dir # 60L D D D Drashed Dir # 60L D D D D D Dir # 60L D D D D D	CareboolP Starbad (* 42L) C O Dracket Not Date of P Date of P Starbad (* 42L) Starbad (* 50L) Starbad (* 50L)

Figure 8-53 Extended MAC ACL (Selected) Window

After selecting the ACL profile and clicking the **Add Rule** button, users can configure the new ACL rule, in the selected ACL profile, as shown below:

dd Ald, Role				
VIC-SCJ. BURN				
ACL Type Do Sequence Hou (1-85505)	Ry NAVE 2011 Nersed NAVE 2011	in geborne konderster oviges (K. A. G. M. Materia (* 196	e Inter	HE HE AT 10
N: 1992	1010- 11 all 6710		aver 1100	14 98-0270
Notes Presser Type 1				
Handy Hand Silver Hand See (Handeley) Hand See Market See Sci. (Second Select 1991	Illeane Select 🔄			
an anna an		J		2004 4004

Figure 8-54 Extended MAC ACL (Add Rule) Window

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Source	 Select and enter the source information here. Options to choose from are: Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's MAC address here. MAC - The Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination	 Select and enter the destination information here. Options to choose from are: Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's MAC address here. MAC - The Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Specify Ethernet Type	Select the Ethernet type option here. Options to choose from are aarp, appletalk, decent-iv, etype-6000, etype-8042, lat, lavc-sca, mop-console, mop-dump, vines-echo, vines-ip, xns-idp, and arp.
Ethernet Type	Enter the Ethernet type hexadecimal value here. This value must be between 0x0 and 0xFFFF. When any Ethernet type profile is selected in the Specify Ethernet Type drop-down list, the appropriate hexadecimal value will automatically be entered.

Parameter	Description
Ethernet Type Mask	Enter the Ethernet type mask hexadecimal value here. This value must be between 0x0 and 0xFFFF. When any Ethernet type profile is selected in the Specify Ethernet Type drop-down list, the appropriate hexadecimal value will automatically be entered.
CoS	Select the CoS value used here. This value is between 0 and 7 .
VID	Enter the VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094.
VLAN Range	Enter the VLAN range here. Enter the minimum and maximum VLAN ID in the range here.
Time Range	Enter the name of the time range to associate with this ACL rule.

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

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

To enable the **Counter State** option or to enter a **Remark** for the profile, click the **Edit** button, next to the specific ACL profile (found in the ACL profile table).

ACL Trp	e 81		D (1-1995)		AGLIERE -	ENEX.	1	9-1
Ana ka	nus a	,			1.1		. 5	11.0
ALC: NO	act same	144 (1995)	STATE SOLID CO. DO.		CAUSER STATE	HARLAN	Se	- ALCON
1	Anter"	Daniard PAC.	4	4	Cratical		4.8	Detel
209	Dikes.W	CONTRACTOR	(3)	4. 10	Calif		1	10-belle
12.99	Eden/Ref.	Terrara 1446 401	10	10	Umbed -		Current .	Colete .
Pfel,	Share a bell	20.000.00.000	71:		+41.01		1.20	L'alers
1001	Sweenson .	HEROMINE ALT	712	944	-00000		L See 1	Relati
						host it		1.
		ten.				charal course La	Interstation .	ade route.
Second	randa. J	karen	10.0e	Ţirv	-Range	Con wat	alanti artest	
19	0 7	aut.	121.4.0				1	

Figure 8-55 Extended MAC ACL (Edit ACL) Window

The fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Stop	Enter the stop sequence number here.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this profile here.

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

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

To view the list of rules, that are associated with an ACL profile, select the ACL profile (found in the ACL profile table). The rule of ACL rules, connected to the selected ACL profile, will be displayed in the ACL rule table, as shown below:

Kalu Type	AI			l l à	Olfana (<mark>state</mark> st		E.	9-1
árai kornus		1				11		441444
11	ALS 10454	5,401,1806	NAT SEPTEMBER 10	Ship	La el log attive	NORM		CHARLES !
1.1	Canada tel?	Starting * KOL	14	-0	Crasher.	1	4.6	Detel
0.900	Exists 27	David Soci P ACC	33 10	0	Diske	E		C. Codelle
100	Lineman	Education PACACE	30	- 0	traded	I.	A	Colere .
221.14	N COONI-	36, a.k. 100-0102		11	++ C&1	L L	100	L'alers
53.00	FOR STAF	+12.3/8/21-4/4/34/5	212	011	+ CAMPER		200	Relat-
						hel tals		1 :
	(D:0000) Suite	1				at care Lane	Same?	ade suite
Sequer co.	no. Acatan	0.0	Time	Ronge	11- 226	oe wet		
100	Paul	Special			100	I malia A	T.	

Figure 8-56 Extended MAC ACL (Rule Display) Window

Click the **Delete** button to remove the specific ACL rule.

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

Extended Expert ACL

After clicking the Add ACL button, users can create a new ACL profile, as shown below:

td ACL Access Lt.	6.	
0.7. 3 •	Estanded Expert Al	
1 (9200-9999)		
3. Hamo.	14 (0970	
		822.9
ole. The lost coars	acter of AZ room a musicitie of being	

Figure 8-57 Extended Expert ACL (Add Profile) Window

The fields that can be configured are described below:

Parameter	Description
АСL Туре	Select the ACL profile type here. Options to choose from are Standard IP ACL, Extended IP ACL, Standard IPv6 ACL, Extended IPv6 ACL, Extended MAC ACL, and Extended Expert ACL.
ID	Enter the ACL ID from 8000 to 9999.
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.

Click the **Apply** button to create the new ACL profile.

After creating an Expert ACL profile, the newly created Expert ACL profile will be displayed in the ACL profile display table, as shown below:

All, Type	AL 7	₩ D(1+14995)		1 0 40	Liters			(* el.
ani kanina				200 - X			1	ALL MA
1 BALLER	644 MILES	801.1939	otari borji anva ka	- 100	Longer state	ween	Se	TANKS C
1.1	Standare F	Variatin's CL	D.	10	Cratical		4.0	Colds.
2002	DANE	DAN SALPAC.	D	0.0	Data		1	C. Colet e
221	Education Co	Elsandersetter	11 11	- 50 C	the start		1 8.46	Liebene
10.01	Half (D-ip)	ernal liter to	- 10	9.	110.000		1 20	Listers
121.003	30303/939	00/03/03/04/04/01		- 90° -	HOUSE		20	Colete
1111	Emploie.	Transfer Pyc. 40	12	. W	Frank		A	Deleter
						(10) E		
1773	Eresti.	Energiere P.A. 40	13	τ.		(ne) 🛤		Si Rin f

Figure 8-58 Extended Expert ACL (Main) Window

Click the **Edit** button to re-configure the specific ACL profile.

Click the **Delete** button to remove the specific ACL profile.

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

To add an ACL rule in the ACL profile, select it (the ACL profile will toggle to the bold font), and click the **Add Rule** button.

Kill Type	41	- 🤟 D (1-1995)		- AC	here mark			
ara karan	èn :							AL 44
C. P.	ana daran	OF JWE	THE SOLVER OF THE	2019	Landse state	weve	54 Å	CALCER OF
19	Chir the di"	Owners PAN.	0	10	Er soled		4.0	C-d-d-s
2000	DANE	Dikaka TVIR.	0	13	D MAN		1	- Robel e
82.0	Education Co.	ENA SOUNCESE	EX.	1) 11	Diable)		1 Sult	Liebers
00.81	Patrick-Gate	The formation theory and	- 31	11	The winter (1.120	Lakers
1101	317(1978	NUMBER OF STREET	3.91	11	HEADING		20	Colors
1111	State of a	Prended Pyride	11	33	Second .			Delete
				111		(311)		
	120000							

Figure 8-59 Extended Expert ACL (Selected) Window

After selecting the ACL profile and clicking the **Add Rule** button, users can configure the new ACL rule, in the selected ACL profile, as shown below:

Add AGL Huik						
Algorizational m material estimate estimate forum en 4x /185556	or al Frences Extension Croans ACL	File Leville L'evalue	alomalitati suitesa ana i			
Yoles Barland Syn Malen Proderer	DP v	**	e. L'ennere			
Scales (* 164) Scales (* 164) Pr Mile (* 1			Decremon (2) Alt (2) Alt (2) Alt (2) Alt (2) Alt (3) (4) (4) (4) (4) (4) (4) (4) (4			
Patrick's Alexan 2 Are 2 Are			Per se an Official State	100 100	With .	
Пан	e Select IV H Select IV	(dessues) <u>Please Serv</u> es		940512		
	n Silvet V Nata Silve Data Silve		17 <u>-</u> 1.4	S-0505 Phone Select 🔄		
127 But existence Cale Printing Cale Printing Search (127) The The printing		The second se				ka I

Figure 8-60 Extended Expert ACL (Add Rule) Window

This is a dynamic page. Every selection made in the **Protocol Type** option will change the bottom part of this window.

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Protocol Type	Select the protocol type option here. Options to choose from are TCP, UDP, ICMP, EIGRP, ESP, GRE, IGMP, OSPF, PIM, VRRP, IP-in-IP, PCP, Protocol ID, and None.

After selecting the **TCP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Add AGL Huik					
Ratival Mal M Rativans Rativans Rativas Socialization (S. 1985) Administration Rativation	e di Eric A L Edented Court ACL St Pro all (110 m) D P	dik Urstaals van se aan se de bestaar van se Brits se			
Value Prices Am - Rei Scarp - P - Maria		browar (An Bea P Marat		
Packet Charac	116 1936 (2013) 116 1936 (2013) 116 1936 (2013)	10 x x 2	Ale The Black	Arni Arni	
Destrates Fot	e Select 🔍	a Thank Select (12) Se Thank Select (12)	3-61513		
 President Production Production 	Based v Based to	ä	-S [Reve Select <u>-</u>]	<i>1</i> 7.	
127 Rea ge a constant (Test Col Der Der Der De			- Ann	iv et.

Figure 8-61 Extended Expert ACL (Add Rule) TCP Window

Parameter	Description
Source IP Address	Select and enter the source information here. Options to choose from are:
	 Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IP address here. IP - The Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are:
	 Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IP address here. IP - The Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are:
	 Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's MAC address here. MAC - The Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.

Parameter	Description
Destination MAC Address	 Select and enter the destination information here. Options to choose from are: Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's MAC address here. MAC - The Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Source Port	 Select and enter the source port value here. Options to choose from are: = - The specific selected port number will be used. > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	 Select and enter the destination port value here. Options to choose from are: = - The specific selected port number will be used. > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).
ToS	After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are ack , fin , psh , rst , syn , and urg .
VID	Enter the VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094.
VLAN Range	Enter the VLAN range here. Enter the minimum and maximum VLAN ID in the range here.
CoS	Select the Class of Service (CoS) value here. Options to choose from are from 0 to 7 .
Time Range	Enter the name of the time range to associate with this ACL rule.

After selecting the **UDP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Add ACL huik	
Agenous Main In Alt Carls Alt Pace Second Soc (1995) Action Remark Lyn Main (1970) Second Sec	e al Second Defended Constrator Defended Constra
$X_{i} = 1 \begin{pmatrix} X_{i} & Y_{i} \\ & Y_{i$	
Centralica Port	Pase Gelo V Pase Gelo V Pase Selo V Pase Selo V Pase Selo V Pase Selo V
 PPriority of OPPriority 	Received in 148 Received 1
g ar 11 Anda 11 An Alberg 12 An Alberg 12 An Alberg 12 An Alberg 12 An Alberg	2 Solition - See Soli

Figure 8-62 Extended Expert ACL (Add Rule) UDP Window

Parameter	Description
Source IP Address	Select and enter the source information here. Options to choose from are:
	 Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IP address here. IP - The Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are:
	 Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IP address here. IP - The Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are:
	 Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's MAC address here. MAC - The Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.

Parameter	Description
Destination MAC Address	Select and enter the destination information here. Options to choose from are:
	 Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's MAC address here. MAC - The Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Source Port	Select and enter the source port value here. Options to choose from are:
	 = - The specific selected port number will be used. > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	Select and enter the destination port value here. Options to choose from are: • = - The specific selected port number will be used.
	 > - All ports greater than the selected port, will be used. < - All ports smaller than the selected port, will be used. ≠ - All ports, excluding the selected port, will be used. Range - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).
ToS	After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
VID	Enter the VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094.
VLAN Range	Enter the VLAN range here. Enter the minimum and maximum VLAN ID in the range here.
CoS	Select the Class of Service (CoS) value here. Options to choose from are from 0 to 7 .
Time Range	Enter the name of the time range to associate with this ACL rule.

After selecting the **ICMP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Add ACL huiv			
Alexandrian Alexandrian Alexandrian Alexandrian Secondri Secondrian Secondrian Seco	e ar beck Edented Coper AOL V. Per all (1) During 1349	eth Alle valee adomático do as (1.200 — Lin grants Decorate 2 - Bro Secondor 2 - Bro Secondor 2 - Bro	
A set Use	114-1434 (2013) 114-1434 (2013) 114-1434 (2013)	р. т.е. С. не. С. соц. С. соц. с. соц.	The Star Article
ar ann a cean Speado, ACM T. Seriarga Tepel, P ICSIP Herriaga Type (KS23)	e ye û dest		
 energian contract 	Plane School (2) Plane school (2)	122	a (a > 4)
(s. 20 (1 4 44) (1 2 4 5 Kingé	÷	11 C	
Colo Plenne Select 🕑 me - ange	o tomet.		

Figure 8-63 Extended Expert ACL (Add Rule) ICMP Window

The dy	namic fi	elds that	can be	configured	are	described below:
	inaniio ii	ondo tinat		ooringaroa	aio	

Parameter	Description
Source IP Address	Select and enter the source information here. Options to choose from are:
	 Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IP address here. IP - The Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are:
	 Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IP address here. IP - The Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are:
	 Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's MAC address here. MAC - The Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.

Parameter	Description
Destination MAC Address	 Select and enter the destination information here. Options to choose from are: Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's MAC address here. MAC - The Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Specify ICMP Message Type	Select the ICMP message type used here.
ICMP Message Type	When the ICMP Message Type is selected in the Specify ICMP Message Type drop-down list, this numerical value will automatically be entered. When the ICMP Message Type is not selected in the Specify ICMP Message Type drop-down list, enter the ICMP Message Type numerical value used here.
Message Code	When the ICMP Message Type is selected in the Specify ICMP Message Type drop-down list, this numerical value will automatically be entered. When the ICMP Message Type is not selected in the Specify ICMP Message Type drop-down list, enter the Message Code numerical value used here.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).
ToS	After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
VID	Enter the VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094.
VLAN Range	Enter the VLAN range here. Enter the minimum and maximum VLAN ID in the range here.
CoS	Select the Class of Service (CoS) value here. Options to choose from are from 0 to 7 .
Time Range	Enter the name of the time range to associate with this ACL rule.

After selecting the **EIGRP**, **ESP**, **GRE**, **IGMP**, **OSPF**, **PIM**, **VRRP**, **IP-in-IP**, **PCP**, **Protocol ID**, or **None** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

Add AGL Rule				
Agenous Seale III Autorianis Autorianis Autorianis Seale Seale Record Seale Record Seale Record Seale	e di Dec All District Coast ACL Coast of Coast of Coast ACL Coast of Coast o	La vaka akanaka casana 1941 - La warate		
E Am Control (Print) Print (Print) Print (Print) Print (Print)		Browner Contraction Contractio		
A set A set	196-9036-22130 196-9036-22130 196-9036-22130	in en Perine an () succ vertexet vertexet	The BLSP AFTER The Silve After The Silve After	
 вологир вологир 	Protocialist 15 Protocialist 15	tax Pina	u Seluci 🕑	
in ACTHORN C MAXBarge Set Diversion A → California California	+ > from			1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Figure 8-64 Extended Expert ACL (Add Rule) EIGRP Window

Parameter	Description
Fragments	Select the Fragments option to include packet fragment filtering.
Source IP Address	 Select and enter the source information here. Options to choose from are: Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's IP address here. IP - The Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	 Select and enter the destination information here. Options to choose from are: Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's IP address here. IP - The Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	 Select and enter the source information here. Options to choose from are: Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host's MAC address here. MAC - The Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.

Parameter	Description
Destination MAC Address	 Select and enter the destination information here. Options to choose from are: Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host's MAC address here. MAC - The Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
IP Precedence	Select the IP precedence value used here. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).
ToS	After selecting the IP precedence value, select the Type-of-Service (ToS) value that will be used here. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
VID	Enter the VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094.
VLAN Range	Enter the VLAN range here. Enter the minimum and maximum VLAN ID in the range here.
CoS	Select the Class of Service (CoS) value here. Options to choose from are from ${f 0}$ to ${f 7}$.
Time Range	Enter the name of the time range to associate with this ACL rule.

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

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

To enable the **Counter State** option or to enter a **Remark** for the profile, click the **Edit** button, next to the specific ACL profile (found in the ACL profile table).

ALL T(p)	e 24	+ + 0	(1- 4995)		C Alchere	11 I	(
ara ka					1711		
and and the	ALL BATTA	667 1679	STRT SERVICES NO.		ASSESSION OF	991.07	and the second sec
1.	Queent?	Outlad 1400	9	9	Crisb ad	54	Colds.
2000	Dist.ff."	Data Read THOL	100	0.0	CALIF	I to a	C Colefe
100	EducWG:	Edde Art MAG ACL	30	3	inited.	- Alt	Delete
	et talates participation	making the second second	12	12.	Disabled •	L.ero.	. Lator
etan.	Other providence in the	2010/01/2016/01/20	90		-WEST	100 M	Liskis_
fires.	anth	Zeneral Polices			20Est		Belde
						30) (11) (1)	
	quert (De 0000) P					Ban All Counter LiGeen Counter	Ade Sule
C	icelto. No	den 🗍	D.H-	Tine R	11.5	Contra	

Figure 8-65 Extended Expert ACL (Edit ACL) Window

Parameter	Description
Start Sequence No.	Enter the start sequence number here.

Parameter	Description
Stop	Enter the stop sequence number here.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this profile here.

Click the Apply button to accept the changes made.

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

To view the list of rules, that are associated with an ACL profile, select the ACL profile (found in the ACL profile table). The rule of ACL rules, connected to the selected ACL profile, will be displayed in the ACL rule table, as shown below:

CL Trpe	Al •	·杜···································		E AG	Late Build			(and)
árai karolas		service of the servic						-
1 Parties	11.0.140m	AL LOW	THE REAL PROPERTY IN THE	2015	LEAVE STOP	www	52 Š	- ANDER
19	Shir the di"	Sancard P.A.S.	0	12	Erspied		5.0	C-d-d-s
2000	DUNK	Dikalen Fisika	0	12	D. Max		1 10	C Delete
82.6	Education Co.	Education and education	HT.	- 0	to add to		1 640	Delete
99.8	Patrick-Page 1	+10+0+0+040000000		10	- Faiter		1 20	Lakes
121.001	MACHINE	NUMBER OF STREET	31.	110	HOWER		20	Delete:
1112	Dancour	Services State	11	14.	Stands.			Delete
				445		(10) E	1	
	i (De OCOO) Ratia					A Cara La	an Courtan	Adv fork
Seconde	ia Action	Dule	Tire Ra	6.5	6	a na l		

Figure 8-66 Extended Expert ACL (Rule Display) Window

Click the **Delete** button to remove the specific ACL rule.

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

ACL Interface Access Group

This window is used to view and configure the ACL interface access group settings.

To view the following window, click **ACL > ACL Interface Access Group**, as shown below:

	tsear dee La laintei ⊥ la	ran katar biya <u>k</u> i jawa (ki ji pikua	ACI HARA	- Apply
L' KONG	and the second second			
		3	1	
Par.	17 ACL	PASACL	MAC ACL	Coat ACL
651321				
do152				
0.000				
0.009		(f)		
1000		1		
ets1.55.55				
station				
63163		0		
5.414.2				
0010101				
Mind to mil		11		
str4/2-7				

Figure 8-67 ACL Interface Access Group Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction here. Option to choose from is In.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Туре	Select the ACL type here. Options to choose from are IP ACL , IPv6 ACL , MAC ACL , and Expert ACL .
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.

Click the **Please Select** button to choose the ACL profile that has been created.

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

ACL VLAN Access Map

This window is used to view and configure the ACL VLAN access map settings.

To view the following window, click **ACL > ACL VLAN Access Map**, as shown below:

earain Majorante Xearaing Senater (S.K.e.e.e.)	17 Sea	_					
wa	Forward						200.0
No. 50 Maritan	22.000		Canala Guil	Displication -	a		See.
Access Machine	Sec.				(Alternational Standards)	Charles	.F.s.
Tors Entries 1							
da na sin Mana dia mit	ale Mari Saintine 🗄	ille men	64.0	i i mana di mil	Conda Sur		
Acta March		CONAL.			CANS	Diric na	Dalese

Figure 8-68 ACL VLAN Access Map Window

The fields that can be configured are described below:

Parameter	Description
Access Map Name	Enter the access map's name here. This name can be up to 32 characters long.
Sub Map Number	Enter the sub-map's number here. This value must be between 1 and 65535.
Action	Select the action that will be taken here. Options to choose from are Forward , Drop , and Redirect . When the Redirect option is selected, select the redirected interface from the drop-down list.
Counter State	Select whether to enable or disable the counter state.

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

Click the **Clear All Counter** button to clear the counter information for all the access maps.

Click the **Clear Counter** button to the clear the counter information for the specified access map.

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

Click the **Binding** button to configure a new match access list.

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

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

After clicking the **Binding** button, the following page will appear.

locata Maphiane 🗧	Fictorica Hop		
SECTION NUMBER	°a		
∃ Malert-Accelling	최		
1	I. George Select I	Accy	Calaca
00	1		
D Vake Providence			*
D. Markel Providence	LPA		Datates
Ē	184		Diligia
Di Koke (Pvi) socere Di Di Dalah (KA) Asaan	Les 		

Figure 8-69 Match Access-List Window

The fields that can be configured are described below:

Parameter	Description
Match IP Access-List	Select the standard or extended IP ACL.
Match IPv6 Access-List	Select the standard or extended IPv6 ACL.
Match MAC Access-List	Select the standard or extended MAC ACL.

Click the Please Select button to choose the ACL profile that has been created.

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

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

ACL VLAN Filter

This window is used to view and configure the ACL VLAN filter settings.

I o view the followi	ing window, click AC	CL > ACL VLAN Filter, as shown	below:
ACL VEAN Dater			
AGL XLAB Dire			
Avera Marine Same	77 900		
66.01	A41		
- MCLW	110	P KPCON	12
Teni Enidech	6241		12
Antak	an Vane	AND Lm.	
A23.48	(Visp.	1	Profession -

Figure 8-70 ACL VLAN Filter Window

40.0

19.

Parameter	Description
Access Map Name	Enter the access map's name here. This name can be up to 32 characters long.

Parameter	Description
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
VID List	Enter the VLAN ID list that will be used here. Select the All VLANs option to apply this configuration to all the VLANs configured on this switch.

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

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.

9. Security

Port Security 802.1X AAA RADIUS TACACS+ **IMPB DHCP Server Screening ARP Spoofing Prevention BPDU Attack Protection MAC** Authentication Web-based Access Control Japanese Web-based Access Control **Network Access Authentication** Safeguard Engine **Trusted Host** Traffic Segmentation Settings Storm Control Settings **DoS Attack Prevention Settings** SSH SSL **Network Protocol Port Protection Settings**

Port Security

Port Security Global Settings

This window is used to view and configure the port security global settings. 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.

To view the following window, click **Security > Port Security > Port Security Global Settings**, as shown below:

Port Security Global Settings		
Fort Security Theo Seldings		
Trans Clarke	H Crakers - ja Crakers	A de termina
Part Streetly Transfeld: Settings (
implementaria,	1	ir the second
Tal Smith from Sillip		
eyddiaeta oen Ardess (Cele Ar	The set	- Act

Figure 9-1 Port Security Global Settings Window

The fields that can be configured for Port Security Trap Settings are described below:

Parameter	Description
Trap State	Click to enable or disable port security traps on the Switch.

Click the Apply button to accept the changes made.

The fields that can be configured for **Port Security Trap Rate Settings** are described below:

Parameter	Description
Trap Rate	Enter the number of traps per second. The range is from 0 to 1000. The default value 0 indicates an SNMP trap to be generated for every security violation.

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

The fields that can be configured for **Port Security System Settings** are described below:

Parameter	Description
System Maximum Address	Enter the maximum number of secure MAC addresses allowed. If not specified, the default value is No Limit. The valid range is from 1 to 6656. Tick the No Limit checkbox to allow the maximum number of secure MAC address.

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

Port Security Port Settings

This window is used to view and configure the port security port settings.

To view the following window, click **Security > Port Security > Port Security Port Settings**, as shown below:

	a Port Secto n Flor		ana -	Normal X-000	Volation a dire	Decardy United	Argen) Time 10-12	40) - Fig. 10 T)	p#
w att	150. 180	atifo 😥	Nex Med. 8	7 22	Protect	Deleto en Timeo	(v)	Aberia	7 (V)
NTE SAR	hgi Madhan	Current Ha	Websteen Auflice	Website Coal	Scata Vade	édan Shás	Carto di Sala	AssaTas	UTBO2
48-12.1	15	4	Presest	-	Rentedo Trakat.	20080	17	4	Absolute
121194	17	0	(Web)d	8	Dalars-ov-Treasure	- Nobiel	40	1	Absolute
	22	ð.,	Preside	12	Debra-co-Treerat	Clashed	46	3.	Abesime
48133					Demo-co-Times.	Studies .		/1	Absorb
49123	12	9	Crewd.	1.00		the second s			
41121		9. 0	Cread Cread		Delate the Transit	Disabilitati	47	3	Abicolana 1
	12	7.4 .	100000	1.125		Clead or Decidient		1 2	Abecima Abecima
4.433	12 22	a .	Prest		Delate one" was at	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	+		

Figure 9-2 Port Security Port Settings Window

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the port security feature on the port(s) specified.
Maximum	Enter the maximum number of secure MAC addresses that will be allowed on the port(s) specified. This value must be between 0 and 6656. By default, this value is 32.
Violation Action	Select the violation action that will be taken here. Options to choose from are:

Parameter	Description
	 Protect - Specifies to drop all packets from the insecure hosts at the port-security process level, but does not increment the security-violation count. Restrict - Specifies to drop all packets from the insecure hosts at the port-security process level and increments the security-violation count and record the system log. Shutdown - Specifies to shut down the port if there is a security violation and record the system log.
Security Mode	 Select the security mode option here. Options to choose from are: Permanent - Specifies that all learned MAC addresses are not be purged out unless the user manually deletes those entries. Delete-on-Timeout - Specifies that all learned MAC addresses are purged out when an entry is aged out or when the user manually deletes these entries.
Aging Time	Enter the aging time value used for auto-learned dynamic secured addresses on the specified port here. This value must be between 0 and 1440 minutes.
Aging Type	 Select the aging type here. Options to choose from are: Absolute - Specifies that all the secure addresses on this port age out exactly after the time specified and is removed from the secure address list. This is the default type. Inactivity - Specifies that the secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

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

Port Security Address Entries

This window is used to view, clear, and configure the port security address entries.

To view the following window, click **Security > Port Security > Port Security Address Entries**, as shown below:

	Part	MAC Address	240.04004		
1.61	1.1.5.101 (A)	CRAMMER PROVIDE THE PROPERTY OF	#12 · · · ·		
				ana analytal	Charles Ly 1995
Tajal Palaese	635				- strend
Port	¥ 00	WAC ACCINE	Address Trace	Terral dis Trees al	ne.
MP 10 ²	1.5	65-64-57-60-65-08	Carriera	+	

Figure 9-3 Port Security Address Entries Window

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
MAC Address	Enter the MAC address here. Tick the Permanent check box so that all learned MAC addresses would not be purged out unless the user manually deletes those entries.
Parameter	Description
-----------	--
VID	Enter the VLAN ID here. This value must be between 1 and 4094.

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

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

Click the Clear by Port button to clear the information based on the port selected.

Click the Clear by MAC button to clear the information based on the MAC address entered.

Click the **Clear All** button to clear all the information in this table.

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

802.1X

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:



Figure 9-4 The 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.



Figure 9-5 The three roles of 802.1X

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.



Figure 9-6 The Authentication Server

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.



Figure 9-7 The Authenticator

Three steps must be implemented on the Switch to properly configure the Authenticator.

• The 802.1X state must be enabled. (Security > 802.1X > 802.1X Global Settings)

- The 802.1X settings must be implemented by port (Security > 802.1X > 802.1X Port Settings)
- A RADIUS server must be configured on the Switch. (Security > RADIUS > RADIUS Server Settings)

<u>Client</u>

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.



Figure 9-8 The Client

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 the port is unlocked, normal traffic is allowed to pass through the port. The following figure displays a detailed explanation of how the authentication process is completed between the three roles stated above.



Figure 9-9 The 802.1X Authentication Process

The D-Link implementation of 802.1X allows network administrators to choose between two types of Access Control used on the Switch, which are:

- **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.
- Host-based Access Control Using this method, the Switch will automatically learn up to a maximum of 448 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-topoint 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.



Figure 9-10 Example of Typical Port-based Configuration

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.



Figure 9-11 Example of Typical Host-based Configuration

802.1X Global Settings

This window is used to view and configure the 802.1X global settings.

To view the following window, click Security > 802.1X > 802.1X Global Settings, as shown below:

802.48 Global Settings		
HE IT SUP	Grand e	
NETS DEPEN	The state	Apple

Figure 9-12 802.1X Global Settings Window

The fields that can be configured are described below:

Parameter	Description
802.1X State	Select to enable or disable the 802.1X global state here.
802.1X Trap State	Select to enable or disable the 802.1X trap state here.

802.1X Port Settings

This window is used to view and configure the 802.1X port settings.

To view the following window	click Security	> 802.1X > 802.1X Port Settings,	as shown below:
	, CHER Security -	~ 002. IA ~ 002. IA FUIL Sellings,	as shown below.

ile Port a								
as not here	ey							
		Twarfed.		To 741		Direction		
	164	2012/01/2012	16	- Sjanaa	(a)	Main 👾		
at Cardina		1 ma a 193		(Marth a)	234	ANY HERE AND A		
Auro -	- E	This shield		1		Directied 7		
Server The establish	58535	Caterral C	0.01489281		11-65525			
iŭ.	1000	140.00	DAC.	4.0	162			- Aprile
No.	New Area	Peri Kontra	Chicken 1101	war i	150-Automatication	s Sarah Lana A	- segulation	JX N IN 1
COLUMN .	inte	A/I	Distance	12	HO III	X	ж	3
1 (L.H)	*.#C	24.26	16	19	19.19			34
10120	2.4	(a, m	Discolo.	1	H	×	×	20
- MILH	Lar	Act.	Din sie o	2	II ROW	×	34	12
10.8	100	0.14	Histohoft II	1	10.06	4	72	81
100	1.2.4	Ar, in t	Des de l	8	1.00.00	8	(Ħ	29
ent 91	Lab	Set at	Disubled:	2 S	No te	×	26	(0) (0)
111.10	1.00	10.14	16.000	())	Receil .	0		84
1.12	Entry .	10.00	Dip.etc.1	() ()	HL.m.	X	×	39
ph-10410	1.05	Au .	Disable:	12	NOT	×	2	12
wint .	1.00	(4)(4)	3.862.562)	and the second sec			84
451001	14	76.0	The offer	12	1.44	7	1	30
#F5945	1.0	Aca	Disa Med	4	10210	×	×	31
90'03 PT	1 e 10* -	24.74	140.1501	- 22	19549			24
40.000	1.00	Xe e	Disc ale i	2	His		100	10.
ut:10/16	1.00	20 T	Distance of	12	10/8	×	30	21
Ministers :	100	20.75	Deck see for	4	80.00	. A.	.e.	71
4 6.815	1.0	Sec.	They also have	12	14.00	1	a.	- 22
# 1212	1.8	Action	Dischet	2	rions	×	×	30
Minister)	a hir	(60) ·	10013081	1	Figure 1	4		A.
- 10.00 f	1.64	(e. e	Stea de F	<u></u>	44.00		4	2.0
#11/223	1.10	16.7	Diss the d	1	Nom	×	X	3
MCNO51	(an	202	DBM SM C	4	10.00	14 - C		

Figure 9-13 802.1X Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction here. Options to choose from are Both and In . This option configures the direction of the traffic on a controlled port as unidirectional (In) or bidirectional (Both). The In control direction is only valid when the Host Mode is configured as Multi Host in the Network Access Authentication Port Settings window.
Port Control	 Select the port control option here. Options to choose from are: ForceAuthorized - Specifies that the port is not controlled in both directions. Auto - Specifies that access to the port for the controlled direction needs to be authenticated. ForceUnauthorized - Specifies that access to the port for the controlled direction is blocked.
Forward PDU	Select to enable or disable the forward PDU option here.
MaxReq	Enter the maximum required times value here. This value must be between 1 and 10. By default, this option is 2. This option configures the maximum number of times that the backend

Parameter	Description
	authentication state machine will retransmit an Extensible Authentication Protocol (EAP) request frame to the supplicant before restarting the authentication process.
PAE Authenticator	Select to enable or disable the PAE authenticator option here. This option configures a specific port as an IEEE 802.1X port access entity (PAE) authenticator.
Server Timeout	Enter the server timeout value here. This value must be between 1 and 65535 seconds. By default, this value is 30 seconds.
Supp Timeout	Enter the supplicant timeout value here. This value must be between 1 and 65535 seconds. By default, this value is 30 seconds.
TX Period	Enter the transmission period value here. This value must be between 1 and 65535 seconds. By default, this value is 30 seconds.

Authentication Session Information

This window is used to view and configure the authentication session information.

To view the following window, click **Security > 802.1X > Authentication Session Information**, as shown below:



Figure 9-14 Authentication Session Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

Click the Init by Port button to initiate the session information based on the selections made.

Click the **ReAuth by Port** button to re-authenticate the session information based on the selections made.

Authenticator Statistics

This window is used to view and clear the authenticator statistics.

To view the following window, click **Security > 802.1X > Authenticator Statistics**, as shown below:

Authentic	ariar Sibila	tikos	_	_	_		_	_	_	_		
Antesinca	en statistica -											
118 (1 📼		ſ	'reri	ch/01						<u> </u>	Clear Canadasa Clear Al
Unit 1 and												
Total Data	in: C											
Part	HOUTHAN	Hanses	янт	Kaligio	Logor	Rig	калра	ыыр	Instanti Instanti	HOST	Last Version	Last Source
	HIS .	13		13		12	IN I	118	122			

Figure 9-15 Authenticator Statistics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this query here.
Port	Select the appropriate port used for the query here.

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

Click the **Clear Counters** button to clear the counter information based on the selections made.

Click the Clear All button to clear all the information in this table.

Authenticator Session Statistics

This window is used to view and clear the authenticator session statistics.

To view the following window, click **Security > 802.1X > Authenticator Session Statistics**, as shown below:

	1000		provide the second s			0.000.000.000
	(1981)	0004041	12		100 M	Chi S a da
						2 minute
ALC: NORMAL CONTRACTOR						

Figure 9-16 Authenticator Session Statistics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this query here.
Port	Select the appropriate port used for the query here.

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

Click the Clear Counters button to clear the counter information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

Authenticator Diagnostics

This window is used to view and clear the authenticator diagnostics information.

To view the following window, click **Security > 802.1X > Authenticator Diagnostics**, as shown below:

umentedos Diagnóstica	
news an ingentia	
Lat F [4] Tot [anyth [4]	to factoria
	cherol
town service	
Tra Doore C	

Figure 9-17 Authenticator Diagnostics Window

The fields that can be configured are described below:

Parameter	Description	
Unit	Select the switch unit that will be used for this query here.	
Port	Select the appropriate port used for the query here.	

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

Click the Clear Counters button to clear the counter information based on the selections made.

Click the Clear All button to clear all the information in this table.

AAA

AAA Global Settings

This window is used to enable or disable the Authentication, Authorization, and Accounting (AAA) global state.

To view the following window, click Security > AAA > AAA Global Settings, as shown below:

AnA Global Settin	98-	
- AAA State Settings		
855 SEM	gi baabaa - (ji krabaa	
	di recursi di scincia	

Figure 9-18 AAA Global Settings Window

The fields that can be configured are described below:

Parameter	Description
AAA State	Select to enable or disable the Authentication, Authorization, and Accounting (AAA) global state.

Application Authentication Settings

This window is used to view and configure the application authentication settings.

To view the following window, click **Security > AAA > Application Authentication Settings**, as shown below:

ferencelere carterigs.		
- Li de altra	Ligne Michael (1)	
Em 100	0.6.8	- Lin -
Tenkt	inde all	10.00
2004	and at	1.10
10254	1 K M H	

Figure 9-19 Application Authentication Settings Window

The fields that can be configured are described below:

Parameter	Description
Login Method List	After clicking the Edit button for the specific entry, enter the login method list name used here.

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

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

Application Accounting Settings

This window is used to view and configure the application accounting settings.

To view the following window, click **Security > AAA > Application Accounting Settings**, as shown below:

	a din bin		Fact Midland Link	
i	Tm.00			and Later and
	To be			
	2004			14-
	19254			and the second
energia de la com	anay sarahas Metalo		10010-000-000-000-000-000-000-000-000-0	
opication	denotes The	um (1007)	Commente Method Las D2 cham	14.6
and extension of			Contract Statement Assess	
	Ausi crike	Land	Comments Method List	
	AT ST CREAT			

Figure 9-20 Application Accounting Settings Window

The fields that can be configured are described below:

Parameter	Description	
Exec Method List	After clicking the Edit button for the specific entry, enter the EXEC method list name used here.	
Application	Select the application used here. Options to choose from are Console , Telnet , and SSH .	

Parameter	Description
	Select the privilege level used here. Options to choose from are levels 1 to 15 .
Commands Method List	Enter the commands method list name used here.

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

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

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

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

Authentication Settings

This window is used to view and configure the AAA network and EXEC authentication settings.

To view the following window, click **Security > AAA > Authentication Settings**, as shown below:

huminiosi	ion Seltenjis				
276.5.896	READING HERMONY	AAS AGENERATION HARS			
AAN CARDING	camera logia Ass				
Strat	Obstabled	-			
Ref and (Farry later		M = 0	- Physics Selection (F)	
Bustress 3	** F.1 26.83	E	Netrod 4	HERENAL PI	1
	ana .www.				
38. m	26 Alkd	12			
Part as 1	E Falwy School	1.71	Medical 2	Phase Select (*)	
inieran b	11,2,2,2,2,1		46.934	P8 = = 10 S - (+-)	C. AND
	CONTRACTOR				
(B.)w)	Otrabled	- - -			
instruct.	We are here to		Herea 5	1964 - State 191	
Ref and	1011101		54/ w 13	Three Send	1
AAR AN BOARD	ana Wits Anto				
Shina	Décebér 5	4			
Referre	10000000		34/30/10	19	
Mid-mid-	Taxa Seed	-	40.0034	Tisara Delact. 1-	· · · · ·

Figure 9-21 Authentication Settings Window

The fields that can be configured for AAA Authentication 802.1X are described below:

Parameter	Description	
Status Select to enable or disable the AAA 802.1X authentica here.		
Method 1 to 4 Select the method lists that will be used for this configur Options to choose from are none, local, group and rac		

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

The fields that can be configured for AAA Authentication JWAC are described below:

Parameter	Description	
Status	Select to enable or disable the AAA JWAC authentication state here.	
Method 1 to 4	Select the method lists that will be used for this configuration here. Options to choose from are none , local , group and radius .	

The fields that can be configured for **AAA Authentication MAC-Auth** are described below:

Parameter	Description
Status	Select to enable or disable the AAA MAC authentication state here.
Method 1 to 4	Select the method lists that will be used for this configuration here. Options to choose from are none , local , group and radius .

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

The fields that can be configured for AAA Authentication WEB-Auth are described below:

Parameter	Description
Status	Select to enable or disable the AAA Web authentication state here.
Method 1 to 4	Select the method lists that will be used for this configuration here. Options to choose from are none , local , group and radius .

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

After clicking the AAA Authentication Exec tab, the following page will appear.

ation hartwood	AAA. Automotionee bals,				
ito -nanet					
Statist					
Fabric Lifer		54.0 C	Please Select		
1222522		Methodal	HERENES EL		1
015491					
22.256.9					
162.6		96632	Phase Select T		
TRACTORIES.		1012035	$H_{0,\infty,\alpha} \approx S + (-++)$		C. ANY
_	5000				
	Marined 1	Medice 3	Webed 3	Vetral 4	
0	2 hours	100 CONTRACTOR 100			1.224 928
	10000000000000000000000000000000000000	es vienet Diskt hd Paren Starr = Rate Seren = = Starspin 2000 m Resk Paren St. = Meined ()	e Merced a M	A entropy Constant Constant of Constant o	Charter Main of the state o

Figure 9-22 AAA Authentication Exec Window

The fields that can be configured for **AAA Authentication Enable** are described below:

Parameter	Description
Status	Select to enable or disable the AAA authentication enable state here.
Method 1 to 4	Select the method lists that will be used for this configuration here. Options to choose from are none , enable , group , radius , and tacacs+ .

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

The fields that can be configured for **AAA Authentication Login** are described below:

Parameter	Description
List Name	Enter the method list name that will be used with the AAA authentication login option here.
Status	Select to enable or disable the AAA authentication login state here.

Parameter	Description
Method 1 to 4	Select the method lists that will be used for this configuration here. Options to choose from are none , enable , group , radius , and tacacs+ .

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

Accounting Settings

This window is used to view and configure the AAA accounting settings.

To view the following window, click **Security > AAA > Accounting Settings**, as shown below:

060.898	entry service.	Ann Accounting System	(652)	And an and a set	CONVERSION CONTRACTOR	
Derinan.	Control -	r.				
www.	Proton & Auto	-1	1001032	Para Sector	1-1	
2.0.02	Taxes Celem	-	140.0014	Charle Select		and Andrews

Figure 9-23 Accounting Settings Window

The fields that can be configured are described below:

Parameter	Description
Default	Select to enable or disable the use of the default method list here.
Method 1 to 4	Select the method lists that will be used for this configuration here. Options to choose from are none , group , radius , and tacacs+ .

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

After clicking the AAA Accounting System tab, the following page will appear.

NAN 2505	a uting bacadas	Anno more intensis operation	0.000	water and the second	Coort Associating Literatures	
Derinan.	[Carbol	न				
0.0141	Holen-Z.Sett	-1	16/16/12	Para Netto	1-1	
218.005	Taxes Deler		Mo. 16 J 4	Chaste Calent: -	17 C	And Taking

Figure 9-24 AAA Accounting System Window

The fields that can be configured are described below:

Parameter	Description
Default	Select to enable or disable the use of the default method list here.
Method 1 to 4	Select the method lists that will be used for this configuration here. Options to choose from are none , group , radius , and tacacs+ .

After clicking the **AAA Accounting Exec** tab, the following page will appear.

the second strength of the second	 Ans exclusion op- 	00 000 000 000	e Hars Con Ascal e	ng Lannalack	
the Name					
eret low	-1	960K00 Pt 0	o set let		
MEALS Traces	Culture T	New J4	the Selection of the		and design
ee Lemmest			1-0000 M 100		
No. of Concession, No. of Conces	K ing a	Nr. 5 m 2	Without 1	Witness .	

Figure 9-25 AAA Accounting Exec Window

The fields that can be configured are described below:

Parameter	Description
List Name	Enter the method list name that will be used with the AAA accounting EXEC option here.
Method 1 to 4	Select the method lists that will be used for this configuration here. Options to choose from are none , group , radius , and tacacs+ .

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

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

After clicking the AAA Accounting Commands tab, the following page will appear.

ANA Accounting S	even 20	A As could ap Syntem	AAA Accounting Colo		seathg Commands 👘 📗	
90 (<u>F</u>	121					
Then Mean						
TANK ISTO	<u> </u>		kerwa 2		1	
rite i <u>Para</u>			Antonia il	Pierce Solvel	<u>ц</u>	130
ra Holes T						
(Inst)	Annt	Holis a 1	the Bank 2	Marine 2	(Malified A	and the second second

Figure 9-26 AAA Accounting Commands Window

The fields that can be configured are described below:

Parameter	Description		
Level	Select the privilege level used here. Options to choose from are levels 1 to 15 .		
List Name	Enter the method list name that will be used with the AAA accounting commands option here.		
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are none , group , and tacacs+ . The none option is only available for Method 1 .		

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

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

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

Server RADIUS Dynamic Author Settings

This window is used to view and configure the dynamic author settings for the RADIUS server.

To view the following window, click **Security > AAA > Server RADIUS Dynamic Author Settings**, as shown below:

	rie Author Clobal S						
in war too and	Ender	2	ees beward	1			Apply
over GAD US Datas	n Actus & Deps	61					
Cieff? / Alexa	1 (Cirk - 14)		C. Miller, Box Mary	207 11 10			
₩C in H1 Address			College Baseline a				
e nar Kiry Type	Fan Tec	<u>1</u>	, VCI/a, Hve Near / Server Kay	Contra in Contra		-	raoh
ę: Chard II P. Address Se over King, Type Inst. Heckows: 1					=	-	

Figure 9-27 Server RADIUS Dynamic Author Settings Window

The fields that can be configured for **Server RADIUS Dynamic Author Global Settings** are described below:

Parameter	Description		
Dynamic Author	Select to enable or disable the dynamic author function here. Dynamic authorization allows an external policy server to dynamically send updates to a device.		
Port	Enter the port number that is used for the data transmission of the update packets here. The range is from 1 to 65535.		

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

The fields that can be configured for **Server RADIUS Dynamic Author Settings** are described below:

Parameter	Description
Client IP Address	Select and enter the IP address of the RADIUS client here.
Client Host Name	Select and enter the hostname of the RADIUS client here.
Server Key Type	 Select the RADIUS server key type here. Options to choose from are: Plain Text - Select this option to use the plain text RADIUS server key type. Encrypted - Select this option to use the encrypted RADIUS server key type.
Server Key	When Plain Text is selected as the key type, enter the key for the RADIUS server connection in the plain text form here. This key can be up to 32 characters long. When Encrypted is selected as the key type, enter the key for the RADIUS server connection in the encrypted form here. This key can be up to 64 characters long.

Click the **Apply** button to add a new entry.

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

RADIUS

RADIUS Global Settings

This window is used to view and configure the RADIUS global settings.

To view the following window, click Security > RADIUS > RADIUS Global Settings, as shown below:

RADIUS Globel Settings				
RADIUS Granul Soldings				
TRADIES (COPIE)	1	Thin		Apok I
BADD'S Bland I've South Literation	1			
That SADIL'S Scarce Interface State:	Umblet	1		
IN4 SADILS Scare Interface Type	VLAN.	1	Medice 12 (HOR)	*goly
RADID GOM HIS SHITE RINKS				
Phil State & Scale & John State	DACKE	×.		
MARY MILLS and Adding Space	d(14)		taxanturta.8x	Apph
RADUS Server Alabaia Sellingy				
Rectific cover encode level in some	w		1	
RADIES Saver Attracts Seven-Timore		nd (1	<u>.</u>	\mathcal{F}_{B} do

Figure 9-28 RADIUS Global Settings Window

The fields that can be configured for **RADIUS Global Settings** are described below:

Parameter	Description
Dead Time	Enter the dead time value for the RADIUS server connection here. This is used to improve the authentication processing time by setting the dead time to skip unresponsive server host entries. The range is from 0 to 1440 minutes. By default, this value is 0 minutes. When this option is 0, the unresponsive server will not be marked as dead.

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

The fields that can be configured for RADIUS Global IPv4 Source Interface are described below:

Parameter	Description			
IPv4 RADIUS Source Interface State	Select to enable or disable the state of the IPv4 RADIUS source interface here.			
IPv4 RADIUS Source Interface Type	Select the IPv4 RADIUS source interface type here. Options to choose from are:			
	 VLAN - Specifies the IPv4 RADIUS source interface type as VLAN. 			
Interface ID	Enter the VLAN interface ID here. The range is from 1 to 4094.			

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

The fields that can be configured for RADIUS Global IPv6 Source Interface are described below:

Parameter	Description
	Select to enable or disable the state of the IPv6 RADIUS source interface here.

Parameter	Description
IPv6 RADIUS Source Interface Type	 Select the IPv6 RADIUS source interface type here. Options to choose from are: VLAN - Specifies the IPv6 RADIUS source interface type as VI AN.
Interface ID	Enter the VLAN interface ID here. The range is from 1 to 4094.

The fields that can be configured for **RADIUS Server Attribute Settings** are described below:

Parameter	Description
RADIUS Server Attribute NAS-IP-Address	Enter the IPv4 address of the RADIUS server attribute 4 in the RADIUS packet here.
RADIUS Server Attribute Event-Timestamp	Select to enable or disable the RADIUS server attribute event- timestamp function here.

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

RADIUS Server Settings

This window is used to view and configure the RADIUS server settings.

To view the following window, click **Security > RADIUS > RADIUS Server Settings**, as shown below:

A BELLE MARKET AND AND AND		1120200		100000		
in Trademin Trademini trademini trademini	3817	🗇 Evili-da		1000 C	_	
	- Sal			1000 cc	1.00	
idenal XOX	2					
Cristian -	Plain Task int	6. 		12.82403		
una karine h						
Pre Freakhors	Andre Brater (Post	Acrossients Post	Thread	Paterne.	. Key	LL Store C
1.21.20.25+	100	1915	5.0	11		Delaw

Figure 9-29 RADIUS Server Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the RADIUS server's IPv4 address here.
IPv6 Address	Enter the RADIUS server's IPv6 address here.
Authentication Port	Enter the authentication port number used here. This value must be between 0 and 65535. By default, this value is 1812. If no authentication is used, use the value 0.
Accounting Port	Enter the accounting port number used here. This value must be between 0 and 65535. By default, this value is 1813. If no accounting is used, use the value 0.
Retransmit	Enter the retransmit value used here. This value must be between 0 and 20. By default, this value is 3. To disable this option, enter the value 0.
Timeout	Enter the timeout value used here. This value must be between 1 and 255 seconds. By default, this value is 5 seconds.

Parameter	Description
Кеу Туре	Select the key type that will be used here. Options to choose from are Plain Text and Encrypted .
Кеу	Enter the key, used to communicate with the RADIUS server, here. This key can be up to 32 characters long.

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

RADIUS Group Server Settings

This window is used to view and configure the RADIUS group server settings.

To view the following window, click **Security > RADIUS > RADIUS Group Server Settings**, as shown below:

ADIUS Group Server Settin	60. ·					
in approximation and	10 min	12				
ARAH KANIMA						
STATISTICS	Recent.					395)
sem Cintrian: 2						
Hinny Grove Mane			Traditive data was		And the State of the second second	
0.5.0	122.150.1	11.43	a - Diele setende	1	 Sheet and	De cre
Cite Manager	and the second	and the second se			 a producer and the second	5 (12.54C)



The fields that can be configured are described below:

Parameter	Description
Group Server Name	Enter the name of the RADIUS group server here. This name can be up to 32 characters long.
IPv4 Address	Enter the IPv4 address of the RADIUS group server here.
IPv6 Address	Enter the IPv6 address of the RADIUS group server here.

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

Click the Show Detail button to view and configure detailed settings for the RADIUS group server.

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

After clicking the **Show Detail** button, the following page will be available.

oop Server Nemis Goop I				
Pur And Buck Service Interface plane	0.6306-0	9		
Pyr Peter, orderande internade Type	V 28	1	anamata in pirraina	
PvS Rebuild charge intertace plate.	Cischler,	0121616		
INS RADICE de ante intertade Type	W-28		interface (C (1-1044)	4 8 45
taup wisan tautus Hisaup?				
	Addson		1	-0
(82.15	0.1251		tin i	

Figure 9-31 RADIUS Group Server Settings - Detail Window

The fields that can be configured are described below:

Parameter	Description
IPv4 RADIUS Source Interface State	Select to enable or disable the state of the IPv4 RADIUS source interface here.
IPv4 RADIUS Source Interface Type	Select the IPv4 RADIUS source interface type here. Options to choose from are:
	 VLAN - Specifies the IPv4 RADIUS source interface type as VLAN.
	Interface ID - Enter the VLAN interface ID for the IPv4 RADIUS source interface here. The range is from 1 to 4094.
IPv6 RADIUS Source Interface State	Select to enable or disable the state of the IPv6 RADIUS source interface here.
IPv6 RADIUS Source Interface Type	Select the IPv6 RADIUS source interface type here. Options to choose from are:
	 VLAN - Specifies the IPv6 RADIUS source interface type as VLAN.
	Interface ID - Enter the VLAN interface ID for the IPv6 RADIUS source interface here. The range is from 1 to 4094.

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

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

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

RADIUS Statistic

This window is used to view and clear the RADIUS statistics information.

n weste			
: Sever Nerre (Fiscen Falser 14)			100 200
ANNAL 1			
DAD US-Server Address	Auformatication First	Accountry Fort	9.6
1.00.00.25	102	012	Ske S
		198	HERE BE ROOT
998 - 1995 - 1979 M			22
DS Sarver Audreng HEBCBODON			100
Sauran	An den de antier Pers		Acculture Peer
Pare Ling Tare			-1.
Same Second	22		96
ACCRET ACCREDE	14		365
- Anno 18 april 1			W.
Acres Order and			366
Jacob Rangaans	ia,		
Wind Minground	94		10
The los that Block - 11			1
rear to the to it of a pointer i	- U		1
THE REPORT	1		1
As a Tak A	3		1
Times.in	() ()		11
- 16/19/ . 18			1

To view the following window, click **Security > RADIUS > RADIUS Statistic**, as shown below:

Figure 9-32 RADIUS Statistic Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Select the RADIUS group server name from this list here.

Click the **Clear** button to clear the information based on the selections made.

Click the Clear All button to clear all the information in this table.

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

TACACS+

TACACS+ Global Settings

This window is used to display and configure the global TACACS+ server settings.

To view the following window, click **Security > TACACS+ > TACACS+ Global Settings**, as shown below:

Second and second and second				
AC805 · Clobal IPv9 Scurpe I similare				
PUT FALLACION SELECT INS AND SERA	DAGA	12		
NYT DADAGER Security intertaken Light	M. on	(V)	Internet Discouting	Ander

Figure 9-33 TACACS+ Global Settings Window

The fields that can be configured in TACACS+ Global IPv4 Source Interface are described below:

Parameter	Description
IPv4 TACACS+ Source Interface State	Select to enable or disable the state of the IPv4 TACACS+ source interface here.
IPv4 TACACS+ Source Interface Type	Select the IPv4 TACACS+ source interface type here. Options to choose from are:
	• VLAN - Specifies the IPv4 TACACS+ source interface type as VLAN.
Interface ID	Enter the VLAN interface ID here. The range is from 1 to 4094.

Click the Apply button to accept the changes made.

The fields that can be configured in TACACS+ Global IPv6 Source Interface are described below:

Parameter	Description
IPv6 TACACS+ Source Interface State	Select to enable or disable the state of the IPv6 TACACS+ source interface here.
IPv6 TACACS+ Source Interface Type	Select the IPv6 TACACS+ source interface type here. Options to choose from are:
	 VLAN - Specifies the IPv6 TACACS+ source interface type as VLAN.
Interface ID	Enter the VLAN interface ID here. The range is from 1 to 4094.

TACACS+ Server Settings

This window is used to view and configure the TACACS+ server settings.

To view the following window, click **Security > TACACS+ > TACACS+ Server Settings**, as shown below:

ACTIVATION PROTOCOLOGI					
Makey Transation		(17/d) Address	2012.1		
e I (1-68535)	49		Travel 0.489	5. art.	
er Type	BunTest	E.	60g	254 chate	1.20
ani Eniritea (†					
IPWRP/CA	dunera	Part	Timesul	Kej	
-122,135		0.41			Del des

Figure 9-34 TACACS+ Server Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the TACACS+ server's IPv4 address here.
IPv6 Address	Enter the TACACS+ server's IPv6 address here.
Port	Enter the port number used here. This value must be between 1 and 65535. By default, this value is 49.
Timeout	Enter the timeout value here. This value must be between 1 and 255 seconds. By default, this value is 5 seconds.
Кеу Туре	Select the key type that will be used here. Options to choose from are Plain Text and Encrypted .
Кеу	Enter the key, used to communicate with the TACACS+ server, here. This key can be up to 254 characters long.

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

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

TACACS+ Group Server Settings

This window is used to view and configure the TACACS+ group server settings.

To view the following window, click **Security > TACACS+ > TACACS+ Group Server Settings**, as shown below:

ACAES+ Course Server Se	Een							
Geogramianan © Prickstman © Prickstman		377.50		1				
THE PERSON NAMES	_	_	_		ANNES -	_	_	
Grand	127.430	122		100 A	+		1.2	100 M
8.78/2			1.1				-	

Figure 9-35 TACACS+ Group Server Settings Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Enter the name of the TACACS+ group server here. This name can be up to 32 characters long.
IPv4 Address	Enter the IPv4 address of the TACACS+ group server here.
IPv6 Address	Enter the IPv6 address of the TACACS+ group server here.

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

Click the Show Detail button to view and configure detailed settings for the TACACS+ group server.

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

After clicking the **Show Detail** button, the following page will be available.

EVELOS/CONSERVATION DE LA CONSERVATIONALIZA 0 s d A col 0 EVELOS/CONSERVATIONALIZA 0 s d A col 0 EVELOS/CONSERVATIONALIZACIONALIZZACIONALIZACIONALIZACIONALIZZACIONE	
INVESTIGATION Sector Products Type V V Investigation (D. (C. 1040)) INVESTIGATION County Products States Investigation Investigation (D. (C. 1040)) INVESTIGATION County Products States Investigation Investigation (D. (C. 1040)) INVESTIGATION County Products Investigation Investigation (D. (C. 1040))	
IPAG TACACON Selara ina tase dalam III - d	
Nove, when some many	
Houp sector ways Houp?	$e \in \mathcal{B}_{n}$
Ph&Tv5.8ddxp.	
(82402139) Disk -	

Figure 9-36 TACACS+ Group Server Settings - Detail Window

The fields that can be configured are described below:

Parameter	Description
IPv4 TACACS+ Source Interface State	Select to enable or disable the state of the IPv4 TACACS+ source interface here.
IPv4 TACACS+ Source Interface Type	Select the IPv4 TACACS+ source interface type here. Options to choose from are:

Parameter	Description
	 VLAN - Specifies the IPv4 TACACS+ source interface type as VLAN.
	Interface ID - Enter the VLAN interface ID for the IPv4 TACACS+ source interface here. The range is from 1 to 4094.
IPv6 TACACS+ Source Interface State	Select to enable or disable the state of the IPv6 TACACS+ source interface here.
IPv6 TACACS+ Source Interface Type	Select the IPv6 TACACS+ source interface type here. Options to choose from are:
	 VLAN - Specifies the IPv6 TACACS+ source interface type as VLAN.
	Interface ID - Enter the VLAN interface ID for the IPv6 TACACS+ source interface here. The range is from 1 to 4094.

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

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

TACACS+ Statistic

This window is used to view and clear the TACACS+ statistic information.

To view the following window, click Security > TACACS+ > TACACS+ Statistic, as shown below:

antes structure							
lang sa na na na	 Instruction 	Select [V]				der	Current
ivul Entition t	Contraction of the second						
aul Debler: 1 TACAS St Server Materia	- State	Sciel Open	Societ Clarge	Total Factoria Soul	Teld Packshiller	Tafanace Cotal	

Figure 9-37 TACACS+ Statistic Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Select the TACACS+ group server name from this list here.

Click the Clear button to clear the information based on the group selected.

Click the Clear All button to clear all the information in this table.

Click the **Clear** button to clear all the information for the specific port.

IMPB

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 (IMPB) 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. Active and inactive entries use the same database. The function is port-based, meaning a user can enable or disable the function on the individual port.

IPv4

DHCPv4 Snooping

DHCP Snooping Global Settings

This window is used to view and configure the DHCP snooping global settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Global Settings**, as shown below:

BHCP Snooping Global Sattle	1 9 5		
Decide Antonping Village Antonpy			
DI ICP Orcepine	Crecked	Dissibled	
Information Option Allow Unburged	2 Endoled	2 Discoled	
Source NAG Verliculler	C FINISHING	g Fica de t	
White Have Long	🖂 Enebled	😠 Dian bie d	Ag ph

Figure 9-38 DHCP Snooping Global Settings Window

The fields that can be configured are described below:

Parameter	Description
DHCP Snooping	Select to enable or disable the DHCP snooping global status.
Information Option Allow Untrusted	Select to enable or disable the option to globally allow DHCP packets with the relay Option 82 on the untrusted interface.
Source MAC Verification	Select to enable or disable the verification that the source MAC address in a DHCP packet matches the client hardware address.
Station Move Deny	Select to enable or disable the DHCP snooping station move state. When DHCP snooping station move is enabled, the dynamic DHCP snooping binding entry with the same VLAN ID and MAC address on the specific port can move to another port if it detects that a new DHCP process belong to the same VLAN ID and MAC address.

DHCP Snooping Port Settings

This window is used to view and configure the DHCP snooping port settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Port Settings**, as shown below:

an and a present of the sector of the			
	(i x)		
etar Pat	vi 383 🚊		
Do Fra	ad (11) a		
ANY REPORT OF A	1 7 pours		
A DEBC (BO)			and the second se
hatel	(k) T		- Ande
÷xit.	Traced	REALINE.	10771878
£73,21	-74	593.00	No Limit
at 11 18	- Sec.	2.12.00	Belle at
65100	*.a	Solution (H, Dell
ATT H	18	to Linut	100 1070
44.8	54	5-01 / ml	Fig. () and
Sel 18	- 16	8.2L mit	H.D. al
ent 20	*.8	0.91.00	Round
at 16 16		A set and	Physics of
6.4.20	50-	A stored	B. D. 4
ALCOND.		SSLINE	No Link
at (ef) (54	3.02.000	British
9.00	54	5.0.10	19. 15 cf
86,0040	7.9	ASL:10	Ho Link
11.24	74	101 (ml	Bellear
-4 1003		5 (1, m)	Holand
1000	1.3	Solum	No Unit
30% (C)	54°	231.38	reformation and a second
4.10913	54	S of set	Real and
#19249	7.2	t a Lindi	Ho Umil
- MEYAR AND	73.	550.00	- Include
4.901	54	S. O. off	Bulling
et 1922	-8-	sol, with	iss Limit
MATTER REA	58.	551.00	64106

Figure 9-39 DHCP Snooping Port Settings Window

The fields that can	he configured	are described below:
The lielus that can	i be configured	are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Entry Limit	Enter the entry limit value here. This value must be between 0 and 1024. Tick the No Limit option to disable the function.
Rate Limit	Enter the rate limit value here. This value must be between 1 and 300. Tick the No Limit option to disable the function.
Trusted	Select the trusted option here. Options to choose from are No and Yes . Ports connected to the DHCP server or to other switches should be configured as trusted interfaces. The ports connected to DHCP clients should be configured as untrusted interfaces. DHCP snooping acts as a firewall between untrusted interfaces and DHCP servers.

DHCP Snooping VLAN Settings

This window is used to view and configure the DHCP snooping VLAN settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping VLAN Settings**, as shown below:

DECP Stooping VLAN Settings		
certal version and micro exceptions		
sben (196	Orde Franker R	4.6
THERE IS NOT THE OWNER OF		

Figure 9-40 DHCP Snooping VLAN Settings Window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list used here.
State	Select to enable or disable the DHCP snooping VLAN setting here.

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

DHCP Snooping Database

This window is used to view and configure the DHCP snooping database settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Database**, as shown below:

LA ICI" Service and List	atmen .			
пнои номена полема				
🔲 ils Dyler, (50-56400) -	P ×	and the basical		- 4.40
size of the second of	ana -			
9m.	TITE S	a a grad i fag ar th de al la de a de a		₹µ.k clen
Loui Dritti? Secole e Dui				
1br	liele V			1 April 1
(# 1) 	4 (104) (m)	a magentic according to the		1 6256
The grand branage on	date:			
Bardela Sol Gene	(J. 1997)	Eq.(a, e h, e, c	10	
encola energian	.e	a na separate a cons		
Para de calence		12	a .	A +

Figure 9-41 DHCP Snooping Database Window

The fields that can be configured for **DHCP Snooping Database** are described below:

Parameter	Description
Write Delay	Enter the write delay time value here. This value must be between 60 and 86400 seconds. By default, this value is 300 seconds. Select the Default option to use the default value.

The fields that can be configured for Store DHCP Snooping Database are described below:

Parameter	Description
URL	Select the location from the drop-down list and enter the URL where the DHCP snooping database will be stored to here. Location to choose from is TFTP .

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

Click the **Clear** button to clear the stored DHCP snooping database.

The fields that can be configured for Load DHCP Snooping Database are described below:

Parameter	Description
URL	Select the location from the drop-down list and enter the URL where the DHCP snooping database will be loaded from here. Location to choose from is TFTP .

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

Click the **Clear** button to clear all the counter information.

DHCP Snooping Binding Entry

This window is used to view and configure the DHCP snooping binding entries.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Binding Entry**, as shown below:

H-C Actives	00-04-07-02-04-0	Keen (
ear dailige						
Adams	The second					
	100	- S T				
5	##1997	124				
(351/2014) (03-102-102 ⁻¹ 2015)		loc l				
						and the second
CALENTING 1				And in case of the local division of the loc	2424 (243)	
rai Evenis: 1 WAC Addrese	¥D.	12 Addama	5 101	Luny	Pres -	

Figure 9-42 DHCP Snooping Binding Entry Window

Parameter	Description
MAC Address	Enter the MAC address of the DHCP snooping binding entry here.
VID	Enter the VLAN ID of the DHCP snooping binding entry here. This value must be between 1 and 4094.
IP Address	Enter the IP address of the DHCP snooping binding entry here.
Unit	Select the switch unit that will be used for this configuration here.
Port	Select the appropriate port used for the configuration here.
Expiry	Enter the expiry time value used here. This value must be between 60 and 4294967295 seconds.

The fields that can be configured are described below:

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

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

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

Dynamic ARP Inspection

ARP Access List

This window is used to view and configure the dynamic ARP inspection settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Access List**, as shown below:

ARP Access List		
ARP ASSAST BO		
ARE Access List Name	XI then	
Total Exclusion		
	ARP Access Uni Name	
	ANY Processed at	

Figure 9-43 ARP Access List Window

The fields that can be configured are described below:

Parameter	Description
ARP Access List Name	Enter the ARP access list name used here. This name can be up to 32 characters long.

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

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

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

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

n Santa Santa Tana Ang Mata Ang		Sumo T Sense Se			Cardo Pilita Santario Nu		-
							asch oppie
eP Accessi wi Rom	. 469° Ar 2014 1 42						and ora-
NP ACCESSION FOR BAR	e ANPA serve I at	babil!	Reads 11 March	WBD 1gr =	Xende Milt	R to B 1965 (1964-6	

Figure 9-44 ARP Access List - Edit Window

Parameter	Description
Action	Select the action that will be taken here. Options to choose from are Permit and Deny .
IP	Select the type of sender IP address that will be used here. Options to choose from are Any , Host , and IP with Mask .
Sender IP	After selecting the Host or IP with Mask options as the type of IP , enter the sender IP address used here.

The fields that can be configured are described below:

Parameter	Description
Sender IP Mask	After selecting the IP with Mask option as the type of IP , enter the sender IP mask used here.
MAC	Select the type of sender MAC address that will be used here. Options to choose from are Any , Host , and MAC with Mask .
Sender MAC	After selecting the Host or MAC with Mask options as the type of MAC , enter the sender MAC address used here.
Sender MAC Mask	After selecting the MAC with Mask option as the type of MAC , enter the sender MAC mask used here.

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

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

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

ARP Inspection Settings

This window is used to view and configure the ARP inspection settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Settings**, as shown below:

Add Inspection	Seriisrque				
and employees see					
20.0 12.91	Center	Setting (a)			
(MANA)	FEREN	\$10.000			
1-	(*+4.4) (**	\$1925.00			ages.
ANT Logistics Mile	Millionarea				
Taxa: Coldect (1
VD	ACL Loggie	0	SHC ² Logging		
1 1 1	iyana.		North	24	
The second			22.0.2		1 w
ASP imposize Tile	é.				
AN- ACOUNTS	ne -	io mini			
2010		2,34			
001001/00		No		455	De sta
Sections:					
WD NO		AMPA a ma l	olfine.	Sec.	e. 40%
3 01 ····		8.40.4	3/	1100	1
1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -			310		
					and the second sec

Figure 9-45 ARP Inspection Settings Window

The fields that can be configured for ARP Inspection Validation are described below:

Parameter	Description
Src-MAC	Select to enable of disable the source MAC option here. This option specifies to check for ARP requests and response packets and the consistency of the source MAC address in the Ethernet header against the sender MAC address in the ARP payload.
Dst-MAC	Select to enable of disable the destination MAC option here. This option specifies to check for ARP response packets and the consistency of the destination MAC address in the Ethernet header against the target MAC address in the ARP payload.
IP	Select to enable of disable the IP option here. This option specifies to check the ARP body for invalid and unexpected IP addresses. It

Parameter	Description
	also specifies to check the validity of IP address in the ARP payload. The sender IP in both the ARP request and response and target IP in the ARP response are validated. Packets destined for the IP addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses are dropped. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

Click the **Edit** button to configure the ARP inspection VLAN logging settings.

After clicking the **Edit** button, the following fields can be configured:

Parameter	Description
ACL Logging	Select the ACL logging action here. This specifies the logging criteria for packets that are dropped or permitted based on ACL matches. Options to choose from are:
	 Deny - Specifies logging when denied by the configured ACL. Permit - Specifies logging when permitted by the configured ACL. All - Specifies logging when permitted or denied by the configured ACL. None - Specifies that ACL-matched packets are not logged.
DHCP Logging	Select the DHCP logging action here. This specifies the logging criteria for packets dropped or permitted based on matches against the DHCP bindings. Options to choose from are:
	 Deny - Specifies logging when denied by DHCP bindings. Permit - Specifies logging when permitted by DHCP bindings. All - Specifies logging when permitted or denied by DHCP bindings. None - Specifies to prevent the logging of all packets permitted or denied by DHCP bindings.

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

The fields that can be configured for **ARP Inspection Filter** are described below:

Parameter	Description
ARP Access List Name	Enter the ARP access list name used here. This name can be up to 32 characters long.
VID List	Enter the VLAN ID list used here.
Static ACL	Select whether to use a static ACL or not here by either selecting Yes or No .

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

Click the **Delete** button to remove an 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.

ARP Inspection Port Settings

This window is used to view and configure the ARP inspection port settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Port Settings**, as shown below:

- C	162	Ŀ.	Hamilton	0.04	<u>ا</u>	10.00	(0.00 g
ale Line (> 50	1	p sei	Cardenava (Net)	1	2 How		
Viel P. al.	Clasked	Ē				and the second	an is calcul
POR	3	nin sata -		tama luhan (apa)	2	50,000	niesi
10-10	0	L'Anterio de la constante de l		-0-			
10.000	8	1.85256		10		+	
4.47	1 C	1.00 m 10		<u>.</u>	15	1	
. 18 - 18 M	6	Ann.		25			
AP2VA		TAULUS		10		+	1
#.'eA	6	1.4.4.4		10	10	-	
19.30	· .	Life in 19		15			
Mr 160		Lanara .		15	1		
114126.0		E di artist		2	11	-	
14.44		line, a		24			
. etc. (6)	1.	Litrarie -		12	4		
100.18.2	o.	(Barbarta		(9)		+	
0.000	7.	Latin at		54			
10 K.	4).	L-Warted		#	10		2
00010.41		1.07.07.04		Au.			
		140.0		H			
10.00	ð :	Laborates		15 (C)			
00.18.7	1.00	C.W.W.W.					
1.00	5:	100		(月)			
48.103		a thran pri		95. 29			
our tely		0.0000000		14.		+	
in the second		Call of the					
10 .52		Univer		16			
Minug		CARLEN .		S	1		
10.70.7	4.	10.00					
	X	L. W. H. L. M.					

Figure 9-46 ARP Inspection Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Rate Limit	Enter the rate limit value here. This value must be between 1 and 150 packets per seconds.
Burst Interval	Enter the burst interval value here. This value must be between 1 and 15. Tick the None option to disable the option.
Trust State	Select to enable or disable the trust state here.

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

Click the **Set to Default** button to change the information to the default values.

ARP Inspection VLAN

This window is used to view and configure the ARP inspection VLAN settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection VLAN**, as shown below:

har napacia			
(#107)	li es	≪w [tested] <u>m</u>	(Coursely)
AST meacon (Destac VID		

Figure 9-47 ARP Inspection VLAN Window

Parameter	Description
VID List	Enter the VLAN ID list used here.
State	Select to enable or disable the ARP inspection option's state for the specified VLAN here.

The fields that can be configured are described below:

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

ARP Inspection Statistics

This window is used to view and clear the ARP inspection statistics information.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Statistics**, as shown below:

900 B		1.00						Clearte	ALAL
	evict .								
	1. State 1 1 1 1 1 1	and the second	LINC F LINES	ALL LANGE	DECK PARENT	713 Perman.	SHEREBOOK AS BOOK	LINE WAS A REAL	IN WARDON IN ALL IN Y
M 86	Lowelland.	a la segura de la se	and the second	COLUMN TWO IS NOT	The second second second	and a second second	THE REAL PROPERTY IN COMPANY	And the second second	



The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list used here.

Click the Clear by VLAN button to clear the information based on the VLAN ID(s) entered.

Click the Clear All button to clear all the information in this table.

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

ARP Inspection Log

This window is used to view, configure, and clear the ARP inspection log information.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Log**, as shown below:

AND REPORTED IN					
Legitarity (141304)	<u>pa</u>	1			And a start
Table Filteration					
Pat		W./M	les nomr på	seasar Marx.	Cocarmena

Figure 9-49 ARP Inspection Log Window

The fields that can be configured are described below:

Parameter	Description
	Enter the log's buffer value used here. This value must be between 1 and 1024. By default, this value is 32.

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

Click the **Clear Log** button to clear the log.

IP Source Guard

IP Source Guard Port Settings

This window is used to view and configure the IP source guard port settings.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Port Settings**, as shown below:

P Source Guard	i Port Sellings			
uni Dan Pat Vale	i al adritti a branini al	To Fail Mainteir	etitti a	
	Pai		Veliciation Tape	
	67613600			

Figure 9-50 IP Source Guard Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the IP source guard's state for the specified port(s) here.
Validation	Select the validation method used here. Options to choose from are IP and IP-MAC . Selecting IP means that the IP address of the received packets will be checked. Selecting IP-MAC means that the IP address and the MAC address of the received packets will be checked.

IP Source Guard Binding

This window is used to view and configure the IP source guard binding settings.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Binding**, as shown below:

2 Source Gaure	Hindog				_				
P Son extinction 5	CONTRACTOR OF THE OWNER OF								
Rec Address	100.000	4.4.5							
90.0.4654									
P Address									
Lan	(1. same								
From Fort	1110	1.77		1000	121	-		201	
11 States Realing a									
1.0	1								
Honi Hon	Kas	1.1		13-37		Hara .	1.0		
P.M.Nay	1.000			We share	8 I.	Line Sector	and the second se		
MIC (S. M. SA).	0.	12		1000		20	÷.	1	<u> </u>
Test Cristics									
UNC.	(dava)	P Action	Lee	er Land	Tun	VLAS	Pari		
11.4	oston in	11.8.11.5.4		daat y	28.6		10.318*	Coles	
							201 10 10		90

Figure 9-51 IP Source Guard Binding Window

The fields that can be configured for **IP Source Binding Settings** are described below:

Parameter	Description				
MAC Address	Enter the MAC address of the binding entry here.				
VID	Enter the VLAN ID of the binding entry here.				
IP Address	Enter the IP address of the binding entry here.				
Unit	Select the switch unit that will be used for this configuration here.				
From Port / To Port	Select the appropriate port range used for the configuration here.				

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

The fields that can be configured for IP Source Binding Entry are described below:

Parameter	Description				
Unit	Select the switch unit that will be used for this query here.				
From Port / To Port	Select the appropriate port range used for the query here.				
IP Address	Enter the IP address of the binding entry here.				
MAC Address	Enter the MAC address of the binding entry here.				
VID	Enter the VLAN ID of the binding entry here.				
Туре	Select the type of binding entry to find here. Options to choose from are:				
	 All - Specifies that all the DHCP binding entries will be displayed. DHCP Snooping - Specifies to display the IP-source guard binding entry learned by DHCP binding snooping. 				

Parameter	Description
	 Static - Specifies to display the IP-source guard binding entry that is manually configured.

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

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

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

IP Source Guard HW Entry

This window is used to view the IP source guard hardware entries.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard HW Entry**, as shown below:

			satur 1		ind.
dat Destance					
Fait	1000	enter anter Activa	Narie Refer	MAG 723764	1.10

Figure 9-52 IP Source Guard HW Entry Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this query here.
From Port / To Port	Select the appropriate port range used for the query here.

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.

Advanced Settings

IP-MAC-Port Binding Settings

This window is used to view and configure the IP-MAC-Port binding settings.

To view the following window, click **Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Settings**, as shown below:

MADE HAT HE WAS							
rap stars	903 800 3	to examine	ay (002000)				ie sk
MALEND HAVE	a sector as	6					
	Ŷ.	(X)		1.000 00			
and Hart	120.00		in the second second	500000	1.1		
kde :	Disabled	-	100	States -	2.2.2.		100
		Pott	_	_	_	Fish	100,000
		100 A	-	_		California	
		- 10 - 10 - 10 - 10 - 10 - 10 - 10 - 10		_		10.00	
		4.000				0.4.4	
		#1924				Cutel	
		2001 B				10.000	
		4.000				6.445	
		#10,07				Cited	
		ACC / 10				115 15	
		1000				12.414	
		10.040				Cable	
		MC ACT.				1110.50	
		4.14.14				210.000	
		ar etc.				Dided	
		Serve and				Line is t	
		in take				11.4.4	
		11 11 16				5.4.4	
		Market I				Citized-	
		A Sales				The second se	
		1. 19 12				C.A.A.	
		M. 1.2				Citabres :	
		ar 14 (21)				17.4.44	
		17. 671				5.4.4	

Figure 9-53 IP-MAC-Port Binding Settings Window

The fields that can be configured for IP-MAC-Port Binding Trap Settings are described below:

Parameter	Description
Trap State	Select the enable or disable the IP-MAC-Port binding option's trap state.

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

The fields that can be configured for IP-MAC-Port Binding Port Settings are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Mode	Select the mode of access control that will be used here. Options to choose from are Disabled , Strict , and Loose . When a port is enabled for IMPB strict-mode access control, a host can only access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host passes the binding check. To pass the binding check, the source IP address, source
Parameter	Description
-----------	--
	MAC address, VLAN ID, and arrival port number must match any of the entries defined by either the IP source guard static binding entry or the DHCP snooping learned dynamic binding entry. When a port is enabled for IMPB loose-mode access control, a host will be denied to access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host does not pass the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port must match any of the entries defined by either the IP source guard static binding entry or the DHCP snooping learned dynamic binding entry.

IP-MAC-Port Binding Blocked Entry

This window is used to view and clear the IP-MAC-Port binding blocked entry table.

To view the following window, click **Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Blocked Entry**, as shown below:

-MAC-Port Ending Block	kes E-by					_
argebra tat <u>iv</u> i	han Ast <u>statute and s</u>	TOPO CONTRA	*	Carino -	()(2)(0)(0)	- Abohr
Trail Decision 4		1				
E. AND	M 86			WH 74	likerse	

Figure 9-54 IP-MAC-Port Binding Blocked Entry Window

The fields that can be configured are described below:

Parameter	Description
Clear All	Leave all fields unselected and click the Apply button to clear all IMPB blocked entry information.
Clear by Port	Select this option to clear the entry table based on the port(s) selected.
Unit	Select the switch unit that will be clear here.
From Port / To Port	Select the appropriate port range that will be cleared here.
Clear by MAC	Select this option to clear the entry table based on the MAC address entered. Enter the MAC address that will be cleared in the space provided.
Clear All	Select this option to clear all entries that contain MAC addresses.

IPv6

IPv6 Snooping

This window is used to view and configure the IPv6 snooping settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 Snooping**, as shown below:

Sec. 17	and the second second					and a state of the
Callshi Plane	Storia 🗐					4.6
t <mark>el Zonaca, t</mark> er	ag hologis					
Patrone		hi a se	1			
he désignées			R MIN			
T the sec		C to black 🐨				
- 19 for		B. #K	17			4cg4
Islat Filtrand T						
Second as	Policy Policy	ed Extension	n/Com	Chevel WAR		
Trail		51			P.61 (1	- Ala

Figure 9-55 IPv6 Snooping Window

The fields that can be configured for Station Move Setting are described below:

Parameter	Description
Station Move	Select the station move options here. Options to choose from are Permit and Deny .

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

Parameter	Description
Policy Name	Enter the IPv6 snooping policy name used here. This name can be up to 32 characters long.
Limit Address Count	Enter the address count limit value used here. This value must be between 0 and 511. Tick the No Limit option to disable this option.
Protocol	Select the protocol that will be associated with this policy here. Options to choose from are Disabled , DHCP , NDP , and All . DHCPv6 Snooping sniffs the DHCPv6 packets sent between the DHCPv6 client and server in the address assigning procedure. When a DHCPv6 client successfully got a valid IPv6 address, DHCPv6 snooping creates its binding database. ND Snooping is designed for a stateless auto-configuration assigned IPv6 address and manually configured IPv6 address. Before assigning an IPv6 address, the host must perform Duplicate Address Detection first. ND snooping detects DAD messages (DAD NS and DAD NA) to build its binding database. The NDP packet (NS and NA) is also used to detect whether a host is still reachable and determine whether to delete a binding or not.
VID List	Enter the VLAN ID list used here.

The fields that can be configured for IPv6 Snooping Policy Settings are described below:

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

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

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

IPv6 ND Inspection

This window is used to view and configure the IPv6 ND inspection settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 ND Inspection**, as shown below:

naminin Vila a Suato NHC Fragment Lata Patriacia			a no gi se gi	jaman aj	10.000 (10.000 (10	
	and the second second second	19284	National Source MAC	arget Port	10 10 10	2.00

Figure 9-56 IPv6 ND Inspection Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name used here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are Host and Router . By default, the device's role is set as host and inspection for NS and NA messages are performed. If the device role is set as router, the NS and NA inspection is not performed. When performing NS/NA inspection, the message will be verified against the dynamic binding table learned from the ND protocol or from the DHCP.
Validate Source-MAC	Select to enable or disable the validation of the source MAC address option here. When the Switch receives an ND message that contains a link-layer address, the source MAC address is checked against the link-layer address. The packet will be dropped if the link-layer address and the MAC addresses are different from each other.
Target Port	Tick this option to specify the target port.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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

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

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

IPv6 RA Guard

This window is used to view and configure the IPv6 Router Advertisement (RA) guard settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 RA Guard**, as shown below:

ReS RA Guard								
		a de s						
Device Rule		Heat in						
ilden Tvö Avenus da.		Please Sele						
TagatPat	126	- Rade 2.86	Danifat 🖬		To Post	40/10/1	191	Agak/
lossi Carries: 1								
Fig. 6, y. Marson	Une		Make The Access U.A.	the second se		-	- 69	7.00
Policy	1000	ad .	Extended Pack 21		206	1.1	h Dete	1. The second

Figure 9-57 IPv6 RA Guard Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are Host and Router . By default, the device's role is Host , which will block all the RA packets. If the device's role is Router , RA packets will be forwarded according to the port's bound ACL.
Match IPv6 Access List	Enter or select the IPv6 access list to match here.
Target Port	Tick this option to specify the target port.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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

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

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

IPv6 DHCP Guard

This window is used to view and configure the IPv6 DHCP guard settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 DHCP Guard**, as shown below:

	With Iter' Grand								
Maker Prefix and ub. Mass Laker L. Targal Par. Latin L. Targal Par. Latin Total Carrier: 1 Mass Rock Maker Prefix Rock Mass Rock			and the second second	<u></u>					
Perky News Diversities Welch Perl Access List. Read Dal	hlikin 1969, anarula.	26	Neare De	kat l	ল	To Post	49-001		Agot:
	Total Corries: 1		1960 1990						
Polo Carl Dances Pols and adult on neur	Paley Mean	U.s.s	e Roder	Weich Phil August Ltd.	Torget P	ul			5 (C
	Polic		iest -	Estended PetrA21	adr.(6)	1		8.80 E	Defense in the second s

Figure 9-58 IPv6 DHCP Guard Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are Client and Server . By default, the device's role is set as Client , which will block all the DHCPv6 packets from the DHCPv6 Server. If the device's role is set as Server , DHCPv6 Server packets will be forwarded according to the port's bound ACL.
Match IPv6 Access List	Enter or select the IPv6 access list to match here.
Target Port	Tick this option to specify the target port.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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

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

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

IPv6 Source Guard

IPv6 Source Guard Settings

This window is used to view and configure the IPv6 source guard settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Source Guard > IPv6 Source Guard Settings**, as shown below:

Pvi ingres Suard a	shings -						
FOR RELAX DESIGN PARTY							
Tolog Harrs Second to contragine History The Tologr		Para T					
ETA SUPERI	2006	101	Ten 34	[1153215]	D.T.s.	frank le	
3417 5477	18.4	d kanafasiyar Addama	3	land a ditaik	Tag (Pa)		
*.en		Pre an		Den		400 C	24 els



Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Global Auto-Configure Address	Select to permit of deny data traffic from the auto-configured global address. It is useful when all global addresses on a link are assigned by DHCP and the administrator that wants to block hosts with self-configured addresses from sending traffic.
Link Local Traffic	Select to permit of deny hardware permitted data traffic send by the link-local address.
Target Port	Tick this option to specify the target port.
Unit	Select the switch unit that will be used for this configuration here.

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.

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

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

IPv6 Neighbor Binding

This window is used to view and configure the IPv6 neighbor binding settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Neighbor Binding**, as shown below:

Pvá bia girátor Bina	ing .					
Feb halot and so w	ntags					
NAC Actions	06923000					
waren amit	L.					
Tri Alban	21X1.1					
	[tief					
(n = 15)	48-12-1 E	1997-00	•# UUT			- rest
First Subgroter Data and G	any .					
1#	17					
TOP FOR	1667 B	i o Part	Real Contemporation	12		
And field an	2.01	Wet have	1.2.2			
10 (1 - 00-0						in the second second
Test Entret1						
Deci Achieve.	A REAL CARGES	e butte	8143	Sec. et al.	the shift a	
(79) L	First station	0	5 2 1	86	14.14	cales:
					- <u>190</u> []]	

Figure 9-60 IPv6 Neighbor Binding Window

The fields that can be configured for IPv6 Neighbor Binding Settings are described below:

Parameter	Description	
MAC Address	Enter the MAC address used here.	
VID	Enter the VLAN ID used here. This value must be between 1 and 4094.	
IPv6 Address	Enter the IPv6 address used here.	
Unit	Select the switch unit that will be used for this configuration here.	
From Port / To Port	Select the appropriate port range used for the configuration here.	

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

The fields that can be configured for IPv6 Neighbor Binding Entry are described below:

Parameter	Description	
Unit	Select the switch unit that will be used for this search here.	
From Port / To Port	Select the appropriate port range used for the search here.	
IPv6 Address	Enter the IPv6 address to find here.	
MAC Address	Enter the MAC address to find here.	
VID	Enter the VLAN ID to find here.	

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

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

DHCP Server Screening

This function allows users to not only to restrict all DHCP server packets but also to receive any specified DHCP server packet by any specified DHCP client. It is useful when one or more DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients.

The first time the DHCP filter is enabled it will create both an access profile entry and an access rule per port entry, it will also create other access rules. These rules are used to block all DHCP server packets. In addition to a permit DHCP entry it will also create one access profile and one access rule entry the first time the DHCP client MAC address is used as the client MAC address. The Source IP address is the same as the DHCP server's IP address (UDP port number 67). These rules are used to permit the DHCP server packets with specific fields, which the user has configured.

When DHCP server filter function is enabled all DHCP server packets will be filtered from a specific port.

DHCP Server Screening Global Settings

This window is used to view and configure the DHCP server screening global settings.

To view the following window, click **Security > DHCP Server Screening > DHCP Server Screening Global Settings**, as shown below:

	kesthing Gobal Ko				
Trap Calls	[Castor 7]				4.6
an shina -					
	p2 0 m				
De MAL	FILL CRIME				- Acob
tela Parany di					
i and the second second	Arctine Marte		CHARAC		
	37814		004740000	1.200 A	State Not. 4
a hitra ka					
n de la bén	्य प्रवेद 👘	1			at a literator
history C					
2	176	Sectors B1	Chevrol March 1		(Las montais

Figure 9-61 DHCP Server Screening Global Settings Window

The fields that can be configured for Trap Settings are described below:

Parameter	Description
Trap State	Select to enable or disable the DHCP server screening trap here.

Click the Apply button to accept the changes made.

The fields that can be configured for Profile Settings are described below:

Parameter	Description
Profile Name	Enter the DHCP server screening profile name here. This name can be up to 32 characters long.
Client MAC	Enter the MAC address used here.

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

Click the **Delete Profile** button to remove the specified profile.

The fields that can be configured for **Log Information** are described below:

Parameter	Description
Log Buffer Entries	Enter the logged buffer entries value here. This value must be between 10 and 1024. By default, this value is 32.

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

Click the **Clear Log** button to clear the log.

DHCP Server Screening Port Settings

This window is used to view and configure the DHCP server screening port settings.

To view the following window, click **Security > DHCP Server Screening > DHCP Server Screening Port Settings**, as shown below:

North Article States	ang Profilosogik			
i Danis aj site	al Teñal A let journa le	Caller Caller (19-146 d)=	The lates	- 4p-ek.
i Nort	(WW)	Environ .	WWW-Rawn	35
100000	00.00.0			Q.197
200.00	DF.M.I.			Contraction of the second
00000	Childhid .	*		
at 19.84	Circle March			and the state
AL 104	DS ALL		(1)	- 101.0
10.426	Ottumed		24	24.0
MALE AND	(burnlaw):			and the second
4.558	(Pr)			10 Th - 10 Oct
10:108	Citation d			CDark.
West	LEA YOU T			10 N 10 10 10 10 10 10 10 10 10 10 10 10 10
THE REAL PROPERTY.	Or an i			-1014
18 - C-C	Countred :	10 A		1.544
ANTIG TO	10/10/3	~		and the second
alard.	De da 4			
10.001	Chaded			1749.4
WE HERE	15030541			100 h 100 h
100100711	De ab il			
·唐·公方	Official and a second s			1.144
MCR. Th				1
101201	The Mark			
A 1021	Double 1			- The
MP 422	United the second	17	51	1.540
1.2	De ale a			18.7
6.24				1.00.0
401022	Carabies Carabies	*	114	

Figure 9-62 DHCP Server Screening Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

Parameter	Description
State	Select to enable or disable the DHCP server screening function on the port(s) specified.
Server IP	Enter the DHCP server's IP address here.
Profile Name	Enter the DHCP server screening profile that will be used for the port(s) specified here.

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

ARP Spoofing Prevention

This window is used to view and configure the ARP spoofing prevention settings. When an entry is created, ARP packets whose sender IP address matches the gateway IP address, of an entry, but its sender MAC address field does not match the gateway MAC address, of the entry, will be dropped by the system. The ASP will bypass the ARP packets whose sender IP address doesn't match the configured gateway IP address.

If an ARP address matches a configured gateway's IP address, MAC address, and port list, then bypass the Dynamic ARP Inspection (DAI) check no matter if the receiving port is ARP trusted or untrusted.

To view the following window, click **Security > ARP Spoofing Prevention**, as shown below:

er specificares	man copping state				
ADD Sporting Preve	0.077/7	Canabas (4	Dirabled		* q.0.
	e liver	- 199 - 1994 			
18-6 T		ন			
ENIC POT		3	(A BAR	0191 V	
CAMP F	Lat a to		Galaxies 2002	2011/22/21-44 14	
		- 64			1.28%
fulations f					
i ka ka sa	• P	Hak wang Mil	6	1900	
1 104 -	01:	1321-23-44	NIC .	#11070	Calaia

Figure 9-63 ARP Spoofing Prevention Window

The fields that can be configured for ARP Spoofing Prevention Logging State are described below:

Parameter	Description
ARP Spoofing Prevention Logging State	Select to enable or disable the ARP spoofing logging state here.

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

The fields that can be configured for **ARP Spoofing Prevention** are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Gateway IP	Enter the gateway's IP address used here.
Gateway MAC	Enter the gateway's MAC address used here.

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

BPDU Attack Protection

This window is used to view and configure the BPDU attack protection settings. In generally, there are two states in the BPDU attack protection function. One is normal state, and another is under attack state. The under attack state have three modes: drop, block, and shutdown. A BPDU protection enabled port will enter an under attack state when it receives one STP BPDU packet and it will take action based on the configuration. Thus, BPDU protection can only be enabled on the STP-disabled port.

BPDU protection has a higher priority than the FBPDU setting configured by configure STP command in the determination of BPDU handling. That is, when FBPDU is configured to forward STP BPDU but BPDU protection is enabled, then the port will not forward STP BPDU.

BPDU protection also has a higher priority than the BPDU tunnel port setting in determination of BPDU handling. When a port is configured as a BPDU tunnel port for STP, it will forward STP BPDU but if the port is BPDU protection enabled, the port will not forward STP BPDUs.

en al vers a versa e la Referencia managen es		Sec.	is more a Concernent						1
FIRE STACK (WANTERS F	e series								
041	FundPed.		3#Emi		59(9)		Note:		
[V]	et (0.0	191	wh1001	19 C	Costled	×	Station	×	(. Yada
Unit Status			5354.0		1.11			111	
Frei			Skie			Mode		11	Baran.
(A160	53		Durinket -		· ·	Stables			Nera:
10.000			1 Distance			States			Sec. a.
0.005	6		12 Added			58. at A. in			Alt in
0.08			17-2-8-8			287 at 5 at			Wexas
(30e			Developed			ST. if it an			WEITER
11116			1 sparana			Station			WITE
anter-			(chánha			. 81.01000			1417140
279.15.49	6		10,520,990			81.030	22		Witte
er010			1 (dictance			St. annor			serra.
10110			1.333044			St. Baller	10		WITH.

To view the following window, click **Security > BPDU Attack Protection**, as shown below:

Figure 9-64 BPDU Attack Protection Window

Parameter Description **BPDU Attack Protection** Select to enable or disable the BPDU attack protection feature's State global state here. **BPDU Attack Protection Trap** Select to enable or disable the BPDU attack protection feature's State trap state here. Unit Select the switch unit that will be used for this configuration here. From Port / To Port Select the appropriate port range used for the configuration here. State Select to enable or disable the BPDU attack protection feature's state on the port(s) specified. Select the BPDU attack protection feature's mode that will be Mode applied to the port(s) specified. Options to choose from are:

The fields that can be configured are described below:

Parameter	Description
	 Drop - Drop all received BPDU packets when the port enters under attack state. Block - Drop all packets (include BPDU and normal packets) when the port enters under attack state. Shutdown - Shut down the port when the port enters under attack state.

MAC Authentication

This window is used to view and configure the MAC authentication settings. MAC authentication is a feature designed to authenticate a user by MAC address when the user is trying to access the network via the Switch. The Switch itself can perform the authentication based on a local database or be a RADIUS client and perform the authentication process via the RADIUS protocol with a remote RADIUS server.

To view the following window, click **Security > MAC Authentication**, as shown below:

AL: Authentication						
A.C. Antheretication Global Settings						
NACIONAL CONTRACTOR OF A		o tire and				
NPC Action loads that that	CLEANING 9	o Cuadra				
AC Astheric des Cavillans and	Personward Sala agu					
umishne Mainn	liveo 🖉	Canvest .	MAL.	_ ∃ever ⊻	near.	706.4
Del calendario e un sorrige						
	tat Cal	BD		and a		
1	1000 (V	arts18001	~	Tushled .		2016
1	(P (1))				Sldg	
	23/4/1				110000	
	11110				1000	
	10110-02				I HIGHLAN	
	and west				KAD WI	
	ICROMM ¹				10.00 (91	
eu ()				inverse)		
	ano 60				Technik I.	
	6701415				Disk wy	
	1001030				Tripple for	

Figure 9-65 Port Security Global Settings Window

The fields that can be configured for **MAC Authentication Global Settings** are described below:

Parameter	Description
MAC Authentication State	Select to enable or disable the MAC authentication feature's global state.
MAC Authentication Trap State	Select to enable or disable the MAC authentication feature's trap state.

The fields that can be configured for **MAC Authentication User Name and Password Settings** are described below:

Parameter	Description
User Name	Enter the username used for MAC authentication here. This name can be up to 16 characters long. Tick the Default option to restore the username to the client's MAC address here.
Password	Enter the password used for MAC authentication here. Tick the Encrypt option save this password in the encrypted form. Tick the Default option to restore the password to the client's MAC address here.

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

The fields that can be configured for MAC Authentication Port Settings are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable MAC authentication for the port(s) specified here.

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

Web-based Access Control

Web-based Access Control (WAC) is a feature designed to authenticate a user when the user is trying to access the Internet via the Switch. The authentication process uses the HTTP or HTTPS protocol. The Switch enters the authenticating stage when users attempt to browse Web pages (e.g., http://www.dlink.com) through a Web browser. When the Switch detects HTTP or HTTPS packets and this port is unauthenticated, the Switch will launch a pop-up user name and password window to guery users. Users are not able to access the Internet until the authentication process is passed.

The Switch can be the authentication server itself and do the authentication based on a local database, or be a RADIUS client and perform the authentication process via the RADIUS protocol with a remote RADIUS server. The client user initiates the authentication process of WAC by attempting to gain Web access.

D-Link's implementation of WAC uses a virtual IP that is exclusively used by the WAC function and is not known by any other modules of the Switch. In fact, to avoid affecting a Switch's other features, WAC will only use a virtual IP address to communicate with hosts. Thus, all authentication requests must be sent to a virtual IP address but not to the IP address of the Switch's physical interface.

Virtual IP works like this, when a host PC communicates with the WAC Switch through a virtual IP, the virtual IP is transformed into the physical IPIF (IP interface) address of the Switch to make the communication possible. The host PC and other servers' IP configurations do not depend on the virtual IP of WAC. The virtual IP does not respond to any ICMP packets or ARP requests, which means it is not allowed to configure a virtual IP on the same subnet as the Switch's IPIF (IP interface) or the same subnet as the host PCs' subnet.

As all packets to a virtual IP from authenticated and authenticating hosts will be trapped to the Switch's CPU, if the virtual IP is the same as other servers or PCs, the hosts on the WAC-enabled ports cannot communicate with the server or PC, which really own the IP address. If the hosts need to access the server or PC, the virtual IP cannot be the same as the one of the server or PC. If a host PC uses a proxy to access the Web, to make the authentication work properly the user of the PC should add the virtual IP to the exception of the proxy configuration. Whether or not a virtual IP is specified, users can access the WAC pages through the Switch's system IP. When a virtual IP is not specified, the authenticating Web request will be redirected to the Switch's system IP.

The Switch's implementation of WAC features a user-defined port number that allows the configuration of the TCP port for either the HTTP or HTTPS protocols. This TCP port for HTTP or HTTPs is used to identify the HTTP or HTTPs packets that will be trapped to the CPU for

authentication processing, or to access the login page. If not specified, the default port number for HTTP is 80 and the default port number for HTTPS is 443. If no protocol is specified, the default protocol is HTTP.

The following diagram illustrates the basic six steps all parties go through in a successful Web Authentication process:



Figure 9-66 RADIUS Authentication Server

Conditions and Limitations

- If the client is utilizing DHCP to attain an IP address, the authenticating VLAN must provide a DHCP server or a DHCP relay functions so that client may obtain an IP address.
- Certain functions exist on the Switch that will filter HTTP packets, such as the Access Profile function. The user needs to be very careful when setting filter functions for the target VLAN, so that these HTTP packets are not denied by the Switch.
- If a RADIUS server is to be used for authentication, the user must first establish a RADIUS Server with the appropriate parameters, including the target VLAN, before enabling Web Authentication on the Switch.

Web Authentication

This window is used to view and configure the Web authentication settings.

To view the following window, click **Security > Web-based Access Control > Web Authentication**, as shown below:

To Hereita and Tanana			(Leev)
Carbon & Dansac	0.000.002	20 AUG 11 11	
Conversion of the local sector	VIPAL WA		
TX DOD	Didenti(4/9-3	13000	his has a
	Carolec & Data	C Dataset	C Tables & Datast Viras via (2011)

Figure 9-67 Port Security Global Settings Window

Parameter	Description
Web Authentication State	Select to enable or disable the Web authentication feature's global state.
Trap State	Select to enable or disable the Web authentication feature's trap state.
Virtual IPv4	Enter the virtual IPv4 address used here. The virtual IP of Web authentication is just the characterization of the Web authentication function on the Switch. All Web authentication processes communicate with this IP address, however, the virtual IP does not respond to any ICMP packet or ARP request. Therefore, it's not allowed to configure virtual IP in the same subnet as the Switch's IP interface or the same subnet as the host PCs' subnet, otherwise the Web authentication cannot operate correctly. The defined URL only takes effect when the virtual IP address is configured. The users get the FQDN URL stored on the DNS server to get the virtual IP address. The obtained IP address must match the virtual IP address configured by the command. If the IPv4 virtual IP is not configured, the IPv4 access cannot start a Web authentication.
Virtual IPv6	Enter the virtual IPv6 address used here. If the IPv6 virtual IP is not configured, the IPv6 access cannot start a Web authentication.
Virtual URL	Enter the virtual URL used here. This URL can be up to 128 characters long.
Redirection Path	Enter the redirection path here. This path can be up to 128 characters long.

The fields that can be configured are described below:

WAC Port Settings

This window is used to view and configure the WAC port settings.

To view the following window, click Security > Web-based Access Control > WAC Port Settings,
as shown below:

inder From details	ogie -				
of the second se					
-	FastNt.	Tartel	Sec.		
1 - E	and the set of the	which [m]	Dearbox (#		Apple
	896			2000	_
	100 A	102		Cricke	
2	10766	2		Second.	
	A.44			C.A.A.	
	Minio-	400		C (Mined	
	in the second	6 ()		20.000	
	10 AV			(C)4(4)	
	67.0	<u>10</u>		Drib H	
1	10.0	s1		Turning .	
	A.40			C. 4.4	
	15 15	21/i		District	
	All the factor	4		CAMPAR .	
	(4.7a)	1		COLANA.	
	18-14-	1.		Cristeet	
	APPER A	ja -		a for include	
	24 Set			Children -	
	dt 161	8		Cristian	
	MOTO IN	11 · · · · · · · · · · · · · · · · · ·		LUNCING	
	10.147	¥		11.414	
	11.11	8		Crister	
	MC 4.72	5		Lincat .	
	a 1477	0.0		the dead	
	d 4/2	d);		Cridint .	
	60110.12	42		C.) screp	
	la sele	¢.		10.010	
	1 1/2			Codevil	
	W 6/2			0.110.40	

Figure 9-68 WAC Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the WAC feature on the port(s) specified.

WAC Customize Page

This window is used to view and configure the WAC customized login page.

To view the following window,	click Security >	> Web-based Access Cor	trol > WAC Customize
Page, as shown below:			

WAC Customize Page				
	HOME IN THE RELEASE	est man nite konstration.		
	Current Stature Un	Automostor		
	Authentication Logis			
	User Same			
	Research			
		False	Circa.	
	Logent From The Balwark			
			Linguist .	
	Notification			
				Set to Defect: Apply

Figure 9-69 WAC Customize Page Window

The fields that can be configured are described below:

Parameter	Description
Page Title	Enter a custom page title message here. This message can be up to 128 characters long.
Login window Title	Enter a custom login window title here. This title can be up to 64 characters long.
User Name Title	Enter a custom username title here. This title can be up to 32 characters long.
Password Title	Enter a custom password title here. This title can be up to 32 characters long.
Logout window Title	Enter a custom logout window title here. This title can be up to 64 characters long.
Notification	Enter additional information to display in the notification area here. This information can be up to 128 characters long for each line. There a 5 lines available for additional information.

Click the Set to Default button to replace the information with the default information.

Japanese Web-based Access Control

JWAC Global Settings

This window is used to view and configure the Japanese Web-based Access Control (JWAC) global settings.

To view the following window, click **Security > Japanese Web-based Access Control > JWAC Global Settings**, as shown below:

INNA Globar Settings					
BACKS SAMENE AND AND					
www.comme	1: HOME (41)	elected in the second			2p.ek
MAX: NEW JP					
Liver long	- Sector	·	and a week	P/P	
11.6.20	Pes	-	Artik en (1)		1
Post of mail	20161		m +3.4	E 1400 E	í í
Rec. C. Dr. Bull	which age to	2 m	And Cuby This (C. C)	1.]e/ loovee
Departmenting Server Settlege					
$T_{\rm M} := A \mathcal{O} \mathbb{R} \mathcal{R} \mathbb{R}$		- Daabled	E m	P. A. I.	
Enders Server Sellings					
and seven the second	Co.A. CHILLS	- ii	Net the car the left desire	A. 2017-00	1
For (1452).7		31707 (1500			14
Telal Courses 1					
Vister	and P	NCP Part	MIP Por		
12	6.30/10	7			- In t

Figure 9-70 JWAC Global Settings Window

The fields that can be configured for **JWAC Global Settings** are described below:

Parameter	Description
JWAC State	Select to enable or disable the JWAC feature's global state here.

Click the Apply button to accept the changes made.

The fields that can be configured for JWAC Settings are described below:

Parameter	Description
UDP Filtering	Select to enable or disable UDP filtering here.
Authentication Method	Select the authentication method used here. Options to choose from are MD5 , CHAP , PAP , MS-CHAP , and MS-CHAP-v2 .
Virtual IP	Select the virtual IP option used here. Options to choose from are IPv4, IPv6, and URL.
IPv4 Address	After selecting IPv4 as the Virtual IP , the following field will be available. Enter the virtual IPv4 address used here. All JWAC authentication processes communicate with this IP address, however, the virtual IP does not respond to any ICMP packets or ARP requests. Therefore, it's not allowed to configure virtual IP in the same subnet as the switch's IP interface or the same subnet as the host PCs' subnet, otherwise JWAC authentication cannot operate correctly.
	The defined URL only takes effect when the virtual IP address is configured. The users get the FQDN URL stored on the DNS

Parameter	Description
	server to get the virtual IP address. The obtained IP address must match the virtual IP address configured by the command. If the IPv4 virtual IP is not configured, the IPv4 access cannot start JWAC authentication.
IPv6 Address	After selecting IPv6 as the Virtual IP , the following field will be available. Enter the virtual IPv6 address used here. If the IPv6 virtual IP is not configured, the IPv6 access cannot start a JWAC authentication.
Virtual URL	After selecting URL as the Virtual IP , the following field will be available. Enter the virtual URL used here.
Forcible Logout	Select to enable or disable the forcible logout option here. When the forcible logout feature is enabled, a ping packet from an authenticated host to the JWAC switch with a TTL of 1 and a destination IP the same as virtual IP will be regarded as a logout request and the host will be moved back to unauthenticated state.
Redirect State	Select to enable or disable the redirection state here. When redirect is enabled, all Web access is redirected to the quarantine server or JWAC login page.
Redirect Destination	Select the redirect destination here. Options to choose from are Quarantine Server and JWAC Login Page . When redirecting to the quarantine server, the unauthenticated host will be redirected to the quarantine server when it tries to access a random URL. When redirecting to the JWAC login page, the unauthenticated host will be redirected to the JWAC login page in the switch to finish authentication. When redirecting to the quarantine server is specified, a quarantine server must be configured first before enabling the JWAC function globally. When redirect is disabled, all Web access is denied except for access to the quarantine server or JWAC login page.
Redirect Delay Time	Enter the redirect delay time value here. This value must be between 0 and 10 seconds. By default, this value 1 second.

The fields that can be configured for **Quarantine Server Settings** are described below:

Parameter	Description
Timeout	Enter the quarantine server's timeout value here. This value must be between 5 and 300 seconds. By default, this value is 30 seconds.
Monitor	Select to enable or disable the monitor option here. When the JWAC quarantine server monitor feature is enabled, the JWAC switch will monitor the quarantine server to ensure the server is okay. If the switch detects no quarantine server, it will redirect all unauthenticated HTTP accesses to the JWAC Login Page if the redirect option is enabled and the redirect destination is configured to be quarantine server.
URL	Select the whether the quarantine server uses an IPv4 or IPv6 address and enter the respective IP address in the space provided.

The fields that can be configured for Update Server Settings are described below:

Parameter	Description
IPv4 Network Prefix/Prefix Length	Enter the update server's IPv4 address and prefix length here. Any servers (like update.microsoft.com or some sites of Antivirus software companies, which ActiveX needs to access to accomplish the authentication before the client passes the authentication) should be added with its IP address or with the network address. By adding the network address, an entry can serve multiple update servers on the same network. Multiple update server addresses or network addresses can be configured.
IPv6 Network Prefix/Prefix Length	Enter the update server's IPv6 address and prefix length here.
Port	Enter the update server's port used here. This value must be between 1 and 65535. Also, select whether this port is a TCP or UDP port.

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 specified entry.

JWAC Port Settings

This window is used to view and configure the JWAC port settings.

To view the following window, click **Security > Japanese Web-based Access Control > JWAC Port Settings**, as shown below:

when when it								
	Crow Fast		176.251		Stark 1		Max Active desides Over (> 00)	
5	- Lann	[T]	(30)3/1	1	16.24.6	-1	100	deab
	Put		later.				Van Ainthemskaling Uiter	
	MP167		Circuites					
1	AND AND A		100.4603				- 0.0	
	di (0)		Distable d				100	
	48.064		ELMOND .					
1	(all (all (a)))		140,4603				0.4	
	ACC 1		Cr. 46. J				103	
	HP107		Enabled				-100	
	Margaret 1		(series)				1.4	
	9169		Clevinsky d				100	
	401001		Distilied					
	ARCH. 1		DOM: NO					
	101977		Dischief.				8.9	
	1000	1	Disched				100	
	Augusta 1		1001000				5.0	
	100000		Double 1				8.4	
	481611		Christed				0	
	AND NO.		Langerg				- 1941	
	10.0000	1	134, 66 (1)				5.4	
	481421		Disabled				10	
	ANTINUM -		LUCIONO				- 19.0	
	1000071		De da i				294	
	Naix's	1	Disatisd				100	
	40010,00		Lauracies a				- 10	
	1910220		Pariate 1				0.00	
	10103		Dischled				100	
	40111.0		LUUDIO					

Figure 9-71 JWAC Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select whether JWAC is enabled or disabled on the port(s) specified.
Max Authenticating User	Enter the maximum number of authentication users allowed here. This value must be between 1 and 100.

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

JWAC Customize Page Language

This window is used to view and configure the JWAC customize page's language.

To view the following window, click **Security > Japanese Web-based Access Control > JWAC Customize Page Language**, as shown below:

JWAC Customize Page Language		
Lawas caused an edge Language Caused as Mage Language (p) Hagina	🗇 тарана	2prob.



The fields that can be configured are described below:

Parameter	Description
Customize Page Language	Select the language option that will be used when the JWAC login page is displayed.

JWAC Customize Page

This window is used to view and configure the JWAC customize page settings.

To view the following window,	click Security >	Japanese Web-based	Access Control > JWAC
Customize Page, as shown b	elow:		

JWAC Customize Page	
	Carrier Blain Alt-Authoritics (Alter)
Aufternitzuten Louin	
UMPRATE	
Put and	
	Litter Vier
Lauru Fren Tie Ke	
	Lopout
Notification	
	Set to Defeale Apple

Figure 9-73 JWAC Customize Page (English) Window

Parameter	Description
Page Title	Enter a custom page title message here. This message can be up to 128 characters long.
Login window Title	Enter a custom login window title here. This title can be up to 64 characters long.
User Name Title	Enter a custom username title here. This title can be up to 32 characters long.
Password Title	Enter a custom password title here. This title can be up to 32 characters long.
Logout window Title	Enter a custom logout window title here. This title can be up to 64 characters long.
Notification	Enter additional information to display in the notification area here. This information can be up to 128 characters long for each line. There a 5 lines available for additional information.

The fields that can be configured are described below:

Click the Set to Default button to replace the information with the default information.

After changing the language to **Japanese** the JWAC customize page will look like this.

JWAC Custometize Page	
- ci-ci⊠ze-cr3: Zr3PrZr3,	
107 - Arig (21-07) /	
S.O	
Film	L Aw
<u>行力でない。</u> 	Topod
Notification	
	Red to Set out

Figure 9-74 JWAC Customize Page (Japanese) Window

Click the Set to Default button to replace the information with the default information.

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

Network Access Authentication

Guest VLAN

This window is used to view and configure the network access authentication guest VLAN settings.

To view the following window, click **Security > Network Access Authentication > Guest VLAN**, as shown below:

NO VERSION				
al bi	Deste: Jessan (e	fafed = V (V _ s)	+0++364 	25.00
	Fet		•D	
	6.54501		1.5	CHI HE

Figure 9-75 Guest VLAN Window

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
VID	Enter the VLAN ID used here. This value must be between 1 and 4094.

The fields that can be configured are described below:

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

Network Access Authentication Global Settings

This window is used to view and configure the network access authentication global settings.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Global Settings**, as shown below:

istaorii Access Authentica	tion Globel Settinge		_	_
indexe is Accurate Authoritization MA				
Sec.	Upprove v			
Idinia.	Del Series			
Delmfanker	2 ×			vgst/
constations				
an and the first of the	121			
ine area saw	Dicative 📃 😒			
una ana Star	<u>Find</u>			48.44
eer information				
re-serv	C.C.W.B	301(124-0)	-	1
"anteroid Type	Plain Text 📃 😒	Timesed	72 dien -	1 1. 4.40
Tend Extrine 1				
inter hundh	P M Sanda	Pression a spirit	South:	
liter		Twint-		Celete

Figure 9-76 Network Access Authentication Global Settings Window

The fields that can be configured for **Network Access Authentication MAC Format Settings** are described below:

Parameter	Description
Case	Select the case format that will be used for the network access authentication MAC address here. Options to choose from are Lowercase and Uppercase .
Delimiter	Select the delimiter that will be used for the network access authentication MAC address here. Options to choose from are Hyphen , Colon , Dot , and None .
Delimiter Number	Select the delimiter number option here. Options to choose from are 1 , 2 , and 5 .

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

The fields that can be configured for General Settings are described below:

Parameter	Description
Max Users	Enter the maximum amount of users allowed here. This value must be between 1 and 1000. By default, this option is 1000.
Deny MAC-Move	Select to enable or disable the deny MAC-move feature here. This option controls whether to allow authenticated hosts to do roaming across different switch ports and only controls whether a host, which is authenticated at a port set to the multi-authenticate mode is allowed to move to another port.

Parameter	Description
	If a station is allowed to move, there are two situations. It may need to be re-authenticated or directly moved to the new port without re- authentication based on the following rule. If the new port has the same authentication configuration as the original port, then re- authentication is not needed. The host will inherit the same authorization attributes with new port. The authenticated host can do roaming from port 1 to port 2, and inherit the authorization attributes without re-authentication. If the new port has the different authentication configuration as the original port, then re- authentication configuration as the original port, then re- authentication is needed. The authenticated host on port 1 can move and re-authenticated by port 2. If the new port has no authentication method enabled, then the station is directly moved to the new port. The session with the original port is removed. The authenticated host on port 1 can be moved to port 2. If this feature is disabled and an authenticated host moves to another port, then this is treated as a violation error.
Authorization State	Select to enable or disable the authorized state here. The option is used to enable or disable the acceptance of an authorized configuration. When authorization is enabled for authentication, the authorized attributes (for example VLAN, 802.1p default priority, bandwidth, and ACL) assigned by the RADIUS server will be accepted if the authorization status is enabled. Bandwidth and ACL are assigned on a per-port basis. If in the multi-authenticated mode, VLAN and 802.1p are assigned on a per-host basis. Otherwise, Bandwidth and ACL are assigned on a per-port basis.

The fields that can be configured for User Information are described below:	

Parameter	Description
User Name	Enter the user name used here. This name can be up to 32 characters long.
VID	Enter the VLAN ID used here.
Password Type	Select the password type option here. Options to choose from are Plain Text and Encrypted .
Password	Enter the password used here.

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

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

Network Access Authentication Port Settings

This window is used to view and configure the network access authentication port settings.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Port Settings**, as shown below:

N 8		Film Plot	158	ù.				
9		11 (10) ×	<u>eta</u>	ian lyr				
est sono i		W-1-9	100	iyani yani		History (11)	0 (B)	
unan 🖻)	- iei -	27,					
eriodic		Beilath Timer (145	(5)(5) inter	telly Class		inacity of Times	120-05125	
dae bed 👘 🔁		2620	et Ch	ealed 🖂			enc.	
white()-5552	8							
	28						1	April 1
ALCONTRACTOR								
tan karaadi Pirk	1knE%ak	WOUM	Cornshak Viele	Man User-	Pakdk	Sectoria.	hasa iz Tina	Desar.
and the second se	and the second second second second second	and includes the second second	and the second state of th	and the second	a second s	and the second se	basis iz Tina Do Inst	Denar. I C
Part	1 km i Node	and includes the second second	Constant Pade	Map User-	Pakik	tekali.	THE REPORT OF THE REPORT OF THE	
Fait Faith	The Date	and includes the second second	Cornschath Made The The	Max Users	Paide	takali Am	Dir Amer	10
tas 1021 ruty	Hon Mark Mark 1 da Mark 1 da	and the state of the	Complete Vede The The	Max Ulary 19-2	Puikile Council Council	Robull A M A M	De Anet De Anet	12 12
200 2012/1 2012/1 2012/2 2012/2	Haitikak Sola tak Sola tak Sola tak	and the state of the	Cornolath Mode Tai Tai Tai	Bat Uary 194 195 195	Peterle Cruziere Chastes	Soluti A U A U A U	te and te and teans	10 10 12
Pat Foto Foto Foto Foto	Hori Made to de trats to de trats to de trats to de trats to de trats	and the state of the	Corpolat Pede Ta Te Te Te Te	Het Urers 19-5 19-5 19-5 19-5 19-5	Puriodie Forzanie Forzanie Chroska Chroska	total a.e. a.e. a.e. a.e. a.e. a.e. a.e. a.	tik diser Hefdrach Ethebiach Ethebiach	10 10 40 61
Fail Former Form	Heri Made Nama an Nama an Nama an Nama an Nama an	and the state of the	Corpolat Vede Ta Te Pe Pe Ag Ag	Use Uses 19-5 19-5 19-5 19-5 19-5 19-5 19-5 19-5	Protodos Francis Francis Chasted Chasted Chasted Chasted	Tobali A II A II A II A II A II A II A II A I	De Aner De Aner Exerner Do abad Dr Alvad	10 10 14 15 15
2015 1012 11 1011 12 1011 12 1011 12 1011 12 1011 12 1011 12 1011 12 1011 12 1011 12 1011 12 10 10 10 10 10 10 10 10 10 10 10 10 10	Heri Mode Solita Alas Solita Alas Molt Alas Solita das Solita das Solita das	and the state of the	Corpolat Vede Tar Pie Pie Pie Pie Pie Pie Pie Pie Pie	Use Users 1915 1915 1926 1921 1921 1921 1921	Protectors Frances Charakes Charakes Charakes Charakes Charakes Charakes	tokuli a.u. a.u. a.u. a.u. a.u. a.u. a.u. a.u	De Anen De Anen Etraphen Disabad Disabad Disabad Disabad	21 21 24 25 25 26 26
***** **** **** **** **** ****	The Disk Color Color Color Color Color Color Color Color Color Color Color Color Color Color Color Color Color	and the state of the	Corpolat Vede Tar Pie Pie Pie Pie Pie Tar Tar	Use Users 1915 1915 1920 1920 1920 1920 1920 1920 1920	Protects Constant Constant Constant Constant Constant Constant Constant Constant	tokal 4.8 4.8 2.0 2.0 2.0 2.0 2.0 2.0 2.0 2.0 2.0 2.0	De Aner De Aner De aner De aber De aber De aber	10 14 44 40 41 47 47



The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Host Mode	Select the host mode option that will be associated with the selected port(s) here. Options to choose from are Multi Host and Multi Auth . If the port is operated in the multi-host mode, and if one of the hosts is authenticated, then all other hosts are allowed to access the port. According to 802.1X authentication, if the re-authentication fails or the authenticated user logs off, the port will be blocked for a quiet period. The port restores the processing of EAPOL packets after the quiet period. If the port is operated in the multi-authenticated mode, then each host needs to be authenticated individually to access the port. A host is represented by its MAC address. Only the authorized host is allowed to access.
VID List	After selecting the Multi Auth option as the Host Mode , the following parameter is available. Enter the VLAN ID used here. This is useful when different VLANs on the Switch have different authentication requirements. After the client is authenticated, the client will not be re-authenticated when received from other VLANs. This option is useful for trunk ports to do per-VLAN authentication control. When a port's authentication mode is changed to multi- host, the previous authentication VLAN(s) on this port will be cleared.
CompAuth Mode	Select the compound authentication mode option here. Options to choose from are:

Parameter	Description	
	 Any - Specifies that if any of the authentication method (802.1X, MAC-based Access Control, WAC, or JWAC) to passes, then passes. MAC-JWAC - Specifies to verify MAC-based authentication first. If the client passes, JWAC will be verified next. Both authentication methods need to be passed. MAC-WAC - Specifies to verify MAC-based authentication first. If the client passes, WAC will be verified next. Both authentication methods need to be passed. 	
Max Users	Enter the maximum users value used here. This value must be between 1 and 1000.	
Periodic	Select to enable or disable periodic re-authentication for the selected port here. This parameter only affects the 802.1X protocol.	
ReAuth Timer	Enter the re-authentication timer value here. This value must be between 1 and 65535 seconds. By default, this value is 3600 seconds.	
Inactivity State	Select to enable or disable the inactivity state here.	
Inactivity Timer	When the Inactivity State is enabled, enter the inactivity timer value here. This value must be between 120 and 65535 seconds. This parameter only affects the WAC and JWAC authentication protocols.	
Restart	Enter the restart time value used here. This value must be between 1 and 65535 seconds.	

Network Access Authentication Sessions Information

This window is used to view and clear the network access authentication session information.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Sessions Information**, as shown below:

507	13 000 3	Cast in Ref. But
MAND THE MAN	PICE PROFILE	Jurkanie ka
10.00	1944C A	Line of Sales a feet
1 - Sec		shunding says
Attantication Sessions Total		
Total Authenticative Health	5	
COMPANY DESCRIPTION OF ADDRESS	3 * 2	
Tomi Bioched Hoth		

Figure 9-78 Network Access Authentication Sessions Information Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the appropriate switch unit and port used for the query here.
MAC Address	Enter the MAC address used here.

Parameter	Description
	Select the protocol option used here. Options to choose from are MAC , WAC , JWAC , and DOT1X .

Click the Clear by Port button to the clear the information based on the port selected.

Click the **Clear by MAC** button to the clear the information based on the MAC address entered.

Click the Clear by Protocol button to the clear the information based on the protocol selected.

Click the **Clear All** button to clear all the information in this table.

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

Click the View All button to locate and display all the entries.

Safeguard Engine

Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP Storm) or other methods. These attacks may increase the switch's CPU load beyond its capability. To alleviate this problem, the Safeguard Engine function was added to the Switch's software.

The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth.

If the CPU load rises above the rising threshold value, the Safeguard Engine function will be activated and the Switch will enter the exhausted mode. In the exhausted mode, the Switch will limit the bandwidth available for ARP and broadcast IP packets. If the CPU load falls below the falling threshold value, the Safeguard Engine will be deactivated and the Switch will exit the exhausted mode and enter the normal mode.

Packets that are destined to the CPU can be classified into three groups. These groups, otherwise known as sub-interfaces, are logical interfaces that the CPU will use to identify certain types of traffic. The three groups are **Protocol**, **Manage**, and **Route**. Generally, the **Protocol** group should receive the highest priority when the Switch's CPU processes received packets and the **Route** group should receive the lowest priority as the Switch's CPU usually does get involved in the processing of routing packets. In the **Protocol** group, packets are protocol control packets identified by the router. In the **Manage** group, packets are destined to any router or system network management interface by means of interactive access protocols, like Telnet and SSH. In the **Route** group, packets are identified as traversing routing packets that is generally processed by the router CPU.

Protocol Name	Sub-interface (Group)	Description
802.1X	Protocol	Port-based Network Access Control
ARP	Protocol	Address resolution Protocol (ARP)
DHCP	Protocol	Dynamic Host Configuration Protocol
DNS	Protocol	Domain Name System
GVRP	Protocol	GARP VLAN Registration Protocol
ICMPv4	Protocol	Internet Control Message Protocol
ICMPv6-Neighbor	Protocol	IPv6 Internet Control Message Protocol Neighbor Discovery Protocol (NS/NA/RS/RA)
ICMPv6-Other	Protocol	IPv6 Internet Control Message Protocol except Neighbor Discovery Protocol (NS/NA/RS/RA)
IGMP	Protocol	Internet Group Management Protocol
LACP	Protocol	Link Aggregation Control Protocol

In the following table a list of supported protocols are displayed with their respective sub-interfaces (groups):

DGS-1510 Series Gigabit Ethernet SmartPro Switch Web UI Reference Guide

Protocol Name	Sub-interface (Group)	Description
SNMP	Manage	Simple Network Management Protocol
SSH	Manage	Secure Shell
STP	Protocol	Spanning Tree Protocol
Telnet	Manage	Telnet
TFTP	Manage	Trivial File Transfer Protocol
Web	Manage	Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS)

A customized rate limit (in packets per second) can be assigned to the Safeguard Engine's subinterfaces as a whole or to individual protocols specified by the user in the management interface. Be careful when customizing the rate limit for individual protocols, using this function, as improper rate limits can cause the Switch to process packets abnormally.



NOTE: When Safeguard Engine is enabled, the Switch will allot bandwidth to various traffic flows (ARP, IP) using the FFP (Fast Filter Processor) metering table to control the CPU utilization and limit traffic. This may limit the speed of routing traffic over the network.

Safeguard Engine Settings

This window is used to view and configure the safeguard engine settings.

To view the following window, click **Security > Safeguard Engine > Safeguard Engine Settings**, as shown below:

Sabiguard Copine Settings		
Sufeguerd Cogleo Sectory		
Selepted Orgine State	Li sabled 🔜	
Trez Sara	L'added 😿	
Single and specific and states	6.500.00	
CHILDRADOS ARDIDE		
August 19 (2016) 2016 - 100%	pu 4	11
Culley Treate & 20% - 100%	(XX) (V)	



The fields that can be configured for Safeguard Engine Settings are described below:

Parameter	Description
Safeguard Engine State	Select to enable or disable the safeguard engine feature here.
Trap State	Select to enable or disable the safeguard engine trap state here.

The fields that can be configured for CPU Utilization Settings are described below:

Parameter	Description
Rising Threshold	Enter the rising threshold value here. This value must be between 20% and 100%. This value is used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level,

Parameter	Description
	the Switch will move into Exhausted mode, based on the parameters provided in this window.
Falling Threshold	Enter the falling threshold value here. This value must be between 20% and 100%. This value is used to configure the acceptable level of CPU utilization as a percentage, where the Switch leaves the Safeguard Engine state and returns to normal mode.

CPU Protect Counters

This window is used to view and clear the CPU protection counter information.

To view the following window, click **Security > Safeguard Engine > CPU Protect Counters**, as shown below:

GPU Protect Counter		
Charles a Product row among		
é esteres	Visip 🐨	
An evaluation from the	ana transfer a	dear dear of

Figure 9-80 CPU Protect Counters Window

The fields that can be configured are described below:

Parameter	Description
Sub Interface	Select the sub-interface option here. Options to choose from are Manage , Protocol , Route , and All . This option specifies to clear the CPU protect related counters of sub-interfaces.
Protocol Name	Select the protocol name option here. Options to choose from are DHCP, ARP, DNS, GVRP, ICMPv4, ICMPv6-Neighbor, ICMPv6-Other, IGMP, LACP, SNMP, SSH, STP, Telnet, TFTP, Web, 802.1X, and All.

Click the **Clear** button to clear the information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

CPU Protect Sub-Interface

This window is used to view and configure the CPU protection sub-interface settings.

To view the following window, click **Security > Safeguard Engine > CPU Protect Sub-Interface**, as shown below:

the indication and	040			
e a la versor	Horys 5	+301004(\$10.9)	par Plan an	Lesk.
a peries here	and a second			
	Naras 🔄			The sector
				100 C
Sala Lindi	124 am			
Televiumit	Dien 101	(m)		i.

Figure 9-81 CPU Protect Sub-Interface Window

The fields that can be configured for **CPU Protect Sub-Interface** are described below:

Parameter	Description
Sub-Interface	Select the sub-interface option here. Options to choose from are Manage , Protocol , and Route .
Rate Limit	Enter the rate limit value used here. This value must be between 0 and 1024 packets per second. Tick the No Limit option to disable the rate limit.

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

The fields that can be configured for **Sub-Interface Information** are described below:

Parameter	Description
Sub-Interface	Select the sub-interface option here. Options to choose from are Manage , Protocol , and Route .

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

CPU Protect Type

This window is used to view and configure the CPU protection type settings.

To view the following window, click **Security > Safeguard Engine > CPU Protect Type**, as shown below:

- 2000 - Contraction - Contrac	10.4	washington and a second	part if Sector	2000 C 2000
Automotive Status	10.4. 15	Contraction (see a los	for a second	Ar Sh
ona typersonan	sh i			
TELES SHEET	dia 🔄			Rect.
an Unit	EN on		and the second	

Figure 9-82 CPU Protect Type Window

The fields that can be configured for CPU Protect Type are described below:

Parameter	Description
Protocol Name	Select the protocol name option here. Options to choose from are DHCP, ARP, DNS, GVRP, ICMPv4, ICMPv6-Neighbor, ICMPv6-Other, IGMP, LACP, SNMP, SSH, STP, Telnet, TFTP, Web, and 802.1X.
Rate Limit	Enter the rate limit value used here. This value must be between 0 and 1024 packets per second. Tick the No Limit option to disable the rate limit.

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

The fields that can be configured for Protect Type Information are described below:

Parameter	Description
Protocol Name	Select the protocol name option here. Options to choose from are DHCP, ARP, DNS, GVRP, ICMPv4, ICMPv6-Neighbor, ICMPv6-

Parameter	Description
	Other, IGMP, LACP, SNMP, SSH, STP, Telnet, TFTP, Web, and 802.1X.

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

Trusted Host

This window is used to view and configure the trusted host settings.

To view the following window, click **Security > Trusted Host**, as shown below:

Trusted Host		_		
Traded Had				
ACT NAMES	D' D'AN	1790	Toles	- Apple
Source: The first shared	er of ACL name must be	a inters		
Lotal Electron 1				
Tap			ACL Name	
Tsine	d.		Ofernetwork PAACE	Delete

Figure 9-83 Trusted Host Window

Parameter	Description
ACL Name	Enter the ACL name used here. This name can be up to 32 characters long.
Туре	Select the trusted host type here. Options to choose from are Telnet , SSH , Ping , HTTP , and HTTPS .

The fields that can be configured are described below:

Click the Apply button to accept the changes made.

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

Traffic Segmentation Settings

This window is used to view and configure the traffic segmentation settings. When the traffic segmentation forwarding domain is specified, packets received by the port will be restricted in Layer 2 packet forwarding to interfaces within the domain. When the forwarding domain of a port is empty, Layer 2 forwarding for packets received by the port is not restricted.

The traffic segmentation member list can be comprised of different interface types, for example port and port-channel in the same forwarding domain. If the interfaces specified by the command include a port-channel, all the member ports of this port-channel will be included in the forwarding domain.

If the forwarding domain of an interface is empty, then there is no restriction on Layer 2 forwarding of packets received by the port.

To view the following window, click **Security > Traffic Segmentation Settings**, as shown below:

offer segure	anatalog satalogis					
	Sarta: Leasn Je	Tared extext is the	Torrend unit 1 mil	Ton Forward Peri annun (al	To Forward Cod + 612 61 - 20	54 Case
kat 1 Kelor		100		2011/01/01/00/02/2		
	Vet			i arkistang begr		
1	401/6/16			HE1621	1.11	

Figure 9-84 Traffic Segmentation Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the receiving switch unit that will be used for this configuration here.
From Port / To Port	Select the receiving port range used for the configuration here.
Forward Unit	Select the forward switch unit that will be used for this configuration here.
From Forward Port / To Forward Port	Select the forward port range used for the configuration here.

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

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

Storm Control Settings

This window is used to view and configure the storm control settings.

To view the following window, click **Security > Storm Control Settings**, as shown below:

AND STATISTICS (Statistics of the state of	ownood.					
lao Sala	Nor I	-				- See
inini Tenno Polini						
0.540.581	E	(m)	(9.6 g. (9.280)	S Real	16 m al.	APP?
am Contri Port à	an spi					
ME C	Prote Part :	To Pari 1	127/09	Actor (Level Type)	erstern Xolensent	
<u>,</u> 101	10001 ×	[Booketiv	NAN V -PC V	3021-018 2041 (A.2)	Let I
		(SH		M		4007
va telka 11 Nat		9.ene	Action	AL - 10.4%	105 107 11	
			State of the last	Tinusiada	Durani	State 1
		803000		Webser	Cural	State And State
- enclose	; ¹	10000	0.04	Tincshold		100000
	5	N99129				EVEN.
สหรับ		Marketan Malanan				encia escua escua bacia
		Norman Vilian Urban			-	eneral escola
สหรับ		wysego Villow Origina Original	Grø.		-	encia escue escue textue
etv1127		Norman Validae Ordens Ordens Ordens Values	0w		-	ENTON ENTON ENTON ENTON ENTON ENTON
ents* .a.itt2		Nonica Valent Orbert Orbert Valent Orbert	Grø.		-	ENTER DATUR ERCOR ERCOR ERCOR ERCOR ERCOR
enter witte		wowich Value Orioat Discort Value Orioat Hare J	0w	* + +	-	8.97.97 5.97.97 8.85.99 8.85.99 8.85.95 8.85.95 8.85.95 8.87.95
ens: wits:		Warward Valuer Ordeat Dissourt Valuer Oracid Harward Valuer	0w		-	EVEN Derine Exclus Exclus Exclus Exclus Exclus Exclus Exclus Exclus Exclus
enter uniter		Warward Validar Ordeat Discord Validar Oracid Harwight Validar Harwight	0w	* + +		Everyon Barrino Barrino Barrino Barrino Barrino Barrino Barrino

Figure 9-85 Storm Control Settings Window

The fields that can be configured for Storm Control Trap Settings are described below:

Parameter	Description
Trap State	Select the storm control trap option here. Options to choose from are:
	 None - No traps are sent. Storm Occur - A trap notification is sent when a storm event is detected. Storm Clear - A trap notification is sent when a storm event is cleared. Both - A trap notification is sent when a storm event is detected or cleared.

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

The fields that can be configured for **Storm Control Polling Settings** are described below:

Parameter	Description	
Interval	Enter the interval value used here. This value must be between 5 and 600 seconds. By default, this value is 5 seconds.	
Retries	Enter the retries value used here. This value must be between 0 and 360. By default, this value is 3. Tick the Infinite option to disable this feature.	

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Туре	Select the type of storm attack that will be controlled here. Options to choose from are Broadcast , Multicast , and Unicast . When the action is configured as the shutdown mode, the unicast refers to both known and unknown unicast packets; that is, if the known and unknown unicast packets hit the specified threshold, the port will be shutdown. Otherwise, unicast refers to unknown unicast packets.
Action	 Select the action that will be taken here. Options to choose from are: None - Specifies not to filter the storm packets. Shutdown - Specifies to shut down the port when the value specified for rise threshold is reached. Drop - Specifies to discard packets that exceed the risen threshold.
Level Type	Select the level type option here. Options to choose from are PPS , Kbps , and Level .
PPS Rise	Enter the rise packets per second value here. This option specifies the rise threshold value in packets count per second. This value must be between 0 and 2147483647 packets per second. If the low PPS value is not specified, the default value is 80% of the specified risen PPS.
PPS Low	Enter the low packets per second value here. This option specifies the low threshold value in packets count per second. This value must be between 0 and 2147483647 packets per second. If the low PPS value is not specified, the default value is 80% of the specified risen PPS.

The fields that can be configured for **Storm Control Port Settings** are described below:

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

After selecting the Kbps option as the Level Type, the following parameters are available.

unit 👘	Fight Poll	Tr Cvil	Tax	Adke	Land Type	8029347.84 312142-8354271	10701 av. 10.214/00/04/0
1	with letters in the	athibit v	Crostcent [V]	Nove	v stor vi	100000000000000000000000000000000000000	Sat.

Figure 9-86 Storm Control (Kbps) Window

The fields that can be configured are described below:

Parameter	Description
KBPS Rise	Enter the rise KBPS value used here. This option specifies the rise threshold value as a rate of kilobits per second at which traffic is received on the port. This value must be between 0 and 2147483647 Kbps.
KBPS Low	Enter the low KBPS value used here. This option specifies the low threshold value as a rate of kilobits per second at which traffic is received on the port. This value must be between 0 and 2147483647 Kbps. If the low KBPS is not specified, the default value is 80% of the specified risen KBPS.

After selecting the Level option as the Level Type, the following parameters are available.

UNC .	Tran Pell	To Post	Tax	Ada	LondType	and Ban. 3. In C	-urve ion -many
1	v enter w	abiWi 💌	Crostcent [V]	Note v1	Level y	100000000	100000-

Figure 9-87 Storm Control (Level) Window

The fields that can be configured are described below:

Parameter	Description
Level Rise	Enter the rise level value used here. This option specifies the rise threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. This value must be between 0% and 100%.
Level Low	Enter the low-level value used here. This option specifies the low threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. This value must be between 0% and 100%. If the low level is not specified, the default value is 80% of the specified risen level.

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

DoS Attack Prevention Settings

This window is used to view and configure the Denial-of-Service (DoS) attack prevention settings. The following well-known DoS types, which can be detected by most switches:

- Land Attack: This type of attack involves IP packets where the source and destination address are set to the address of the target device. It may cause the target device to reply to itself continuously.
- **Blat Attack**: This type of attack will send packets with the TCP/UDP source port equal to the destination port of the target device. It may cause the target device to respond to itself.
- **TCP-Null:** This type of attack involves port scanning by using specific packets, which contain a sequence number of 0 and no flags.
- **TCP-Xmas:** This type of attack involves port scanning by using specific packets, which contain a sequence number of 0 and the Urgent (URG), Push (PSH), and FIN flags.
- **TCP SYN-FIN:** This type of attack involves port scanning by using specific packets, which contain SYN and FIN flags.
- TCP SYN SrcPort Less 1024: This type of attack involves port scanning by using specific packets, which contain source port 0 to 1023, and SYN flag.
- **Ping of Death Attack:** A ping of death is a type of attack on a computer that involves sending a malformed or otherwise a malicious ping to a computer. A ping is normally 64 bytes in size (many computers cannot handle a ping larger than the maximum IP packet size) which is 65535 bytes. The sending of a ping of this size can crash the target computer. Traditionally, this bug has been relatively easy to exploit. Generally, sending a 65536 byte ping packet is illegal according to networking protocol, but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash.
- **TCP Tiny Fragment Attack:** The Tiny TCP Fragment attacker uses IP fragmentation to create extremely small fragments and force the TCP header information into a separate packet fragment to pass through the check function of the router and issue an attack.
- All Types: All of above types.

To view the following window, click Security > DoS Attack Prevention Settings, as shown below:

	Intel cost Mittings			
Trap Calle	Dated	a		4.6
s <mark>s</mark> ättest menne	and a second			
DESTYCH SHREED				
PLINGABLE RETERION THE RATION		of a state grant for hard and sold and	a tigh prite at the s	VCT KAN 2017 Deptember 2018 -
**	seller.			
Seattle 1 5	Dep			
1	ins ispe		-12M	(2314)
54	1.913-01.92		14033860	ante -
1	- 10 A. 10		14-14-1	H.a.
	TOP IN		Disc dec	D a
	That we wanted		1.00.0 5000	ung
	ACCOUNTS OF SHE		tes dat	the state of the s
127	5-164, 74 June 10	84	Olive place	Dr.n.
			10001111000	And the set of
	Pagi di Lava Attao-		(Determine)	Drag.

Figure 9-88 DoS Attack Prevention Settings Window

The fields that can be configured for SNMP Server Enable Traps DoS Settings are described below:

Parameter	Description	
Trap State	Select to enable or disable the DoS attack prevention trap state here.	

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

The fields that can be configured for DoS Attack Prevention Settings are described below:

Parameter	Description	
DoS Type Selection	Tick the DoS type option that will be prevented here.	
State	Select to enable or disable the DoS attack prevention feature's global state here.	
Action	Select the action that will be taken when the DoS attack was detected here. The only option to select here is Drop .	

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

SSH

Secure Shell (SSH) is a program allowing secure remote login and secure network services over an insecure network. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH client) and the Switch (the SSH server) are as follows:

Create a user account with admin-level access using the User Accounts window. This is
identical to creating any other admin-level User Account on the Switch, including specifying a
password. This password is used to logon to the Switch, once a secure communication path
has been established using the SSH protocol.
- Configure the User Account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the SSH User Authentication Mode window. There are three choices as to the method SSH will use to authorize the user, which are Host Based, Password, and Public Key.
- Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH client and the SSH server, using the SSH Authentication Method and Algorithm Settings window.
- Finally, enable SSH on the Switch using the SSH Configuration window.

After completing the preceding steps, a SSH Client on a remote PC can be configured to manage the Switch using a secure, in band connection.

SSH Global Settings

This window is used to view and configure the SSH global settings.

To view the following window, click **Security > SSH > SSH Global Settings**, as shown below:

ase worker artifungs			
SNEDAVEN MITTINGE			
a Star Survey State	26.958.1	3	
CONSERVER Forth-C.S.S.	12		
Adde for any an Minda	92		
Automouting The rest (\$2.800)	03	. 101	
-Automatication (Automatication)	43.000	19646	
Alter Carcineter (C.D)	5.	The MC	

Figure 9-89 SSH Global Settings Window

Parameter	Description
IP SSH Server State	Select to enable or disable the SSH server's global state.
IP SSH Service Port	Enter the SSH service port number used here. This value must be between 1 and 65535. By default, this number is 22.
Authentication Timeout	Enter the authentication timeout value here. This value must be between 30 and 600 seconds. By default, this value is 120 seconds.
Authentication Retries	Enter the authentication retries value here. This value must be between 1 and 32. By default, this value is 3.

The fields that can be configured are described below:

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

Host Key

This window is used to view and generate the SSH host key.

To view the following window, click **Security > SSH > Host Key**, as shown below:

844	
201 · · ·	GENERAL CONTR
- 1889 (a. [1])	
82.45 (P., 2000 (C. 9)	
na Versiliaso «Streegescalessinessinessinessi	
	1887 (a) 1887 (a) 1847 (7, 1989) (31) 764

Figure 9-90 Host Key Window

The fields that can be configured for Host Key Management are described below:

Parameter	Description
Crypto Key Type	Select the crypto key type used here. Options to choose from are the Rivest Shamir Adleman (RSA) key type and the Digital Signature Algorithm (DSA) key type.
Key Modulus	Select the key modulus value here. Options to choose from are 360 , 512 , 768 , 1024 , and 2048 bit.

Click the Generate button to generate a host key based on the selections made.

Click the **Delete** button to remove a host key based on the selections made.

The fields that can be configured for Host Key are described below:

Parameter	Description
Crypto Key Type	Select the crypto key type used here. Options to choose from are the Rivest Shamir Adleman (RSA) key type and the Digital Signature Algorithm (DSA) key type.

SSH Server Connection

This window is used to view the SSH server connections table.

To view the following window, click Security > SSH > SSH Server Connection, as shown below:

SSII Server Connection				
SSIITable				
Total Finitias: 1				
50	Waster	Cipita	User 10	Cliveri, IP Addresia
Û	10 10	and 0.00 -city/innac-strail	a diniin	1170-108-192

Figure 9-91 SSH Server Connection Window

SSH User Settings

This window is used to view and configure the SSH user settings.

To view the following window, click **Security > SSH > SSH User Settings**, as shown below:

SUG eer Setdinge				
Unit filling	SC chara	Authenticator Method	answerd w	
5 m + 10	202.0144	He, No. 4	155. A. a.	
s Petakon		C PSSARAA	2011.1	Apply .
Total Environ: 1				
User Hare	Autoritation Period	terne .	How Henry	Boi P
12.00	Pasyvert			



The fields that can be configured are described below:

Parameter	Description
User Name	Enter the SSH user's username used here. This name can be up to 32 characters long.
Authentication Method	Select the authentication methods used here. Options to choose from are Password , Public Key , and Host-based .
Key File	After selecting the Public Key or Host-based option as the Authentication Method , enter the public key here.
Host Name	After selecting the Host-based option as the Authentication Method , enter the host name here.
IPv4 Address	After selecting the Host-based option as the Authentication Method , select and enter the IPv4 address here.
IPv6 Address	After selecting the Host-based option as the Authentication Method , select and enter the IPv6 address here.

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

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

SSL

Secure Sockets Layer (SSL) is a security feature that will provide a secure communication path between a server 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:

- Key Exchange: The first part of the cipher suite 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 server as they "exchange keys" in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
- 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) and the Advanced Encryption Standard (AES) to create the encrypted text.
- 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 three hash algorithms, MD5 (Message Digest 5), SHA (Secure Hash Algorithm), and SHA256.

These three parameters are uniquely assembled in four choices on the Switch to create a threelayered encryption code for secure communication between the server and the client. 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 or the Switch file system. The Switch supports TLS 1.0, TLS 1.1, and TLS 1.2. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to server.

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). 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. Currently, the Switch comes with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

SSL Global Settings

This window is used to view and configure the SSL feature's global settings.

SSL Global Settings		
55L Cicbal Settingy 201. Status	C Rusled & Divided	
Service Talky	C	Cop do
import File		
File Selvel.	Breeze (the life interview state state)	
Destination File Harre	32 share	digg dis
Note: You can access the File S	ystam pege to menege these imported films.	
- SAL Self Algueri Certificate		
Se Svipred Certificate		theorem of a

To view the following window, click Security > SSL > SSL Global Settings, as shown below:



The fields that can be configured for SSL Global Settings are described below:

Parameter	Description
SSL Status	Select to enable or disable the SSL feature's global status here.

Parameter	Description
-	Enter the service policy name here. This name can be up to 32 characters long.

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

The fields that can be configured for Import File are described below:

Parameter	Description
File Select	Select the file type that will be loaded here. Options to choose from are Certificate and Private Key . After selecting the file type, browse to the appropriate file, located on the local computer, by pressing the Browse button.
Destination File Name	Enter the destination file name used here. This name can be up to 32 characters long.

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

Click the **Generate** button in the **SSL-Self-signed Certificate** section to generate a new self-signed certificate, regardless if there is a built-in self-signed certificate or not. The certificate generated does not affect the user-downloaded certificates.



NOTE: The SSL self-signed certificate only supports self-signature RSA certificates with a key length of 2048 bits.

Crypto PKI Trustpoint

This window is used to view and configure the crypto PKI trust point settings.

To view the following window, click Security > SSL > Crypto PKI Trustpoint, as shown below:

lusiocint	2.000				and the	er bei
and and	201 are					
6 The Code to Task	jour powert	Terror.	pitter.			
The section state	94.367K3	1910	Level .	la:		- Apph
and Entropy 1.1						

Figure 9-94 Crypto PKI Trustpoint Window

The fields that can be configured are described below:
--

Parameter	Description
Trustpoint	Enter the name of the trust-point that is associated with the imported certificates and key pairs here. This name can be up to 32 characters long.
File System Path	Enter the file system path for certificates and key pairs here.
Password	Enter the encrypted password phrase that is used to undo encryption when the private keys are imported here. The password

Parameter	Description
	phrase is a string of up to 64 characters. If the password phrase is not specified, the NULL string will be used.
TFTP Server Path	Enter the TFTP server's path here.
Туре	Select the type of certificate that will be imported here. Options to choose from are:
	 Both - Specifies to import the CA certificate, local certificate, and key pairs. CA - Specifies to import the CA certificate only. Local - Specifies to import local certificate and key pairs only.

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 **Delete** button to remove the specified entry.

SSL Service Policy

This window is used to view and configure the SSL service policy settings.

To view the following window, click Security > SSL > SSL Service Policy, as shown below:



Figure 9-95 SSL Service Policy Window

Parameter	Description
Policy Name	Enter the service policy name here. This name can be up to 32 characters long.
Version	Select the TLS version that will be used here. Options to choose from are TLS 1.0 , TLS 1.1 , and TLS1.2 .
Session Cache Timeout	Enter the session cache timeout value used here. This value must be between 60 and 86400 seconds. By default, this value is 600 seconds.

The fields that can be configured are described below:

Parameter	Description
Secure Trustpoint	Enter the secure trust point's name here. This name can be up to 32 characters long.
Cipher Suites	Select the cipher suites that will be associated with this profile here.

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

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

Network Protocol Port Protection Settings

This window is used to display and configure the network protocol port protection settings.

To view the following window, click **Security > Network Protocol Port Protection Settings**, as shown below:



Figure 9-96 Network Protocol Port Protect Settings Window

The fields that can be configured are described below:

Parameter	Description
TCP Port Protect State	Select to enable or disable the TCP port network protocol protection function here.
UDP Port Protect State	Select to enable or disable the UDP port network protocol protection function here.

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

10. OAM

Cable Diagnostics DDM

Cable Diagnostics

The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.

To view the following window, click **OAM > Cable Diagnostics**, as shown below:

NUM TRADE SUPPA					
Sec.	PROFPEL	111223	TUPA		a
	en:11	<u> </u>	enter Enter		- Seed
Cold & Sectionity					Cipor All
Pat	Ton:	Line, States	Tri Radi	Calify La sub IN	the state of the s
			- 1013 103/170 det		
WHERE .	the exce-	A set Marcel	PAN 2.26 m 522		Test
		Contract Contract (Pair)	Pak 3 Dire 59		
			7 at 2 Cover at 204		
4132	1000/08/	LinkBurn			C nort
1.1.1.1.1	URB22E	1.4.0			2.000
OUTCOME.	104004	Low Oren .			7.654
APA: Is a	20.000	1.00/02/04			.Co.e
Altside	10000436-1	Lairflever	- +		L'ass.
HPADIT .	*C0006420-*	LinkDow	100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100		2.84
str 100	000466-1	Link Diam	14		2.007
2010/202	1000455	Lint.Down			C toor
i defindet	14.6788	Lat Day			Cherry

Figure 10-1 Cable Diagnostics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

Click the Test button to test the specific port.

Click the **Clear** button to clear all the information for the specific port.

Click the Clear All button to clear all the information in this table.

DDM

This folder contains windows that perform Digital Diagnostic Monitoring (DDM) functions on the Switch. There are windows that allow the user to view the digital diagnostic monitoring status of SFP modules inserting to the Switch and to configure alarm settings, warning settings, temperature

threshold settings, voltage threshold settings, bias current threshold settings, Tx power threshold settings, and Rx power threshold settings.

DDM Settings

The window is used to configure the action that will occur for specific ports when an exceeding alarm threshold or warning threshold event is encountered.

To view the following window, click **OAM > DDM > DDM Settings**, as shown below:

CM Settings				
the second writings				
term at an international terms (Advances	Date of Proper			
function that are function of the				144.9
				1.33
ON Stationer Gerings	1980.0			
Unit Tree Fast	Tofet	2644	Situation in	
1 10 1011	an 131	Einsbled im	Shakirun Alann m	
and 1 Swillings				
			Alat	
d 132		India:		R.
-6.4359	144	14- (d. (m))	210	

Figure 10-2 DDM Settings Window

Parameter	Description
Transceiver Monitoring Traps Alarm	Select this option to enable or disable sending alarm level trap.
Transceiver Monitoring Traps Warning	Select this option to enable or disable sending warning level trap.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Use the drop-down menu to enable or disable the DDM state.
Shutdown	Specify whether to shut down the port, when the operating parameter exceeds the Alarm or Warning threshold.
	 Alarm - Shutdown the port when the configured alarm threshold range is exceeded. Warning - Shutdown the port when the configured warning threshold range is exceeded. None - The port will never shutdown regardless if the threshold ranges are exceeded or not. This is the default.

The fields that can be configured are described below:

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

DDM Temperature Threshold Settings

This window is used to configure the DDM Temperature Threshold Settings for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Temperature Threshold Settings**, as shown below:

C	Peri	Action	Title	Viewie (* 199-127,9		
12	25000 C 20	au 1 <u>×</u>	Les Maren 11	8	inn X	-knoly
1 Glap						
10000120						
(1. 1 .)	One of the	Mark Alex	n (Cebeled 🔰 👘 👬	di Maning Debetari	Crow Manning (Coloring)	Los Mars (Orbits)
1.00 (100 (100))	Onriel 2004		niched He Bl	d Maning Telson. (4:00)	Constitution of the second s	Treadelines (Mekson) Totolik



The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Туре	Select the type of temperature threshold. Options to choose from are Low Alarm , Low Warning , High Alarm , and High Warning .
Value	Enter the threshold value. This value must be between -128 and 127.996 °C.

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

DDM Voltage Threshold Settings

This window is used to configure the DDM Voltage Threshold Settings for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Voltage Threshold Settings**, as shown below:

4 C	Pet	Action	Tree	Velvie (3-5.55)		
150	satest in the	2.0 12	Les More 1011	6 ()	1.40	de de
1000000						
2.2.1.	Ownet	16.4.5		Had Weiner 25	Los Wanter (V)	trasation (10)
COLUMN .	4.431		() II	2.16.00	2 (6)	2) 10
	2015		999	1400	23,900	100

Figure 10-4 DDM Voltage Threshold Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Туре	Select the type of voltage threshold. Options to choose from are Low Alarm, Low Warning, High Alarm, and High Warning.
Value	Enter the threshold value. This value must be between 0 and 6.55 Volt.

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

DDM Bias Current Threshold Settings

This window is used to configure the threshold of the bias current for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Bias Current Threshold Settings**, as shown below:

4 () (Pari	Action	Tree	Million (B-32)		
19	antest in the	2.6 12	Les More 1991	6	WA:	dealy.
12.50	Oasal			the particular of participants	nas Weinstein (* 1945 - 1	free the extent t
COLUMN .	2.84		101	(1) (III)	1.5	41.69 2.109
1.119.28	2281		280	12.400		172.00



Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Туре	Select the type of bias current threshold. Options to choose from are Low Alarm, Low Warning, High Alarm, and High Warning.
Value	Enter the threshold value. This value must be between 0 and 131 mA.

The fields that can be configured are described below:

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

DDM TX Power Threshold Settings

This window is used to configure the threshold of TX power for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM TX Power Threshold Settings**, as shown below:

	Ped	Actor	Tree	Cover Unit	Verue X-0.5235	
12	atura 🐼	0.8 I <u>N</u>	Location 111	el bro tell		vi. 🔜 skraty
191ap						
0.62.52						
i teto	Ownel	1911		LightWard to (1997)	Lase We along (saW)	Tax Alara (1966)
0.000	8167		19-0-1 19-0	1.61	-1.61	0.91
1.112.28	8,901		100	1.276	(38	1.141



The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Туре	Select the type of TX power threshold. Options to choose from are Low Alarm, Low Warning, High Alarm, and High Warning.
Power Unit	Select the power unit here. Options to choose from are mW and dBm .
Value	Enter the threshold value. When selecting mW in the Power Unit drop-down list, this value must be between 0 and 6.5535. When selecting dBm in the Power Unit drop-down list, this value must be between -40 and 8.1647.

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

DDM RX Power Threshold Settings

This window is used to configure the threshold of RX power for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM RX Power Threshold Settings**, as shown below:

i Step	ninen 😿	Polar Anno 192	Tran contribute (1997)	zi lov ly	Verve X-6.5335 Let	i Araty
tel.	0.0101	- Age Al		Light Warman (1997)	Lase Weining (LaW)	LawAtan 2 Mil
CONTRACT.	0.43		1.8	1.79	-1.10	a (46)
1.113.78	8,980		1.1	(214)	0.305	R.O.W

Figure 10-7 DDM RX Power Threshold Settings Window

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Туре	Select the type of RX power threshold. Options to choose from are Low Alarm, Low Warning, High Alarm, and High Warning.
Power Unit	Select the power unit here. Options to choose from are mW and dBm .
Value	Enter the threshold value. When selecting mW in the Power Unit drop-down list, this value must be between 0 and 6.5535. When selecting dBm in the Power Unit drop-down list, this value must be between -40 and 8.1647.

The fields that can be configured are described below:

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

DDM Status Table

This window is used to display the current operating digital diagnostic monitoring parameters and their values on the SFP module for specified ports.

To view the following window, click **OAM > DDM > DDM Status Table**, as shown below:

Skin Tuše					
E FERRICE				4	
122	Longerman gives a s	490 BACK	HAR CAMPELING	La Porte (1991)	RS FORM (TWO
#11/2/25	25,903	2.2%	7 917	1572	2.002
21/1/2/28	33.33	0.300	7.10	1807.	0.01

Figure 10-8 DDM Status Table Window

11. Monitoring

Utilization Statistics Mirror Settings sFlow Device Environment

Utilization

Port Utilization

This window is used to display the percentage of the total available bandwidth being used on the port.

To view the following window,	click Monitoring > Utilization > Port Utilizatio	n, as shown below:
-------------------------------	--	--------------------

T LOOP AND A			
ini 🖂		1997 (1991) (1991) (1991)	Fed State
isot.	1X que le frend	HS backdologi	Unite
40.4.5	X)	10	
Altra Br	(¢	0	
49120	1	¢	4
V015364		<u>8</u>	9
100.00	() () () () () () () () () ()	(i)	0.
99000au)	S		5.11
404.37	i.	6	0.05
10030		6	6
40/13/2	6	0	0
0.000	(). ().	15	
rottett	i i	10 E	- 41
1001-001			. 46.2
etradali	¢		
alt (2014	C.	6	4
48.01013	() () () () () () () () () ()	() (¢)	9
0.500	6. (B)		
(antier)	S (1)	6	
4921030	i i	63	- 0
edra (Selli	6	¢	6
4811003	6	6	4
4,8,76951	C C	6	- Q -
enter d	s (
(er(100)	· · · · · · · · · · · · · · · · · · ·		1.01
48:0003		6	9
4811025		¢	4
6801003	6	¢0	0

Figure 11-1 Port Utilization Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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

Click the **Refresh** button to refresh the display table.

Statistics

Port

This window is used to display the packet statistics of ports.

	+ +20	-at <u>at 10-1</u>	-	10.000	ach 1974 1 m			I by	Rohan
ini.		63 649	1 6		ŧ	íx Isir	1.4		
	Interview.	acchette ber	, Mrs	jacet ris	Inkolas	nakhha	1000	por la fe	
100.000	$\overline{O}(J)$	- 39	\$07°29	2504	06775	67	2001701	768	(Linestonic)
2010	0	0	100 - E	1	() i	x.		E	I the brief
2105	0	0	2	3	2	2	- 19	6.2	the instantion
Storate -	0	0	() () () () () () () () () ()	1	1		1	1.5	Takes see 1
1111	3. P	<u>, (1</u>	1.		1.1	1	1	1.7	and when the
928 MIL	1.0	<u>.</u>	1.	4	1	36) 	1 A.	1	Ston Decil
7019	- 6	6	<u>)</u>	1)		1	1	Same Tread
e 100 -	0	\$	1	1	2	1	1	1	Contraction of the
0.100	0	0	9.5	1	1	2	10	1	Lines and the last
100200	199	<u>_0</u>		1	- 10			1	l abos secol
0.0015	11	11	÷.	1	4	9.	1.5	E S	Cristin Dece (
319.215	0	(Q	1	100	1	(B)	13	1.5	They Devid
al CPD in	0	0	à i	- Ch	2	3	1.S	E	L-Printerall
aDC94	0	¢.	- X -	123	1	5	1	1	Plain In sul
11215	0	0	3.	- 1	3	3	1.1	E.	anter peralt

To view the following window, click **Monitoring > Statistics > Port**, as shown below:

Figure 11-2 Port Window

The fields that can be configured are described below:

Parameter	Description				
Unit	Select the switch unit that will be used for this configuration here.				
From Port / To Port	Select the appropriate port range used for the configuration here.				

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

Click the **Refresh** button to refresh the display table.

Click the Show Detail button to see the detail information of the specific port.

After clicking the **Show Detail** button, the following page will appear.

art Detail	
on lanat	
	Hards Kellende
(80.80)	
RX reta	52 bylevstar.
TS MA	W Nytowa w.
12Urlis	250514
TX bytes	4035727
85.075	0.02.02.02.02.02.02
TX rely	0 ox dwh/w c
RX panariti	3.00
13 podežu	310)
RX multicast	03
KS, Tend Bowt	10
RECORD IN NO	3
RX Ladentza	3
800 U.W. 7, 120	1
RXX fragment	3
ext parate	4
RX slop and Filts	2
ROMINAL CARDING	3
DCORCION	3
TX as caraitys defented	3
Lis single collision	4
TX is availy valid an	2
TX life collution	3
LK reflexer	1

Figure 11-3 Port Detail Window

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

Click the **Refresh** button to refresh the display table.

Port Counters

This window is used to display port counter statistics.

- Service -									
			<u>entti •</u>	10.937	10110			Fre	Petrot
No.	Tela.b.b.	https://ks	hPost95	Monstella	U.O.A.A.A.	CellinAltin	0.0Maxx0Wa	Oath strifts	
Annyat.	$\mathcal{I}((2))^{\pm ij}$	31422	(A)	190	7(47341)	201	1	1.12	Shew Story
eh:13.2	0.	6	1	11		¢	E.c.	10	See See
011322	9	9	1	1	1	6	E	1	- Barne Barnet
10.000	0	15 -	100	1 11	1	0	1	15 1	der and
0.135	10.		1		1		F	- K 1	200 3000
ary out	14	6.5	6	1	100	- F.)	E	1	Shele Orters
603.37	0.	100	1	1.1	1	E.	1	1	See Sten
65523	× 1	- C -		1		- C	1	2	State Annual
16.02.9	5	6	1	1	1.1	6	E	3	day mar
AR SHE	- U		1	- 3	3	- U.	10 C	1	See and
10.2010	- 10	i i i	1		. 9		1	4.1	200 300
AT 18814	. 11	12	1 F	2.3	24	1.1	1.1	10 N	See Store
48-1213	<u>.</u>	¢ .	1	- 1	1	6	1	1	Same brain
40.9911	2	Q 2	1	1.11	11	Q	1	20.11	Star Beach
30.5089	0	(()		1	- 1	<u> (</u>	1	1	(Accounted)
10.500	. H.	60	100	3.4	13	10		1	100.000
distance.		6.9	1	10 A	1	• • • •	E.	1	Shew Strang
MP 5018	<u>.</u>	- C.	14	1	14	1	E S	¥.7	See Stars
- 48 3/2 (B)	5	62	1	1	1.1	ć .	1	3	Same Area
48 (322)	÷.	¢	1 (L)	1	1	e	4 2	3 1 1	Assesses
140/001	0	10. ²	1	2.1	1	6	1.1	10	Cree mar
Supercess.	11	E.	1.1	1	- 20-1		r	(1) (2)	Shew Street
or suit	11	- CC-		1	1		L.	4.6	Dave Store
all: 10.24	0	£7,	1	- 1	1	C C	1.1	100	See. See.
4811065	2	(c)	(T)	1	. (J)	C ()	1 (L	1.	Rine Area
10000	10 C	10 C	T.			<u>e 1</u>	100	10	discourses.

To view the following window, click **Monitoring > Statistics > Port Counters**, as shown below:

Figure 11-4 Port Counters Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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

Click the **Refresh** button to refresh the display table.

Click the **Show Errors** button to see all error counters of the specific port.

After clicking the Show Errors button, the following page will appear.

ouniers Errors		
Sources in ports		
	Hard, Ref.	end.
e 11 d'16 des alters. Here es		
Algri-On	3	
Erz, Erz	1	
for Br	3	
Understan	3	
2012 H 2	1	
DulDiversio	3	
Ringle-Col	1	
Mole Col	Ţ	
Late-Col	3	
Homese tant	3	
Cent-Ove	3	
Rentz	3	
Samio	1	
Symbol Dr	3	
800-17/0 Her	4	
Dala weTa	2	
int/JacTo	a la	
In MacRee	1	

Figure 11-5 Counters Errors Window

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

Click the **Refresh** button to refresh the display table.

Counters

This window is used to display all port counters, and clear the port counters of the specified or all ports.

THE M		
	() * 10803 <u>#\$100</u>	Dree Deserver
Ref. 1	lek base?	
A97.085		Store Dec 4
40100		(Sector)
sali 00		A search of
680042	(iii)	Store people
e in the second s	19	1 Shoe Dept 1
exten		Enon Dett 1
renove.		Envertex ()
401/04	3	Anim Truck
48109	3	L transferration
STRATE	() ()	Show sets 1
eurer.		Show Detril
mita!		Enon Dep 1
m1090	3	(Printe) (
60C014	3	Reinsteine I
019235		and could be

To view the following window, click **Monitoring > Statistics > Counters**, as shown below:

Figure 11-6 Counters Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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

Click the **Refresh** button to refresh the display table.

Click the **Clear** button to clear all the information for the specific ports.

Click the Clear All button to clear all the information in this table.

Click the Show Detail button to see the detail information of the specific port.

After clicking the **Show Detail** button, the following page will appear.

n classical tobe		
		dab brimit
18757 Caleron		
n Steatsa	25%	
nde, severa	198.6	
er (3) es d'été.	20 H	
th/COnsoltVar	10.00	
an-12/6-14-20-16	181	
410V-8-3476-2	(E)6	
re-references un	2011	
att fra harve	-22	
ni 100 dete	200200	
Net 11 N.	10.0.0.5	
* 178340.80	25	
Discrete Silvers	429	
	. 129	
of CPN258-51 Colvia	22	
and second state states.	21	
 CPR R044415 (DCslvin) 	2	
S-CPIPCERAD X SAD	10	
n/101962040604065Celeb	٥	
u-tati e a de de tati	M. en	
ADDPRISED	975	
northe 2017 form)CX(
an entre alette els	199	
ph/CP825Bot (Fócies)	1500	
SEC FRANCE ENTRY	18	

Figure 11-7 Port Counters Detail Window

Click the $\ensuremath{\textbf{Back}}$ button to return to the previous window.

Click the **Refresh** button to refresh the display table.

Mirror Settings

This window is used to view and configure the mirror feature's settings. The Switch allows users to copy frames transmitted and received on a port and redirect the copies to another port. Attach a

monitoring device to the mirroring 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.

un son els										
evolve Neetve	1									
	and the second s		Ucl		191					
Nv6.e3s)	F East		Ur A	1	end (all	1				
			060		fors?at		Tafat		Trans Text	
xua ([Pat	প	-	1. C	entro 1		972-172-1	10	Dvt.	ল
								E	1941	The dr.
ner Sevale i Toble										
U Sendor 💿 👳	1 N									i bala
	Service Barriet	_	_	32	stan Iga		_			_
	the state of the s									

To view the following window, click **Monitoring > Mirror Settings**, as shown below:

Figure 11-8 Mirror Settings Window

Parameter	Description
Session Number	Select the mirror session number for this entry here. This number is between 1 and 4.
Destination	Tick the checkbox, next to the Destination option, to configure the destination for this port mirror entry.
	In the first drop-down menu, select the Port option.
	In the second drop-down menu, select the destination switch's Unit ID.
	In the third drop-down menu, select the destination switch's port number.
Source	Tick the checkbox, next to the Source option, to configure the source for this port mirror entry.
	In the first drop-down menu, we can select the source type. Options to choose from are:
	 Port - In the first drop-down menu, select the source switch's Unit ID. From the From Port drop-down menu, select the starting port number and from the To Port drop-down menu, select the ending port number. Lastly select the Frame Type option from the fifth drop-down menu. Options to choose from as the Frame Type are Both, RX, TX, and TX Forwarding. When selecting Both, traffic in both the incoming and outgoing directions will be mirrored. When selecting RX, traffic in only the incoming direction will be mirrored. When selecting TX, traffic in only the outgoing direction will be mirrored only when the port(s) is/are in the STG forwarding state. ACL - Enter the ACL profile name in the space provided.

The fields that can be configured for Mirror Settings are described below:

Click the Add button to add the newly configured mirror entry based on the information entered.

Click the **Delete** button to delete an existing mirror entry based on the information entered.

The fields that can be configured for Mirror Session Table are described below:

Parameter	Description
Mirror Session Type	Select the mirror session type of information that will be displayed from the drop-down menu. Options to choose from are All Session , and Session Number .
	After selecting the Session Number option, select the session number from the second drop-down menu. This number is from 1 to 4.

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

Click the **Show Detail** button to see the detail information of the specific session.

After clicking the **Show Detail** button, the following window will appear.

Gesalor Number	1
Oversion Type	Local Gerator
Solo Port.	v@10015-cb10018
HC Pel	
1 S Hart	
13. Howarding Had	
Fice Rased Foreign	
Destination Post	Elenetro 14

Figure 11-9 Mirror Session Detail Window

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

sFlow

sFlow (RFC3176) is a technology for monitoring traffic in data networks containing switches and routers. The sFlow monitoring system consists of an sFlow Agent (embedded in a switch or router or in a standalone probe) and a central sFlow Collector. The architecture and sampling techniques used in the sFlow monitoring system were designed for providing continuous site-wide (and enterprise-wide) traffic monitoring of high speed switched and routed networks.

sFlow Agent Information

This window is used to view the sFlow agent information.

To view the following window, click **Monitoring > sFlow > sFlow Agent Information**, as shown below:

aFlow Agent Information		_
Allow Again Latercation		
a Dow Agent Version	1.3 D-Link Conservation Inc. 1.00	
A HOW Agent A carries	1 March 10	
e Mese Agent, Kvil Artikese	HERE'S A THE REPORT FOR A STREET	

Figure 11-10 sFlow Agent Information Window

sFlow Receiver Settings

This window is used to view and configure receivers for the sFlow agents. Receivers cannot be added to or removed from the sFlow agent.

To view the following window, click **Monitoring > sFlow > sFlow Receiver Settings**, as shown below:

	nan samula Nasi 196	1		Oranya Namy			[22 citaty	-
Carley The	a (1-200000)		vs Thildy	Viet Debug an Sta	736-1426		1400	25.45
Selecter 2	désa	155	ve 2015 of 100	007 Pet (1-68535			8040	
								1.16
							2 C - C - C - C - C - C - C - C - C - C	1.10.00
							2 D	. 1.945
and the second		100000000000000000000000000000000000000			200	200		
and the second	ka 4 Grint	Cust Fee	Cuscul Cous How 17 me	Mice De Jages en Silve	Addama	Park.	Celegra Versian	
86		Court Fee	Casad Ove Row 17 ee	Mile De Jean et Suz	Addenie	Park.	Canadra Witera	
i dire		Coder Time	Canad Cose Row 17 ar			CONTRACTOR OF STREET,		
43 Die 120		1	10	14.8	a a a si .	1.000	10 ⁻¹	Tited

Figure 11-11 sFlow Receiver Settings Window

The fields that can be configured are described below:

Parameter	Description
Receiver Index	Enter the index number of the receiver here. This number must be between 1 and 4.
Owner Name	Enter the owner name of the receiver here. This name can be up to 32 characters long.
Expire Time	Enter the expiration time for the entry here. The parameters of the entry will reset when the timer expired. The range is from 1 to 2000000 seconds. Selecting Infinite specifies that the entry will not expire.
Max Datagram Size	Enter the maximum number of data bytes of a single sFlow datagram here. The range is from 700 to 1400 bytes. By default, this value is 1400 bytes.
Collector Address	Enter the remote sFlow collector's IPv4 or IPv6 address here.
UDP Port	Enter the remote sFlow collector's UDP port number here. This number must be between 1 and 65535. By default, this value is 6343.

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

Click the Reset button to reset the specified entry's settings to the default settings.

sFlow Sampler Settings

This window is used to view and configure sFlow Sampler settings.

To view the following window, click **Monitoring > sFlow > sFlow Sampler Settings**, as shown below:

1000000000						
inen Mail	Acres .	w.k.w.5-144	en transfer t	ter to	X MARK BARRIER	Viceoscie / Date:
ch 1974 - An	and the state of the					1.8. 1.100
10000000000	100000000000000000000000000000000000000	1.	1.9.17	- Algerta and		sizeby .
						1
6						
(Internet and	Motoryan	TOTAL	A MILL RAD	Asheosone	MAR HOWEY SIZE	12
te drete a	Contraction of the local distance of the loc		COURSE & COURSES			
	4 <u>196 v</u>	199 <u>, 1999 - 1</u>	199 <u>8 -</u> 1999, 1997 - 1	1170 <u>×</u> [16604] [9]	1997 <u>v</u> 1999 v v v v v v v v v v v v v v v v v	



The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Instance	Enter the instance's index number if multiple samplers are associated with one interface. The valid range is from 1 to 65535.
Receiver	Enter the receiver's index for this sampler. If not specified, the value is 0. This value must be between 1 and 4.
Mode	Select the mode here. Options to choose from are:
	 Inbound - Specifies to sample ingress packets. This is the default direction of a sampler. Outbound - Specifies to sample egress packets.
Sampling Rate	Enter the packet-sampling rate here. This value must be between 0 and 65536. Entering 0 will disable this function. If not specified, the default value is 0.
Max Header Size	Enter the maximum number of bytes that should be copied from sampled packets. This value must be between 18 and 256 bytes. By default, this value is 128 bytes.

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

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

sFlow Poller Settings

This window is used to view and configure the sFlow Poller settings.

To view the following window, click **Monitoring > sFlow > sFlow Poller Settings**, as shown below:

Flow Poller Se					
	- Front and the	to for a second state (reference	Record (Fig. 194	A10-100	
1 91	antifut y	Creation (M)	and the second s	ws.	Aprily.
teki tauka -		Inkes		Internal	<i></i>
and the second se					



The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Instance	Enter the instance's index number if multiple samplers are associated with one interface. The valid range is from 1 to 65535.
Receiver	Enter the receiver's index value for this poller here. This value must be between 1 and 4.
Interval	Enter the maximum number of seconds between successive polling samples. This value must be between 0 and 120 seconds. Entering 0 will disable this feature. By default, this value is 0.

Click the Apply button to accept the changes made.

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

Device Environment

The device environment feature displays the Switch internal temperature status.

100	inge of a tooset	LATING CONTRACTOR IN AND
addined in the		270/16/790
dei vede ? Konovador	UNALL REAL AND	
HI KAR ATTEL		
10 P. N.		
	- FREES	subata A
	201	1
18	Rub (Per)	100
	How the off	(38)
d Francisco A		
IL KEVEL STREET		

To view the following window, click **Monitoring > Device Environment**, as shown below:

Figure 11-14 Device Environment Window

12. Green

Power Saving EEE

Power Saving

This window is used to configure the power saving settings of the Switch.

To view the following window, click **Green > Power Saving**, as shown below:

Power Sceleg Global Settings Power S	celog Soudown feitinge	
HINT RE WORK	A.P.F	
Link Defection Forest Caving	🔿 Orablet 👍 Olashi es	
Length Set a set Have a Haway	Contraction of the data	
Som is to Post standow Prizes Som g	j Frank in Danka.	
Stores an electronic Provinsions	C FILMA & INNON	
Scheduled El m-LCC Pover Saving	() Trailed 🔅 Daab ee	
Ada anticala / Cira USD	, land a bala	
Swer Saving		
Power Scenes Closed Settings America	Saving Statisticum Gettinge	
Sucke Vester	182	
	3.63	
Sandha Vasaka Gali Unisa karangan Salang	163 ⊖ Fentus - ⊊ Dankins	[
U Nacika Yasia Int Coloria Paris North Attourne verstanisko - verstovatj	160 ⊖ Fenties - Denties ⊖ Homen - Arientes	[
Sandon Vasion Di Constant Provis Konna Altanoma ven enamen - Para Storija Schedure Direkt Di Prove Saving Astan anthe Carl III.	107 C Fortus & Danies C Fortus & Invent C Fortus & Danies C Fortus & Danies	
Sanchen Volation De Clos sinte Hones Volation Autoritation et la contrata de Hones Volation Schedulen Mars LED Proper Sandag Agnan Jacober (1994-20) Time Ronge Gerlings	5.03 - Fonders - Dentines - Fonders - Alternation - Fonders - Alternation	

Figure 12-1 Power Saving Window

The fields that can be configured are described below:

Parameter	Description
Link Detection Power Saving	Select this option to enable or disable the link detection state. When 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.
Length Detection Power Saving	Select this option to enable or disable the cable length detection power saving feature. This feature will allow the Switch to automatically detect the cable length connected to the port and increase or reduce the required power to this port accordingly to save power.
Scheduled Port-shutdown Power Saving	Select this option to enable or disable applying the power saving by scheduled port shutdown.
Scheduled Hibernation Power Saving	Select to enable or disable the scheduled hibernation power saving function here.

Parameter	Description
Scheduled Dim-LED Power Saving	Select this option to enable or disable applying the power saving by scheduled dimming LEDs.
Administrative Dim-LED	Select this option to enable or disable the port LED function.
Туре	Select the type of power saving. Options to choose from are Dim - LED and Hibernation .
Time Range	Enter the name of the time range to associate with the power saving type.

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

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



NOTE: The **hibernation** feature can only be configured when physical stacking is disabled on this switch.

After clicking the **Power Saving Shutdown Settings** tab, the following page will appear.

Power Severa Olotal Sedinazy,	News) Severe Shatdown Scheres				
a.). 4 •	ner Ma Let Me	ina. entret	tinyawa. Diama		/apb
N In 1 Sections					
1941		n Honge			
st (3)				Delete	
sJ.132				Delete	
A3 130				Delete	
40.034				Delete	
4.8 1935				Delete	
(11)41				Detet:	
CI VIZ				Read-	
100.00				Pedda	

Figure 12-2 Power Saving Shutdown Settings Window

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port Select the appropriate port range used for the configuration	
Time Range	Enter the name of the time range to associate with the ports.

The fields that can be configured are described below:

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

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

EEE

Energy Efficient Ethernet (EEE) is defined in IEEE 802.3az. It is designed to reduce the energy consumption of a link when no packets are being sent.

en e	Franker	1000e	30.00	
1	Mildi -	33.713	D'adat a	100 V
nt i Solino	MARKON	110000000	C-2322000-232	
	Hori		389 1	
	official 1		A MC/MI/W	
	497.16		THORNE	
	CERTH		Disabled	
	10.22		Dimitive	
	W0005-		Disukiya	
	4.581		Januari en la companya de la company	
	All of the second se		190,000	
	strain)		Tinacae	
	48139		Dirishied	
	01/040		DevAlve	
1	0.0001		DOUBLE:	
	entent2		191,00700	
	experience		WARANCE.	
	40:011		Danie en	
	(注)(空間)		Directives	
	GE 0011		DEUGN	
	0.0000000		146.45 m	

To view the following window, click **Green > EEE**, as shown below:

Figure 12-3 EEE Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port Select the appropriate port range used for the configuration h	
State	Select this option to enable or disable the state of this feature here.

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

13. Toolbar

Save	
Tools	
Wizard	
Online Help	
Surveillance Mode	1
Logout	

Save

Save Configuration

This window is used to save the running configuration to the start-up configuration or the file system of the Switch. This is to prevent the loss of configuration in the event of a power failure.

To view the following window, click **Save > Save Configuration**, as shown below:

Save Configuration		
Save Exercises Unit 1 - Markets	C./w.m/g.c/p	* a do

Figure 13-1 Save Configuration Window

The fields that can be configured are described below:

Parameter	Description	
Unit	Select the switch unit that will be used for this configuration here.	
File Path	Enter the filename and path in the space provided.	

Click the **Apply** button to save the configuration.

Tools

Firmware Upgrade & Backup

Firmware Upgrade from HTTP

This window is used to initiate a firmware upgrade from a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP**, as shown below:

umiearie Dpgrat				
(etc	<u> </u>			
Spans the	1	Erona .		
Destination File	A dan			

Figure 13-2 Firmware Upgrade from HTTP Window

The fields that can be configured are described below:

Parameter	Description	
Unit	Select the switch unit that will be used for this configuration here.	
Source File	Enter the source filename and path of the firmware file located on the local PC. This field can be up to 64 characters long. Alternatively click the Browse button to navigate to the location of the firmware file located on the local PC.	
Destination File	Enter the destination filename and path where the new firmware should be stored on the Switch. This field can be up to 64 characters long.	

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Upgrade from TFTP

This window is used to initiate a firmware upgrade from a TFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > firmware Upgrade from TFTP**, as shown below:

Furnisaria Upgra	de hom 10-10"	
00	A	
THE Same P	(R. P.4	
	CINA .	
Statistics in	off (Early)	
Station (19)	74 H a 1	
		Userade

Figure 13-3 Firmware Upgrade from TFTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
TFTP Server IP	Enter the TFTP server's IP address here.
	When the IPv4 option is selected, enter the IPv4 address of the TFTP server in the space provided.
	When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
Source File	Enter the source filename and path of the firmware file located on the TFTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Backup to HTTP

This window is used to initiate a firmware backup to a local PC using HTTP.



NOTE: The **Source File** (name and path) can be found in the **File System** window on page 89.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP**, as shown below:

Firmware Liackup to HT II'				
Uelt	1			
Source File	(A charte			
		Salaci		

Figure 13-4 Firmware Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the firmware backup. Wait for the Web browser to prompt where to save the file on the local PC.

Firmware Backup to TFTP

This window is used to initiate a firmware backup to a TFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to TFTP**, as shown below:

), i unimaris l'addau	pta II II"	
	· · · · · ·	
THE Same P	R.P.4	
	i in the second	
naarini Debaarin	of they	
Section 199.	54 11 11 1	
		Tadas

Figure 13-5 Firmware Backup to TFTP Window

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
TFTP Server IP	Enter the TFTP server's IP address here.
	When the IPv4 option is selected, enter the IPv4 address of the TFTP server in the space provided.
	When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path where the firmware should be stored on the TFTP server. This field can be up to 64 characters long.

The fields that can be configured are described below:

Click the **Backup** button to initiate the firmware backup.

Configuration Restore & Backup

Configuration Restore from HTTP

This window is used to initiate a configuration restore from a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP**, as shown below:

	estore from UTTP		
or:	<u>A</u>		
date the		Elovar.	
Castington (Re.	Vel shah		The stategies of giff the special g
Rection			
			Kethre

Figure 13-6 Configuration Restore from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Source File	Enter the source filename and path of the configuration file located on the local PC. This field can be up to 64 characters long. Alternatively click the Browse button to navigate to the location of the configuration file located on the local PC.
Destination File	Enter the destination filename and path where the configuration file should be stored on the Switch. This field can be up to 64 characters long.
	Select the running-config option to restore and overwrite the running configuration file on the Switch.
	Select the startup-config option to restore and overwrite the start- up configuration file on the Switch.
Replace	Select this option to replace the current running configuration.

Click the **Restore** button to initiate the configuration restore.

Configuration Restore from TFTP

This window is used to initiate a configuration restore from a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from TFTP**, as shown below:

Figure 13-7 Configuration Restore from TFTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
TFTP Server IP	Enter the TFTP server's IP address here. When the IPv4 option is selected, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
Source File	Enter the source filename and path of the configuration file located on the TFTP server here. This field can be up to 64 characters long.
Destination File Enter the destination filename and path where the coshould be stored on the Switch. This field can be up characters long.	
	Select the running-config option to restore and overwrite the running configuration file on the Switch.
	Select the startup-config option to restore and overwrite the start- up configuration file on the Switch.
Replace	Select this option to replace the current running configuration.

Click the **Restore** button to initiate the configuration restore.

Configuration Backup to HTTP

This window is used to initiate a configuration file backup to a local PC using HTTP.



NOTE: The **Source File** (name and path) can be found in the **File System** window on page 89.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP**, as shown below:

	lackup to I LI II.	
alt:	<u> </u>	
Store River	H INT	The energy scoring The Average scoring

Figure 13-8 Configuration Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. Select the running-config option to back up the running configuration file from the Switch.
	Select the startup-config option to back up the start-up configuration file from the Switch.

Click the **Backup** button to initiate the configuration file backup. Wait for the Web browser to prompt where to save the file on the local PC.

Configuration Backup to TFTP

This window is used to initiate a configuration file backup to a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to TFTP**, as shown below:

Graiguration D	ictup to (1-11		
ar:			
THE Same P		Pet	
	() () () () () () () () () ()	PM	
8 a 10 - 11	Millury .	Constraint Charles and	
Orchiele He.	24 cl.ant		
		Tadas	

Figure 13-9 Configuration Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
TFTP Server IP	Enter the TFTP server's IP address here. When the IPv4 option is selected, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
Source File	Enter the source filename and path of the configuration file located on the switch here. This field can be up to 64 characters long. Select the running-config option to back up the running configuration file from the Switch. Select the startup-config option to back up the start-up configuration file from the Switch.
Destination File	Enter the destination filename and path where the configuration file should be stored on the TFTP server. This field can be up to 64 characters long.

Click the **Backup** button to initiate the configuration file backup.

Log Backup

Log Backup to HTTP

This window is used to initiate a system log backup to a local PC using HTTP.

To view the following window, click Tools > Log Backup > Log Backup to HTTP, as shown below:

Log Backup to HTTP				
Log Lype	😥 System Log 👘 Allack Log			
		Öskup		

Figure 13-10 Log Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Log Type	Select the log type that will be backed up to the local PC using HTTP.
	When System Log is selected, the system log will be backed up.
	When Attack Log is selected, the attack log will be backed up.

Click the **Backup** button to initiate the system log backup. Wait for the Web browser to prompt where to save the file on the local PC.

Log Backup to TFTP

This window is used to initiate a system log backup to a TFTP server.

To view the following window, click **Tools > Log Backup > Log Backup to TFTP**, as shown below:

Log Daskup In 1	1.11	
TITT Server P	8 P4 0 P4	
tanangantewi Togayya	ia dat Sistem og ji stating	
100.000	and an off the second	Zadan

Figure 13-11 Log Backup to TFTP Window

Parameter	Description
TFTP Server IP	Enter the TFTP server's IP address here. When the IPv4 option is selected, enter the IPv4 address of the TFTP server in the space provided.
	When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
Destination File	Enter the destination filename and path where the log file should be stored on the TFTP server. This field can be up to 64 characters long.
Log Туре	Select the log type that will be backed up to the TFTP server. When System Log is selected, the system log will be backed up. When Attack Log is selected, the attack log will be backed up.

The fields that can be configured are described below:

Click the **Backup** button to initiate the system log backup.

Ping

Ping is a small program that sends ICMP Echo packets to the IPv4/IPv6 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.

To view the following window, click Tools	> Ping.	, as shown	below:
---	---------	------------	--------

Pvi Pha			
in anyther content	A constant		
C) Homen second	NAMENT		
Ring Times at -2030		2 7 94	
Transit (104)	fe .	and the second	
Databa (Per Activate)			
			28.5
Not Pierg			
aged evel spannel	(wart)		
Ping Tenenari-Mila	L.	Granes.	
Transis (1994)	ŧ	P46	
Spiers Pel-Acarest	1		
			R +

Figure 13-12 Ping Window

Parameter	Description
Target IPv4 Address	Select and enter an IP address to be pinged.
Domain Name	Select and enter the domain name of the system to discover.
Ping Times	Enter the number of times desired to attempt to Ping the IPv4 address configured in this window. Users may enter a number of times between 1 and 255. Tick the Infinite check box to keep sending ICMP Echo packets to the specified IP address until the program is stopped.
Timeout	Select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. If the packet fails to find the IP address in this specified time, the Ping packet will be dropped.
Source IPv4 Address	Enter the source IPv4 address. If the current switch has more than one IP address, you can enter one of them to this field. When entered, this IPv4 address will be used as the packets' source IP address sent to the remote host, or as primary IP address.

The fields that can be configured for **IPv4 Ping** are described below:

The fields that can be configured for IPv6 Ping are described below:

Parameter	Description	
Target IPv6 Address	Enter an IPv6 address to be pinged.	
Ping Times	Enter the number of times desired to attempt to Ping the IPv6 address configured in this window. Users may enter a number of times between 1 and 255. Tick the Infinite check box to keep sending ICMP Echo packets to the specified IPv6 address until the program is stopped.	
Timeout	Select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. If the packet fails to find the IP address in this specified time, the Ping packet will be dropped.	

Parameter	Description
Source IPv6 Address	Enter the source IPv6 address. If the current switch has more than one IPv6 address, you can enter one of them to this field. When entered, this IPv6 address will be used as the packets' source IP address sent to the remote host, or as primary IP address.

Click the Start button to initiate the Ping Test for each individual section.

After clicking the **Start** button in **IPv4 Ping** section, the following **IPv4 Ping Result** section will appear:

նույ		
VE Ping Rawall		
al search them tax agents.		
[7] Depthy Cross 187, 188, 214 [3] Depthy Screen 152 (188, 21)	 Almost (12 mm) T Level (12 mm) 	
(i) Deply from 153.300.73.		
Aing continuits for in	1.100.10.1	
Recharded Sharp - 4, No.	enter l'est d'antis d'est e	
		2.6
2010 II 2000 II	i de la constante de	
3698 <u>3666</u>		
a ing		
Target Driv Address	Distance The Control of Control o	
Ping Times 14200:	erre .	
Teses # (1446)	1 182	
provide succession	1	
122010100000000000000000000000000000000		
		248.1

Figure 13-13 Ping - IPv4 Ping Result Window

Click the **Stop** button to halt the Ping Test.

Click the **Back** button to return to the IPv4 Ping section.

After clicking the **Start** button in **IPv6 Ping** section, the following **IPv6 Ping Result** section will appear:

Ping			_	_	
IP/IP	Plag				
÷	larget Pv4 Address				
0	Domain Name	255 chara			
	Phys Three (1,288)		≥ hihitiy		
	Time cul. (1-99)	ti i	2 8 C		
	Source ITv1 Addres n	1. A.			
					Start
(1) (2) (2) (4) (4)	Douly from 2014::1, by Regly from 2014::4, by Regly from 2014::4, by Regly from 2014:14, by Regly from 2014:4, by Regly from 2014:4, by Regly from 2014:4, by	tes=100 timexi0 te Les=100 timexi0 te Les=100 timexi0 es 1			
	Step Back				

Figure 13-14 Ping - IPv6 Ping Result Window

Click the Stop button to halt the Ping Test.

Click the **Back** button to return to the IPv4 Ping section.
Trace Route

The trace route page allows the user to trace a route between the Switch and a given host on the network.

To view the following window, click	Tools > Trace Route , as shown below:
-------------------------------------	---

i naz	a konte		
19vi	Trupe Reas		
*0	International Restances Rest (Restance) Rest (Restance) Restances (Restance) Restances (Restance)	10 school 10 school 10 sch 10 sch 10 sch 10 sch	9
-151	Normalitation Pref Addition Data (TTL (1950) Data (1985) Transf (1985) Product Terrey (1970)	20 27474 5	

Figure 13-15 Trace Route Window

The fields that can be configured for IPv4 Trace Route are described below:

Parameter	Description
IPv4 Address	Select and enter the IPv4 address of the destination here.
Domain Name	Select and enter the domain name of the destination here.
Max TTL	Enter the Time-To-Live (TTL) value of the trace route request here. 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	Enter the port number here. The value range is from 1 to 65535.
Timeout	Enter the timeout period while waiting for a response from the remote device here. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.
Probe Times	Enter the probe time number here. The range is from 1 to 9. If unspecified, the default value is 1.

The fields that can be configured for IPv6 Trace Route are described below:

Parameter	Description		
IPv6 Address	Select and enter the IPv6 address of the destination here.		
Max TTL	Enter the TTL value of the trace route request here. 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	Enter the port number here. The value range is from 1 to 65535.		
Timeout	Enter the timeout period while waiting for a response from the remote device here. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.		

Parameter	Description
Probe Times	Enter the probe time number here. The range is from 1 to 9. If unspecified, the default value is 1.

Click the Start button to initiate the route trace for each individual section.

After clicking the **Start** button in **IPv4 Trace Route** section, the following **IPv4 Trace Route Result** section will appear:

Pvi Trupy Robin Revell			
11 11 200	0.085 1251 1201 1201		
Cece			
Matoriania.			
$(a,a) \mapsto (a,b) = (a,b)$	Sance		
	0.03	1	
(measure and	1	jsoc.	
			- B

Figure 13-16 Trace Route - IPv4 Trace Route Result Window

Click the **Back** button to stop the trace route and return to the IPv4 Trace Route section.

After clicking the **Start** button in **IPv6 Trace Route** section, the following **IPv6 Trace Route Result** section will appear:

line	e lósate			
19ye	Tiupe Raua			
A	ever ordered.		Ĩ.	
135	Former spraw	12 10 10 100 30 32 10 4	68	
	We TO (SW)	30		
	Part (HCX/0)			
	Trace (1843)	7	244	
	Probe Times (-4)			9×**
125	Negrest tober out.			
	 Request times out; Request times out; Detrain times out; Thomas times out; Thomas times out; 	ġ.		
				~
	Re A			

Figure 13-17 Ping - IPv6 Ping Result Window

Click the **Back** button to stop the trace route and return to the IPv6 Trace Route section.

Language Management

This window is used to install the language file to the Switch.

To view the following window, click **Tools > Language Management**, as shown below:

Language Mara	gement				
Composiço Fale		Browse .	opply		

Figure 13-18 Language Management Window

The fields that can be configured are described below:

Parameter	Description
Language File	Click the Browse button to navigate to the location of the firmware file located on the local PC.

Click the Apply button to initiate the language pack installation.

Reset

This window is used to reset the Switch's configuration to the factory default settings.

To view the following window, click **Tools > Reset**, as shown below:



Figure 13-19 Reset Window

Select one of the following options:

- The Switch will be reset to its factory defaults including IP address and stacking information, and the will save, reboot. To reset the Switch's configuration to its factory default settings.
- The Switch will be reset to its factory default except IP address, and then will save, reboot To reset the Switch's configuration to its factory default settings. This option will exclude the IP address from being changed.
- The Switch will be reset to its factory defaults including IP address To reset the Switch's configuration to its factory default settings.

Click the Apply button to initiate the factory default reset and reboot the Switch.

Reboot System

This window is used to reboot the Switch and alternatively save the configuration before doing so.

To view the following window, click **Tools > Reboot System**, as shown below:

Reboot System	
Boton Syste	
Deva matteries and mail after the	selast -
Frederick and the address of the state of the state of the but	

Figure 13-20 Reboot System Window

When rebooting the Switch, any configuration changes that was made during this session, will be lost unless the **Yes** option is selected when asked to save the settings.

Click the **Reboot** button to alternatively save the settings and reboot the Switch.

Saving	and rebootin	g system, ph	easo wait	
		10%		

Figure 13-21 Reboot System - Rebooting Window

Wizard

Click this option to start the Smart Wizard. For more information about the Smart Wizard, refer to **Smart Wizard** on page 4.

Online Help

D-Link Support Site

Click this option to connect to the D-Link support website. An Internet connection is required.

User Guide

Click this option to connect to the online user guide for the Switch. An Internet connection is required.

Surveillance Mode

Click the **Surveillance Mode** button in the toolbar to change the Web UI mode and style from Standard Mode to Surveillance Mode. An unsuccessful change will display a warning message.

NOTE: All active Web UI user sessions can only access the same Web UI mode at the same time. The mode can only be changed when one user session is active. The mode cannot be changed when another user session is connected to the Web UI.

After clicking the **Surveillance Mode** option in the **Toolbar**, the following window will appear.



Figure 13-22 Surveillance Mode Confirmation Message

The window above displays a message that the abovementioned configurations need to be changed when access to the Surveillance Mode is given.

Click the **OK** button to continue.

Click the Cancel button to return to the Standard Mode.

After successfully switching to the Surveillance Mode on the Web UI of the Switch, the following window will appear.

Congratulations!	
If you require assistance, please click 🕐 Help on toolbar.	
Yes! I understand.	

Figure 13-23 Surveillance Mode 'Congratulations' Message

Click the Yes! I understand button to continue.

Logout

Click this option to log out of the Web UI of the Switch

14. Surveillance Mode

Surveillance Overview Port Information IP-Camera Information NVR Information PoE Information PoE Scheduling Management Time Surveillance Settings Surveillance Log Health Diagnostic Toolbar

Surveillance Overview

In this window, the **Surveillance Topology** and **Device Information** are displayed. It appears automatically when you access the Surveillance Mode in the Web UI of the Switch.

Surveillance Topology

This window provides more information about what is connected to each port. Hover with the mouse pointer over each device icon to get more information about the recognized device (such as the number of devices, device type, IP address, power consumption, link speed, and errors). Click on the '**more'** link to get more information about the devices connected to the port.



To return to the Surveillance Overview window after viewing other windows, click the **DGS-1510-28XMP** link.

Figure 14-1 Surveillance Overview Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit ID of the Switch in the stack that will be used here.

The following icons are available in this window and are described below:

Parameter	Description
Etamere x 3	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.
PCanaca x 0	This displays the total amount of D-Link legacy IP cameras (detected by ASV 1.0) connected to the Ethernet ports on the Switch.
<mark>.</mark> _{№ин} х 1	This displays the total amount of Network Video Recorders (NVRs) connected to the Ethernet ports on the Switch.
<u>Δ</u> χ 0	This displays the amount of surveillance warnings generated on the Switch.
🧼 x 1	This displays the amount of other devices connected to the Ethernet ports on the Switch.
*	This displays the device connected to the Ethernet port on the Switch. The green border around the image indicates that the device is a non-PoE device. The PD Alive function cannot be used on this device.
S	This displays the device connected to the Ethernet port on the Switch. The blue border around the image indicates that the device is a PoE device and is receiving power from the Switch using PoE. The PD Alive function can be used on this device.
<u>ம</u>	Click this icon to disable PoE on the port.
СU U	Click this icon to enable PoE on the port.

After clicking the 😃 icon, the following window will appear:

an-yai simi	ini wanto sh	atie PaF on port 82	
		26	 1. <u>2</u> . 1.
			 The Part of the Pa

After clicking the 🛄 icon, the following window will appear:

eE Contiguration		
we you sum you want to enable PorF on port \$2		
	C Frankine	rw/
	144.7	Carcel

Figure 14-2 PoE Configuration Window

The fields that can be configured are described below:

Parameter	Description
ΡοΕ	Select the maximum power that will be supplied on the PoE port. Options to choose from are Auto , 4W , 7W , 15.4W , 30W , and a configurable value from 1000 mW to 30000 mW. The unit is either in watt or milliwatt.

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

Click the Cancel button to discard the changes made.

After hovering (with the mouse pointer) over the **network device** icon, the following additional information will be displayed:



Figure 14-3 Additional Device Information

After clicking (left-click) the network device icon, the following window will appear.

D'Alive State	Directiled 🗠
D-F Addees	192 198 - 9 - 23
967	Eat V
·····	Ang Tert Apply Set to Default Cancel
	Ang Tert Apply Sterits Celevit Cancel
a nosen	

Figure 14-4 PD Alive Configuration Window

The fields that can be configured are described below:

Parameter	Description
PD Alive State	Select to enable or disable the PD Alive function here.
PD IP Address	Enter the IP address of the PD here.
Action	 Select the action that will be taken here. Options to choose from are: Reset - Specifies to reset the PoE port state (turn PoE off and on). Notify - Specifies to send logs and traps to notify the administrator. Both - Specifies to send logs and traps to notify the administrator and to reset the PoE port state (turn PoE off and on).

Click the **Ping Test** button to initiate the ping test to check if the PD is active or not.

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

Click the Set to Default button to return the settings to the default settings for this PD.

Click the **Cancel** button to discard the changes made.

After clicking **Ping Test** button, the following window will appear.

PD Alve Slate	Disabled w
PD-IP Addres	182-176-0 33
6 diam	Eat V
nių Kosuti –	Neg Text Apply Set to Default Cancel
I Request times out :	

Figure 14-5 PD Alive Configuration Window (Ping Result)

The **Ping Result** will be displayed.



NOTE: A breakdown of the device icons can be found by clicking the **Help** menu in the toolbar.



NOTE: The Switch uses ONVIF traffic to monitor the status of the surveillance device, but some third party devices do not fully comply with the ONVIF standard. If you are having problems with surveillance devices not being detected, please check ONVIF compatibility with the manufacturer of the original surveillance device.

Device Information

After clicking the **Device Information** tab, the following window will appear.

	12 WEB		E 04-0	
enningen Understationerkaligenderen sonen operationen All enaligender POWITION (ar valend to Valet Geraenau Weit with test	978-96482 374-55.9 636-8 354-5044-63803	and read react inners react bases The base The	example of the plane 1, 1990 of 91 WE 2004 (MISCH) 96 Devic 20 92 10
ine (inter				
(1) (1)	1211			
	00 00 00			
and Ukaba			18	CALIFIC AND IN

Figure 14-6 Device Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit ID of the Switch in the stack that will be used here.

Click the **1000 Mbps** button to change the maximum bandwidth displayed in the **Bandwidth Utilization** chart to 1 Gbps.

Click the **50 Mbps** button to change the maximum bandwidth displayed in the **Bandwidth Utilization** chart to 50 Mbps.

Port Information

This window is used to display port information like throughput, distance of the network cable, PoE provisioning status, power consumption, Loopback Detection status, group, and how many IP cameras, NVRs, and other devices are connected to the ports.



To view the following window, click Port Information, as shown below:

Figure 14-7 Port Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit ID of the Switch in the stack that will be used here.

Parameter	Description
🗹 x 5	This displays the total amount of Ethernet devices connected to the Ethernet ports on the Switch.
Me 6 Mbps	The displays the total amount of inbound bandwidth that is being used by the Ethernet devices connected to the Ethernet ports on the Switch.
Samera X 3	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.
NVB X 1	This displays the total amount of NVRs connected to the Ethernet ports on the Switch.

Parameter	Description			
🥗 x 1	This displays the total amount of other Ethernet devices connected to the Ethernet ports on the Switch.			
ch170/1	This displays the Ethernet port number on the Switch.			
VV 0 Mbps	This displays the amount of inbound bandwidth that is being used by the Ethernet device connected to the respective Ethernet port.			
** -	This displays the Ethernet cable length between the device and the Ethernet port on the Switch.			
U PoE DN	This displays the PoE status on the port.			
3.9W/15.4W	This displays the power consumption and power class of the PD connected to the Ethernet port.			
🥕 Normal	This displays the Loopback Detection status on the Ethernet port.			
🖌 Lloop	Normal - Specifies that there are no loops in the network.			
	Loop - Specifies that there is a loop in the network. Click the Loop link to navigate to the Health Diagnostic window.			
Group Details	If an ONVIF IP camera or NVR is connected to the port, the Group Details link will be available. Select the Group Details link to access the Group Details window.			
Video Management Server	If a network device is connected to the port that is neither an ONVIF IP camera nor NVR, the device type can be selected. Options to choose from are Video Management Server, VMS Client/Remote Viewer, Video Encoder, Network Storage, and Other IP Surveillance Device.			

Group Details

After clicking Group Details link, the following window will appear.

Port Information / Group Details			
/ Group Details			🔇 Back
Port eth1/01			
🛞 io 🖓 i Pomora	E 00000101/00004301	🎨 I - 180 KAO 2106-68-84-85-87-425 💬 I	

Figure 14-8 Port Information / Group Details Window

Parameter	Description
Port eth1/0/5	This displays the Ethernet port number on the Switch.
🛞 I o	This displays the group ID of the IP camera or NVR on the port.
් iP-Camera	This displays the type of device connected to the port. The can be either IP-Camera or NVR .

Parameter	Description
CC8-5211L / DC8-5211L	This displays the model name of the IP camera.
📸 192.168.0.23(29-10-7B-04-60-EC)	This displays the IP Address and MAC Address of the IP camera or NVR.
💬 DCS-942LB1	This displays the description of the device connected to the port.

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

IP-Camera Information

This window is used to display IP camera information.

To view the following window, click IP-Camera Information, as shown below:

a (1	(F)	
P rov x 3		
	🚮 K.M. 🖉 L. KOMORO 🌊 KOMORO (K. K. SKRATOV)	in clutics 📷 case 👔 case nor
1001-0-101 000-942104	æ ø	000-51251. 🥶 😎
48.04%	🔤 t 2001	
	1921-00-00-00-00-00-00-00-00-00-00-00-00-00	
DCS-SS11.		

Figure 14-9 IP-Camera Information Window

The fields that can be configured are described below:

Parameter	Description	
Unit	Select the unit ID of the Switch in the stack that will be used here.	

Parameter	Description	
Come x 3	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.	

Parameter	Description
W OMbps	The displays the total amount of inbound bandwidth that is being used by the ONVIF IP cameras connected to the Ethernet ports on the Switch.
🧧 4.4w / 15.4w	The displays the total power consumption and power class (of PDs) used by the ONVIF IP cameras connected to the Ethernet ports on the Switch.
i eth1/0/1	This displays the Ethernet port number on the Switch.
0CS-942LB1 DCS-942LB1	This displays a photo, the manufacturer, and the model name of the IP camera connected to the port. D-Link IP cameras will display the photo of the specific model connected to the port. Non-D-Link camera will display a generic IP camera photo.
VV 0 Mbps	This displays the amount of inbound bandwidth that is being used by the IP camera.
🛐 4.411 HS.411	This displays the power consumption and power class of the IP camera.
(2) 192 168.0.21 (B0-C5-54-26-B7-A3)	This displays the IP address and MAC address of the IP camera.
💬 DCS-942L81 🔗	This displays the description for the IP camera. Click the icon to modify the description.
9	Enter the description for the IP camera here. Click the 🥝 icon to apply the modified description.

NVR Information

This window is used to display NVR information.

WR Internation

To view the following window, click NVR Information, as shown below:



The fields that can be configured are described below:

Parameter	Description	
Unit	Select the unit ID of the Switch in the stack that will be used here.	

Parameter	Description			
<mark>Ч</mark> ыма х 1	This displays the total amount of NVRs connected to the Ethernet ports on the Switch.			
W Ombps	The displays the total amount of inbound bandwidth that is being used by the NVRs connected to the Ethernet ports on the Switch.			
ieth1/0/2	This displays the Ethernet port number on the Switch.			
NVR	This displays a generic photo of the NVR connected to the port.			
Mbps	This displays the amount of inbound bandwidth that is being used by the NVR.			
(Ba-70-F4-B0-42-A1)	This displays the IP address and MAC address of the NVR.			
9 Ø	This displays the description for the NVR. Click the ficon to modify the description.			
\$	Enter the description for the NVR here. Click the 🥝 icon to apply the modified description.			
Group 1	This displays the group ID of the NVR.			
📮 💷	This displays the number of ONVIF IP cameras managed by this NVR.			
C10/05 (192.168.0.23) (28-10-78-04-60-EC)	This displays information about the ONVIF IP camera that is managed by this NVR.			

PoE Information

This window is used to display Power-over-Ethernet (PoE) information.

	0.0 0 1 1 0.0	lw 🗳 22 ↔		毁 x 1	₩ x0
1101	() (** 10	3 a.w.	ch140/2	🔕 - e III.	🔘 (c 20
66	dewoning 🔬	2 20070EA	0	<u>es</u> -	C MARK
1000	() N F ()	😨 1w	childen	🛞 - 94 at .	🔘 (sum
3	dia dia mandritra	D ROMORN	(19)	<u>&</u> -	C Lemace
00%)	🛞 -~+ m	CO 3. 10	aly DOM	🕐 -se us	- CD (1.24
-	📥 : Crème inc	0.0500.0540	(19)	2	

To view the following window, click **PoE Information**, as shown below:

Figure 14-11 PoE Information Window

The fields that can be configured are described below:

Parameter	Description	
Unit	Select the unit ID of the Switch in the stack that will be used here.	

Parameter	Description
193w	This displays the maximum PoE budget that can be provided by the Switch.
💈 3.5 w / 15.4 w	This displays the total PoE consumption and power class of PDs connected to the Switch.
🗳 22 %	This displays the current PoE utilization (in percentage).
PoE x 1	This displays the number of PoE devices connected to the Switch that is using 15 Watts of power per port.
PoE+ sow x 0	This displays the number of PoE devices connected to the Switch that is using 30 Watts of power per port.
eth1/0/5	This displays the Ethernet port number on the Switch.
🕛 PoE ON	This displays the PoE state on the port. This can be either PoE ON or PoE OFF .

Parameter	Description
15,411	This displays the maximum PoE budget available on this port.
Delivering	This displays the current PoE status on the port. This status can be one of the following: -, Searching, Delivering, or Power Denied. When the Power Denied message is displayed, click on the link to
	redirect the Health Diagnostic window for more information.
💈 3.5W/ 15.4W	This displays the PoE consumption and power class of the PD connected to the port.

PoE Scheduling

This window is used to display and configure the PoE scheduling settings.

To view the following window, click **PoE Scheduling**, as shown below:

oE Soheih	ding					
Time Range						
Barry Harr	-	adus ≡ 0	uly.			
Iran Tine	(Versill)	San 💌 00 💌 📷				
Du Done (A	(8aa y 10 y 📷				ip de
	-					
	Kanga Naras			h.		
	••	More I	Re:	Sec.3	The	
Pair Caninga						
ine Text	HOLENS MALEY M	enter er	Enersage Desse Selective			Acole
1 (20)	Sector 1					
	Pal		The Design			
	e#1/24				Delete	
	: dis 17 82				veice -	
	6811/00				Delete	
	<81004				Orders	
	00206				Tick (r	
	4811/00				Delete	
	101120				Delete	
	4011/09				Debute	
	10.010				veles	
	4015010				Data de	
	<800011				Delete	
	100000				Debrie	
	edn/0410				Deleta	

Figure 14-12 PoE Scheduling Window

The fields that can be configured in the **Time Range** section are described below:

Parameter	Description
Range Name	Enter the name of the time range schedule here.
From: Time (Week/HH)	Select the starting day and hour in the time range schedule here. Alternatively, click the icon to open a calendar for easy day and hour selection.
To: Time (Week/HH)	Select the ending day and hour in the time range schedule here. The schedule will end at the end of the selected hour.

Parameter	Description
	Alternatively, click the ¹⁰⁰ icon to open a calendar for easy day and hour selection.

Click the $\ensuremath{\textbf{Apply}}$ button to accept the changes made.

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

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

The fields that can be configured in the **PoE Configuration** section are described below:

Parameter	Description
Unit	Select the unit ID of the Switch in the stack that will be used here.
From Port / To Port	Select the port range that will be used here.
Time Range	Select the time range schedule that will be applied to the selected port(s) here.

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

Click the **Delete** button to remove the time range schedule from the specified port.

After clicking the III icon, the following window will appear:

Lur	Mon	iue.	Wed	ine.	14	54
00	1.91	12	10	04	05	100
07	08	29	10	11	17	13
- 14	15	16	120	18	119	200
1.21	22	22				

Figure 14-13 Day and Hour Window

Click the **OK** button to use the Day and Hour selected.

Management

File System

This window is used to display and configure the file system settings.

To view the following window, click **Management > File System**, as shown below:

e System				
un: Path				0
E.go				
Dive	Mode Type	See (MII)	File System Taylor	Label
4	HAA.		HH I	



The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit ID of the Switch in the stack that will be used here.
Path	Enter the path string here.

Click the **Go** button to navigate to the path entered.

Click the <u>c:</u> hyperlink to navigate the C: drive.

After clicking the <u>c</u>: hyperlink, the following window will appear.

		1						X.
EN.	NAR .		kacara 📃	000				
in here i	1000	TANK!	1. 50 3755	illy to be not	n (Maria)	M		111
1	HTS2		THIN.	Le 18.200 (19.3) 45	DECEMBER & AND	The state of	Lorger -	ful-te-
-1	07034		-226-1	Av: 01 0000 00:30:34	100/2010	OPEN OF	Nor sime	Lidese'
100	1	- 2-	the state	im 25 2300 0000002	CZ IE	4.		esi (18

Figure 14-15 File System (c:) Window

Click the **Previous** button to return to the previous window.

Click the Create Directory button 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 **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 windows will appear.

File System						
Unit Deb		1 💌			Ge	
Copy File						
Searce	Unit	1 🗵	statup-cardig 🛛 🗵	C /coefig.clip		
Destrution	(init)	1 2	sussing-costig 🔍	C-/config.clg	C Pepiera	
					Roph Centrel	

Figure 14-16 File System (Copy) Window

The fields that can be configured are described below:

Parameter Description	
Source	Specifies to configure the source file that will be copied.
Destination	Specifies to configure the destination file that will be copied.
Unit	Select the unit ID of the Switch in the stack that will be used here.

Parameter	Description
startup-config	Select this option to use the startup configuration of the Switch in the copy.
running-config	Select this option to use the running configuration of the Switch in the copy.
Source File	Select this option and then manually enter the path and name of the source file that will be copied in the space provided.
Destination File	Select this option and then manually enter the path and name of the destination file that will be copied in the space provided.
Replace	Select this option to replace the current running configuration with the source file.

Click the **Apply** button to initiate the copy.

Click the **Cancel** button the discard the process.

Time

Clock Settings

This window is used to display and configure the time settings on the Switch.

To view the following window, click **Time > Clock Settings**, as shown below:

Clock Settings		
Clock Relings		
Tetra (4418MSS)	10.04.09	
Date (DD I MILLI YYYY)	2/1/2000	
		Apply

Figure 14-17 Clock Settings Window

The fields that can be configured are described below:

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

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

SNTP Settings

This window is used to display and configure the Simple Network Time Protocol (SNTP) settings.

To view the following window, click **Time > SNTP Settings**, as shown below:

SNTP Settings				
MITP CAUSAI Refitings				
Current Time Source ONTP* State Put Interval (30-99999)	System Clock Disabled V			Japatry
SMIP Server Selling				
Print Address				Add
Total Entries: 1				
MIT GROUP	Nitration	Version	Last Receive	
18.95 MI.125			-	Ordete

Figure 14-18 SNTP Settings Window

The fields that can be configured in the SNTP Global Settings section are described below:

Parameter	Description
SNTP State	Select to enable or disable the SNTP feature here.
Poll Interval	Enter the poll interval value here. The range is from 30 to 99999 seconds. By default, this value is 720 seconds.

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

The fields that can be configured in the SNTP Server Setting section are described below:

Parameter	Description
IPv4 Address	Enter the IPv4 address of the SNTP server here.

Click the Add button to add the SNTP server to the configuration.

Click the **Delete** button to remove the SNTP server from the configuration.

Surveillance Settings

This window is used to display and configure the surveillance settings. The Switch has only one Surveillance VLAN. This surveillance VLAN also supports to recognize the surveillance devices, like IP Cameras (IPC) and Network Video Recorders (NVR), using the ONVIF protocol.

To view the following window, click **Surveillance Settings**, as shown below:

Surveillance Settings					
Server ence WLAM Server					
valuum putma)	678 1				a sply
12 Xali lage.					
Get if them	Sante 🖂				
P Allers.	172 18 69 27.5				
in sec	255 + 255 + 246 + -0				
Selaray	172 18 71 784				a spily
AltMP Real for large					
Hor PH Adonte	1. A. A. A.				A role
Testal Paralese di					
Read IP distribution	A SEP Version	UNIN Presi	Zeen near sity. Sining & ABMPvA Here:	Law .	
97210.0510	s2:	10	p.bk		Velva
Log Server					
HORINH ABOTHS					A sply
Total Performent					
Annual P	Branky	Parallely (Street window Marine	1197	
1211036-11	Bringer view	E		84	Coloria
Optick Port Milliongs					
Unit From Port	lo fot Marina i 🖂				Ada
INTERNET					
	Fe	-			
	ere i	ALC: NO		alan alam	

Figure 14-19 Surveillance Settings Window

The fields that can be configured in the **Surveillance VLAN Settings** section are described below:

Parameter	Description
VLAN ID	Enter the ID of the surveillance VLAN here. The range is from 2 to 4094.

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

The fields that can be configured in the **IP Settings** section are described below:

Parameter	Description	
Get IP From	Select the method used to configure the IP address settings on the Switch here. Options to choose from are:	
	 Static - Specifies that the IP address settings will be manually configured. DHCP - Specifies that the IP address settings will be automatically obtained from a DHCP server on the network. 	
IP Address	Enter the IPv4 address of the Switch here.	
Mask	Enter the IPv4 subnet mask of the Switch here.	
Gateway	Enter the IPv4 address of the default gateway here.	

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

The fields that can be configured in the **SNMP Host Settings** section are described below:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the SNMP host here.

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

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

The fields that can be configured in the **Log Server** section are described below:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the syslog server here.

Click the Apply button to accept the changes made.

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

The uplink ports join all surveillance VLANs since they forward surveillance traffic to other switches. It is recommended to connect uplink ports to the other switches because the discovery process is disabled on these ports.

The fields that can be configured in the Uplink Port Settings section are described below:

Parameter	Description
Unit	Select the unit ID of the Switch in the stack that will be used here.
From Port / To Port	Select the uplink port range that will be used here.

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

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

Surveillance Log

This window is used to display the surveillance log.

To view the following window, click Surveillance Log, as shown below:

			2014 (1916)
-KK	<u> </u>	- Vine	Las Lastration
0	100-169 (C-221)	-00%A	MAL REPORT OF A DATA REPORT OF A DATA
a	according to be a	BOX N	We make with the weak to see the
	2010 T 1000 T	1004	ward war to ward at the other work of a state of the second
	annais annais	10004	Desides where its reaction of the
9	appointe à l'anne st	6953	Mar 4 more (March 10-52) kind as date at the
	TOTALS DUMAL	40000	Life and the opposed because with any face of
	20.000-0-0.000		ACTIVATION OF A CONTRACT OF A
100	201112-01001	400.0	Australia Chicago (Bay 222 - House & Chicago)
are in	20110-0-201	100531	CONVERSION AND A REPORT OF A REPORT OF A REPORT OF



Click the Refresh button to refresh the information displayed in the table.

Click the **Backup** button to upload the surveillance log to the PC using HTTP.

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

Health Diagnostic

This window is used to display Health Diagnostics information, Discovered Surveillance Devices information, and initiate a cable distance test on all or selected ports on the Switch. For each link-up port, the system will check the link status, PoE status and error counters periodically. This page will refresh every 30s.

To view the following window, click **Health Diagnostic**, as shown below:

411						
1						Defect of
(99)	Lappence (Ministran) Ministra	Calification	the Richard	1.0% (1%) Cale 10	Description of the second second	. (Mail Descrip
1920-023	(ST.M	- 44	Densting	62	1	Desce
with the	Her on all		SMAT N	2.1	1	Gener
aire na	BURNA .		Salating	24	I.	Deter
1.24						Lerosco
1996	5.0x00	-2.07	(2.0652-017)	- 62	1.5	My.e
n 189			1.12		- 65 L	- Diversity
Min (92	14 (j. 1	22	194	1 (A)	20	DO.1
NO. NO.			1.3	1 m 1	+	Paracel
weilige -						Orier.
ann fa						(Marce)

Figure 14-21 Health Diagnostic Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit ID of the Switch in the stack that will be used here.

Parameter	Description
Port	This field displays the Ethernet port number.
Loopback Detection Status	This field displays the Loopback Detection status on the Ethernet port. It can be one of the following:
	 Normal - No loop is detected on the port. Loop - A loop is detected on the port.
Cable Link	This field displays the cable link status. It can be one of the following:
	 PASS - The port link is up and operating in the full-duplex mode. 10M Half - The port link is up and operating at 10 Mbps speed and in the half-duplex mode. 100M Half - The port link is up and operating at 100 Mbps speed and in the half-duplex mode.
PoE Status	This field displays the PoE status. It can be one of the following: PASS , MPS (Maintain Power Signature) Absent , PD Short ,

The fields that are displayed in the table are described below:

Parameter	Description	
	Overload, Power Denied, Thermal Shutdown, Startup Failure, or Classification Failure .	
Tx/Rx CRC Counter	This field displays the TX/RX CRC counter.	
Discovered Surveillance Devices	This field displays the number of ONVIF IP cameras and NVRs discovered on the port. Click the hyperlink (<u>1</u>) to view the group details associated with IP camera or NVR connected to the port. For more information, refer to Group Details on page 397.	
Detect Distance	Click the Detect button to initiate a cable distance test on the specified port.	

Click the **Detect All** button to initiate a cable distance test on all the ports of the Switch.

Toolbar

Wizard

Click this option to start the Smart Wizard. For more information about the Smart Wizard, refer to **Smart Wizard** on page 4.

Tools

Firmware Upgrade & Backup

Firmware Upgrade from HTTP

This window is used to initiate a firmware upgrade from a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP**, as shown below:

I	Firmware Upgrade from HTTP				
ſ					
	Unit	44 V			
	Secure File	Downe			
	Orotination File	64 chum			
		Upprefe			



Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Source File	Enter the source filename and path of the firmware file located on the local PC. This field can be up to 64 characters long. Alternatively click the Browse button to navigate to the location of the firmware file located on the local PC.
Destination File	Enter the destination filename and path where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

The fields that can be configured are described below:

Click the Upgrade button to initiate the firmware upgrade.

Firmware Backup to HTTP

This window is used to initiate a firmware backup to a local PC using HTTP.

NOTE: The **Source File** (name and path) can be found in the **File System** window on page 403.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP**, as shown below:

Firmware Backup to HTTP		
[
Unit	1 ×	
Totalice Pille	and carbons	
		Bardage

Figure 14-23 Firmware Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the firmware backup. Wait for the Web browser to prompt where to save the file on the local PC.

Configuration Restore & Backup

Configuration Restore from HTTP

This window is used to initiate a configuration restore from a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP**, as shown below:

Configuration Regions from HTTP				
Unit Al V				
Source File Decesse.				
Devilmation: File 84 chum Insming-config Inship-config				
Replace				
Lotieve				

Figure 14-24 Configuration Restore from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Source File	Enter the source filename and path of the configuration file located on the local PC. This field can be up to 64 characters long. Alternatively click the Browse button to navigate to the location of the configuration file located on the local PC.

Parameter	Description
Destination File	Enter the destination filename and path where the configuration file should be stored on the Switch. This field can be up to 64 characters long.
	Select the running-config option to restore and overwrite the running configuration file on the Switch.
	Select the startup-config option to restore and overwrite the start- up configuration file on the Switch.
Replace	Select this option to replace the current running configuration.

Click the **Restore** button to initiate the configuration restore.

Configuration Backup to HTTP

This window is used to initiate a configuration file backup to a local PC using HTTP.



NOTE: The **Source File** (name and path) can be found in the **File System** window on page 403.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP**, as shown below:

	Configuration Backup	to HTTP	
ſ			
	Unit	1 V	
Ш	Tourse Pile	Ref citizen	Consult-could Consult-could
			Enclose

Figure 14-25 Configuration Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. Select the running-config option to back up the running
	configuration file from the Switch.
	Select the startup-config option to back up the start-up configuration file from the Switch.

Click the **Backup** button to initiate the configuration file backup. Wait for the Web browser to prompt where to save the file on the local PC.

Language Management

This window is used to install the language file to the Switch.

To view the following window, click **Tools > Language Management**, as shown below:

Language Nanugement					
Language Pile	Deceme				

Figure 14-26 Language Management Window

The fields that can be configured are described below:

Parameter	Description
	Click the Browse button to navigate to the location of the firmware file located on the local PC.

Click the **Apply** button to initiate the language pack installation.

Reset

This window is used to reset the Switch's configuration to the factory default settings.

To view the following window, click **Tools > Reset**, as shown below:

Reest	
Jisan .	
The limited with the matrix is its factory obtaining syntaxing 6 ² address; and starting information, and they will may account (). The Build's will be work in factors information information and the matrix information information in a second and a second start of the second of the factors.	
C The Bolt A of the word to do further, collection and any P whereas	Acolo



Select one of the following options:

- The Switch will be reset to its factory defaults including IP address and stacking information, and the will save, reboot. To reset the Switch's configuration to its factory default settings.
- The Switch will be reset to its factory default except IP address, and then will save, reboot To reset the Switch's configuration to its factory default settings. This option will exclude the IP address from being changed.
- The Switch will be reset to its factory defaults including IP address To reset the Switch's configuration to its factory default settings.

Click the Apply button to initiate the factory default reset and reboot the Switch.

Reboot System

This window is used to reboot the Switch and alternatively save the configuration before doing so.

To view the following window, click **Tools > Reboot System**, as shown below:

Rebot System				
Federal Typins				
Do you exect to save the settings 1 (a) Yes () No Eyes do not save the settings, all changes made in this secolor will be lost.	Related			

Figure 14-28 Reboot System Window

When rebooting the Switch, any configuration changes that was made during this session, will be lost unless the **Yes** option is selected when asked to save the settings.

Click the **Reboot** button to alternatively save the settings and reboot the Switch.

Save

Save Configuration

This window is used to save the running configuration to the start-up configuration or the file system of the Switch. This is to prevent the loss of configuration in the event of a power failure.

To view the following window, click **Save > Save Configuration**, as shown below:

Save Conf	iguration				
T Rate Cost	yunation				
UR	1 💌	Re Path	Culture ling of g		Apple

Figure 14-29 Save Configuration Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
File Path	Enter the filename and path in the space provided.

Click the **Apply** button to save the configuration.

Help

Click this option to access the built-in Surveillance Help window.



After clicking the Help option, the following window will appear.

Figure 14-30 Help (Diagram) Window



Figure 14-31 Help (Table) Window

Online Help

D-Link Support Site

Click this option to connect to the D-Link support website. An Internet connection is required.

User Guide

Click this option to connect to the online user guide for the Switch. An Internet connection is required.

Standard Mode

Click the **Standard Mode** button in the toolbar to change the Web UI mode and style from Surveillance Mode to Standard Mode.



NOTE: All active Web UI user sessions can only access the same Web UI mode at the same time. The mode can only be changed when one user session is active. The mode cannot be changed when another user session is connected to the Web UI.

Logout

Click this option to log out of the Web UI of the Switch

Appendix A - System Log Entries

The following tables list the system log entries and their corresponding meanings that will appear in the System Log of this switch.

802.1X

Log Description	Severity
Event Description: 802.1X Authentication failure.	Critical
Log Message: 802.1X authentication fail [due to <reason>] from (Username: <username>, <interface-id>, MAC: <mac-address>)</mac-address></interface-id></username></reason>	
Parameters Description:	
reason: The reason for the failed authentication. The possible reason may be:	
(1) user authentication failure.	
(2) no server(s) responding.	
(3) no servers configured.	
(4) no resources.	
(5) user timeout expired.	
username: The user that is being authenticated.	
interface-id: The switch interface number.	
mac-address: The MAC address of the authenticated device.	
Event Description: 802.1X Authentication successful.	Informational
Log Message: 802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>)</mac-address></interface-id></username>	
Parameters Description:	
username: The user that is being authenticated.	
interface-id: The interface name.	
mac-address: The MAC address of the authenticated device.	

AAA

Log Description	Severity
Event Description: This log will be generated when AAA global state is enabled or disabled.	Informational
Log Message: AAA is <status></status>	
Parameters Description:	
status: The status indicates the AAA enabled or disabled.	
Event Description: This log will be generated when login successfully.	Informational
Log Message: Successful login through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>)</username></server-ip></aaa-method></client-ip></exec-type>	
Parameters Description:	
exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).	
client-ip: It indicates the client's IP address if valid through IP protocol.	
aaa-method: It indicates the authentication method, e.g.: none, local, server.	
server-ip: It indicates the AAA server IP address if authentication method is remote server.	
Username: It indicates the username for authentication.	
Event Description: This log will be generated when login failure.	Warning

Log Description	Severity
Log Message: Login failed through <exec-type> [from <client-ip>]</client-ip></exec-type>	
authenticated by AAA <aaa-method> <server-ip> (Username: <username>)</username></server-ip></aaa-method>	
Parameters Description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH,	
Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol.	
aaa-method: It indicates the authentication method, e.g.: local, server. server-ip: It indicates the AAA server IP address if authentication	
method is remote server.	
username: It indicates the username for authentication.	
Event Description: This log will be generated when the remote server does not respond to the login authentication request.	Warning
Log Message: Login failed through <exec-type> [from <client-ip>] due to AAA server <server-ip> timeout (Username: <username>)</username></server-ip></client-ip></exec-type>	
Parameters Description:	
exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).	
client-ip: It indicates the client's IP address if valid through IP protocol.	
server-ip: It indicates the AAA server IP address.	
username: It indicates the username for authentication.	
Event Description: This log will be generated when enable privilege successfully.	Informational
Log Message: Successful enable privilege through <exec-type> [from <client-< td=""><td></td></client-<></exec-type>	
ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>)</username></server-ip></aaa-method>	
Parameters Description:	
exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).	
client-ip: It indicates the client's IP address if valid through IP protocol.	
aaa-method: It indicates the authentication method, e.g.: none, local, server.	
server-ip: It indicates the AAA server IP address if authentication method is remote server.	
Username: It indicates the username for authentication.	
Event Description: This log will be generated when enable privilege failure.	Warning
Log Message: Enable privilege failed through <exec-type> [from <client-ip>] authenticated by AAA <aa-method> <server-ip> (Username: <username>)</username></server-ip></aa-method></client-ip></exec-type>	
Parameters Description:	
exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).	
client-ip: It indicates the client's IP address if valid through IP protocol.	
aaa-method: It indicates the authentication method, e.g.: local, server.	
server-ip: It indicates the AAA server IP address if authentication method is remote server.	
username: It indicates the username for authentication.	
Event Description: This log will be generated when the remote server does not respond to the enable password authentication request.	Warning
Log Message: Enable privilege failed through <exec-type> [from <client-ip>] due to AAA server <server-ip> timeout (Username: <username>)</username></server-ip></client-ip></exec-type>	
Parameters Description:	
exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).	
client-ip: It indicates the client's IP address if valid through IP protocol.	
	I

	scription	Severity
	server-ip: It indicates the AAA server IP address.	
	username: It indicates the username for authentication.	
	escription: This log will be generated when RADIUS assigned a valid Dattributes.	Informational
	ssage: RADIUS server <server-ip> assigned VID: <vid> to port ce-id> (Username: <username>)</username></vid></server-ip>	
Parame	ters Description:	
	server-ip: It indicates the RADIUS server IP address.	
	vid: The assign VLAN ID that authorized by from RADIUS server.	
	Interface-id: It indicates the port number of the client authenticated.	
	Username: It indicates the username for authentication.	
	escription: This log will be generated when RADIUS assigned a valid Ith attributes.	Informational
	ssage: RADIUS server <server-ip> assigned <direction> bandwidth: bld> to port <interface -id=""> (Username: <username>)</username></interface></direction></server-ip>	
Parame	ters Description:	
	server-ip: It indicates the RADIUS server IP address.	
	Direction: It indicates the direction for bandwidth control, e.g.: ingress or egress.	
	Threshold: The assign threshold of bandwidth that authorized by from RADIUS server.	
	interface-id: It indicates the port number of the client authenticated.	
	Username: It indicates the username for authentication.	
priority a Log Mes	escription: This log will be generated when RADIUS assigned a valid attributes. ssage: RADIUS server <server-ip> assigned 802.1p default priority: > to port <interface -id=""> (Username: <username>)</username></interface></server-ip>	Informational
	ters Description:	
	server-ip: It indicates the RADIUS server IP address.	
	priority: The assign priority that authorized by from RADIUS server.	
	interface-id: It indicates the port number of the client authenticated.	
	Username: It indicates the username for authentication.	
	escription: This log will be generated when RADIUS assigned ACL it fails to apply to the system due to insufficient resource.	Warning
Log Mes	ssage: RADIUS server <server-ip> assigns <username> ACL failure at terface -id> (<acl-script>)</acl-script></username></server-ip>	
Parame	ters Description:	
	server-ip: It indicates the RADIUS server IP address.	
	username: It indicates the username for authentication.	
	interface-id: It indicates the port number of the client authenticated.	
	acl-script: The assign ACL script that authorized by from RADIUS server.	
	escription: This log is generated when the RADIUS assigned ACL applied to the system due to insufficient resources.	Informational
	ssage: RADIUS server <server-ip> assigns <username> ACL success interface -id> (<acl-script>)</acl-script></username></server-ip>	
at port <	ters Description:	
at port < Parame		
at port < Parame	ters Description:	

ARP Spoofing Prevention

Log Description	Severity
Event Description: A fake ARP packet detected by ARP Spoofing Prevention. Log Message: Gateway <ipaddr> is under attack by <macaddr> from <interface-id></interface-id></macaddr></ipaddr>	Warning
Parameters Description:	
ipaddr: The IP address of the gateway. macaddr: The MAC address of a hacker.	
interface-id: The interface where a hacker is located.	

Auto Save Configuration

Log Description	Severity
Event Description: Record the event when the configure information of DDP is saved automatically.	Informational
Log Message:CONFIG-6-DDPSAVECONFIG: [Unit <unitid>,]Configuration automatically saved to flash due to configuring from DDP(Username: <username>, IP: <ipaddr>)</ipaddr></username></unitid>	
Parameters Description:	
Unit: Box ID	
username: Represent current login user.	
ipaddr: Represent client IP address.	

Auto Surveillance VLAN

Log Description	Severity
Event Description: When a new surveillance device is detected on an interface.	Informational
Log Message: New surveillance device detected (<interface-id>, MAC: <mac-address>)</mac-address></interface-id>	
Parameters Description:	
interface-id: Interface name.	
mac-address: Surveillance device MAC address.	
Event Description: When an interface which is enabled surveillance VLAN joins the surveillance VLAN automatically.	Informational
Log Message: <interface-id> add into surveillance VLAN <vid></vid></interface-id>	
Parameters Description:	
interface-id: Interface name.	
vid: VLAN ID.	
Event Description: When an interface leaves the surveillance VLAN and at the same time, no surveillance device is detected in the aging interval for that interface, the log message will be sent.	Informational
Log Message: <interface-id> remove from surveillance VLAN <vid></vid></interface-id>	
Parameters Description:	
interface-id: Interface name.	
vid: VLAN ID.	
Event Description: When an IPC is added in the surveillance VLAN, the log message will be sent.	Informational
Log Message: ASV: Add IPC(<ipaddr>)</ipaddr>	
Parameters Description:	
ipaddr: Represent the IP address of the IPC.	

Log Description	Severity
Event Description: When an IPC is removed from the surveillance VLAN, the log message will be sent.	Informational
Log Message: ASV: Remove IPC(<ipaddr>)</ipaddr>	
Parameters Description:	
ipaddr: Represent the IP address of the IPC.	
Event Description: When an NVR is added in the surveillance VLAN, the log message will be sent.	Informational
Log Message: ASV: Add NVR(<ipaddr>)</ipaddr>	
Parameters Description:	
ipaddr: Represent the IP address of the NVR.	
Event Description: When an NVR is removed from the surveillance VLAN, the log message will be sent.	Informational
Log Message: ASV: Remove NVR(<ipaddr>)</ipaddr>	
Parameters Description:	
ipaddr: Represent the IP address of the NVR.	
Event Description: When the mode of ASV 2.0 is changed by Web GUI, the log message will be sent.	Informational
Log Message: ASV: Mode change from <mode> to <mode></mode></mode>	
Parameters Description:	
mode: Represent the mode of ASV 2.0 and the mode can be standard or surveillance.	

BPDU Attack Protection

Log Description	Severity
Event Description: Record the event when the BPDU attack happened. Log Message: <interface-id> enter STP BPDU under protection state (mode: <mode>)</mode></interface-id>	Informational
Parameters Description: interface-id: Interface on which detected STP BPDU attack. mode: BPDU Protection mode of the interface. Mode can be drop, block, or shutdown	
Event Description: Record the event when the STP BPDU attack recovered. Log Message: <interface-id> recover from BPDU under protection state Parameters Description: interface-id: Interface on which detected STP BPDU attack.</interface-id>	Informational

Configuration/Firmware

Log Description	Severity
Event description: Firmware upgraded successfully. Log Message: [Unit <unitid>,]Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverip>, File Name: <pathfile>) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address.</pathfile></serverip></macaddr></ipaddr></username></session></unitid>	Informational

Log Description	Severity
pathFile: Path and file name on server.	
Event description: Firmware upgraded unsuccessfully.	
Log Message: [Unit <unitid>,]Firmware upgraded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverip>, File Name: <pathfile>)</pathfile></serverip></macaddr></ipaddr></username></session></unitid>	
Parameters description:	
unitID: The unit ID.	
session: The user's session.	Warning
username: Represent current login user.	
ipaddr: Represent client IP address.	
macaddr : Represent client MAC address.	
serverIP: Server IP address.	
pathFile: Path and file name on server.	
Event description: Firmware uploaded successfully. Log Message: [Unit <unitid>,]Firmware uploaded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverip>, File Name: <pathfile>)</pathfile></serverip></macaddr></ipaddr></username></session></unitid>	
Parameters description:	
unitID: The unit ID.	Informational
session: The user's session.	mormational
username: Represent current login user.	
ipaddr: Represent client IP address.	
macaddr : Represent client MAC address.	
serverIP: Server IP address.	
pathFile: Path and file name on server.	
Event description: Firmware uploaded unsuccessfully. Log Message: [Unit <unitid>,]Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverip>, File Name: <pathfile>)</pathfile></serverip></macaddr></ipaddr></username></session></unitid>	
Parameters description:	
unitID: The unit ID.	
session: The user's session.	Warning
username: Represent current login user.	
ipaddr: Represent client IP address.	
macaddr : Represent client MAC address.	
serverIP: Server IP address.	
pathFile: Path and file name on server.	
Event description: Configuration downloaded successfully.	
Log Message: [Unit <unitid>,]Configuration downloaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverip>, File Name: <pathfile>)</pathfile></serverip></macaddr></ipaddr></username></session></unitid>	
Parameters description:	
unitID: The unit ID.	Informational
session: The user's session.	Informational
username: Represent current login user.	
ipaddr: Represent client IP address.	
macaddr : Represent client MAC address.	
serverIP: Server IP address.	
pathFile: Path and file name on server.	
Log Description	Severity
--	---------------
Log Message: [Unit <unitid>,]Configuration downloaded by <session></session></unitid>	
unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverip>, File Name: <pathfile>)</pathfile></serverip></macaddr></ipaddr></username>	
Parameters description:	
unitID: The unit ID.	
session: The user's session.	
username: Represent current login user.	
ipaddr: Represent client IP address.	
macaddr : Represent client MAC address.	
serverIP: Server IP address.	
pathFile: Path and file name on server.	
Event description: Configuration uploaded successfully.	
Log Message: [Unit <unitid>,]Configuration uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverip>, File Name: <pathfile>)</pathfile></serverip></macaddr></ipaddr></username></session></unitid>	
Parameters description:	
unitID: The unit ID.	Informational
session: The user's session.	
username: Represent current login user.	
ipaddr: Represent client IP address.	
macaddr : Represent client MAC address.	
serverIP: Server IP address.	
pathFile: Path and file name on server.	
Event description: Configuration uploaded unsuccessfully. Log Message: [Unit <unitid>,]Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverip>, File Name: <pathfile>)</pathfile></serverip></macaddr></ipaddr></username></session></unitid>	
Parameters description:	
unitID: The unit ID.	Warning
session: The user's session.	Wanning
username: Represent current login user.	
ipaddr: Represent client IP address.	
macaddr : Represent client MAC address. serverIP: Server IP address.	
pathFile: Path and file name on server.	
·	
Event description: Configuration saved to flash by console. Log Message: [Unit <unitid>,]Configuration saved to flash by console (Username: <username>)</username></unitid>	Informational
Parameters description:	
unitID: The unit ID.	
username: Represent current login user.	
Event description: Configuration saved to flash by remote.	
Log Message: [Unit <unitid>,]Configuration saved to flash (Username: <username>, IP: <ipaddr>)</ipaddr></username></unitid>	
Parameters description:	Informational
unitID: The unit ID.	
username: Represent current login user.	
ipaddr: Represent client IP address. Event description: Log message uploaded successfully.	

Log Description	Severity
Parameters description:	
unitID: The unit ID.	
session: The user's session.	
username: Represent current login user.	
ipaddr: Represent client IP address.	
macaddr: Represent client MAC address.	
Event description: Log message uploaded unsuccessfully.	
Log Message: [Unit <unitid>,] Log message uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>])</macaddr></ipaddr></username></session></unitid>	
Parameters description:	
unitID: The unit ID.	Warning
session: The user's session.	
username: Represent current login user.	
ipaddr: Represent client IP address.	
macaddr: Represent client MAC address.	
Event description: Unknown type files downloaded unsuccessfully.	
Log Message: [Unit <unitid>,]Downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverip>, File Name: <pathfile>)</pathfile></serverip></macaddr></ipaddr></username></session></unitid>	
Parameters description:	
unitID: The unit ID.	
session: The user's session.	Warning
username: Represent current login user.	
ipaddr: Represent client IP address.	
macaddr : Represent client MAC address.	
serverIP: Server IP address.	
pathFile: Path and file name on server.	



NOTE: 1. The user's session refers to Console, Web, SNMP, Telnet, and SSH sessions.

- 2. If the Switch is in the standalone state, there will be no unit ID in the log message.
- 3. If the configuration or firmware was downloaded or uploaded through the console, there will be no IP address and MAC address information in the log message.

DAI

Log Description	Severity
Event Description: This log will be generated when DAI detect invalid ARP packet.	Warning
Log Message: Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac- address>, VLAN <vlan-id>, on <interface-id>)</interface-id></vlan-id></mac- </ip-address></type>	
Parameters Description:	
type: The type of ARP packet, it indicates that ARP packet is request or ARP response.	
Event Description: This log will be generated when DAI detect valid ARP packet.	Informational
Log Message: Legal ARP <type> packets (IP: <ip-address>, MAC: <mac- address>, VLAN <vlan-id>, on <interface-id>).</interface-id></vlan-id></mac- </ip-address></type>	

Log Description	Severity
Parameters Description:	
type: The type of ARP packet, it indicates that ARP packet is request or ARP response.	

DDM

Log Description	Severity
Event Description: when the any of SFP parameters exceeds from the warning threshold.	Warning
Log Message: Optical transceiver <interface-id> <component> <high-low> warning threshold exceeded</high-low></component></interface-id>	
Parameters Description:	
interface-id: port interface ID.	
component: DDM threshold type. It can be one of the following types:	
temperature	
supply voltage	
bias current	
TX power	
RX power	
high-low: High or low threshold.	
Event Description: when the any of SFP parameters exceeds from the alarm threshold.	Critical
Log Message: Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded</high-low></component></interface-id>	
Parameters Description:	
interface-id: port interface ID.	
component: DDM threshold type. It can be one of the following types:	
temperature	
supply voltage	
bias current	
TX power	
RX power	
high-low: High or low threshold.	
Event Description: when the any of SFP parameters recovers from the warning threshold.	Warning
Log Message: Optical transceiver <interface-id> <component> back to normal</component></interface-id>	
Parameters Description:	
interface-id: port interface ID.	
component: DDM threshold type. It can be one of the following types:	
temperature	
supply voltage	
bias current	
TX power	
RX power	

DHCPv6 Client

Log Description	Severity
Event Description: DHCPv6 client interface administrator state changed. Log Message: DHCPv6 client on interface <ipif-name> changed state to [enabled disabled]</ipif-name>	Informational

Log Description	Severity
Parameters Description:	
<ipif-name>: Name of the DHCPv6 client interface.</ipif-name>	
Event Description: DHCPv6 client obtains an ipv6 address from a DHCPv6 server.	Informational
Log Message: DHCPv6 client obtains an ipv6 address <ipv6address> on interface <ipif-name></ipif-name></ipv6address>	
Parameters Description:	
ipv6address: ipv6 address obtained from a DHCPv6 server.	
ipif-name: Name of the DHCPv6 client interface.	
Event Description: The ipv6 address obtained from a DHCPv6 server starts renewing.	Informational
Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts renewing</ipif-name></ipv6address>	
Parameters Description:	
ipv6address: ipv6 address obtained from a DHCPv6 server.	
ipif-name: Name of the DHCPv6 client interface.	
Event Description: The ipv6 address obtained from a DHCPv6 server renews success.	Informational
Log Message: The IPv6 address <ipv6address> on interface <ipif-name> renews success</ipif-name></ipv6address>	
Parameters Description:	
ipv6address: ipv6 address obtained from a DHCPv6 server.	
ipif-name: Name of the DHCPv6 client interface.	
Event Description: The ipv6 address obtained from a DHCPv6 server starts rebinding.	Informational
Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts rebinding</ipif-name></ipv6address>	
Parameters Description:	
ipv6address: ipv6 address obtained from a DHCPv6 server.	
ipif-name: Name of the DHCPv6 client interface.	
Event Description: The ipv6 address obtained from a DHCPv6 server rebinds success.	Informational
Log Message: The IPv6 address <ipv6address> on interface <ipif-name> rebinds success</ipif-name></ipv6address>	
Parameters Description:	
ipv6address: ipv6 address obtained from a DHCPv6 server.	
ipif-name: Name of the DHCPv6 client interface.	
Event Description: The ipv6 address from a DHCPv6 server was deleted.	Informational
Log Message: The IPv6 address <ipv6address> on interface <ipif-name> was deleted</ipif-name></ipv6address>	
Parameters Description:	
ipv6address: ipv6 address obtained from a DHCPv6 server.	
ipif-name: Name of the DHCPv6 client interface.	

DHCPv6 Relay

Log Description	Severity
Event Description: DHCPv6 relay on a specify interface's administrator state changed.	Informational
Log Message: DHCPv6 relay on interface <ipif-name> changed state to [enabled disabled]</ipif-name>	
Parameters Description:	

Log Description	Severity
ipif-name>: Name of the DHCPv6 relay agent interface.	

DNS Resolver

Log Description	Severity
Event Description: Duplicate Domain name cache added, leads a dynamic domain name cache be deleted.	Informational
Log Message: Duplicate Domain name case name: <domainname>, static IP: <ipaddr>, dynamic IP:<ipaddr></ipaddr></ipaddr></domainname>	
Parameters Description:	
domainname: the domain name string.	
ipaddr: IP address.	

DoS Prevention

Log Description	Severity
Event Description: Detect DOS attack.	Notice
Log Message: <dos-type> is dropped from (IP: <ip-address> Port <interface- id>)</interface- </ip-address></dos-type>	
Parameters Description:	
dos-type: DOS attack type	
ip-address: IP address.	
interface-id: Interface name	

ErrDisable

Log Description	Severity
Event Description: When a port enters the error-disabled state.	Warning
Log Message: Port <interface-id> enters error disable state due to <reason-id></reason-id></interface-id>	
Parameters Description:	
interface-id: The port number.	
reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, Digital Diagnostics Monitoring, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving.	
Event Description: When a port leaves the error-disabled state.	Warning
Log Message: Port <interface-id> leaves the error disable state which is previously caused by <reason-id></reason-id></interface-id>	
Parameters Description:	
interface-id: The port number.	
reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, Digital Diagnostics Monitoring, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving.	
Event Description: When a port enters the error-disabled state.	Warning
Log Message: Port <interface-id> VLAN <vid> enters error disable state due to <reason-id></reason-id></vid></interface-id>	
Parameters Description:	
interface-id: The port number.	
reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, Digital Diagnostics Monitoring, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving.	

Log Description	Severity
vid: The VLAN ID.	
Event Description: When a port leaves the error-disabled state. Log Message: Port <interface-id> VLAN <vid> leaves the error disable state which is previously caused by <reason-id></reason-id></vid></interface-id>	Warning
Parameters Description: interface-id: The port number.	
reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, Digital Diagnostics Monitoring, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving.	
vid: The VLAN ID.	

Interface

Log Description	Severity
Event Description: When port is down.	Informational
Log Message: Port <port-type> <interface-id> link down</interface-id></port-type>	
Parameters Description:	
port-type: port type	
interface-id: Interface name	
Event Description: When port is up.	Informational
Log Message: Port <port-type> <interface-id> link up, <link-speed></link-speed></interface-id></port-type>	
Parameters Description:	
port-type: port type	
interface-id: Interface name	
link-speed: port link speed.	
Event Description: Port is linked on half duplex mode.	Informational
Log Message: ASV: Port < interface-id> Half duplex detected	
Parameters Description:	
interface-id: Interface name	

JWAC

Log Description	Severity
Event Description: when a host has passed the authentication.	Informational
Log Message: JWAC host login success (Username: <string>, IP: <ipaddr <br="">ipv6address>, MAC: <mac-address>, <interface-id>, VID: <vlan-id>)</vlan-id></interface-id></mac-address></ipaddr></string>	
Parameters Description:	
Username: The host username.	
IP: The host IP address	
mac-address: The host MAC addresses.	
interface-id: The interface on which the host is authenticated.	
vlan-id: The VLAN ID on which the host exists.	
Event Description: When a host fail to pass the authentication.	Critical
Log Message: JWAC host login fail (Username: <string>, IP: <ipaddr <br="">ipv6address>, MAC: <mac-address>, <interface-id>, VID: <vlan-id>)</vlan-id></interface-id></mac-address></ipaddr></string>	
Parameters Description:	
Username: The host username.	
IP: The host IP address	
mac-address: The host MAC addresses.	
interface-id: The interface on which the host is authenticated.	

Log Description	Severity
vlan-id: The VLAN ID on which the host exists.	
Event Description: when the authorized user number on the whole device has reached the maximum user limit. Log Message: JWAC enters stop learning state	Warning
Event Description: when the authorized user number on the whole device is below the maximum user limit in a time interval. Log Message: JWAC recovers from stop learning state	Warning

LACP

Log Description	Severity
Event Description: Link Aggregation Group link up.	Informational
Log Message: Link Aggregation Group <group_id> link up</group_id>	
Parameters Description:	
group_id: The group id of the link down aggregation group.	
Event Description: Link Aggregation Group link down.	Informational
Log Message: Link Aggregation Group <group_id> link down</group_id>	
Parameters Description:	
group_id: The group id of the link down aggregation group.	
Event Description: Member port attach to Link Aggregation Group.	Informational
Log Message: <ifname> attach to Link Aggregation Group <group_id></group_id></ifname>	
Parameters Description:	
ifname: The interface name of the port that attach to aggregation group.	
group_id: The group id of the aggregation group that port attach to.	
Event Description: Member port detach from Link Aggregation Group.	Informational
Log Message: <ifname> detach from Link Aggregation Group <group_id></group_id></ifname>	
Parameters Description:	
ifname: The interface name of the port that detach from aggregation group.	
group_id: The group id of the aggregation group that port detach from.	

LBD

Log Description	Severity
Event Description: Record the event when an interface detect loop. Log Message: <interface-id> LBD loop occurred Parameters Description: interface-id: Interface on which loop is detected.</interface-id>	Critical
Event Description: Record the event when an interface detect loop. Log Message: <interface-id> VLAN <vlan-id> LBD loop occurred Parameters Description: interface-id: Interface on which loop is detected. vlan-id: VLAN on which loop is detected.</vlan-id></interface-id>	Critical
Event Description: Record the event when an interface loop recovered. Log Message: <interface-id> LBD loop recovered Parameters Description: interface-id: Interface on which loop is detected.</interface-id>	Critical
Event Description: Record the event when an interface loop recovered.	Critical

Log Description	Severity
Log Message: <interface-id> VLAN <vlan-id> LBD loop recovered</vlan-id></interface-id>	
Parameters Description:	
interface-id: Interface on which loop is detected.	
vlan-id: VLAN on which loop is detected.	
Event Description: Record the event when the number of VLANs that loop back has occurred exceeds a reserved number.	Critical
Log Message: Loop VLAN numbers overflow	

LLDP-MED

Log Description	Severity
Event Description: LLDP-MED topology change detected.	Notice
Log Message: LLDP-MED topology change detected (on port <portnum>. chassis id: <chassistype>, <chassisid>, port id: <porttype>, <portid>, device class: <deviceclass>)</deviceclass></portid></porttype></chassisid></chassistype></portnum>	
Parameters Description:	
portNum: The port number.	
chassisType: chassis ID subtype.	
Value list:	
1. chassisComponent(1)	
2. interfaceAlias(2)	
3. portComponent(3)	
4. macAddress(4)	
5. networkAddress(5)	
6. interfaceName(6)	
7. local(7)	
chassisID: chassis ID.	
portType: port ID subtype.	
Value list:	
1. interfaceAlias(1)	
2. portComponent(2)	
3. macAddress(3)	
4. networkAddress(4)	
5. interfaceName(5)	
6. agentCircuitId(6)	
7. local(7)	
portID: port ID.	
deviceClass: LLDP-MED device type.	
Event Description: Conflict LLDP-MED device type detected.	Notice
Log Message: Conflict LLDP-MED device type detected (on port <portnum>, chassis id: <chassistype>, <chassisid>, port id: <porttype>, <portid>, device class: <deviceclass>)</deviceclass></portid></porttype></chassisid></chassistype></portnum>	
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)	

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

Login/Logout CLI

Log Description	Severity
Event Description: Login through console successfully.	Informational
Log Message: [Unit <unitid>,]Successful login through Console (Username: <username>)</username></unitid>	
Parameters Description:	
unitID: The unit ID.	
username: Represent current login user.	

Log Description	Severity
Event Description: Login through console unsuccessfully.	Warning
Log Message: [Unit <unitid>,] Login failed through Console (Username: <username>)</username></unitid>	
Parameters Description:	
unitID: The unit ID.	
username: Represent current login user.	
Event Description: Console session timed out.	Informational
Log Message: [Unit <unitid>,] Console session timed out (Username: <username>)</username></unitid>	
Parameters Description:	
unitID: The unit ID.	
username: Represent current login user.	
Event Description: Logout through console. Log Message: [Unit <unitid>,] Logout through Console (Username: <username>)</username></unitid>	Informational
Parameters Description:	
unitID: The unit ID.	
username: Represent current login user.	
Event Description: Login through telnet successfully. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>)</ipaddr></username>	Informational
Parameters Description:	
username: Represent current login user.	
ipaddr: Represent client IP address.	
Event Description: Login through telnet unsuccessfully.	Warning
Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>)</ipaddr></username>	
Parameters Description:	
username: Represent current login user.	
ipaddr: Represent client IP address.	
Event Description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP:</username>	Informational
<ipaddr>) Parameters Description:</ipaddr>	
username: Represent current login user.	
ipaddr: Represent client IP address.	
Event Description: Logout through telnet.	Informational
Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>)</ipaddr></username>	
Parameters Description:	
username: Represent current login user.	
ipaddr: Represent client IP address.	
Event Description: Login through SSH successfully.	Informational
Log Message: Successful login through SSH (Username: <username>, IP: <ipaddr>)</ipaddr></username>	
Parameters Description:	
username: Represent current login user.	
ipaddr: Represent client IP address.	
Event Description: Login through SSH unsuccessfully.	Critical
Log Message: Login failed through SSH (Username: <username>, IP:</username>	
<ipaddr>)</ipaddr>	

Log Description	Severity
Parameters Description:	
username: Represent current login user.	
ipaddr: Represent client IP address.	
Event Description: SSH session timed out.	Informational
Log Message: SSH session timed out (Username: <username>, IP: <ipaddr>)</ipaddr></username>	
Parameters Description:	
username: Represent current login user.	
ipaddr: Represent client IP address.	
Event Description: Logout through SSH.	Informational
Log Message: Logout through SSH (Username: <username>, IP: <ipaddr>)</ipaddr></username>	
Parameters Description:	
username: Represent current login user.	
ipaddr: Represent client IP address.	

MAC-based Access Control

Log Description	Severity
Event Description: A host has passed the authentication.	Informational
Log Message: MAC-based Access Control host login success (MAC: <mac- address>, <interface-id>, VID: <vlan-id>)</vlan-id></interface-id></mac- 	
Parameters Description:	
mac-address: The host MAC address.	
interface-id: The interface on which the host is authenticated.	
vlan-id: The VLAN ID on which the host exists after it is authenticated.	
Event Description: A host has aged out.	Informational
Log Message: MAC-based Access Control host aged out (MAC: <mac- address>, <interface-id>, VID: <vlan-id>)</vlan-id></interface-id></mac- 	
Parameters Description:	
mac-address: The host MAC address.	
interface-id: The interface on which the host is authenticated.	
vlan-id: The VLAN ID on which the host exists before it is aged out.	
Event Description: A host failed to pass the authentication.	Critical
Log Message: MAC-based Access Control host login fail (MAC: <mac- address>, <interface-id>, VID: <vlan-id>)</vlan-id></interface-id></mac- 	
Parameters Description:	
mac-address: The host MAC address.	
interface-id: The interface on which the host is authenticated.	
vlan-id: The originated VLAN ID on which the host exists.	
Event Description: The authorized user number on the whole device has reached the maximum user limit.	Warning
Log Message: MAC-based Access Control enters stop learning state	
Event Description: The authorized user number on the whole device is below the maximum user limit in a time interval.	Warning
Log Message: MAC-based Access Control recovers from stop learning state	
Event Description: The authorized user number on an interface has reached the maximum user limit.	Warning
Log Message: <interface-id> enters MAC-based Access Control stop learning state</interface-id>	
Parameters Description:	
interface-id: The interface on which the host is authenticated.	

Log Description	Severity
Event Description: The authorized user number on an interface is below the maximum user limit in a time interval.	Warning
Log Message: <interface-id> recovers from MAC-based Access Control stop learning state</interface-id>	
Parameters Description:	
interface-id: The interface on which the host is authenticated.	

MSTP Debug Enhancement

Log Description	Severity
Event Description: Used to record the event that Spanning Tree Protocol is enabled.	Informational
Log Message: Spanning Tree Protocol is enabled	
Event Description: Used to record the event that Spanning Tree Protocol is disabled.	Informational
Log Message: Spanning Tree Protocol is disabled	
Event Description: Used to record MSTP instance topology change event.	Notice
Log Message: Topology changed (Instance : <instance-id>,<interface_id>, MAC:<macaddr>)</macaddr></interface_id></instance-id>	
Parameters Description:	
Instance-id: MST instance id. Instance 0 represents for default instance, CIST.	
interface_id: The port number which detect or receive topology change information.	
macaddr: The system of bridge mac address.	
Event Description: Used to record MSTP instance new root bridge selected. Log Message: [CIST CIST Regional MSTI Regional] New Root bridge selected ([Instance: <instance-id>] MAC: <macaddr> Priority :<priority>)</priority></macaddr></instance-id>	Informational
Parameters Description:	
Instance-id: MST instance id. Instance 0 represents for default instance, CIST.	
macaddr: The system of bridge mac address.	
priority: The bridge priority value must be divisible by 4096.	
Event Description: Used to record MSTP instance new root port selected.	Notice
Log Message: New root port selected (Instance: <instance-id>, <interface_id>)</interface_id></instance-id>	
Parameters Description:	
Instance-id: MST instance id. Instance 0 represents for default instance, CIST.	
interface_id: The port number which detect or receive topology change information.	
Event Description: Used to record MSTP instance port state change event.	Notice
Log Message: Spanning Tree port status change (Instance : <instance-id>, <interface_id>) <old_status> -> <new_status></new_status></old_status></interface_id></instance-id>	
Parameters Description:	
Instance-id: MST instance id. Instance 0 represents for default instance, CIST.	
interface_id: The port number which detect or receive topology change information.	
old status:	
new status:	
The port of STP state. The value may be Disable, Discarding, Learning, Forwarding	

Log Description	Severity
Event description: Used to record MSTP instance port role change event.	Informational
Log Message: Spanning Tree port role change (Instance : <instance-id>, <interface_id>) <old_role> -> <new_role></new_role></old_role></interface_id></instance-id>	
Parameters description:	
Instance-id: MST instance id. Instance 0 represents for default instance, CIST.	
Interface_id: The port number which detect or receive topochange information.	
old role:	
new role :	
The port role of stp. The value may be DisabledPort, AlternatePort, BackupPort, RootPort, DesignatedPort, MasterPort.	
Event Description: Use to record action to create an MST instance.	Informational
Log Message: Spanning Tree instance created (Instance : <instance-id>)</instance-id>	
Parameters Description:	
Instance-id: MST instance id. Instance 0 represents for default instance, CIST.	
Event Description: Use to record action to delete an MST instance.	Informational
Log Message: Spanning Tree instance deleted (Instance : <instance-id>)</instance-id>	
Parameters Description:	
Instance-id: MST instance id. Instance 0 represents for default instance, CIST.	
Event Description: Use to record action to change the STP version.	Informational
Log Message: Spanning Tree version change (new version : <new_version>)</new_version>	
Parameters Description:	
new_version: Running under which version of STP.	
Event Description: Used to record the configuration name and revision level changed in the MST Configuration Identification.	Informational
Log Message: Spanning Tree MST configuration ID name and revision level change (name: <name>, revision level <revision_level>)</revision_level></name>	
Parameters Description:	
name: The name given for a specified MST region.	
revision_level: Switches using the same given name but with a different revision level are considered members of different MST regions.	
Event Description: Use to record action to maps a VLAN(s) to an MST instance.	Informational
Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <instance-id> add vlan <startvlanid> [- <endvlanid>])</endvlanid></startvlanid></instance-id>	
Parameters Description:	
Instance-id: MST instance id. Instance 0 represents for default instance, CIST.	
startvlanid: The start vid of add vlan range.	
endvlanid: The end vid of add vlan range.	
Event Description: Use to record action to delete a VLAN(s) from an MST instance.	Informational
Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <instance-id> delete vlan <startvlanid> [- <endvlanid>])</endvlanid></startvlanid></instance-id>	
Parameters Description:	
Instance-id: MST instance id. Instance 0 represents for default instance, CIST.	
startvlanid: The start vid of delete vlan range.	

Log Description	Severity
endvlanid: The end vid of delete vlan range.	
Event Description: Used to record the event that port role change to alternate due to guard root.	Informational
Log Message: Spanning Tree port role change (Instance : <instance-id>, <interface-id>) to alternate port due to the guard root</interface-id></instance-id>	
Parameters Description:	
Instance-id: MST instance id. Instance 0 represents for default instance, CIST.	
Interface_id: The port number which detect the event.	

Peripheral

Log Description	Severity
Event Description: Fan Recovered.	Critical
Log Message: Unit <id>, <fan-descr> back to normal</fan-descr></id>	
Parameters Description:	
Unit <id>: The unit ID.</id>	
fan-descr: The FAN ID and position.	
Event Description: Fan Fail.	Critical
Log Message: Unit <id> <fan-descr> failed</fan-descr></id>	
Parameters Description:	
Unit <id>: The unit ID.</id>	
fan-descr: The FAN ID and position.	
Event Description: Temperature sensor enters alarm state.	Critical
Log Message: Unit <unit-id> <thermal-sensor-descr> detects abnormal temperature <degree></degree></thermal-sensor-descr></unit-id>	
Parameters Description:	
unitID: The unit ID.	
thermal-sensor-descr: The sensor ID and position.	
degree: The current temperature.	
Event Description: Temperature recovers to normal.	Critical
Log Message: Unit <unit-id> <thermal-sensor-descr> temperature back to normal</thermal-sensor-descr></unit-id>	
Parameters Description:	
unitID: The unit ID.	
thermal-sensor-descr: The sensor ID and position.	
Event Description: Power failed.	Critical
Log Message: Unit <unit-id> <power-descr> failed</power-descr></unit-id>	
Parameters Description:	
unitID: The unit ID.	
power-descr: The power position and ID.	
Event Description: Power is recovered.	Critical
Log Message: Unit <unit-id> <power-descr> back to normal</power-descr></unit-id>	
Parameters Description:	
unitID: The unit ID.	
power-descr: The power position and ID.	
Event Description: Press the factory reset button.	Critical
Log Message: Unit <unit-id> factory reset button pressed</unit-id>	
Parameters Description:	
unitID: The unit ID.	

ΡοΕ

Log Description	Severity
Event Description: Total power usage threshold is exceeded Log Message: Unit <unit-id> usage threshold <percentage> is exceeded Parameters Description: unit-id: The box ID.</percentage></unit-id>	Warning
percentage: The usage threshold.	
Event Description: Total power usage threshold is recovered.	Warning
Log Message: Unit <unit-id> usage threshold <percentage> is recovered Parameters Description: unit-id: The box ID. percentage: The usage threshold.</percentage></unit-id>	
Event Description: PD doesn't reply the ping request.	Warning
Log Message: PD alive check failed. (Port: <portnum>, PD: <ipaddr>) Parameters Description: portNum: The port number. ipaddr: The IP (IPv4/IPv6) address of PD.</ipaddr></portnum>	Warning
Event Description: Power removal due to absence of Maintain Power Signature (MPS).	Warning
Log Message: ASV: Port <port-type><interface-id> PoE MPS Absent Parameters Description: port-type: The port type.</interface-id></port-type>	
interface-id: The interface name.	
Event Description: Short circuit condition detected. Log Message: ASV: Port <port-type><interface-id> PoE PD short Parameters Description: port-type: The port type. interface-id: The interface name.</interface-id></port-type>	Warning
Event Description: Overload condition detected. Log Message: ASV: Port <port-type><interface-id> PoE Overload Parameters Description: port-type: The port type. interface-id: The interface name.</interface-id></port-type>	Warning
Event Description: Power has been denied or removed due to fault. Log Message: ASV: Port <port-type><interface-id> PoE Power Denied Parameters Description: port-type: The port type. interface-id: The interface name.</interface-id></port-type>	Warning
Event Description: Power has been denied or removed due to overheat. Log Message: ASV: Port <port-type><interface-id> PoE Thermal Shutdown Parameters Description: port-type: The port type. interface-id: The interface name.</interface-id></port-type>	Warning
Event Description: PoE startup failure on port. Log Message: ASV: Port <port-type><interface-id> PoE Startup Failure Parameters Description: port-type: The port type. interface-id: The interface name.</interface-id></port-type>	Warning

Log Description	Severity
Log Message: ASV: Port <port-type><interface-id> PoE Classification Failure</interface-id></port-type>	
Parameters Description:	
port-type: The port type.	
interface-id: The interface name.	

Port Security

Log Description	Severity
Event Description: Address full on a port.	Warning
Log Message: MAC address <macaddr> causes port security violation on <interface-id></interface-id></macaddr>	
Parameters Description:	
macaddr: The violation MAC address.	
interface-id: The interface name.	
Event Description: Address full on system.	Warning
Log Message: Limit on system entry number has been exceeded	

Safeguard

Log Description	Severity
Event Description: the host enters the mode of exhausted.	Warning
Log Message: Unit <unit-id>, Safeguard Engine enters EXHAUSTED mode</unit-id>	
Parameters Description:	
unit-id: The Unit ID	
Event Description: the host enters the mode of normal.	Informational
Log Message: Unit <unit-id>, Safeguard Engine enters NORMAL mode</unit-id>	
Parameters Description:	
unit-id: The Unit ID	

SNMP

Log Description	Severity
Event Description: SNMP request received with invalid community string. Log Message: SNMP request received from <ipaddr> with invalid community string</ipaddr>	Informational
Parameters Description:	
ipaddr: The IP address.	

SSH

Log Description	Severity
Event Description: SSH server is enabled. Log Message: SSH server is enabled	Informational
Event Description: SSH server is disabled. Log Message: SSH server is disabled	Informational

Stacking

Log Description	Severity
Event Description: Hot insertion.	Informational

Log Description	Severity
Log Message: Unit: <unitid>, MAC: <macaddr> Hot insertion</macaddr></unitid>	
Parameters Description:	
unitID: Box ID.	
Macaddr: MAC address.	
Event Description: Hot removal.	Informational
Log Message: Unit: <unitid>, MAC: <macaddr> Hot removal</macaddr></unitid>	
Parameters Description:	
unitID: Box ID.	
Macaddr: MAC address.	
Event Description: Stacking topology change.	Informational
Log Message: Stacking topology is <stack_tp_type>. Master(Unit <unitid>, MAC:<macaddr>)</macaddr></unitid></stack_tp_type>	
Parameters Description:	
Stack_TP_TYPE: The stacking topology type is one of the following:	
1. Ring,	
2. Chain.	
unitID: Box ID.	
Macaddr: MAC address.	
Event Description: Backup master changed to master.	Informational
Log Message: Backup master changed to master. Master (Unit: <unitid>)</unitid>	
Parameters Description:	
unitID: Box ID.	
Parameters Description: unitID: Box ID.	
Event Description: Box ID conflict.	Critical
Log Message: Hot insert failed, box ID conflict: Unit <unitid> conflict (MAC: <macaddr> and MAC: <macaddr>)</macaddr></macaddr></unitid>	
Parameters Description:	
unitID: Box ID.	
macaddr: The MAC addresses of the conflicting boxes.	
Event Description: Stacking port linkup. A Stacking port will act as a SIO interface or a member of a SIO interface (SIO Trunk). This log entry is only available on projects that stacking port has got a port number indicator on device's panel.	Critical
Log Message: Stacking port <port> link up</port>	
Parameters Description:	
port: Represents the logical port number of a Stacking port.	
Event Description: Stacking port link down. A Stacking port will act as a SIO interface or a member of a SIO interface (SIO Trunk). This log entry is only available on projects that stacking port has got a port number indicator on device's panel.	Critical
Log Message: Stacking port <port> link down</port>	
Parameters Description:	
port: Represents the logical port number of a Stacking port.	
Event Description: SIO interface linkup. For SIO Trunk, the first member port link up will trigger this event.	Critical
Log Message: SIO interface Unit <unitid> <sion> link up</sion></unitid>	
Parameters Description:	
unitID: Box ID.	

Log Description	Severity
SIOn: Represents the SIO interface number. Current Supported SIO interface number should be SIO1 and SIO2.	
Event Description: SIO interface link down. For SIO Trunk, the last member port link down will trigger this event.	Critical
Log Message: SIO interface Unit <unitid> <sion> link down</sion></unitid>	
Parameters Description:	
unitID: Box ID.	
SIOn: Represents the SIO interface number. Current Supported SIO interface number should be SIO1 and SIO2.	

Storm Control

Log Description	Severity
Event Description: Storm occurrence.	Warning
Log Message: <broadcast multicast="" unicast="" =""> storm is occurring on <interface-id></interface-id></broadcast>	
Parameters Description:	
Broadcast: Storm is resulted by broadcast packets(DA = FF:FF:FF:FF:FF).	
Multicast: Storm is resulted by multicast packets, including unknown L2 multicast, known L2 multicast, unknown IP multicast and known IP multicast.	
Unicast: Storm is resulted by unicast packets, including both known and unknown unicast packets	
interface-id: The interface ID on which a storm is occurring.	
Event Description: Storm cleared.	Informational
Log Message: <broadcast multicast="" unicast="" =""> storm is cleared on <interface-id></interface-id></broadcast>	
Parameters Description:	
Broadcast: Broadcast storm is cleared.	
Multicast: Multicast storm is cleared.	
Unicast: Unicast storm (including both known and unknown unicast packets) is cleared.	
interface-id: The interface ID on which a storm is cleared.	
Event Description: Port shut down due to a packet storm.	Warning
Log Message: <interface-id> is currently shut down due to the <broadcast <br="">Multicast Unicast> storm</broadcast></interface-id>	
Parameters Description:	
interface-id: The interface ID on which is error-disabled by storm.	
Broadcast: The interface is disabled by broadcast storm.	
Multicast: The interface is disabled by multicast storm.	
Unicast: The interface is disabled by unicast storm (including both known and unknown unicast packets).	

System Log Summary

Log Description	Severity
Event Description: This log will be generated when system warm start. Log Message: [Unit <unitid>,]System warm start Parameters Description: unitID: The unit ID.</unitid>	Critical
Event Description: This log will be generated when system cold start.	Critical

Log Description	Severity
Log Message: [Unit <unitid>,]System cold start</unitid>	
Parameters Description:	
unitID: The unit ID.	
Event Description: This log will be generated when system start up.	
Log Message: [Unit <unitid>,]System started up.</unitid>	Oritical
Parameters Description:	Critical
unitID: The unit ID.	

Telnet

Log Description	Severity
Event Description: Successful login through Telnet.	Informational
Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>)</ipaddr></username>	
Parameters Description:	
ipaddr: The IP address of telnet client.	
username: the user name that used to login telnet server.	
Event Description: Login failed through Telnet.	Warning
Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>)</ipaddr></username>	
Parameters Description:	
ipaddr: The IP address of telnet client.	
username: the user name that used to login telnet server.	
Event Description: Logout through Telnet.	Informational
Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>)</ipaddr></username>	
Parameters Description:	
ipaddr: The IP address of telnet client.	
username: the user name that used to login telnet server.	
Event Description: Telnet session timed out.	Informational
Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>)</ipaddr></username>	
Parameters Description:	
ipaddr: The IP address of telnet client.	
username: the user name that used to login telnet server.	

Voice-VLAN

Log Description	Severity
Event Description: When a new voice device is detected on an interface.	Informational
Log Message: New voice device detected (<interface-id>, MAC: <mac- address>)</mac- </interface-id>	
Parameters Description:	
interface-id: Interface name.	
mac-address: Voice device MAC address	
Event Description: When an interface which is in auto voice VLAN mode joins the voice VLAN.	Informational
Log Message: <interface-id> add into voice VLAN <vid></vid></interface-id>	
Parameters Description:	
interface-id: Interface name.	
vid: VLAN ID	

Log Description	Severity
Event Description: When an interface leaves the voice VLAN and at the same time, no voice device is detected in the aging interval for that interface, the log message will be sent.	Informational
Log Message: <interface-id> remove from voice VLAN <vid></vid></interface-id>	
Parameters Description:	
interface-id: Interface name.	
vid: VLAN ID	

Web

Log Description	Severity
Event Description: Successful login through Web.	Informational
Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>)</ipaddr></username>	
Parameters Description:	
username: The use name that used to login HTTP server.	
ipaddr: The IP address of HTTP client.	
Event Description: Login failed through Web.	Warning
Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>)</ipaddr></username>	
Parameters Description:	
username: The use name that used to login HTTP server.	
ipaddr: The IP address of HTTP client.	
Event Description: Web session timed out.	Informational
Log Message: Web session timed out (Username: <username>, IP: <ipaddr>)</ipaddr></username>	
Parameters Description:	
username: The use name that used to login HTTP server.	
ipaddr: The IP address of HTTP client.	
Event Description: Logout through Web.	Informational
Log Message: Logout through Web (Username: <username>, IP: <ipaddr>)</ipaddr></username>	
Parameters Description:	
username: The use name that used to login HTTP server.	
ipaddr: The IP address of HTTP client.	
Event Description: Successful login through Web (SSL).	Informational
Log Message: Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>)</ipaddr></username>	
Parameters Description:	
username: The use name that used to login SSL server.	
ipaddr: The IP address of SSL client.	
Event Description: Login failed through Web (SSL).	Warning
Log Message: Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>)</ipaddr></username>	
Parameters Description:	
username: The use name that used to login SSL server.	
ipaddr: The IP address of SSL client.	
Event Description: Web (SSL) session timed out.	Informational
Log Message: Web (SSL) session timed out (Username: <username>, IP: <ipaddr>)</ipaddr></username>	
Parameters Description:	
username: The use name that used to login SSL server.	

Log Description	Severity
ipaddr: The IP address of SSL client.	
Event Description: Logout through Web(SSL).	Informational
Log Message: Logout through Web(SSL) (Username: <username>, IP: <ipaddr>)</ipaddr></username>	
Parameters Description:	
username: The use name that used to login SSL server. ipaddr: The IP address of SSL client.	

Web-Authentication

Log Description	Severity
Event Description: When a host has passed the authentication.	Informational
Log Message: Web-Authentication host login success (Username: <string>, IP: <ipaddr ipv6address="" ="">, MAC: <mac-address>, <interface-id>, VID: <vlan- id>)</vlan- </interface-id></mac-address></ipaddr></string>	
Parameters Description:	
Username: The host username.	
IP: The host IP address	
mac-address: The host MAC addresses.	
interface-id: The interface on which the host is authenticated.	
vlan-id: The VLAN ID on which the host exists.	
Event Description: When a host fail to pass the authentication.	Critical
Log Message: Web-Authentication host login fail (Username: <string>, IP: <ipaddr ipv6address="" ="">, MAC: <mac-address>, <interface-id>, VID: <vlan-id>)</vlan-id></interface-id></mac-address></ipaddr></string>	
Parameters Description:	
Username: The host username.	
IP: The host IP address	
mac-address: The host MAC addresses.	
interface-id: The interface on which the host is authenticated.	
vlan-id: The VLAN ID on which the host exists.	
Event Description: when the authorized user number on the whole device has reached the maximum user limit.	Warning
Log Message: Web-Authentication enters stop learning state	
Event Description: when the authorized user number on the whole device is below the maximum user limit in a time interval.	Warning
Log Message: Web-Authentication recovers from stop learning state	

Appendix B - Trap Entries

The following tables list the trap log entries and their corresponding meanings that will appear in the switch.

802.1X

Trap Name	Description	OID
dDot1xExtLoggedSuccess	The trap is sent when a host has successfully logged in (passed 802.1X authentication). Binding objects: (1) ifIndex (2) dnaSessionClientMacAddress	1.3.6.1.4.1.171 .14.30.0.1
	(3) dnaSessionAuthVlan(4) dnaSessionAuthUserName	
dDot1xExtLoggedFail	The trap is sent when a host failed to pass 802.1X authentication (login failed). Binding objects: (1) ifIndex (2) dnaSessionClientMacAddress	1.3.6.1.4.1.171 .14.30.0.2
	(3) dnaSessionAuthVlan(4) dnaSessionAuthUserName(5) dDot1xExtNotifyFailReason	

Authentication Fail

Trap Name	Description	OID
authenticationFailure	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.	1.3.6.1.6.3.1.1. 5.5

BPDU Attack Protection

Trap Name	Description	OID
dBpduProtectionAttackOccur	This trap is sent when the BPDU attack happened on an interface.	1.3.6.1.4.1.171 .14.47.0.1
	Binding objects:	
	(1) ifIndex	
	(2) dBpduProtectionIfCfgMode	
dBpduProtectionAttackRecover	This trap is sent when the BPDU attack recovered on an interface.	1.3.6.1.4.1.171 .14.47.0.2
	Binding objects:	
	(1) ifIndex	

DDM

Trap Name	Description	OID
	A notification is generated when an abnormal alarm situation occurs or recovers from an abnormal alarm	1.3.6.1.4.1.171 .14.72.0.1

Trap Name	Description	OID
	situation to normal status. Only when the current value> low warning or current value <high recover="" send="" td="" trap.<="" warning="" will=""><td></td></high>	
	Binding objects:	
	(1) dDdmNotifyInfolfIndex	
	(2) dDdmNotifyInfoComponent	
	(3) dDdmNotifyInfoAbnormalLevel	
	(4) dDdmNotifyInfoThresholdExceedOrRecover	
dDdmWarningTrap	A notification is generated when an abnormal warning situation occurs, or recovers from an abnormal warning situation to normal status.	1.3.6.1.4.1.171 .14.72.0.2
	Binding objects:	
	(1) dDdmNotifyInfolfIndex	
	(2) dDdmNotifyInfoComponent	
	(3) dDdmNotifyInfoAbnormalLevel	
	(4) dDdmNotifyInfoThresholdExceedOrRecover	

DHCP Server Screen Prevention

Trap Name	Description	OID
dDhcpFilterAttackDetected	When DHCP Server Screen is enabled, if the switch received the forge DHCP Server packet, the switch will trap the event if any attacking packet is received.	1.3.6.1.4.1.171 .14.133.0.1
	Binding objects:	
	(1) dDhcpFilterLogBufServerlpAddr	
	(2) dDhcpFilterLogBufClientMacAddr	
	(3) dDhcpFilterLogBufferVlanId	
	(4) dDhcpFilterLogBufferOccurTime	

DoS Prevention

Trap Name	Description	OID
dDosPreveAttackDetectedPacket	The trap is sent when detect DoS attack. Binding objects: (1) dDoSPrevCtrlAttackType (2) dDosPrevNotiInfoDropIpAddr (3) dDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.171 .14.59.0.2

ErrDisable

Trap Name	Description	OID
dErrDisNotifyPortDisabledAssert	The trap is sent when a port enters into error disabled state.	1.3.6.1.4.1.171 .14.45.0.1
	Binding objects:	
	(1) dErrDisNotifyInfoPortIfIndex	
	(2) dErrDisNotifyInfoReasonID	
dErrDisNotifyPortDisabledClear	The trap is sent when a port loop restarts after the interval time.	1.3.6.1.4.1.171 .14.45.0.2
	Binding objects:	
	(1) dErrDisNotifyInfoPortIfIndex	
	(2) dErrDisNotifyInfoReasonID	

General Management

Trap Name	Description	OID
dGenMgmtLoginFail	This trap is sent when the user login failed to the switch.	1.3.6.1.4.1.171 .14.165.0.1
	Binding objects:	
	(1) dGenMgmtNotifyInfoLoginType	
	(2) dGenMgmtNotifyInfoUserName	

Gratuitous ARP Function

Trap Name	Description	OID
agentGratuitousARPTrap	The trap is sent when IP address conflicted. Binding objects: (1) ipaddr (2) macaddr (3) portNumber (4) agentGratuitousARPInterfaceName	1.3.6.1.4.1.171 .14.75.0.1

IMPB

Trap Name	Description	OID
dImpbViolationTrap	The address violation notification is generated when IP-MAC-Port Binding address violation is detected.	1.3.6.1.4.1.171 .14.22.0.1
	Binding objects:	
	(1) ifIndex	
	(2) dImpbViolationIpAddrType	
	(3) dImpbViolationIpAddress	
	(4) dImpbViolationMacAddress	

LACP

Trap Name	Description	OID
linkUp	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 (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.	1.3.6.1.6.3.1.1. 5.4
	Binding objects:	
	(1) ifIndex	
	(2) if AdminStatus	
	(3) ifOperStatu	
linkDown	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 (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.	1.3.6.1.6.3.1.1. 5.3
	Binding objects:	
	(1) ifIndex	
	(2) if AdminStatus	
	(3) ifOperStatu	

Trap Name	Description	OID
dLbdLoopOccurred	This trap is sent when an interface loop occurs. Binding objects: (1) dLbdNotifyInfolfIndex	1.3.6.1.4.1.171 .14.46.0.1
dLbdLoopRestart	This trap is sent when an interface loop restarts after the interval time. Binding objects: (1) dLbdNotifyInfolfIndex	1.3.6.1.4.1.171 .14.46.0.2
dLbdVlanLoopOccurred	This trap is sent when an interface with a VID loop occurs. Binding objects: (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171 .14.46.0.3
dLbdVlanLoopRestart	This trap is sent when an interface loop with a VID restarts after the interval time. Binding objects: (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171 .14.46.0.4

LLDP

Trap Name	Description	OID
IldpRemTablesChange	An 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. Binding objects: (1) IldpStatsRemTablesInserts (2) IldpStatsRemTablesDeletes (3) IldpStatsRemTablesDrops (4) IldpStatsRemTablesAgeouts	1.0.8802.1.1.2. 0.0.1
IldpXMedTopologyChangeDetecte d	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. Binding objects: (1) IldpRemChassisIdSubtype (2) IldpRemChassisId (3) IldpXMedRemDeviceClass	1.0.8802.1.1.2. 1.5.4795.0.1

MAC-based Access Control

Trap Name	Description	OID
dMacAuthLoggedSuccess	The trap is sent when a MAC-based Access Control host is successfully logged in. Binding objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.171 .14.153.0.1

Trap Name	Description	OID
dMacAuthLoggedFail	The trap is sent when a MAC-based Access Control host login fails.	1.3.6.1.4.1.171 .14.153.0.2
	Binding objects:	
	(1) ifIndex	
	(2) dnaSessionClientMacAddress	
	(3) dnaSessionAuthVlan	
dMacAuthLoggedAgesOut	The trap is sent when a MAC-based Access Control host ages out.	1.3.6.1.4.1.171 .14.153.0.3
	Binding objects:	
	(1) ifIndex	
	(2) dnaSessionClientMacAddress	
	(3) dnaSessionAuthVlan	

MAC-notification

Trap Name	Description	OID
dL2FdbMacNotification	This trap indicates the MAC addresses variation in the address table.	1.3.6.1.4.1.171 .14.3.0.1
	Binding objects:	
	(1) dL2FdbMacChangeNotifyInfo	

MSTP

Trap Name	Description	OID
newRoot	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.	1.3.6.1.2.1.17. 0.1
topologyChange	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.	1.3.6.1.2.1.17. 0.2

Peripheral

Trap Name	Description	OID
dEntityExtPowerStatusChg	Power Status change notification. Binding objects: (1) dEntityExtEnvPowerUnitId (2) dEntityExtEnvPowerIndex (3) dEntityExtEnvPowerStatus	1.3.6.1.4.1.171 .14.5.0.3
dEntityExtFanStatusChg	Fan status change notification. Binding objects: (1) dEntityExtEnvFanUnitId (2) dEntityExtEnvFanIndex (3) dEntityExtEnvFanStatus	1.3.6.1.4.1.171 .14.5.0.1
dEntityExtThermalStatusChg	Temperature status change notification. Binding objects:	1.3.6.1.4.1.171 .14.5.0.2

Trap Name	Description	OID
	(1) dEntityExtEnvTempUnitId	
	(2) dEntityExtEnvTempIndex	
	(3) dEntityExtEnvTempStatus	
dEntityExtFactoryResetButton	Press factory reset button notification.	1.3.6.1.4.1.171
	Binding objects:	.14.5.0.5
	(1) dEntityExtUnitIndex	

ΡοΕ

Trap Name	Description	OID
pethMainPowerUsageOnNotificati on	This trap indicates PSE Threshold usage indication is on, the usage power is above the threshold. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects:	1.3.6.1.2.1.105 .0.2
	(1) pethMainPseConsumptionPower	
pethMainPowerUsageOffNotificati on	This trap indicates PSE Threshold usage indication is off, the usage power is below the threshold. At least 500 msec must elapse between notifications being emitted by the same object instance.	1.3.6.1.2.1.105 .0.3
	Binding objects:	
	(1) pethMainPseConsumptionPower	
dPoelfPowerDeniedNotification	This Notification indicates if PSE state diagram enters the state POWER_DENIED. At least 500 msec must elapse between notifications being emitted by the same object instance.	1.3.6.1.4.1.171 .14.24.0.1
	Binding objects:	
	(1) pethPsePortPowerDeniedCounter	
dPoelfPowerOverLoadNotification	This trap indicates if PSE state diagram enters the state ERROR_DELAY_OVER. At least 500 msec must elapse between notifications being emitted by the same object instance.	1.3.6.1.4.1.171 .14.24.0.2
	Binding objects:	
	(1) pethPsePortOverLoadCounter	
dPoelfPowerShortCircuitNotificati on	This trap indicates if PSE state diagram enters the state ERROR_DELAY_SHORT. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects:	1.3.6.1.4.1.171 .14.24.0.3
	(1) pethPsePortShortCounter	
dPoelfPdAliveFailOccurNotificatio n	This trap indicates if the PD device has the stop working or no response problem. At least 500 msec must elapse between notifications	1.3.6.1.4.1.171 .14.24.0.4
	being emitted by the same object instance.	
	Binding objects:	
	(1) pethMainPseGroupIndex	
	(2) pethPsePortIndex	
	(3) dPoelfPdAliveCfgPdIpType	
	(4) dPoelfPdAliveCfgPdIpAddr	

Port

Trap Name	Description	OID
linkUp	A notification is generated when port linkup. Binding objects: (1) ifIndex (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1. 5.4
linkDown	A notification is generated when port linkdown. Binding objects: (1) ifIndex (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1. 5.3

Port Security

Trap Name	Description	OID
dPortSecMacAddrViolation	When the port security trap is enabled, new MAC addresses that violate the pre-defined port security configuration will trigger trap messages to be sent out.	1.3.6.1.4.1.171 .14.8.0.1
	Binding objects:	
	(1) ifIndex	
	(2) dPortSecIfCurrentStatus	
	(3) dPortSecIfViolationMacAddress	

RMON

Trap Name	Description	OID
risingAlarm	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue	1.3.6.1.2.1.16. 0.1
	(5) alarmRisingThreshold	
fallingAlarm	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16. 0.2

Safeguard

Trap Name	Description	OID
dSafeguardChgToExhausted	This trap indicates System change operation mode from normal to exhaust. Binding objects:	1.3.6.1.4.1.171 .14.19.1.1.0.1

Trap Name	Description	OID
	(1) dSafeguardEngineCurrentMode	
dSafeguardChgToNormal	This trap indicates system change operation mode from exhausted to normal.	1.3.6.1.4.1.171 .14.19.1.1.0.2
	Binding objects:	
	(1) dSafeguardEngineCurrentMode	

Stack

Trap Name	Description	OID
dStackInsertNotification	Unit Hot Insert notification. Binding objects: (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.171 .14.9.0.1
dStackRemoveNotification	Unit Hot Remove notification. Binding objects: (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.171 .14.9.0.2
dStackFailureNotification	Unit Failure notification. Binding objects: (1) dStackNotifyInfoBoxId	1.3.6.1.4.1.171 .14.9.0.3
dStackTPChangeNotification	The stacking topology change notification. Binding objects: (1) dStackNotifyInfoTopologyType (2) dStackNotifyInfoBoxId (3) dStackInfoMacAddr	1.3.6.1.4.1.171 .14.9.0.4
dStackRoleChangeNotification	The stacking unit role change notification. Binding objects: (1) dStackNotifyInfoRoleChangeType (2) dStackNotifyInfoBoxId	1.3.6.1.4.1.171 .14.9.0.5

SIM

Trap Name	Description	OID
swSingleIPMSColdStart	The commander switch will send this notification when its member generates a cold start notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171 .12.8.6.0.11
swSingleIPMSWarmStart	The commander switch will send this notification when its member generates a warm start notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171 .12.8.6.0.12
swSingleIPMSLinkDown	The commander switch will send this notification when its member generates a link down notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.171 .12.8.6.0.13

Trap Name	Description	OID
swSingleIPMSLinkUp	The commander switch will send this notification when its member generates a link up notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.171 .12.8.6.0.14
swSingleIPMSAuthFail	The commander switch will send this notification when its member generates an authentication failure notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171 .12.8.6.0.15
swSingleIPMSnewRoot	The commander switch will send this notification when its member generates a new root notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171 .12.8.6.0.16
swSingleIPMSTopologyChange	The commander switch will send this notification when its member generates a topology change notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171 .12.8.6.0.17

Start

Trap Name	Description	OID
coldStart	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.	1.3.6.1.6.3.1.1. 5.1
warmStart	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.	1.3.6.1.6.3.1.1. 5.2

Storm Control

Trap Name	Description	OID
dStormCtrlOccurred	This trap is sent when dStormCtrlNotifyEnable is 'stormOccurred' or 'both' and a storm is detected. Binding objects: (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171 .14.25.0.1
dStormCtrlStormCleared	This trap is sent when dStormCtrlNotifyEnable is 'stormCleared' or 'both' and a storm is cleared. Binding objects: (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171 .14.25.0.2

System File

Trap Name	Description	OID
dsfUploadImage	The notification is sent when the user uploads image file successfully.	1.3.6.1.4.1.171 .14.14.0.1
dsfDownloadImage	The notification is sent when the user downloads image file successfully.	1.3.6.1.4.1.171 .14.14.0.2
dsfUploadCfg	The notification is sent when the user uploads configuration file successfully.	1.3.6.1.4.1.171 .14.14.0.3
dsfDownloadCfg	The notification is sent when the user downloads configuration file successfully.	1.3.6.1.4.1.171 .14.14.0.4
dsfSaveCfg	The notification is sent when the user saves configuration file successfully.	1.3.6.1.4.1.171 .14.14.0.5

Web-Authentication

Trap Name	Description	OID
dWebAuthLoggedSuccess	The trap is sent when a host has successfully logged in (passed Web-Authentication).	1.3.6.1.4.1.171 .14.154.0.1
	Binding objects:	
	(1) ifIndex	
	(2) dnaSessionAuthVlan	
	(3) dnaSessionClientMacAddress	
	(4) dnaSessionClientAddrType	
	(5) dnaSessionClientAddress	
	(6) dnaSessionAuthUserName	
dWebAuthLoggedFail	The trap is sent when a host has failed to pass Web- Authentication (login failed).	1.3.6.1.4.1.171 .14.154.0.2
	Binding objects:	
	(1) ifIndex	
	(2) dnaSessionAuthVlan	
	(3) dnaSessionClientMacAddress	
	(4) dnaSessionClientAddrType	
	(5) dnaSessionClientAddress	
	(6) dnaSessionAuthUserName	

Appendix C - RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the DGS-1510 is used in the following modules: Console, Telnet, SSH, Web, 802.1X, MAC-based Access Control, JWAC, and WAC.

The description that follows explains the following RADIUS Attributes Assignment types:

- Privilege Level
- Ingress/Egress Bandwidth
- 802.1p Default Priority
- VLAN
- ACL

To assign the **Privilege Level** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for the bandwidth.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	1	Required
Attribute-Specific Field	Used to assign the privilege level of the user to operate the switch.	Range (1-15)	Required

If the user has configured the privilege level attribute of the RADIUS server (for example, level 15) and the Console, Telnet, SSH, and Web authentication is successful, the device will assign the privilege level (according to the RADIUS server) to this access user. However, if the user does not configure the privilege level attribute and authenticates successfully, the device will not assign any privilege level to the access user. If the privilege level is configured less than the minimum supported value or greater than the maximum supported value, the privilege level will be ignored.

To assign the **Ingress/Egress Bandwidth** by the RADIUS server, the proper parameters should be configured on the RADIUS Server. The table below shows the parameters for bandwidth.

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	2 (for ingress bandwidth) 3 (for egress bandwidth)	Required
Attribute-Specific Field	Used to assign the bandwidth of a port.	Unit (Kbits)	Required

The parameters of the Vendor-Specific attributes are:

If the user has configured the bandwidth attribute of the RADIUS server (for example, ingress bandwidth 1000Kbps), and 802.1X, MAC-based Access Control, JWAC or WAC authentication is successful, the device will assign the bandwidth (according to the RADIUS server) to the port. However, if the user does not configure the bandwidth attribute and authenticates successfully, the device will not assign any bandwidth to the port. If the bandwidth attribute is configured on the RADIUS server with a value of "0", the effective bandwidth will be set "no_limited", and if the bandwidth is configured less than "0" or greater than maximum supported value, the bandwidth will be ignored.

To assign the **802.1p Default Priority** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for 802.1p default priority.

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	4	Required
Attribute-Specific Field	Used to assign the 802.1p default priority of the port.	0 to 7	Required

The parameters of the Vendor-Specific attributes are:

If the user has configured the 802.1p priority attribute of the RADIUS server (for example, priority 7) and 802.1X, MAC-based Access Control, JWAC or WAC authentication is successful, the device will assign the 802.1p default priority (according to the RADIUS server) to the port. However, if the user does not configure the priority attribute and authenticates successfully, the device will not assign a priority to this port. If the priority attribute is configured on the RADIUS server is a value out of range (>7), it will not be set to the device.

To assign the **VLAN** by the RADIUS server, the proper parameters should be configured on the RADIUS server. To use VLAN assignment, RFC 3580 defines the following tunnel attributes in RADIUS packets.

RADIUS Tunnel Attribute	Description	Value	Usage
Tunnel-Type	This attribute indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminator).		Required
Tunnel-Medium-Type	This attribute indicates the transport medium being used.	6 (802)	Required
Tunnel-Private-Group-ID	This attribute indicates group ID for a particular tunneled session.	A string (VID)	Required

The table below shows the parameters for a VLAN:

A summary of the Tunnel-Private-Group-ID Attribute format is shown below.

The table below shows the definition of Tag field (different with RFC 2868):

Tag field value	String field format	
0x01	VLAN name (ASCII)	
0x02	VLAN ID (ASCII)	
Others	When the switch receives the VLAN setting string, it will think it is the VLAN ID first. In other words, the switch will check all existing	

Tag field value	String field format
(0x00, 0x03 ~ 0x1F, >0x1F)	VLAN IDs and check if there is one matched. If the switch can find one matched, it will move to that VLAN. If the switch cannot find the matched VLAN ID, it will think the VLAN setting string as a "VLAN Name". Then it will check that it can find out a matched VLAN Name.



NOTE: A tag field of greater than 0x1F is interpreted as the first octet of the following field.

If the user has configured the VLAN attribute of the RADIUS server (for example, VID 3), and the 802.1X, MAC-based Access Control, JWAC or WAC authentication is successful, the port will be assigned to VLAN 3. However if the user does not configure the VLAN attributes, when the port is not guest VLAN member, it will be kept in its current authentication VLAN, and when the port is guest VLAN member, it will be assigned to its original VLAN.

To assign the **ACL** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for an ACL.

VSA14 ACL Script

The parameters of the Vendor-Specific Attribute are:

RADIUS Tunnel Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	14 (for ACL script)	Required
Attribute-Specific Field	Used to assign the ACL script. The format is based on Access Control List (ACL) Commands.	ACL Script For example: ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;	Required

If the user has configured the ACL attribute of the RADIUS server (for example, ACL script: ip accesslist a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-01-90-10 any; exit;), and the 802.1X, MAC-based Access Control, JWAC or WAC authentication is successful, the device will assign the ACL script according to the RADIUS server. The enter **Access-List Configuration Mode** and exit **Access-List Configuration Mode** must be a pair, otherwise the ACP script will be reject. For more information about the ACL module, please refer to **Access Control List (ACL) Commands** chapter.

NAS-Filter-Rule (92)

The table below shows the parameters for NAS-Filter-Rule:

RADIUS Tunnel Attribute	Description	Value	Usage
NAS-Filter-Rule		A string (concatenating the individual filter rules, separated by a NULL (0x00) octet)	Required

Filter Rule Format

Use the permit command to add a permit entry. Use the deny command to add a deny entry.

{permit | deny} in tcp from any to {any | DST-IP-ADDR | DST-IP-NET-ADDR | DST-IPV6-ADDR | DST-IPV6-NET-ADDR | TCP-PORT-RANGE]

{permit | deny} in udp from any to {any | DST-IP-ADDR | DST-IP-NET-ADDR | DST-IPV6-ADDR | DST-IPV6-NET-ADDR} [UDP-PORT-RANGE]

{permit | deny} in icmp from any to {any | DST-IP-ADDR | DST-IP-NET-ADDR | DST-IPV6-ADDR | DST-IPV6-NET-ADDR} [ICMP-TYPE]

{permit | deny} in ip from any to {any | DST-IP-ADDR | DST-IP-NET-ADDR | DST-IPV6-ADDR | DST-IPV6-NET-ADDR}

{permit | deny} in *IP-PROT-VALUE* from any to {any | *DST-IP-ADDR* | *DST-IP-NET-ADDR* | *DST-IPV6-ADDR* | *DST-IPV6-NET-ADDR*}

Parameter	Description	
in	Specifies the ingress traffic.	
any	Specifies any source IP address or any destination IP address to be configured.	
DST-IP-ADDR	Specifies a specific destination host IP address.	
DST-IP-NET-ADDR	Specifies a group of destination IP addresses with a mask width of the form 1.2.3.4/24.	
DST-IPV6-ADDR	Specifies a specific destination host IPv6 address.	
DST-IPV6-NET-ADDR	Specifies a group of destination IPv6 network of the form 2000::1/64.	
tcp, udp, icmp	Specifies Layer 4 protocols.	
ір	Specifies that any protocol will match.	
IP-PROT-VALUE	Specifies the IP protocol value. The valid value is from 0 to 255.	
TCP-PORT-RANGE	(Optional) Specifies to match TCP port or port range. The form is like: 22-23, 80.	
UDP-PORT-RANGE	(Optional) Specifies to match UDP port or port range. The form is like: 56, 67-68.	
ICMP-TYPE	(Optional) Specifies the ICMP message type. The valid number for the message type is from 0 to 255.	

Parameters

Example

This example shows how to deny host's telnet service on the RADIUS server.

Nas-filter-Rule="deny in tcp from any to any 23" Nas-filter-Rule+="permit in ip from any to any"

This example shows how to limit host to access a group of IP address on the RADIUS server.

Nas-filter-Rule="permit in ip from any to 10.10.10.1/24" Nas-filter-Rule+="permit in ip from any to fe80::d1:1/64"

The parameters of the Vendor-Specific Attribute are:

RADIUS Tunnel Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required

RADIUS Tunnel Attribute	Description	Value	Usage
Vendor-Type	Defines the attribute.	14 (for ACL script)	Required
Attribute-Specific Field	IPv6 filter rule, Used to accept IPv6 address related inputs.	This attribute indicates either of the following IP modes for NAS-Filter-Rule	Required
		1=Forward IPv4 and IPv6 traffic	
		2=Forward IPv4-only traffic (drop any IPv6 traffic)	
		If this attribute is not assigned by RADIUS server, forward IPv4-only traffic, any IPv6 packet will be dropped.	



NOTE: If both proprietary ACL script (VSA14) and standard NAS-Filter-Rule (92) are assigned at the same time, NAS-Filter-Rule (92) will take effect, and VSA14 will be ignored.

Appendix D - IETF RADIUS Attributes Support

Remote Authentication Dial-In User Service (RADIUS) attributes carry specific authentication, authorization, information and configuration details for the request and reply. This appendix lists the RADIUS attributes currently supported by the switch.

RADIUS attributes are supported by the IETF standard and Vendor-Specific Attribute (VSA). VSA allows the vendor to create an additionally owned RADIUS attribute. For more information about D-Link VSA, refer to the **RADIUS Attributes Assignment** Appendix.

IETF standard RADIUS attributes are defined in the RFC 2865 Remote Authentication Dial-In User Service (RADIUS), RFC 2866 RADIUS Accounting, RFC 2868 RADIUS Attributes for Tunnel Protocol Support, and RFC 2869 RADIUS Extensions.

The following table lists the IETF RADIUS attributes supported by the D-Link switch.

Number	IETF Attribute	
1	User-Name	
2	User-Password	
3	CHAP-Password	
4	NAS-IP-Address	
5	NAS-Port	
6	Service-Type	
7	Framed-Protocol	
8	Framed-IP-Address	
12	Framed-MTU	
18	Reply-Message	
24	State	
26	Vendor-Specific	
27	Session-Timeout	
29	Termination-Action	
30	Called-Station-ID	
31	Calling-Station-ID	
32	NAS-Identifier	
60	CHAP-Challenge	
61	NAS-Port-Type	
64	Tunnel-Type	
65	Tunnel-Medium-Type	
77	Connect-Info	
79	EAP-Message	
80	Message-Authenticator	
81	Tunnel-Private-Group-ID	
85	Acct-Interim-Interval	
87	NAS-Port-ID	

RADIUS Authentication Attributes:

Number	IETF Attribute
95	NAS-IPv6-Address

RADIUS Accounting Attributes:

Number	IETF Attribute	
1	User-Name	
4	NAS-IP-Address	
5	NAS-Port	
6	Service-Type	
8	Framed-IP-Address	
31	Calling-Station-ID	
32	NAS-Identifier	
40	Acct-Status-Type	
41	Acct-Delay-Time	
42	Acct-Input-Octets	
43	Acct-Output-Octets	
44	Acct-Session-ID	
45	Acct-Authentic	
46	Acct-Session-Time	
47	Acct-Input-Packets	
48	Acct-Output-Packets	
49	Acct-Terminate-Cause	
52	Acct-Input-Gigawords	
53	Acct-Output-Gigawords	
61	NAS-Port-Type	
95	NAS-IPv6-Address	

Appendix E - ERPS Information

Only hardware-based ERPS (external PHY) supports the fast link drop interrupt feature with a recovery time of 50ms.

Model Name	ERPS	Port 1 to 20
DGS-1510-20	Hardware-based	
	Software-based	V

Model Name	ERPS	Port 1 to 8	Port 9 to 28		
DGS-1510-28	Hardware-based	V			
DGS-1510-28P	Tialuwale-baseu	V			
DGS-1510-28X	Coffware based		N/		
DGS-1510-28XMP	Software-based		V		

Model Name	ERPS	Port 1 to 8	Port 9 to 24	Port 25 to 32	Port 33 to 52
DGS-1510-52	Hardware-based	V		V	
	Software-based		V		V

Model Name	ERPS	Port 1 to 8		Port 25 to 32			Port 51 to 52
DGS-1510-52X (HW: A1)	Hardware-based	V		V		V	
	Software-based		V		V		V

Model Name	ERPS	Port 1 to 16	Port 17 to 24	Port 25 to 40	Port 41 to 48	Port 49 to 52
DGS-1510-52X	Hardware-based		V		V	
(HW: A2) DGS-1510-52XMP	Software-based	V		V		V