5 Configuration

The features and functions of the D-Link Web Smart Switch can be configured for optimum use through the Web-based Management Utility.

Smart Wizard Configuration

After a successful login, the Smart Wizard will guide you through essential settings of the D-Link Web Smart Switch. If you do not plan to change anything, click **Exit** to leave the Wizard and enter the Web Interface. You can also skip it by clicking **Don't show Smart Wizard next time** for the next time you logon to the Web-based Management.

Password Settings

Password setting allows you to change the login password of the device. Type the desired new password in the **Switch Password** box and again in the **Confirm Switch Password**, then click the **Apply** button to make it effective.

<u> </u>			
	SNMP Settings	System Settings	
Control Decomond	-	_	
Switch Password Confirm Switch Password			

Figure 1 – Configure Password in Smart Wizard

SNMP Settings

The SNMP Setting allows you to quickly enable/disable the SNMP function and configure the SNMP community name. For the complete SNMP function, please check "Setup Menu > System > SNMP Settings" in the Web Interface. The default SNMP Setting is Disabled. Click **Enabled**, enter Community names, and then click **Apply** to make it effective.

Read_Only Community: Read-only privilege allows authorized management stations to retrieve MIB objects values. Default Community name is **public**.

Read_Write Community Read/write privilege allows authorized management stations to retrieve and modify MIB object values. Default Community name is **private**.

The Smart Wizard Will guide you to configure som planning to do any change in it, you can click exit to Web Interface.	ne functions all at once. If you are not t to get out of the wizard and go back
Password Settings SNMP Settings	System Settings
SNMP: Enabled Disabled Read_Only Community public Read_Write Community private	Apply Delete Delete Add
Don't show Smart Wizard next time	Exit Apply

Figure 2 - Configure SNMP in Smart Wizard

System Settings

You can manually change the system IP Address, Subnet Mask, and Gateway address by selecting **Static** and clicking **Apply**. You can further configure and read more about the above settings in the "Setup Menu > System > System Settings". The default setting of System IP address is Static. Select **DHCP** to have the switch obtain an IP address from a DHCP server in the network.

5 V.S	e Maan				_
Password 8	Settings	SNMP Settin	ngs		
• Static	ODHCP				
IP Address	10	90	90	90	
Subnet Mask	255	0	0	0	
Gateway	0	0	0	0	

Figure 3 – Configure System IP address in Smart Wizard

NOTE: Changing the system IP address will disconnect you from the current connection. Please enter the correct IP address in the Web browser again and make sure your PC is in the same subnet with the switch. See Login Web-based Management for a detailed description.

If you want to change the IP settings, click **OK** and start a new web browser.

Window	s Internet Explorer 🛛 🛛 🔀
2	The browser will be disconnected. Use new IP address to connect to device.
1	OK Cancel

Figure 4 – Confirm the changes of IP address in Smart Wizard

Web-based Management

DGS-1210-48 System	Device Informati	on		O Safeguard
QoS Security Monitoring ACL	Device Information Device Type System Name System Location Boot Version Firmware Version Protocol Version Hardware Version Serial Number Device Status and Qu RSTP Port Mirroring Storm Control Safeguard Engine IGMP Snooping Power Saving	DGS-1210-48 1.00.002 1.00.005 2.001.004 A1 IMB1733K0000A ick Configurations Disabled <u>Settings</u> Disabled <u>Settings</u> Disabled <u>Settings</u> Disabled <u>Settings</u> Disabled <u>Settings</u> Disabled <u>Settings</u>	System Time System Up Time MAC Address IP Address Subnet Mask Default Gateway Trap IP Login Timeout (minutes) SNMP Status 802.13 Status 802.10 Management VLAN DHCP Client Jumbo Frame	01/01/2009 02:44:13 0 days, 0 hours, 8 mins, 37 seconds 00-0B-A1-12-10-48 172:21:45:84 255:255:240.0 172:21:32:254 0.0.0 5 Disabled Settings Disabled Settings Disabled Settings Disabled Settings Disabled Settings

After clicking the **Exit** button in Smart Wizard you will see the screen below:

Figure 5 – Web-based Management

The above image is the Web-based Management screen. The three main areas are the **Tool Bar** on top, the **Function Tree**, and the **Main Configuration Screen**.

The **Tool Bar** provides a quick and convenient way for essential utility functions like firmware and configuration management.

By choosing different functions in the **Function Tree**, you can change all the settings in the **Main Configuration Screen**. The main configuration screen will show the current status of your Switch by clicking the model name on top of the function tree.

At the upper right corner of the screen the username and current IP address will be displayed.

Under the username is the **Logout** button. Click this to end this session.

NOTE: If you close the web browser without clicking the **Logout** button first, then it will be seen as an abnormal exit and the login session will still be occupied.

Finally, by clicking on the D-Link logo at the upper-left corner of the screen you will be redirected to the local D-Link website.

Tool Bar > Save Menu

The Save Menu provides Save Configuration and Save Log functions.

Save View Tools Save Configuration Save Log Figure 6 – Save Menu

Save Configuration

Select to save the entire configuration changes you have made to the device to switch's non-volatile RAM.

Save Config		O Safeguard
Please press the button to save the config of device.	Save Config	
	Figure 7 – Save Configuration	

Save Log

Save the log entries to your local drive and a pop-up message will prompt you for the file path. You can view or edit the log file by using text editor (e.g. Notepad).

Save Log		O Safeguard
Backup Log to file :	Backup Log	
	Figure 8 – Save Log	

Tool Bar > Tool Menu

The Tool Menu offers global function controls such as Reset, Reset System, Reboot Device, Configuration Backup and Restore, Firmware Backup and Upgrade.



<u>Reset</u>

Provide a safe reset option for the Switch. All configuration settings in non-volatile RAM will be reset to factory default except for the IP address.



Figure 10 – Tool Menu > Reset

Reset System

Provide another safe reset option for the Switch. All configuration settings in non-volatile RAM will reset to factory default and the Switch will reboot.



Figure 11 – Tool Menu > Reset System

Reboot Device

Provide a safe way to reboot the system. Click **Reboot** to restart the switch.





Configuration Backup & Restore

Allow the current configuration settings to be saved to a file (not including the password), and if necessary, you can restore configuration settings from this file. Two methods can be selected: **HTTP** or **TFTP**.

Configuration Backup and Restore		O Safeguard
HTTP Backup current settings to file : Restore saved settings from file :	Backup	
Restore served settings from the .	Restore	
O TFTP		
TFTP Server IP Address		
TFTP File Name		
Backup current settings to file :	Backup	
Restore saved settings from file :	Restore	

Figure 13 – Tool Menu > Configure Backup and Restore

HTTP: Backup or restore the configuration file to or from your local drive.

Click **Backup** to save the current settings to your disk.

Click Browse to browse your inventories for a saved backup settings file.

Click Restore after selecting the backup settings file you want to restore.

TFTP: TFTP (Trivial File Transfer Protocol) is a file transfer protocol that allows you to transfer files to a remote TFTP server. Specify **TFTP Server IP Address** and **File Name** for the configuration file you want to save to / restore from.

Click **Backup** to save the current settings to the TFTP server.

Click Restore after selecting the backup settings file you want to restore.



Note: Switch will reboot after restore, and all current configurations will be lost

Firmware Backup and Upload

Allow for the firmware to be saved, or for an existing firmware file to be uploaded to the Switch. Two methods can be selected: **HTTP** or **TFTP**.

Firmware Backup and Upgrade		O Safeguard
• HTTP		
Backup firmware to file :	Backup	
Upgrade firmware from file :	Browse	
	Upgrade	
O		
TFTP Server IP Address		
TFTP File Name		
Backup firmware to file :	Backup	
Upgrade firmware from file :	Upgrade	

Figure 14 – Tool Menu > Firmware Backup and Upload

HTTP: Backup or upgrade the firmware to or from your local PC drive.

Click **Backup** to save the firmware to your disk.

Click Browse to browse your inventories for a saved firmware file.

Click Upgrade after selecting the firmware file you want to restore.

TFTP: Backup or upgrade the firmware to or from a remote TFTP server. Specify **TFTP Server IP Address** and **File Name** for the configuration file you want to save to / restore from.

Click **Backup** to save the firmware to the TFTP server.

Click **Upgrade** after selecting the firmware file you want to restore.



CAUTION: Do not disconnect the PC or remove the power cord from device until the upgrade completes. The Switch may crash if the Firmware upgrade is incomplete.

Tool Bar > Smart Wizard

By clicking the Smart Wizard button, you can return to the Smart Wizard if you wish to make any changes there.

Tool Bar > Online Help

The Online Help provides two ways of online support: **Online Support Site** will lead you to the D-Link website where you can find online resources such as updated firmware images; **User Guide** can offer an immediate reference for the feature definition or configuration guide.

Online Help	O Safeguard
 Online Support Site Please click "Apply" to go to the D-Link online support site at www.dlink.com. User Guide Please click "Apply" button to open a window and display the guide in PDF format. 	

Figure 15 – Online Help

Online Help

O Safeguard

Online Support Site Please click "Apply" to go to the D-Link online support site at www.dlink.com.

User Guide
 Please click "Apply" button to open a window and display the guide in PDF format.



Figure 16 – User Guide Micro Site

Function Tree

All configuration options on the switch are accessed through the Setup menu on the left side of the screen. Click on the setup item that you want to configure. The following sections provide more detailed description of each feature and function.



Figure 17 –Function Tree

Device Information

The Device Information provides an overview of the switch, including essential information such as firmware & hardware information, and IP address.

It also offers an overall status of common software features:

RSTP: Click **Setting** to link to Configuration > Spanning Tree > STP Global Settings. Default is disabled.

Port Mirroring: Click **Setting** to link to Configuration > Port Mirroring. Default is disabled.

Storm Control: Click Setting to link to Configuration > QoS > Storm Control. Default is disabled.

Safeguard Engine: Click Setting to link to Configuration > Security > Safeguard Engine. Default is enabled.

IGMP Snooping: Click Setting to link to Configuration > IGMP Snooping. Default is disabled.

SNMP: Click **Setting** to link to System > SNMP Setting. Default is disabled.

802.1X: Click Setting to link to Configuration > Security > 802.1X > 802.1X Settings. Default is disabled.

802.1Q Management VLAN: Click **Setting** to link to Configuration > 802.1Q Management VLAN. Default is disabled.

DHCP Client: Click **Setting** to link to System > System Setting. Default is disabled.

Device Information	1			O Safeguard
Device Information				
Device Type	DGS-1210-48	System Time	01/01/2009 02:19:42	
System Name		System Up Time	0 days, 0 hours, 29 mins, 34 seconds	
System Location		MAC Address	00-18-E7-74-26-A3	
Boot Version	1.00.001	IP Address	10.90.90.90	
Firmware Version	1.00.001	Subnet Mask	255.0.0.0	
Protocol Version	2.001.004	Default Gateway	0.0.0.0	
Hardware Version	A1	Trap IP	0.0.00	
Serial Number	1MB1733K0000A	Login Timeout (minutes)	30	
Device Status and Quick	Configurations			
RSTP	Disabled Settings	SNMP Status	Disabled Settings	
Port Mirroring	Disabled Settings	802.1x Status	Disabled Settings	
Storm Control	Disabled Settings	802.1Q Management VLAN	Disabled Settings	
Safeguard Engine	Enabled Settings	DHCP Client	Disabled Settings	
IGMP Snooping	Disabled Settings	Jumbo Frame	Disabled Settings	
Power Saving	Enabled Settings			

Figure 18 – Device Information

System > System Settings

The System Setting allows the user to configure the IP address and the basic system information of the Switch.

IP Information: There are two ways for the switch to obtain an IP address: Static and DHCP (Dynamic Host Configuration Protocol).

When using static mode, the **IP Address**, **Subnet Mask** and **Gateway** can be manually configured. When using DHCP mode, the Switch will first look for a DHCP server to provide it with an IP address (including network mask and default gateway) before using the default or previously entered settings. By default the IP setting is static mode with IP address is **10.90.90.90** and subnet mask is **255.0.00**.

System Information: By entering a **System Name** and **System Location**, the device can more easily be recognized through the SmartConsole Utility and from other Web-Smart devices on the LAN.

Login Timeout: The Login Timeout controls the idle time-out period for security purposes, and when there is no action for a specific time span in the Web-based Management. If the current session times out (expires), the user is required a re-login before using the Web-based Management again. Selective range is from 3 to 30 minutes, and the default setting is 5 minutes.

Group Interval: The D-Link Web Smart Switch will routinely send report packets to the SmartConsole Utility in order to maintain the information integrity. The user can adjust the **Group Interval** to optimal frequency. Selective range is from 120 to 1225 seconds, and 0 means disabling the reporting function.

System Settings			O Safeguard
IP Information			
Static DHCP IP Address Subnet Mask Gateway	10, 90, 90, 90 255, 0, 0, 0 0, 0, 0		
			Apply
System Information			
System Name			
System Location			
Group Interval (120-1225 seconds)	120 (Disable: 0 second)	
			Apply

Figure 19 – System > System Setting

System > Trap Settings For SmartConsole

By configuring the Trap Setting, it allows SmartConsole Utility to monitor specified events on this Web-Smart Switch. By default, Trap Setting is disabled. When the Trap Setting is enabled, enter the **Destination IP** address of the managing station that will receive trap information.

Trap Settings for Sm	artConsole	0 Safeguard
C Enabled Disabled Destination IP	0, 0, 0, 0, 0	
System Event	Device Bootup Illegal Login	
Fiber Port Event	Link Up/ Link Down	
Twisted Pair Port Event	Link Up/ Link Down	
RSTP Port State Change	State Change	
Firmware Upgrade State	Upgrade Success/ Upgrade Failure	

Figure 20 – System > Trap Setting

You can select which event message(s) will be sent to the managing station

System Event: The system level messages, which contains:

Device Bootup - System boot-up information.

Illegal Login - Events of incorrect password logins, recording the IP of the originating PC.

Fiber Port Link Up/Link Down: Fiber port connection information.

Twisted pair Port Link Up/Link Down: Copper port connection information.

RSTP Port State Change: Events of a RSTP port state changes.

Firmware Upgrade State: Information of firmware upgrade success or failure.

System > Port Settings

In the Port Setting page, the status of all ports can be monitored and adjusted for optimum configuration. By selecting a range of ports (**From Port** and **To Port**), the **Speed** can be set for all selected ports by clicking **Apply**. Press the **Refresh** button to view the latest information.

ort Settings					O Safeguar		
rom Port	To Port	Speed Auto	MDI/MDIX	Flow Control Disabled	Apply Refresh		
Port	Link Status	i	Speed	MDI/MDIX	Flow Control		
1	1000M Ful	1	Auto	Auto	Disabled		
2	Down		Auto	Auto	Disabled		
3	Down		Auto	Auto	Disabled		
4	Down		Auto	Auto	Disabled		
5	Down		Auto Auto		Disabled		
6	Down		Auto	Auto	Disabled		
7	Down		Auto		Disabled		
8	Down		Auto	Auto	Disabled		
9	Down		Auto	Auto	Disabled		
10	Down		Auto	Auto	Disabled		
11	Down		Auto	Auto	Disabled		
12	Down	Down		Auto	Disabled		
13	Down		Auto	Auto	Disabled		
14	Down		Auto	Auto	Disabled		
15	Down	Down Auto		Down Auto Auto		Auto	Disabled
16	Down		Auto	Auto	Disabled		
17	Down		Auto	Auto	Disabled		
18	Down		Auto	Auto	Disabled		
19	Down		Auto	Auto	Disabled		
20	Down		Auto	Auto	Disabled		

Figure 21 – System > Port Setting

Speed: Gigabit Fiber connections can operate in 1000M Full Force Mode, Auto Mode or Disabled. Copper connections can operate in Forced Mode settings (1000M Full, 100M Full, 100M Half, 10M Full, 10M Half), Auto, or Disabled. 100M Fiber connections support 100M Full Force Mode, 100M Half Force Mode, or Disabled. The default setting for all ports is **Auto**.



NOTE: Be sure to adjust port speed settings appropriately after changing the connected cable media types.

MDI/MDIX:

A **medium dependent interface (MDI)** port is an Ethernet port connection typically used on the Network Interface Card (NIC) or Integrated NIC port on a PC. Switches and hubs usually use **Medium dependent interface crossover (MDIX)** interface. When connecting the Switch to end stations, user have to use straight through Ethernet cables to make sure the Tx/Rx pairs match up properly. When connecting the Switch to other networking devices, a crossover cable must be used.

This switch provides a configurable **MDI/MDIX** function for users. The switches can be set as an MDI port in order to connect to other hubs or switches without an Ethernet crossover cable.

Auto MDI/MDIX is designed on the switch to detect if the connection is backwards, and automatically chooses MDI or MDIX to properly match the connection. The default setting is "**Auto**" **MDI/MDIX**.

Flow Control: You can enable this function to mitigate the traffic congestion. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control. The default setting is Disabled.

Link Status: Reporting Down indicates the port is disconnected.

System > SNMP Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) protocol 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 or LAN.

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 default SNMP setting is disabled. Click Enabled to set Community Settings and then Apply.

MP Settings				O Safegua
IMP OEnabled 💿 D	isabled			Apply
Community Settings				
Access Right	Community Name		Delete	
Read_Only	public		Delete	
Read_Write	private		Delete	
				Add
Trap Settings				
C Enabled C Disad		Event		
public				
public		SNMP Authentication Traps		
		System Device Bootup		
		Fiber Port Link Up / Link Down		
		Twisted Pair Port Link Up / Link Down		
		BSTP Port State Change		
		- Firmware Upgrade State		

Figure 22 – System > SNMP Setting

Community Setting: In support of SNMP version 1, the Web-Smart Switch accomplishes user authentication by using Community Settings that function as passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from a station that are not authenticated are ignored (dropped).

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

Read_Only: The community with read-only privilege allows authorized management stations to retrieve MIB objects. The default name is **public**.

Read_Write: The community with read/write privilege allows authorized management stations to retrieve and modify MIB objects. The default name is **private**.

Trap Setting: Traps are messages that alert network personnel of events that occur on the Switch. Such events can be as severe as a reboot (someone accidentally turned the Switch OFF), or less serious events such as a port status change. The Switch can generate traps and send them to the trap recipient (i.e. network administrator).

Setting up a Trap: Select **Enable**, enter a Trap Name, add the IP of the device to be monitored, and select the event(s) to trap. The available trap Events to choose from include:

- SNMP Authentication Traps
- System Device Bootup
- Fiber Link Up / Link Down
- Twisted Pair Link Up / Link Down
- RSTP Port State Change
- Firmware Upgrade State



Note: Trap Name must be selected from a Community Name

System > Password Access Control

Setting a password is a critical tool for managers to secure the Web-Smart Switch. After entering the old password and the new password twice, click **Apply** for the changes to take effect.

Password Access Cont	rol	O Safeguard
Old Password		
New Password	(Password should be less than 20 chara	acters)
Confirm Boogword		

Figure 23 – System > Password Access Control

System > System Log Settings

System Logs record and manage events, as well as report errors and informational messages. Message severity determines a set of event messages that will be sent. Click **Enable** so you can start to configure the related settings of the remote system log server, then press **Apply** for the changes to take effect.

System Log Config	System Log Configuration								
System Log	C Enabled Oisabled								
Server IP Address	0. 0. 0. 0	Severity	All \$						
UDP Port (1-65535)	514	Facility	Local 0 ‡						
Time Stamp	Enable ‡								

Figure 24 – System > System Log Settings

Server IP Address: Specifies the IP address of the system log server.

UDP Port: Specifies the UDP port to which the server logs are sent. The possible range is 1 - 65535, and the default value is 514.

Time Stamp: Select Enable to time stamp log messages.

Severity: Specifies the minimum severity from which warning messages are sent to the server. There are three levels. When a severity level is selected, all severity level choices above the selection are selected automatically. The possible levels are:

Warning - The lowest level of a device warning. The device is functioning, but an operational problem has occurred.

Informational - Provides device information.

All - Displays all levels of system logs.

Facility: Specifies an application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overwritten. There are up to eight facilities can be assigned (Local 0 ~ Local 7),

Configuration > Jumbo Frame

D-Link Gigabit Web Smart Switches support jumbo frames (frames larger than the Ethernet frame size of 1536 bytes) of up to 10,000 bytes (tagged). Default is disabled, Select **Enabled** then click **Apply** to turn on the jumbo frame support.

	Jumbo Fran	me Configu	iration		0	Safeguard
	Jumbo Frame:	CEnabled	• Disabled	(Maximum Length is 10,000 bytes)		Apply
6						

Figure 25 – Configuration > Jumbo Frame

Configuration > 802.1Q VLAN

A VLAN is a group of ports that can be anywhere in the network, but communicate as though they were in the same area.

VLANs can be easily organized to reflect department groups (such as R&D, Marketing), usage groups (such as e-mail), or multicast groups (multimedia applications such as video conferencing), and therefore help to simplify network management by allowing users to move devices to a new VLAN without having to change any physical connections.

The IEEE 802.1Q VLAN Configuration page provides powerful VID management functions. The original settings have the VID as 1, no default name, and all ports as "Untagged"

Rename: Click to rename the VLAN group.

Delete VID: Click to delete the VLAN group.

Add New VID: Click to create a new VID group, assigning ports from 01 to 28 as Untag, Tag, or Not Member. A port can be untagged in only one VID. To save the VID group, click Apply.

You may change the name accordingly to the desired groups, such as R&D, Marketing, email, etc.

IEEE 802.1Q VLAN	Configuration			Safeguard
Asymmetric VLAN [Example Note: After enabling Asymme	〕 ○ Enabled	can configure PVID in the following	window.	Apply
(Maximum Entries : 256)				
VID VLAN Name	Untagged VLAN Ports	Tagged VLAN Ports	VLAN Rename	Delete VID
1	02,03,04,05,06,07,08,09, 10,11,12,13,14,15,16,17, 18,19,20,21,22,23,24		Rename	Delete VID
2	01		Rename	Delete VID
			PVID :	ettings Add VID

Figure 26 – Configuration > 802.1Q VLAN > Default Setting

[Example] OE	Enabled 💿 Dis	abled		Apply
g Asymmetric VLAN	by clicking the "Ap	oply" button, users o	can configure PVID in	the following window.
a Untaga	ad VII AN Porte	Taggod VI AN P	orte VIAN Dan	ame Delete V/D
01.02.03	8 04 05 06 07 08	Tagged VENNT		
09,10,11	12,13,14,15,16,			
17,18,19	3,20,21,22,23,24,		11-11-11-11-11-11-11-11-11-11-11-11-11-	_
25,26,27	7,28,29,30,31,32,		Rename	Delete VID
	(Name	should be less tha	in 20 characters)	
All 01 02 03 04 0	5 06 07 08 09	10 11 12 13 14	15 16 17 18 19 2	0 21 22 23 24 25 26
	00000	00000	000000	0000000
	00000	00000	000000	
	$\odot \odot \odot \odot \odot$	00000		
AU 27 20 20 20 2	1 22 22 24 25	26 27 20 20 40	41 42 42 44 45 4	G AT AO AO EO E1 E1
	00000	000000	000000	
		00000		
	[Example] E g Asymmetric VLAN 1e Untagge 01,02,00 09,10,11 17,18,15 25,26,27 33,34,34 -	[Example] Enabled Dis g Asymmetric VLAN by clicking the "Ar ie Untagged VLAN Ports 01,02,03,04,05,06,07,08, 09,10,11,12,13,14,15,16, 17,18,19,20,21,22,23,24, 25,26,27,28,29,30,31,32, 33,34,35,36,37,38,30,40 Image: Constraint of the state	[Example] Enabled Disabled g Asymmetric VLAN by clicking the "Apply" button, users ie Untagged VLAN Ports Tagged VLAN Pr 01,02,03,04,05,06,07,08, 09,10,11,12,13,14,15,16, 17,18,19,20,21,22,23,24, 25,26,27,28,29,30,31,32, 33,34,35,36,37,38,39,40	[Example] Enabled Disabled g Asymmetric VLAN by clicking the "Apply" button, users can configure PVID in ie Untagged VLAN Ports Tagged VLAN Ports VLAN Ren 01,02,03,04,05,06,07,08, 09,10,11,12,13,14,15,16, 17,18,19,20,21,22,23,24, 25,26,27,28,29,30,31,32, 33,34,36,36,37,38,30,40 Rename 33,34,36,36,37,38,39,40 (Name should be less than 20 characters) All 01 02 03,04,05,06,07,08,09 01,01,112,13,14,15,16,00

Figure 27 – Configuration > 802.1Q VLAN > Add VID

EE 802.1Q VLAN Configuration						
VID	VLAN Name	Untag VLAN Ports	Tag VLAN Ports	VLAN Rename	Delete VID	
01	R&D1	01,02,03,04,05,06,07,08	09,10,11,12,13,14,15,16	Rename	Delete VID	
02	R&D2	09,10,11,12,13,14,15,16	17,18,19,20	Rename	Delete VID	
	100 C 100	47 40 40 00 04 00 00 04	01 00 00 01		Delete UTD	

Figure 28 – Configuration > 802.1Q VLAN > Example VIDs

VID	04														
	01														
VLAN Name	R&D1														
Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Untag	All	۲	۲	\odot	۲	۲	۲	\odot	۲	0	0	0	0	0	0
Tag	All	0	0	0	0	0	0	0	0	0	0	0	0	۲	0
Not Member	All	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Port	Select All	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Untag		0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tag	All	۲	۲	0	0	0	0	0	0	0	0	0	0	0	0
Not Member	All	0	0	\bigcirc	\odot	\odot	\odot		\bigcirc	\odot	\odot	\bigcirc			\odot

Figure 29 - Configuration > 802.1Q VLAN > VID Assignments

Configuration > Asymmetric VLAN

This function is located in the 802.1Q Configuration page. It allows devices in different VLANs to communicate with the servers, firewalls or other shared resources in the shared VLAN. This configuration is accomplished in three steps:

- Enabling Asymmetric VLAN function
- Creating shared VLAN and access VLAN
- Configuring the PVID of access VLAN

Asymmetric VLAN is especially effective when used in a small network where a L3 routing device is absent, or if the resource to be shared is not capable of supporting tagged VLAN (for example, a printer).

The example below is a typical application of Asymmetric VLAN. Servers and firewall are located in shared VLAN (default VLAN), and PCs 1, 2 and 3 are located in different VLAN. Because VLANs remain separate, PCs 1, 2, and 3 cannot communicate with each other; but all of them need to access the servers or the Internet behind the firewall.



Figure 30 – Configuration > 802.1Q VLAN > Asymmetric VLAN Example

1. Enable Asymmetric VLAN

Enable Asymmetric VLAN and click the **Apply** button. The overlapping VLAN cannot be configured unless this function is enabled..

EE 8	O Safeguar				
symme	tric VLAN [Example]	Enabled			Apply
ote: Afte	er enabling Asymmetric	/LAN by clicking the "Apply" button, users	can configure PVID in the following	window.	
VID	VLAN Name	Untagged VLAN Ports	Tagged VLAN Ports	VLAN Rename	Delete VID
1000		01,02,03,04,05,06,07,08,			
		09,10,11,12,13,14,15,16,			
01	default	17, 18, 19, 20, 21, 22, 23, 24,		Demonstra	Contract of the second s
01	uciduit	25 26 27 20 20 20 21 22		Rename	Delete VID
01	Gerauit	25,26,27,28,29,30,31,32, 33,34,35,36,37,38,39,40		[Kename]	Delete VID

Figure 31 – Configuration > 802.1Q VLAN > Asymmetric VLAN - Enabling Asymmetric VLAN

2. Configure the shared VLAN (VLAN 1) and access VLANs (VLAN 2, 3, 4)

In this case, the default VLAN is used as shared VLAN, and the ports that are shared in the network are:

- Ports 15-18 are connected to the server
- Port 20 is connected to the firewall

The group of shared ports needs to be included for all the VLANs. Ports 15-18, 20 already belong to VLAN 1, therefore no changes are needed.

VLAN 2 is configured to include ports 15-18, 20 (shared VLAN ports) and the set of ports to be separated from the other VLANs (for example, port 5). VLAN 3 and 4 are then configured to include shared ports and the set of ports to be separated from the other VLANs (for example, port 6 and 7 respectively). Therefore we have three VLANs that share some common ports, but their original membership ports are still separated from each other (for example, port 5, 6, and 7).

The VLAN settings of this example are:

- VLAN 1: default VLAN 1, including all ports with untagged.
- VLAN 2: Member ports are untagged port 5, 15-18, 20.
- VLAN 3: Member ports are untagged port 6, 15-18, 20.
- VLAN 4: Member ports are untagged port 7, 15-18, 20.

IEEE 8	02.1Q Asymmetric	VLAN Configuration			O Safeguard
Asymme Note: Afte	tric VLAN [Example] 《 er enabling Asymmetric VL/	Enabled	can configure PVID in the following	window.	Apply
VID	VLAN Name	Untagged VLAN Ports	Tagged VLAN Ports	VLAN Rename	Delete VID
<u>01</u>	Servers&DFL-800	01,02,03,04,05,06,07,08, 09,10,11,12,13,14,15,16, 17,18,19,20,21,22,23,24, 25,26,27,28,29,30,31,32, 33,34,35,63,738,940, 41,42,43,44,45,46,47,48		Rename	Delete VID
02	SmartSwitch1	05, 15, 16, 17, 18, 20		Rename	Delete VID
03	SmartSwitch2	06,15,16,17,18,20		Rename	Delete VID
04	SmartSwitch3	07, 15, 16, 17, 18, 20		Rename	Delete VID

Figure 32 – Configuration > 802.1Q VLAN > Asymmetric VLAN – Create VLANs

3. Configuring the PVID of access VLAN

Configure the PVID setting located at the bottom of the VLAN configuration page. The user needs to set the shared set of ports as PVID 1, and the other separated groups of ports (for example, port 5, 6, and 7) as PVID 2, 3 and 4 respectively.

The purpose of assigning PVID is to make sure the untagged packets will be transmitted correctly.

Port 01	02	03	04	05	06	07	08	09	.10	11	12
PVID 1	1	1	1	2	3	4	1	1	1	1	1
Port 13	14	15	16	17	18	19	20	21	22	23	24
PVID 1	1	1	1	1	1	1	1	1	1	1	1
										Cancel	Apply

Figure 33 - Configuration > 802.1Q VLAN > Asymmetric VLAN - Assign PVID

After configuration, the user will be able to share the network resources set on the shared group of ports (nominated as PVID 1), with both smaller subsets of VLANs (nominated PVID 2, 3 and 4). However, VLAN 2, 3 and 4 groups are incapable of sharing information with each other directly. Click **Example** to see the example to configure asymmetric VLAN in larger networks.

Note: When Asymmetric VLAN is enabled, IGMP Snooping, Management VLAN, and MAC address table will be reset to default.

Configuration > 802.1Q Management VLAN

The 802.1Q Management VLAN setting allows you to transfer the authority of the switch from the default VLAN to others created by users. This allows managing the whole network more flexible.

By default, the Management VLAN is disabled. You can select any existing VLAN as the management VLAN when this function is enabled. There can only be one management VLAN at a time.

IEEE 802.10	Q Management VLAN Configuration	O Safeguard
Management VLAN	O Enabled ③ Disabled	
VID VLAN Name	01 💌	Apply

Figure 34 – Configuration > 802.1Q Management VLAN

Configuration > Voice VLAN > Voice VLAN Setting

Voice VLAN is a feature that allows you to automatically place the voice traffic from IP phone to an assigned VLAN to enhance the VoIP service. With a higher priority and individual VLAN, the quality and the security of VoIP traffic are guaranteed. The Voice VLAN function will only insert the Voice VLAN tag to untagged packets under corresponding ports. If a VoIP packet comes with a VLAN tag, the Voice VLAN function won't replace the original VLAN tag.

Voice VLAN Setting	í.	0	Safeguar
Voice VLAN	• Enabled O Disabled		
Voice VLAN Global Setting	S		
Vlan ID	100	Aging Time 1 (1~120 hours)	
Priority	High		Apply
Voice Vlan Port Settings			
From Port	To Port Auto	etection	
	28 • Dies		Apply
Port	Auto Detection	Status	6
1	Enabled	None	
2	Enabled	None	
3	Enabled	None	
4	Enabled	None	
5	Enabled	None	
6	Enabled	None	
7	Enabled	None	
8	Enabled	None	
9	Enabled	None	
40	Eachlad	blass	

Figure 35 – Configuration > Voice VLAN > Voice VLAN Setting

Voice VLAN State: Select to enable or disable Voice VLAN. The default is *Disabled.* After you enabled Voice VLAN, you can configure the **Voice VLAN Global Settings**.

VLAN ID: The ID of VLAN that you want to assign voice traffic to. You must first create a VLAN from the 802.1Q VLAN page before you can assign a dedicated Voice VLAN. The member port you configured in 802.1Q VLAN setting page will be the static member port of voice VLAN. To dynamically add ports into the voice VLAN, please enable the **Auto Detection** function

Priority: The 802.1p priority levels of the traffic in the Voice VLAN.

Aging Time: Enter a period of time (in hours) to remove a port from the 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 start. The port will be removed from the voice VLAN after the expiration of the voice VLAN aging timer. Selectable range is from 1 to 120 hours, and default is 1 hour.

From Port / To Port: A consecutive group of ports may be configured starting with the selected port.

Auto Detection: Switch will add ports to the voice VLAN automatically if it detects the device OUI matches the Telephony OUI configured in the Voice VLAN OUI Setting page. Use the drop-down menu to enable or disable the OUI auto detection function. The default is *Disabled*

Click Apply to implement changes made.

Note: Voice VLAN has higher priority than any other features (including QoS). Therefore the voice traffic will be operated according to the Voice VLAN setting and not impacted by the QoS feature.

Configuration > Voice VLAN > Voice VLAN OUI Setting

This window allows the user to configure the user-defined voice traffic's OUI. An Organizationally Unique Identifier (OUI) is the first three bytes of the MAC address. This identifier uniquely identifies a vendor, manufacturer, or other organization.

Voice VLAN OUI	Setting			O Safeguard
Default OUI User defined OUI (Maximum user defined 0	Description 3COM DUI : 10)	Telephony OUI 00-E0-88-00-00-00 (X2	<-XX-XX-XX-XXX-XXX)	Add
ID	Description	Telephony OUI	OUI Mask	Delete

Figure 36 – Configuration > Voice VLAN > Voice VLAN OUI Setting

There are some pre-defined OUIs and when the user configures personal OUI, these pre-defined OUIs must be avoided. Below are the pre-defined voice traffic's OUI:

OUI	Vendor	Mnemonic Name
00:E0:BB	3Com	3com
00:03:6B	Cisco	cisco
00:E0:75	Veritel	veritel
00:D0:1E	Pingtel	pingtel
00:01:E3	Siemens	siemens
00:60:B9	NEC/ Philips	nec&philips
00:0F:E2	Huawei-3COM	huawei&3com
00:09:6E	Avaya	avaya

Default OUI: Pre-defined OUI values, including brand names of 3COM, Cisco, Veritel, Pingtel, Siemens, NEC/Philips, Huawei3COM, and Avaya.

User defined OUI: You can manually create a Telephony OUI with a description. The maximum number of user defined OUIs is 10. It will occupy one ACL rule when selecting a user defined OUI by default, and to configure one user-defined OUI will take extra one ACL rule. System will auto generate an ACL profile (Profile ID: 51) for all the Voice VLAN rules.

Select the OUI and press Add to the lower table to complete the Auto Voice VLAN setting.

Configuration > Link Aggregation > Port Trunking

The Trunking function enables the combining of two or more ports together to increase bandwidth. Up to eight Trunk groups may be created, and each group consists up to eight ports. Select the ports to be grouped together, and then click **Apply** to activate the selected Trunking groups. Two types of link aggregation can be selected:

Static - Static link aggregation.

LACP - LACP (Link Aggregation Control Protocol) is enabled on the device. LACP allows for the automatic detection of links in a Port Trunking Group.

Disable - Remove all members in this trunk group.

	Trunking)											0 8	Bafeguard
Link Ag	ggregation S	State:			20	Enabled	ODisat	bled					(Apply
Edit T	runking Inf	ormation												
ID	03		Туре	LACP	\$								(Apply
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14
													1	M
	15	16	17	18	19	20	21	22	23	24	25	26	27	28
	1	N												
			_	-	0	_		-	0		-			
Note:n Trunki	naximum 8 p ing list	ports in stati	c group and 8	ports in L	ACP group).								
Note:n Trunki	naximum 8 p ing list	ports in stati	c group and 8	ports in L	ACP group).								
Note:n Trunki ID 01	naximum 8 p Ing list	ports in station Type Stati	c group and 8	ports in L P 5,	ACP group orts 6, 7, 8									
Note:n Trunki ID 01 02	naximum 8 p ing list	ports in station Type Stati Stati	c group and 8 c c c	ports in L P 5, 9,	ACP group orts 6, 7, 8 10, 11, 12).								
Note:n Trunki 01 02 03	naximum 8 p ing list	Dorts in station Type Stati Stati LAC	c group and 8 c c c P	ports in L Pr 5, 9, 13	ACP group orts 6, 7, 8 10, 11, 12 3, 14, 15, 1	6								
Note:n Trunki 01 02 03 04	naximum 8 p ing list	Type Stati LAC Disa	c group and 8 c c c P ble	ports in L P 5, 9, 13	ACP group orts 6, 7, 8 10, 11, 12 3, 14, 15, 1	6								
Note:n Trunki 01 02 03 04 05	naximum 8 p Ing list	Type Stati Stati LAC Disa Disa	c group and 8 c c P ble ble	ports in L P 5, 9, 1:	ACP group orts 6, 7, 8 10, 11, 12 3, 14, 15, 1	6								
Note:n Trunki 01 02 03 04 05 06	naximum 8 p ing list	Type Stati Stati LAC Disa Disa Disa	c group and 8 c c c P ble ble ble	ports in L P 5, 9, 1:	ACP group orts 6, 7, 8 10, 11, 12 3, 14, 15, 1	6								
Note:n Trunki 01 02 03 04 05 06 07	naximum 8 p ing list	Type Stati Stati LAC Disa Disa Disa Disa	c group and 8 c c c c P ble ble ble ble ble	Ports in L P 5, 9, 13	ACP group orts 6, 7, 8 10, 11, 12 3, 14, 15, 1	6								,

Figure 37 – Configuration > Link Aggregation > Port Trunking



NOTE: Each combined trunk port must be connected to devices within the same VLAN group.

Configuration > Link Aggregation > LACP Port Settings

The **LACP Port Settings** is used to create port trunking groups on the Switch. The user may set which ports will be active and passive in processing and sending LACP control frames

CP Port	Settings					O Safegu
nk Aggregat om Port 01	ion Port Configuration To Port	Port	Priority(0~65535) 128	Activity Passive	Timeout short (3 sec)	Apply
Port	Port Priority	Activity	1		Timeout	
01	128	Active		L	ona (90 sec)	
02	128	Active		L	ong (90 sec)	
03	128	Active		L	ong (90 sec)	
04	128	Active		Ĺ	ong (90 sec)	
05	128	Active		L	ong (90 sec)	
06	128	Active		L	ong (90 sec)	
07	128	Active		L	ong (90 sec)	
08	128	Active	-	L	ong (90 sec)	
09	128	Active		L	ong (90 sec)	
10	128	Active	-	L	ong (90 sec)	
11	128	Active		L	ong (90 sec)	
12	128	Active		L	ong (90 sec)	
13	128	Active	-	L	ong (90 sec)	
14	128	Active		L	ong (90 sec)	
15	128	Active		L	ong (90 sec)	
16	128	Active		L	ong (90 sec)	
17	128	Active		L	ong (90 sec)	
18	128	Active		L	ong (90 sec)	

Figure 38 – Configuration > Link Aggregation > LACP Port Settings

From Port: The beginning of a consecutive group of ports may be configured starting with the selected port. **To Port:** The ending of a consecutive group of ports may be configured starting with the selected port.

Port Priority (0-65535): Displays the LACP priority value for the port. Default is 128.

Activity: There are two different roles of LACP ports:

Active - Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.

Passive - LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports.

Timeout: Specify the administrative LACP timeout. The possible field values are:

Short (3 Sec) - Defines the LACP timeout as 3 seconds.

Long (90 Sec) - Defines the LACP timeout as 90 seconds. This is the default value.

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

Configuration > IGMP Snooping

With Internet Group Management Protocol (IGMP) snooping, the Web Smart Switch can make intelligent multicast forwarding decisions by examining the contents of each frame's Layer 2 MAC header.

IGMP snooping can help reduce cluttered traffic on the LAN. With IGMP snooping enabled globally, the Web Smart Switch will forward multicast traffic only to connections that have group members attached.

The settings of IGMP snooping is set by each VLAN individually.

GMP Snooping Config	uration			O Safeguard
IGMP Snooping	O Enabled	Oisabled		
IGMP Global Settings				
Host Timeout (130-153025 sec)		260 F	touter Timeout (60-600 sec)	260
Robustness Variable (2-255)		2 L	ast Member Query Interval (1-25	sec) 1
Query Interval (60-600 sec)		125 N	fax Response Time (10-25 sec)	10
Note: The Host Timeout was com The VLAN Settings of IGMP sno	outed automatically in Querier Enabled	by (Robustness Varial	ole * Query Interval + Max Respo	nse Time). Apply
VLAN ID VLAN Name	State	Querier State	Router Ports Settings	Multicast Entry Table

Figure 39 – Configuration > IGMP Snooping Configuration

By default, IGMP is disabled. If enabled, the IGMP Global Settings will need to be entered:

Host Timeout (130-153025 sec): This is the interval after which a learned host port entry will be purged. For each host port learned, a 'Port Purge Timer' runs for 'Host Port Purge Interval'. This timer will be restarted whenever a report message from host is received over that port. If no report messages are received for 'Host Port Purge Interval' time, the learned host entry will be purged from the multicast group. The default value is 260 seconds.

Robustness Variable (2-255 sec): The Robustness Variable allows adjustment for the expected packet loss on a subnet. If a subnet is expected to be lossy, the Robustness Variable may need to be increased. The Robustness Variable cannot be set to zero, and it SHOULD NOT be. Default is 2 seconds.

Query Interval (60-600 sec): The Query Interval is the interval between General Queries sent. By adjusting the Query Interval, the number of IGMP messages can be increased or decreased; larger values will cause IGMP Queries to be sent less often. Default value is 125 seconds.

Router Timeout (60-600 sec): This is the interval after which a learned router port entry will be purged. For each router port learned, a 'Router Port Purge Timer' runs for 'Router Port Purge Interval'. This timer will be restarted whenever a Query control message is received over that port. If there are no Query control messages received for 'Router Port Purge Interval' time, the learned router port entry will be purged. Default is 260 seconds.

Last Member Query Interval (1-25 sec): The Last Member Query Interval is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. This value may be adjusted to modify the "leave latency" of the network. A reduced value results in reduced time to detect the loss of the last member of a group. Default is 1 second.

Max Response Time (10-25 sec): The Max Response Time specifies the maximum allowed time before sending a responding report message. Adjusting this setting effects the "leave latency", or the time between the moment the last host leaves a group and when the multicast server is notified that there are no more members. It also allows adjustments for controlling the frequency of IGMP traffic on a subnet. Default is 10 seconds.

Querier State: D-Link Smart Switch is able to send out the IGMP Queries to check the status of multicast clients. Default is disabled.

To enable IGMP snooping for a given VLAN, select enable and click on the **Apply** button. Then press the **Edit** button under **Router Port Setting**, and select the ports to be assigned as router ports for IGMP snooping for the VLAN. Press **Apply** for changes to take effect. A router port configured manually is a **Static Router Port**, and a **Dynamic Router Port** is dynamically configured by the Switch when a query control message is received.

Router Ports S	ettings																	0	Safe	guard
VLAN ID VLAN Name		1																		
Static Router Ports																				
01 02 03	04 05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
25 26 27	28 29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
Dynamic Router Por	rts																			
01 02 03	04 05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
25 26 27	28 29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
																Pr	evious	Page		pply

Figure 40 – Configuration > IGMP Snooping > IGMP Router port Settings

To view the Multicast Entry Table for a given VLAN, press the View button.



Figure 41 – Configuration > IGMP Multicast Entry Table

Configuration > Port Mirroring

Port Mirroring is a method of monitoring network traffic that forwards a copy of each incoming and/or outgoing packet from one port of the Switch to another port, where the packet can be studied. This enables network managers to better monitor network performances.

ort Mirro	oring Confi	gurati	on										0 5	afeg	uan
Port Mirrorin	g O	Enabled	۲	Disabl	ed										
Target Port		01	~												
Source Port	Selection														
Sniffer Mode	e Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14
ТХ	All														
RX	All														
Both	All														
None	All														
Sniffer Mode	e Select All	15	16	17	18	19	20	21	22	23	24	25	26	27	28
TX	All														
RX	All														
Deth	All														
BOIN															

Figure 42 – Configuration > Port Mirroring

Selection options for the Source Ports are as follows:

TX (transmit) mode: Duplicates the data transmitted from the source port and forwards it to the Target Port. Click "all" to include all ports into port mirroring.

RX (receive) mode: Duplicates the data that is received from the source port and forwards it to the Target Port. Click "all" to include all ports into port mirroring.

Both (transmit and receive) mode: Duplicate both the data transmitted from and data sent to the source port, and forwards all the data to the assigned Target Port. Click "all" to include all ports into port mirroring. **None:** Turns off the mirroring of the port. Click "all" to remove all ports from mirroring.

Configuration > Power Saving

The Power Saving mode feature reduces power consumption automatically when the RJ-45 port is link down or the connected devices are turned off. Less power will be consumed also when the short cable is used (less than 20 meters).

By reducing power consumption, less heat is produced, resulting in extended product life and lower operating costs. By default, the Power Saving mode is enabled. Click **Apply** to make the change effective.

Power Saving Configuration	O Safeguard
Power Saving: Enabled Disabled The Power Saving mode is capable of reducing power consumption automatically when connected devices are switched off or cable length less than a power consumption, less heat is produced, resulting in extended product life and lower operating costs. By default, the Power Saving mode is enabled	Apply 20meters. By reducing 1.

Figure 43 – Configuration > Power Saving

Configuration > Loopback Detection

The Loopback Detection function is used to detect the loop created by a specific port while Spanning Tree Protocol (STP) is not enabled in the network, especially when the down links are hubs or unmanaged switches. The Switch will automatically shutdown the port and sends a log to the administrator. The Loopback Detection port will be unlocked when the Loopback Detection **Recover Time** times out. The Loopback Detection function can be implemented on a range of ports at the same time. You may enable or disable this function using the pull-down menu.

oopback Detection	on Settings		C	Safeguard
State		abled 💿 Disabled		
Loopback Detection Glo Interval (1-32767) Recover Time (0 or 60-100	bal Settings	1 sec 60 sec		Apply
From Port	To Port	State		
1	28 ‡	Disabled +	Apply	Refresh
Port	Loopdetect D	etection State	Loop Status	16
1	Disa	abled	Normal	
2	Disa	abled	Normal	
3	Disa	abled	Normal	
4	Disa	bled	Normal	
	Disa	ibled	Normal	
6	Disa	ibled	Normal	
7				
	Disa	ibled	Normal	
8	Disa	bled	Normal	
8	Disa Disa Disa	abled	Normal Normal Normal	
8 9 10	Disa Disa Disa Disa Disa	ibled	Normal Normal Normal Normal	
8 9 10 11	Disa Disa Disa Disa Disa	ibled	Normal Normal Normal Normal Normal	

Figure 44 – Configuration > Loopback Detection

Loopback Detection State: Use the drop-down menu to enable or disable loopback detection. The default is *Disabled.*

Interval (1-32767): Set a Loop detection Interval between 1 and 32767 seconds. The default is 1 seconds.

Recover Time (0 or 60-1000000): Time allowed (in seconds) for recovery when a Loopback is detected. The Loop Detection Recover Time can be set at *0* seconds, or *60* to *1000000* seconds. Entering *0* will disable the Loop Detection Recover Time. The default is *60* seconds.

From Port: The beginning of a consecutive group of ports may be configured starting with the selected port.

To Port: The ending of a consecutive group of ports may be configured starting with the selected port.

State: Use the drop-down menu to toggle between Enabled and Disabled. Default is Disabled.

Click Apply to implement changes made.

Configuration > SNTP Settings > Time Settings

SNTP or Simple Network Time Protocol is used by the Switch to synchronize the clock of the computer. The SNTP settings folders contain two windows: Time Settings and TimeZone Settings. Users can configure the time settings for the switch, and the following parameters can be set or are displayed in the Time Settings page.

Time Settings		O Safeguard
Clock Source		
Current Time	25/03/2009 10:56:16	
SNTP Server Configuration		
SNTP First Server	0.0.0.0	
SNTP Second Server	0.0.0.0	
SNTP Poll Interval In Seconds (30-99999)	30	
Manually set current time		
Date (DD/MM/YYYY)	25/03/2009	
Time (HH:MM:SS)	10:56:16	
O Set time from PC		
Date (DD/MM/YYYY)	25/03/2009	
Time (HH:MM:SS)	11:02:51	

Figure 45 – Configuration > SNTP Settings > Time Settings

Clock Source: Specify the clock source by which the system time is set. The possible options are:

Local - Indicates that the system time is set locally by the device.

SNTP - Indicates that the system time is retrieved from a SNTP server.

Current Time: Displays the current date and time for the switch.

If choosing **SNTP** for the clock source, then the following parameters will be available:

SNTP First Server: Specify the IP address of the primary SNTP server from which the system time is retrieved.

SNTP Second Server: Specify the IP address of the secondary SNTP server from which the system time is retrieved.

SNTP Poll Interval in Seconds (30-99999): Defines the interval (in seconds) at which the SNTP server is polled for Unicast information. The Poll Interval default is 30 seconds.

Click **Apply** to implement changes made.

When selecting **Local** for the clock source, users can select from one of two options:

Manually set current time: Users input the system time manually.

Set time from PC: The system time will be synchronized from the local computer.

Configuration > SNTP Settings > TimeZone Settings

The TimeZone Setting Page is used to configure time zones and Daylight Savings time settings for SNTP.

TimeZone Settings		_			O Safegue
Daylight Saving Time State Daylight Saving Time Offset in Minutes Time Zone Offset:from GMT in +/-HH:MM	Disabled 60 + +	00 🛟	\$ \$ 00 \$		
DST Annual Settings					
From: Month	Jan	÷)		
From: Day	01	\$			
From: Time In HH MM	00	4 ¥	00	\$	
To: Month	Jan	Å			
To: Day	01	\$)		
To: Time In HH MM	00	\$	00	÷	

Figure 46 – Configuration > SNTP Settings > TimeZone Settings

Daylight Saving Time State: Use this drop-down menu to enable or disable the DST Settings.

Daylight Saving Time Offset in Minutes: Use this drop-down menu to specify the amount of time that will constitute your local DST offset - *30, 60, 90*, or *120* minutes.

Time Zone Offset from GMT in +/- HH:MM: Use these drop-down menus to specify your local time zone's offset from Greenwich Mean Time (GMT.)

DST Annual Settings: Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date must not be in the same month. For example, specify to begin DST on March 8 and end DST on November 1.

From: Month: Enter the month DST will start on, each year.

From: Day: Enter the day of the week DST will start on, each year.

From: Time in HH:MM: Enter the time of day DST will start on, each year.

To: Month: Enter the month DST will end on, each year.

To: Day: Enter the date DST will end on, each year.

To: Time in HH:MM: Enter the time of day that DST will end on, each year.

Click Apply to implement changes made.

Configuration > Spanning Tree > STP Global Settings

The Switch implements two versions of the Spanning Tree Protocol, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1w specification and a version compatible with the IEEE 802.1D STP.

RSTP can operate with legacy equipment implementing IEEE 802.1D, however the advantages of using RSTP will be lost.

The IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations. 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.

By default, Rapid Spanning Tree is disabled. If enabled, the Switch will listen for BPDU packets and its accompanying 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.

After enabling STP, setting the STP Global Setting includes the following options:

RSTP Status	C Enabled Oisabled			
STP Version	RSTP \$	Root Bridge	00:00:00:00:00:00:00:00	
Bridge Priority	32768 ‡	Root Cost	0	
Tx Hold Count (1-10)	6	Root Maximum Age	20	
Maximum Age (6-40 secs)	20	Root Forward Delay	15	
Hello Time (1-10 secs)	2	Root Port	0	
Forward Delay (4-30 secs)	15			

Figure 47 – Configuration > Spanning Tree > STP Global Settings

STP Version: You can choose RSTP or STP Compatible. The default setting is RSTP.

Bridge Priority: This value between 0 and 61410 specifies the priority for forwarding packets: the lower the value, the higher the priority. The default is 32768.

TX Hold Count (1-10): Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from *1* to *10*. The default is *6*.

Maximum Age (6-40 sec): This 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. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that the Switch has the lowest Bridge Identifier, it will become the Root Bridge. A time interval may be chosen between 6 and 40 seconds. The default value is 20. (Max Age has to have a value bigger than Hello Time)

Hello Time (1-10 sec): The user may set the time interval between transmissions of configuration messages by the root device, thus stating that the Switch is still functioning. The default is 2 seconds.

Forward Delay (4-30 sec): This sets the maximum amount of time that the root device will wait before changing states. The default is 15 seconds.

Root Bridge: Displays the MAC address of the Root Bridge.

Root Maximum Age: Displays the Maximum Age of the Root Bridge.

Root Forward Delay: Displays the Forward Delay of the Root Bridge.

Root port: Displays the root port.

Click **Apply** for the settings to take effect. Click **Refresh** to renew the page.

Configuration > Spanning Tree > STP Port Settings

STP can be set up on a port per port basis. In addition to setting Spanning Tree parameters for use on the switch level, the Switch allows for the configuration of the groups of ports, each port-group of which will have its own spanning tree, and will require some of its own configuration settings.

An STP Group spanning tree works in the same way as the switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port is a port of the group that is elected based on port priority and port cost, to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the switch level.

The STP on the switch level blocks redundant links between switches (and similar network devices). The port level STP will block redundant links within an STP Group.

P Port	Settings			_	_			O Safegu
rom Port	(01	To Port	(48	:	State	Disabled	•
xternal Cos -20000000 =AUTO)	t 0; [2000000	Migrate	Disabled	٠	Edge	Auto	•
riority	6	128	P2P	Auto	•	Restricted Role	False	
estricted in		- alao -					Apply	Refresh
Port	State	Priority	External Cost	Edge	P2P	Restricted Role	Restricted TCN	Port State
01	Enable	128	AUTO/20000	Auto	Auto	False	False	Forwarding
02	Enable	128	AUTO/20000	Auto	Auto	False	Falso	Blocking
UL				1 1010		1 0100	1 0130	BIUCKING
03	Enable	128	AUTO/20000	Auto	Auto	False	False	Blocking
03 04	Enable Enable	128 128	AUTO/20000 AUTO/20000	Auto	Auto Auto	False	False	Blocking Blocking
03 04 05	Enable Enable Enable	128 128 128	AUTO/20000 AUTO/20000 AUTO/20000	Auto Auto Auto	Auto Auto Auto	False False False	False False False	Blocking Blocking Blocking Blocking
03 04 05 06	Enable Enable Enable Enable	128 128 128 128 128	AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000	Auto Auto Auto Auto	Auto Auto Auto Auto	False False False False	False False False False False	Blocking Blocking Blocking Blocking Blocking
02 03 04 05 06 07	Enable Enable Enable Enable Enable	128 128 128 128 128 128	AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000	Auto Auto Auto Auto Auto Auto	Auto Auto Auto Auto Auto	False False False False False False	False False False False False False	Blocking Blocking Blocking Blocking Blocking Blocking
02 03 04 05 06 07 08	Enable Enable Enable Enable Enable Enable	128 128 128 128 128 128 128	AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000	Auto Auto Auto Auto Auto Auto Auto	Auto Auto Auto Auto Auto Auto	False False False False False False	False False False False False False False	Blocking Blocking Blocking Blocking Blocking Blocking
02 03 04 05 06 07 08 09	Enable Enable Enable Enable Enable Enable Enable	128 128 128 128 128 128 128 128 128	AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000	Auto Auto Auto Auto Auto Auto Auto Auto	Auto Auto Auto Auto Auto Auto Auto	False False False False False False False	False False False False False False False False	Blocking Blocking Blocking Blocking Blocking Blocking Blocking Blocking
02 03 04 05 06 07 08 09 10	Enable Enable Enable Enable Enable Enable Enable Enable	128 128 128 128 128 128 128 128 128 128	AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000	Auto Auto Auto Auto Auto Auto Auto Auto	Auto Auto Auto Auto Auto Auto Auto Auto	False False False False False False False False	False False False False False False False False	Blocking Blocking Blocking Blocking Blocking Blocking Blocking Blocking Blocking
03 04 05 06 07 08 09 10 11	Enable Enable Enable Enable Enable Enable Enable Enable Enable	128 128 128 128 128 128 128 128 128 128	AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000	Auto Auto Auto Auto Auto Auto Auto Auto	Auto Auto Auto Auto Auto Auto Auto Auto	False False False False False False False False False	False False False False False False False False False False	Blocking Blocking Blocking Blocking Blocking Blocking Blocking Blocking Blocking
02 03 04 05 06 07 08 09 10 11 12	Enable Enable Enable Enable Enable Enable Enable Enable Enable Enable	128 128 128 128 128 128 128 128 128 128	AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000	Auto Auto Auto Auto Auto Auto Auto Auto	Auto Auto Auto Auto Auto Auto Auto Auto	False False False False False False False False False False	False False False False False False False False False False False	Blocking Blocking Blocking Blocking Blocking Blocking Blocking Blocking Blocking Blocking
02 03 04 05 06 07 08 09 10 11 12 13	Enable Enable Enable Enable Enable Enable Enable Enable Enable Enable Enable	128 128 128 128 128 128 128 128 128 128	AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000 AUTO/20000	Auto Auto Auto Auto Auto Auto Auto Auto	Auto Auto Auto Auto Auto Auto Auto Auto	False False False False False False False False False False False False False	False False False False False False False False False False False False False	Blocking Blocking Blocking Blocking Blocking Blocking Blocking Blocking Blocking Blocking Blocking
02 03 04 05 06 07 08 09 10 11 12 13 14	Enable Enable Enable Enable Enable Enable Enable Enable Enable Enable Enable Enable	128 128 128 128 128 128 128 128 128 128	AUTO/2000 AUTO/2000 AUTO/2000 AUTO/2000 AUTO/2000 AUTO/2000 AUTO/2000 AUTO/2000 AUTO/2000 AUTO/2000 AUTO/2000 AUTO/2000 AUTO/2000 AUTO/2000	Auto Auto Auto Auto Auto Auto Auto Auto	Auto Auto Auto Auto Auto Auto Auto Auto	False False False False False False False False False False False False False	False False False False False False False False False False False False False False False	Blocking Blocking Blocking Blocking Blocking Blocking Blocking Blocking Blocking Blocking Blocking Blocking

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

Figure 48 – Configuration > Spanning Tree > STP Port Settings

From Port/To Port: A consecutive group of ports may be configured starting with the selected port.

State: Use the drop-down menu to enable or disable STP by per-port based. It will be selectable after the global STP is enabled.

External Cost: This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is *0* (auto).

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. Default port cost: 100Mbps port = 200000. Gigabit port = 20000.

Value 1-200000000 - Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.

Migrate: Setting this parameter as Yes will set the ports to send out BPDU packets to other bridges, requesting information on their STP setting. If the Switch is configured for RSTP, the port will be capable to migrate from 802.1d STP to 802.1w RSTP. Migration should be set as yes on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP on all or some portion of the segment.

Edge: Selecting the *True* parameter designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge

port status. Selecting the *False* parameter indicates that the port does not have edge port status. Selecting the *Auto* parameter indicates that the port have edge port status or not have edge port status automatically.

Priority: Specify the priority of each port. Selectable range is from 0 to 240, and the default setting is 128. The lower the number, the greater the probability the port will be chosen as a root port.

P2P: Choosing the *True* parameter indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports, however they are restricted in that a P2P port must operate in full-duplex.

Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of *false* indicates that the port cannot have p2p status. *Auto* allows the port to have p2p status whenever possible and operate as if the p2p status were true. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were *False*. The default setting for this parameter is *Auto*.

Restricted Role: Toggle between *True* and *False* to set the restricted role state of the packet. If set to *True*, the port will never be selected to be the Root port. The default value is *False*.

Restricted TCN: Toggle between *True* and *False* to set the restricted TCN of the packet. Topology Change Notification (TCN) is a BPDU that a bridge sends out to its root port to signal a topology change. If set to *True*, it stops the port from propagating received TCN and to other ports. The default value is *False*.

Click **Apply** for the settings to take effect. Click **Refresh** to renew the page.

QoS > Storm Control

The Storm Control feature provides the ability to control the receive rate of broadcast, multicast, and unknown unicast packets. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided.

Storm Control		0 Safeguard
Storm Control	C Enable Olisable	
Storm Control	Multicast & Broadcast & Unknow Unicast	
Threshold (64Kbps * N)	N = (1 ~ 16000) 64Kbps 64Kbps * = unilmited	

Figure 49 – QoS > Storm Control

Storm Control Type: User can select the different Storm type from Broadcast Only, Multicast & Broadcast, and Multicast & Broadcast & Unknown Unicast.

Threshold (64Kbps * N): If storm control is enabled (default is disabled), the threshold is from of $64 \sim 1,024,000$ Kbit per second, with steps (N) of 64Kbps. N can be from 1 to 16000.

Click **Apply** for the settings to take effect.

QoS > Bandwidth Control

The Bandwidth Control page allows network managers to define the bandwidth settings for a specified port's transmitting and receiving data rates.

andwidth Con	trol	_				O Safegu
om Port	To Port	Туре	No Limit	Rate(64-1024000)		
01 🛟	48 🗘	Rx	Disabled 🛟		Kbits/sec	Apply
Port	1	Tx F	Rate (Kbits/sec)		Rx Rate (Kbits/sec)	
01	10		No Limit	2 22	No Limit	
02			No Limit	1	No Limit	
03			No Limit		No Limit	
04			No Limit		No Limit	
05			No Limit		No Limit	
06		No Limit			No Limit	
07	1	No Limit			No Limit	
08			No Limit		No Limit	
09			No Limit		No Limit	
10	0		No Limit		No Limit	
11			No Limit		No Limit	
12			No Limit		No Limit	
13			No Limit		No Limit	
14			No Limit		No Limit	
15			No Limit		No Limit	
16			No Limit		No Limit	
17			No Limit		No Limit	
18			No Limit	£	No Limit	
19			No Limit		No Limit	
20			No Limit	5	No Limit	

Figure 50 – QoS > Bandwidth Control

From Port / To Port: A consecutive group of ports may be configured starting with the selected port.

Type: This drop-down menu allows you to select between *RX* (receive), *TX* (transmit), and *Both*. This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.

No Limit: This drop-down menu allows you to specify that the selected port will have no bandwidth limit. *Enabled* disables the limit.

Rate (64-1024000): This field allows you to enter the data rate, in Kbits per second, will be the limit for the selected port. The value is between 64 and 1024000.

Click **Apply** to set the bandwidth control for the selected ports.

QoS > 802.1p/DSCP Priority Settings

QoS is an implementation of the IEEE 802.1p standard that allows network administrators to reserve bandwidth for important functions that require a larger bandwidth or that might have a higher priority, such as VoIP (voice-over Internet Protocol), web browsing applications, file server applications or video conferencing. Thus with larger bandwidth, less critical traffic is limited, and therefore excessive bandwidth can be saved.

The following figure displays the status of Quality of Service priority levels of each port, higher priority means the traffic from this port will be first handled by the switch. For packets that are untagged, the switch will assign the priority depending on your configuration.

EEE 802.1p De	fault Priority		O Safeguar			
Select QoS Mode:	● 802.1p	ODSCP				
Queuing mechanism:	Strict Priority	WRR (By default is strict priority)	Apply			
adding moondmonn.	Obtable	Contractor delidar lo delide priority				
By default the 802.1p is	s chosen. To enable	DSCP mode, please select the DSCP mode and press "Apply" to go to DSCP Priority Settings page.				
From Port	To Port	Priority				
1	48	* Medium *	Apply			
Port	Priority					
1	Medium					
2	Medium					
3	Medium	For ingress untagged packets, the per port "Default Priority" settings will be applied to packets	s of each port to provide			
4	Medium	port-based traffic prioritization.				
5	Medium	For ingress tagged packets, D-Link Smart Switches will refer to their 802.1p information and prioritize them with				
6	Medium	different priority queues.				
7	Medium					
8	Medium					
9	Medium					
10	Medium					
11	Medium					
12	Medium					
13	Medium					
14	Medium					
15	Medium					

Figure 51 – QoS > 802.1p Default Priority

By selecting the DSCP priority, the web pages will changes as seen below:

SCP Prior	ity Settin	gs	_	_	_	0	Safeguar	
elect QoS Mod	le: 08	302.1p	⊙ DSCP					
Jueuing mechanism: O Strict Priority		Strict Priority	📀 WRR (By d	efault is strict pri	ority)		Apply	
riority Settings rom DSCP vali	page. ue To C	ISCP value	Priority Medium				Apply	
DSCP value	Priority	DSCP value	Priority	DSCP value	Priority	DSCP value	Priority	
0	Medium	16	Medium	32	Medium	48	Medium	
1	Medium	17	Medium	33	Medium	49	Medium	
2	Medium	18	Medium	34	Medium	50	Medium	
3	Medium	19	Medium	35	Medium	51	Medium	
	Medium	20	Medium	36	Medium	52	Medium	
4		20000	1-2001-02000105		NAME OF COMPANY	50	20022102220000	
5	Medium	21	Medium	37	Medium	53	Medium	
4 5 6	Medium Medium	21 22	Medium Medium	37 38	Medium Medium	53	Medium Medium	
4 5 6 7	Medium Medium Medium	21 22 23	Medium Medium Medium	37 38 39	Medium Medium Medium	53 54 55	Medium Medium Medium	
4 5 6 7 8	Medium Medium Medium Medium	21 22 23 24	Medium Medium Medium Medium	37 38 39 40	Medium Medium Medium Medium	53 54 55 56	Medium Medium Medium Medium	
4 5 7 8 9	Medium Medium Medium Medium Medium	21 22 23 24 25	Medium Medium Medium Medium Medium	37 38 39 40 41	Medium Medium Medium Medium Medium	53 54 55 56 57	Medium Medium Medium Medium Medium	

Figure 52 – QoS > DSCP Priority Settings

Select QoS Mode: D-Link Smart Switch allows the user to prioritize the traffic based on the 802.1p priority in the VLAN tag or the DSCP (Differentiated Services Code Point) priority in the IP header. Only one mechanism is selected to prioritize the packets at a time.

Queuing Mechanism: Select Strict Priority to process the packets with the highest priority first. Select WRR (Weighted Round-Robin) to process packets according to the weight of each priority. When a priority level has reached its egress weight, the system will process the packets in the next level even if there are remaining packets. D-Link Smart Switch system's weight of priority levels are: 8 (Highest), 4 (High), 2 (Medium) and 1 (Low) packet. By default, the queuing mechanism is **Strict Priority**.

Default Priority: Default is **Medium**. In 802.1p QoS mode, you can use **From Port** / **To Port** to specify the default priority of each port. In DSCP mode, you can configure the global default priority value by using **From DSCP value** / **To DSCP value**.

Security > Trusted Host

Use Trusted Host function to manage the switch from a remote station. You can enter up to ten designated management stations networks by defining the IP address/Subnet Mask as seen in the figure below.

Trusted Host			0 Safeguard
Trusted Host: Enable	d O Disabled		Apply
Trusted Host Settings (Maximum Entries : 10)			
ID	IP Address	IP Mask	Delete
Input the permitted IP Addre	ss/Mask in below window, the format can be eith	er 192.168.1.1/255.255.255.0 or 192.168.1.1/24	Add Host
IP Address	/ IP Mask		Cancel Apply
Note: Create a list of IP Add	resses that can access the switch. Your local hos	at IP Addresses must be one of the IP Addresses to avo	oid disconnection.

Figure 53 Security > Trusted Host

To define a management station IP setting, click the **Add Host** button and type in the IP address and Subnet mask. Click the **Apply** button to save your settings. You may permit only single or a range of IP addresses by different IP mask settings, the format can either be 192.168.1.1/255.255.255.0 or 192.168.0.1/24. Please see the example below for permitting the IP range

IP Address	Subnet Mask	Permitted IP
192.168.0.1	255.255.255.0	192.168.0.1~192.168.0.255
172.17.5.215	255.0.0.0	172.0.0.1~172.255.255.255

To delete the IP address, simply click the **Delete** button. Check the unwanted address, and then click **Apply**.

Security > Safeguard Engine

D-Link's **Safeguard Engine** is a robust and innovative technology that automatically throttles the impact of packet flooding into the switch's CPU. This function helps protect the Web-Smart Switch from being interrupted by malicious viruses or worm attacks. This option is enabled by default.



Figure 54 – Security > Safeguard Engine

Security > Port Security

Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to stopping auto-learning processing from gaining access to the network.

A given ports' (or a range of ports') dynamic MAC address learning can be stopped such that the current source MAC addresses entered into the MAC address forwarding table can not be changed once the port lock is enabled. Using the drop-down menu, change **Admin State** to *Enabled*, and then click **Apply** to confirm the setting.

Port Security				O Safeguar
From Port	To Port	Admin State	Max Learning Address (0-64)	
01 🛟	48	Disabled 🛟	0	Apply
Port Security				
Port	Admin State	Max Learning	Address	
01	Disabled	0		
02	Disabled	0		
03	Disabled	0		
04	Disabled	0		
05	Disabled	0		
06	Disabled	0		
07	Disabled	0		
08	Disabled	0		
09	Disabled	0		
10	Disabled	0		
11	Disabled	0		
12	Disabled	0		
13	Disabled	0		
14	Disabled	0		
15	Disabled	0		U
16	Disabled	0		
17	Disabled	0		
18	Disabled	0		
19	Disabled	0		
20	Disabled	0		

Figure 55 – Security > Port Security

Security > 802.1X > 802.1X Settings

Network switches provide easy and open access to resources, by simply attaching a client PC. Unfortunately this automatic configuration also allows unauthorized personnel to easily intrude and possibly gain access to sensitive data.

IEEE-802.1X provides a security standard for network access control, especially in Wi-Fi wireless networks. 802.1X holds a network port disconnected until authentication is completed. The switch uses Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol client identity (such as a user name) with the client, and forward it to another remote RADIUS authentication server to verify access rights. The EAP packet from the RADIUS server also contains the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. Depending on the authenticated results, the port is either made available to the user, or the user is denied access to the network.

The RADIUS servers make the network a lot easier to manage for the administrator by gathering and storing the user lists.

802.1X Se	ettings		_		O Safeguard
802.1X		O Enabled O Disat	bled		
802.1X Globa	I Settings				
Radius Server	IP			QuietPeriod (0 - 65535 sec)	60
Kev				SuppTimeout (1 - 65535 sec)	12
Confirm Key				ServerTimeout (1 - 65535 sec)	16
TRANS					10
TxPeriod (1 - 6	5535 Sec)	24		MaxRed (1 - 10)	2
ReAuthEnable	d	Disabled 💠		ReAuthPeriod (1 - 4294967295 sec)	3600
					Apply
802.1X Port A	ccess Control To Port	Cor	itrol		
01 \$	48	÷ (A	uto 👙		Apply Refresh
Port	Control	Port Status	Session Time	User ID	6
01	Force Authorized	*	0	****	
02	Force Authorized	2.	0	24444	
03	Force Authorized	*	0		
04	Force Authorized	*.	0	24424	
05	Force Authorized		0.	2+++2	
06	Force Authorized		0.	*****	

Figure 56 – Security > 802.1X > 802.1X Setting

By default, 802.1X is disabled. To use EAP for security, select enabled and set the 802.1X **Global Settings** for the Radius Server and applicable authentication information.

RADIUS Server IP: The IP address of the external Radius Server. You need to specify an RADIUS server to enable 802.1X authentication.

Key: Masked password matching the Radius Server Key. The max. length is 32 characters.

Confirm Key: Enter the Key a second time for confirmation.

TxPeriod (1 – 65535 sec): This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. Default is 24 seconds.

ReAuthEnabled: This function is to determine whether regular re-authentication will take place on this port(s). When the 802.1X function is enabled, the switch sends an EAP-request/identity packet to client. The ReAuthEnabled function is by default disabled.

QuietPeriod (0 – 65535 sec): Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. Default is 80 seconds

SuppTimeout (1 – 65535 sec): This value determines timeout conditions in the exchanges between the Authenticator and the client. Default is 12 seconds.

ServerTimeout (1 – 65535 sec): Sets the amount of time the switch waits for a response from the client before resending the response to the authentication server. Default is 16 seconds.

MaxReq (1 – 10): This parameter specifies the maximum number of times that the switch retransmits an EAP request (md-5challnege) to the client before it times out the authentication session. Default is 5 times.

ReAuthPeriod (1 – 4294967295 sec): This command affects the behavior of the switch only if periodic reauthentication is enabled. Default is 3600.

To establish 802.1X port-specific assignments, select the From Ports / To Ports and select Enable.

802.1X Port Access Control: Three type of Port Access Control State can be "Force Authorized", "Force UnAuthorized", and "Auto".

Select **Force Authorized** to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client.

If **Force Unauthorized** is selected, the port will remain in the unauthorized state ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface.

If **Auto** is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server.

The default setting is Auto.

Security > MAC Address Table > Static MAC

This feature provides two distinct functions. The **Disable Auto Learning** table allows turning off the function of learning MAC address automatically, if a port isn't specified as an uplink port (for example, connects to a DHCP Server or Gateway). By default, this feature is Off (disabled).

sable auto learning on ports other than the uplink ports configured below On Off 01 02 03 04 05 06 07 08 09 10 11 12 13 14 olink Port Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Off olink Port Image: Colspan="2">Image: Colspan="2">Off olink Port Image: Colspan="2">Image: Colspan="2">Off olink Port Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Off olink Port Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Off olink Port Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Off olink Port Image: Colspan="2">Image: Colspan="2">Image: Colspan="2" Image: Colspa="2" Image: Colspan="2" Image: Colspan="2"	tatic MA	C Co	nfigu	ration	1	_	_	_	_	_	_	_	0	Safe	guard
01 02 03 04 05 06 07 08 09 10 11 12 13 14 olink Port 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)isable auto	learnin	ig on po	orts othe	er than	the upli	nk port	s config	jured be	elow (🔾 On	⊙ Off			
plink Port 20 20 20 20 20 20 20 20 20 20 20 20 20		01	02	03	04	05	06	07	08	09	10	11	12	13	14
15 16 17 18 19 20 21 22 23 24 25 26 27 28 alink Port C C C C C C C C C C C C C C C C C C C	Uplink Port	\checkmark			\checkmark	V	V	V		\checkmark	1	X			1
plink Port D D D D D D D D D D D D D D D D D D D		15	16	17	18	19	20	21	22	23	24	25	26	27	28
vtic MAC Address Lists (Maximum Entries : 256) Delete all	Jplink Port	2		M	X	Υ.	2	2	<u>~</u>	M	2	<u>~</u>	2	×	2
tic MAC Address Lists (Maximum Entries: 256) Delete all														A	noly
auc MAC Address Lists (Maximum Entries 256)							e 1								PPO
	tatic MAC A	adress	LISTS (waximu	nui Eur	ies . zoi	6)							De	lete all
ID Port MAC Address VID	100				-	-			1.00	-					
	ID	P	ort		hd A r	Addro	ee		VID						
	ID	P	ort		MAG	C Addre	SS		VID						
	ID	Р	ort		MAG	C Addre	SS		VID						
	ID	P	ort		MAG	C Addre	SS		VID						
	ID	P	ort		MAC	C Addre	SS		VID						
	ID	Р	ort		MA	C Addre	SS		VID						
	ID	P	ort		MA	C Addre	SS		VID						
	ID	P	ort		MA	C Addre	SS		VID						
	ID	P	ort		MA	C Addre	SS		VID						
	ID	P	ort		MA	C Addre	SS		VID						
	ID	Ρ	ort		MA	C Addre	SS		VID						
	ID	Ρ	ort		MA	C Addre	88		VID						
	ID	Ρ	ort		MA	C Addre	88		VID						
Add MAC	ID.	P	ort		MA	C Addre	88		VID					bA	d MAC
Add MAC	ID	P	ort		MA	C Addre	88		VID					bA	d MAC
Add MAC	ID	Ρ	ort		MA	C Addre	88		VID					Ad	d MAC

Figure 57 – Security > Static Mac Address

To initiate the removal of auto-learning for any of the uplink ports, click **On** to enable this feature, and then select the port(s) for auto learning to be disabled.

The Static MAC Address Setting table displays the static MAC addresses connected, as well as the VID. Click Add Mac to add a new MAC address, you also need to select the assigned Port number. Enter both the Mac Address and VID, and then Click Apply. Click Delete to remove one entry or click Delete all to clear the list. You can also copy a learned MAC address from the Dynamic Forwarding Table (please refer to Security > MAC Address Table > Dynamic Forwarding Table for details).

By disabling Auto Learning capability and specifying the static MAC addresses, the network is protected from potential threats like hackers, because traffic from illegal MAC addresses will not be forwarded by the Switch.

Security > MAC Address Table > Dynamic Forwarding Table

For each port, this table displays the MAC address learned by the Switch. To add a MAC address to the Static Mac Address List, click the **Add** checkbox, and then click **Apply** associated with the identified address.

Dynamic Forwa	rding Table Configu	ration			O Safeguard
Port All				Select all	Find Clean all
ID	Port	MAC Address	VID	Туре	Add
1	1	00-17-F2-F2-A2-D7	1	Dynamic	

Figure 58 – Security > Dynamic Forwarding Table

Monitoring > Statistics

The Statistics screen displays the status of each port packet count.

Statistics				O Safeguard
				Refresh All Clear All Counters
Port	TxOK	RxOK	TxError	RxError
1	470	476	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
I	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
<u>11</u>	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
<u>15</u>	0	0	0	0
<u>16</u>	0	0	0	0
17	0	0	0	0
<u>18</u>	0	0	0	0
<u>19</u>	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	0	0
24	0	0	0	0

Figure 59 – Monitoring > Statistics

Refresh All: Renews the details collected and displayed.

Clear All Counters: To reset the details displayed.

TxOK: Number of packets transmitted successfully.

RxOK: Number of packets received successfully.

TxError: Number of transmitted packets resulting in error.

RxError: Number of received packets resulting in error.

To view the statistics of individual ports, click one of the linked port numbers for details.

		Previous Page Refr	esh Clear Counte
тх		RX	
OutOctets	244399	InOctets	116786
OutUcastPkts	649	InUcastPkts	983
OutNUcastPkts	80	InNUcastPkts	59
OutErrors	0	InDiscards	0
LateCollisions	0	InErrors	0
ExcessiveCollisions	0	FCSErrors	0
InternalMacTransmitErrors	0	FrameTooLongs	0
		InternalMacReceiveErrors	0

Figure 60 – Monitoring > Port Statistics

Previous Page: Go back to the Statistics main page. **Refresh:** To renew the details collected and displayed. **Clear Counter:** To reset the details displayed.

Monitoring > Cable Diagnostics

The Cable Diagnostics is designed primarily for administrators and customer service representatives to examine the copper cable quality. It rapidly determines the type of cable errors occurred in the cable.

Select a port and then click the **Test Now** button to start the diagnosis.

Cabl	e Diagnostics		O Safeguard
Port	01 🛟		Test Now
Port	Test Result	Cable Fault Distance (meters)	Cable Length (meters) [in range]
1	Pair1:OK Pair2:OK Pair3:N/A Pair4:N/A	Pair1:N/A Pair2:N/A Pair3:N/A Pair4:N/A	80 ~ 100
The ca	ble diagnostics feature is designed pri	marily for administrators or customer service representat	ives to verify and test copper cables; it can rapidly determine the
quality	of the cables and the types of error.		
Note: 1. Befo 2. If ca This 3. The 4. It als	re enabling Cable Diagnostics function ble length is displayed as "N/A" it mea is due to the port being unable to obta deviation of "Cable Fault Distance" is so measures cable fault and identifies t	n. clease be sure to disable Power Savino via the Power ns the cable length is "Not Available", in cable length/either because its link speed is 10M or 1 +/2 meters, therefore No cable may be displayed under the fault in length according to the distance from this swi	Savino configuration of Web GUI. 00M, or the cables used are broken and/or bad in quality. Test Result, when the cable used is less than 2 m in length. ch.

Figure 61 – Monitoring > Cable Diagnostic

Test Result: The description of the cable diagnostic results.

• OK means the cable is good for the connection.

• Short in Cable means the wires of the RJ45 cable may be in contact somewhere.

• **Open in Cable** means the wires of RJ45 cable may be broken, or the other end of the cable is simply disconnected.

• **Test Failed** means some other errors occurred during cable diagnostics. Please select the same port and test again.

Cable Fault Distance (meters): Indicates the distance of the cable fault from the Switch port, if the cable is less than 2 meters, it will show "No Cable".

Cable Length (meter): If the test result shows OK, then cable length will be indicated for the total length of the cable. The cable lengths are categorized into four types: <50 meters, 50~80 meters, 80~100 meters and >100 meters.



NOTE: Cable length detection is effective on Gigabit ports only.



NOTE: Please be sure that Power Saving feature is disabled before enabling Cable Diagnostics function.

Monitoring > System Log

The System Log page provides information about system logs, including information when the device was booted, how the ports are operating, when users logged in, when sessions timed out, as well as other system information.

Switc	h History Log		O Safeguard
			Refresh Clear
(Maxim	num Entries : 500)		
ID	Time	Log Description	Severity
1	Jan 2 05:32:47 2009	Spanning Tree Protocol is enabled	info
2	Jan 2 05:32:21 2009	Spanning Tree Protocol is disabled	info
3	Jan 2 05:28:40 2009	Topology changed [(port: 1)]	info
4	Jan 2 05:27:58 2009	Spanning Tree Protocol is enabled	info
5	Jan 2 04:45:33 2009	Successful login through Web (IP: 10.90.90.100)	info
6	Jan 2 04:45:27 2009	Web session timed out (IP: 10.90.90.100)	info
7	Jan 2 03:36:28 2009	Successful login through Web (IP: 10.90.90.100)	info
8	Jan 1 03:34:53 2009	Configuration saved to flash	info
9	Jan 1 03:34:31 2009	Successful login through Web (IP: 10.90.90.100)	info
10	Jan 1 03:34:23 2009	Web session timed out (IP: 10.90.90.100)	info
11	Jan 1 03:24:40 2009	Successful login through Web (IP: 10.90.90.100)	info
12	Jan 1 03:24:34 2009	Web session timed out (IP: 10.90.90.100)	info
13	Jan 1 03:15:09 2009	Successful login through Web (IP: 10.90.90.100)	info
14	Jan 1 03:12:59 2009	Successful login through Web (IP: 10.90.90.100)	info
15	Jan 1 02:59:16 2009	Configuration successfully backup	info
16	Jan 1 02:53:36 2009	Successful login through Web (IP: 10.90.90.100)	info
17	Jan 1 02:53:25 2009	Web session timed out (IP: 10.90.90.100)	info
18	Jan 1 02:45:58 2009	Password was changed.	info
19	Jan 1 02:37:49 2009	Successful login through Web (IP: 10.90.90.100)	info

Figure 62 – Monitoring > System Log

ID: Displays an incremented counter of the System Log entry. The Maximum entries are 500.

Time: Displays the time in days, hours, and minutes the log was entered.

Log Description: Displays a description event recorded.

Severity: Displays a severity level of the event recorded.

Click **Refresh** to renew the page, and click **Clear** to clean out all log entries.

ACL > ACL Configuration Wizard

Access Control List (ACL) allows you to establish criteria to determine whether or not the Switch will forward packets based on the information contained in each packet's header. This criteria can be specified on a basis of the MAC address, or IP address.

The ACL Configuration Wizard will aid with the creation of access profiles and ACL Rules. The ACL Wizard will create the access rule and profile automatically. The maximum usable profiles are 50 and with 240 Rules in total for the switch.

ACL Config	uration Wizard		O Safeguard
General ACL R	iles		
From			
Any	÷		
То			
Any			
Service Type			
Any			
Action			
Permit	•		
Ports			
		ex:(1,2,4-6)	
			Apply
Note:			
ACL Wizard will For advanced ar	create the access profile and rule automatically.	ess Profile List	
, or advanced at	sees promotive seeing, you can manually configure it in rice		

Figure 63 – ACL > ACL Configuration Wizard

From: Specify the origin of accessible packets. The possible values are:

Any - Indicates ACL action will be on packets from any source.

MAC Address - Indicates ACL action will be on packets from this MAC address.

IPv4 Addresses - Indicates ACL action will be on packets from this IPv4 source address.

To: Specify the destination of accessible packets. The possible values are:

Any - Indicates ACL action will be on packets from any source.

MAC Address - Indicates ACL action will be on packets from this MAC address. The field of format is xx-xx-xx-xx-xx-xx.

IPv4 Addresses - Indicates ACL action will be on packets from this IPv4 source address.

Service Type: Specify the type of service. The possible values are:

Any - Indicates ACL action will be on packets from any service type.

Ether type - Specifies an Ethernet type for filtering packets.
ICMP All - Indicates ACL action will be on packets from ICMP packets.
IGMP - IGMP packets can be filtered by IGMP message type.
TCP All - Indicates ACL action will be on packets from TCP Packets.
TCP Source Port - Matches the packet to the TCP Source Port.
TCP Destination Port - Matches the packet to the TCP Destination Port.
UDP All - Indicates ACL action will be on packets from UDP Packets.
UDP Source Port - Matches the packet to the UDP Source Port.
UDP Destination Port - Matches the packet to the UDP Destination Port.

Action: Specify the ACL forwarding action matching the rule criteria. *Permit* forwards packets if all other ACL criteria are met. *Deny* drops packets if all other ACL criteria is met.

Port: Enter a range of ports to be configured.

Press **Apply** for the settings to take effect.



NOTE: Once the ACL rules conflict, rules with the smaller rule ID will take higher priority.



NOTE: Be careful when configuring ACL rules, an inappropriate ACL rule may cause management access failure.

ACL > ACL Profile List

The ACL Profile List provides information for configuring ACL Profiles manually. ACL profiles are attached to interfaces, and define how packets are forwarded if they match the ACL criteria.

Access Prof	ile List			_	O Safeguard	Н
Add ACL Profile	e) Delete Al					
Profile ID	Owner Type	Profile Summary				
1	ACL	Source MAC, Destination MAC	Show Details	Edit/New Rules	Delete	
51	Voice VLAN	Source MAC	Show Details	Show Rules	Delete	
Current/Max. Pro	file: 1/50, Currer	t/Max. Rule: 4/240				

Figure 64 – ACL > ACL Profile List

The contents of Access Profile List table include:

Profile ID: Indicates the profile Identification number. The possible configured profile IDs are 1~50, and profile ID 51 is reserved for Voice VLAN.

Owner Type: The owner type of ACL profile; it can be normal ACL or Voice VLAN.

Profile Summary: Displays the profile summary.

Show Details: To display an ACL's profile details. The ACL profile details are displayed below the ACL table. **Show Rules:** To show the access rule in this profile.

Edit / New Rules: To edit or create an access rule in this profile. To add a new rule, please see Access Rule List in the next section.

Delete: To delete an access profile.

To manually add a profile, click Add ACL Profile:

			O Safeguard
MAC ACL O IPv4 ACL ICMP	÷)		Select
L2 Header	IPv4 DSCP	IPv4 Address	ICMP
]		
(Mask Generate			
	1	MAC ACL IPv4 ACL IPv4 ACL IPv4 ACL IPv4 DSCP Mask Generate Mask Generate Mask Generate	MAC ACL IPv4 ACL IPv4 ACL IPv4 DSCP IPv4 Address Mask Generate Mask Generate Mask Generate

Figure 65 – Add Access Profile

The steps of adding an access profile are described below:

1) After selecting the **Profile ID** and **Frame Type** (MAC or IPv4), specify attributes like Untagged/Tagged (for MAC), or ICMP/IGMP/TCP/UDP (for IPv4). Click *Select* and a simplified frame diagram will be displayed.

2) Selecting the field of interest will display the related columns in the lower part of the page. Enter the filtering mask and click **Create** when done. A filtering mask is to specify the digit that you want to check. For example, if you want to check a network of 192.168.1.0/24, then you should enter the IP mask as 255.255.255.0.



NOTE: You cannot select Payload in a MAC ACL, or L2 Header in IP ACL.

3) After the **Profile ID** has been created, it will go back to the main Access Profile List page, clicking the **Edit** / **New Rules** button to enter the **Access Rule List** page.

Access Ru	le List			O Safeguard
Profile ID	Access ID	Profile Type	Summary Action	
				Add Rule

Figure 66 – Access Rule List

Profile ID: Indicates the corresponding access profile Identification number.

Access ID: Indicates the access rule Identification number.

Profile Type: Displays the profile type.

Summary: Displays the access rule summary.

Action: Displays the access rule action.

To add a new rule, click Add Rule:

Add Access Rule		O Safeguard
Profile Information		
Profile ID	01	
IP Protocol	TCP	
Source IP Mask	255.255.255.128	
Rule Detail		
(Keep an input field as blank to treat	the corresponding option as "don't care")	
Access ID		
Туре	IP	
Source IP Address	192. 168. 1. 50	ex:(192.168.1.10)
IP Protocol :	TCP	
Ports	2	ex:(1,2)
Action	Permit 🗘	
		Previous page Apply

Figure 67 – Add Access Rule

Profile Information displays the information to which the rule is being added to, including **Profile ID** and other fields specified.

In **Rule Detail**, you can specify the details of an access rule. Below are all the possible parameters that can be set.

Access ID: Specify the Access ID (1-65535). Type: Display the type of rule. VLAN ID: The VLAN ID for a previously configured VLAN. Destination MAC Address: Specify the Destination MAC address, the field of format is xx-xx-xx-XX-XX. Source MAC Address: Specify the Source MAC address, the field of format is xx-xx-xx-xx-xx. 802.1p: Specify the 802.1p priority value. Ether Type: Specify the Ethernet Type value. Destination IP Address: Specify the Destination IP address. Source IP Address: Specify the Source IP address. DSCP: Specify the DSCP value. **IP Protocol:** The L4 protocol above IP. Possible values are ICMP, IGMP, TCP, and UDP. **ICMP Type:** Specify the ICMP packet type. ICMP Code: Specify the ICMP packet Code. **IGMP Type:** Specify the IGMP packet type. Source Port: Specify the TCP or UDP source port value. Destination Port: Specify the TCP or UDP destination port value. TCP Flag: Specify the TCP flag value. Ports: Specify the switch ports that you want to implement the access rule to. Action: Specify the ACL forwarding action matching the rule criteria. Permit forwards packets if all other ACL criteria are met. Deny drops packets if all other ACL criteria is met.

Click Apply to make it effective.



NOTE: The switch begins the access rule with the smallest access ID, so be careful in assigning the ID for the expected results.

To modify an existing rule, please click on the Access ID hyperlink.

_
Delete
Delete

Figure 68 – ACL > Access Profile List > Access Rule List

ACL > ACL Finder

This page is used to help find a previously configured ACL entry. To search for an entry, enter the profile ID from the drop-down menu, select a port that you wish to view, define the state and click **Find.** The table on the lower half of the screen will display the entries. To delete an entry click the corresponding **Delete** button.

ACL Find	er			O Safegua	rd
ACL rule fin Profile ID	der helps you id Any 🛟	Ports 2	s been assigned to a specific port	Find)
Profile ID	Access ID	Profile Type	Summary	Action	
1	1	IP	TCP, Source IP	Deny Delete	

Figure 69 – ACL > ACL Finder