



X S T A C K

Web/Installation Guide

Product Model: **xStack**[™] DWS/DXS-3200 Series

Layer 2+ Stackable Gigabit Ethernet Switches with optional XG uplinks

Release 2.0

Table of Contents

DXS/DWS-3227/3227P, DXS/DWS-3250 User Guide Overview	7
Intended Audience	8
Device Description	9
Viewing the Device	9
DXS-3250/DWS Front Panel	9
DXS/DWS-3227 Front Panel	10
DXS/DWS-3227P Front Panel	10
Back Panels	11
Ports Description	12
1000Base-T Gigabit Ethernet Ports	12
10G XFP Fiber port	12
Optional Modules	12
SFP Ports	13
RS-232 Console Port	14
Stacking Ports	14
Cable Specifications	16
LED Definitions	16
Port LEDs	16
SFP LEDs	18
System LEDs	18
Cable, Port, and Pinout Information	20
Pin Connections for the 10/100/1000 Ethernet Interface	20
Physical Dimensions	22
Mounting Device	25
Preparing for Installation	25
Installation Precautions	25
Site Requirements	26
Unpacking	26
Installing the Device	27
Desktop or Shelf Installation	27
Rack Installation	27
Connecting the Device	30
Connecting the Switch to a Terminal	30
AC Power Connection	30
Initial Configuration	31
General Configuration Information	31
Auto-Negotiation	31
Device Port Default Settings	32
Booting the Switch	32
Configuration Overview	34

Initial Configuration	35
Advanced Configuration.....	38
Retrieving an IP Address From a DHCP Server	38
Receiving an IP Address From a BOOTP Server	39
Security Management and Password Configuration.....	40
Software Download and Reboot	42
Software Download through XModem	42
Software Download Through TFTP Server.....	42
Boot Image Download.....	43
Configuring Stacking	44
Startup Menu Functions	46
Download Software	46
Erase FLASH File	47
Erase FLASH Sectors.....	47
Password Recovery	48
WLAN Licence Key	48
Getting Started.....	51
Starting the D-Link Embedded Web Interface.....	52
Understanding the D-Link Embedded Web Interface.....	54
Device Representation.....	55
Using the D-Link Embedded Web Interface Management Buttons	56
Using Screen and Table Options	57
Adding Configuration Information	57
Modifying Configuration Information	57
Deleting Configuration Information	58
Resetting the Device	59
Logging Off from the Device	60
Managing Device Information	61
Defining the System Description	61
Defining Advanced System Settings	63
Managing Power over Ethernet Devices.....	65
Defining PoE System Information	66
Displaying and Editing PoE System Information.....	68
Managing Stacking	71
Understanding the Stack Topology	72
Stacking Failover Topology.....	72
Stacking Members and Unit ID	72
Removing and Replacing Stacking Members	73
Exchanging Stacking Members.....	74
Switching the Stacking Master	74
Configuring Stacking	75

Configuring Device Security.....	77
Configuring Management Security	78
Configuring Authentication Methods.....	78
Configuring Passwords.....	95
Configuring Network Security	99
Network Security Overview.....	99
Defining Network Authentication Properties	101
Defining Port Authentication	103
Configuring Traffic Control.....	108
Defining DOS Protection Security	113
Configuring Ports	115
Viewing Port Properties	118
Aggregating Ports	121
Configuring LACP	122
Defining LAG Members	124
Configuring VLANs	125
Defining VLAN Properties.....	126
Defining VLAN Membership	128
Defining VLAN Interface Settings	130
Configuring GARP	132
Defining GARP	132
Defining GVRP	134
Configuring Multicast VLANs	136
Defining VLAN Groups	137
Defining WLAN	141
Defining WLAN System Properties.....	142
Enabling WLAN	142
Defining WLAN Security	143
Viewing WLAN Rogues	147
Viewing WLAN Stations.....	149
Defining WLAN Access Points	150
Defining WLAN Access Point Properties	151
Adding a New Access point.....	152
Configuring WLAN VLANs.....	153
Configuring WLAN Template Settings	154
Configuring WLAN Radio Settings	156
Defining WLAN Radio Settings.....	156
Defining BSS Settings	158
Defining WLAN Power Settings.....	162
Viewing WLAN Statistics	164
Viewing Access Point Statistics.....	164
Viewing Radio Interfaces Statistics.....	166
Viewing BSS Statistics.....	168

Viewing WLAN Stations	169
Configuring IP Information	171
Configuring IP Interfaces.....	171
Defining IP Addresses	172
Defining Default Gateways	174
Configuring DHCP	175
Configuring ARP	177
Configuring Domain Name Servers	179
Defining DNS Servers.....	179
Defining DNS Host Mapping.....	181
Defining the Forwarding Database and Static Routes	183
Defining Static Forwarding Database Entries	184
Defining Dynamic Forwarding Database Entries	186
Configuring Routing	188
Configuring Spanning Tree	191
Defining Classic Spanning Tree.....	192
Defining STP on Interfaces	194
Defining Rapid Spanning Tree.....	197
Defining Multiple Spanning Tree	198
Defining MSTP Instance Settings	200
Defining MSTP Interface Settings.....	202
Configuring Multicast Forwarding	205
Defining IGMP Snooping.....	206
Defining Multicast Bridging Groups.....	208
Defining Multicast Forward All Settings	210
Configuring Multicast TV	212
Defining IGMP Snooping for Multicast TV	212
Viewing Multicast TV Members.....	214
Configuring SNMP	215
SNMP v1 and v2c	215
SNMP v3	215
Configuring SNMP Security	215
Defining SNMP Security	216
Defining SNMP Views.....	217
Defining SNMP Group Profiles	219
Defining SNMP Group Members	222
Defining SNMP Communities	225
Configuring SNMP Notifications.....	227
Defining SNMP Notification Global Parameters.....	228
Defining SNMP Notification Filters.....	229
Defining SNMP Notification Recipients.....	231

Configuring Quality of Service	237
Quality of Service Overview	238
VPT Classification Information.....	238
CoS Services	238
Defining General QoS Settings	238
Configuring QoS General Settings	238
Restoring Factory Default QoS Interface Settings.....	241
Configure Bandwidth Settings	241
Defining Queues	243
Configuring QoS Mapping	244
Mapping CoS Values to Queues	244
Mapping DSCP Values to Queues	245
Configuring Advanced QoS Settings	246
Defining Policy Properties.....	246
Defining Tail Dropping	248
Defining Policy Profiles.....	253
Managing System Files.....	257
File Management Overview	257
Downloading System Files	258
Firmware Download.....	258
Configuration Download	259
Uploading System Files.....	260
Upload Type	260
Software Image Upload	261
Configuration Upload	261
Activating Image Files	262
Copying Files	263
Restoring the Default Configuration File.....	263
Managing System Files	264
Managing System Logs	265
Enabling System Logs.....	266
Viewing the Device Memory Logs	268
Clearing Device Memory Logs.....	268
Viewing the FLASH Logs.....	269
Clearing FLASH Logs	269
Defining Servers Log Parameters	270
Managing Device Diagnostics.....	273
Configuring Port Mirroring	274
Viewing Integrated Cable Tests.....	277
Viewing Optical Transceivers	279
Viewing the CPU Utilization.....	280

Configuring System Time.....	281
Configuring Daylight Savings Time	281
Configuring SNTP	285
Polling for Unicast Time Information	285
Polling for Anycast Time Information	285
Broadcast Time Information.....	285
Defining SNTP Global Settings	286
Defining SNTP Authentication.....	288
Defining SNTP Servers	290
Defining SNTP Interface Settings	292
Viewing Statistics	295
Viewing Interface Statistics	295
Viewing Device Interface Statistics	296
Resetting Interface Statistics Counters.....	297
Viewing Port Utilization Statistics	298
Viewing Etherlike Statistics	299
Resetting Etherlike Statistics Counters.....	300
Viewing GVRP Statistics.....	301
Resetting GVRP Statistics Counters.....	302
Viewing EAP Statistics.....	303
Managing RMON Statistics	305
Viewing RMON Statistics	306
Resetting RMON Statistics Counters.....	307
Configuring RMON History	308
Defining RMON Alarms.....	315
Appendix A, WLAN Country Settings	317
Appendix B, Device Specifications & Features	325
Appendix B, Troubleshooting	333
Problem Management.....	334
Troubleshooting Solutions.....	334
Contacting D-Link Technical Support.....	337
Warranty.....	365
Product Registration.....	369
International Offices	371

Preface

The *Embedded Web System* (EWS) is a network management system. The D-Link Embedded Web Interface configures, monitors, and troubleshoots network devices from a remote web browser. The D-Link Embedded Web Interface web pages are easy-to-use and easy-to-navigate. In addition, The D-Link Embedded Web Interface provides real time graphs and RMON statistics to help system administrators monitor network performance.

This preface provides an overview to the D-Link Embedded Interface User Guide, and includes the following sections:

- DXS/DWS-3227/3227P, DXS/DWS-3250 User Guide Overview
- Intended Audience

DXS/DWS-3227/3227P, DXS/DWS-3250 User Guide Overview

This section provides an overview to the D-Link Web System Interface User Guide. The D-Link Web System Interface User Guide provides the following sections:

- **Section 1, Device Description** — Provides a system description including the hardware components.
- **Section 2, Mounting Device** — Provides step-by-step instructions for installing the device.
- **Section 3, Initial Configuration** — Provides step-by-step instructions for the initial device configuration.
- **Section 4, Getting Started** — Provides information about using the EWS, including The D-Link Embedded Web Interface interface, management, and information buttons, as well as information about adding, modifying, and deleting device information.
- **Section 5, Managing Device Information** — Provides information about opening the device zoom view, defining general system information, and enabling Jumbo frames.
- **Section 6, Managing Power over Ethernet Devices** — Provides information about configuring PoE on the device.
- **Section 7, Managing Stacking** — Provides information about stacking devices.
- **Section 8, Configuring Device Security** — Provides information about configuring device security for management security, traffic control, and network security.
- **Section 9, Configuring Ports** — Provides information about configuring ports.
- **Section 10, Aggregating Ports** — Provides information about configuring Link Aggregated Groups and LACP.
- **Section 11, Configuring VLANs** — Provides information about configuring and managing VLANs, including information about GARP and GVRP, and defining VLAN groups.
- **Section 12, Defining WLAN** — Provides information for managing and monitoring WLAN access points.
- **Section 13, Configuring IP Information** — Provides information about defining device IP addresses, ARP, and Domain Name Servers.
- **Section 14, Defining the Forwarding Database and Static Routes** — Provides information about configuring and managing both static and dynamic MAC addresses.
- **Section 15, Configuring Spanning Tree** — Provides information about configuring Spanning Tree Protocol and the Rapid Spanning Tree Protocol.
- **Section 16, Configuring Multicast Forwarding** — Provides information about Multicast Forwarding.
- **Section 17, Configuring SNMP** — Provides information about defining SNMP v1,v2c, and v3 management, including SNMP filters and notifications.

- **Section 18, Configuring Quality of Service** — Provides information about configuring Quality of Service on the device.
- **Section 19, Managing System Files** — Provides information about downloading, uploading, and copying system files.
- **Section 20, Managing System Logs** — Provides information about enabling and defining system logs.
- **Section 21, Managing Device Diagnostics** — Provides information about configuring port mirroring, testing copper and fiber cables, and viewing device health information.
- **Section 22, Configuring System Time** — Provides information about configuring system time, including Daylight Savings Time parameters and Simple Network Time Protocol (SNTP) parameters.
- **Section 23, Viewing Statistics** — Provides information about viewing device statistics, including RMON statistics, device history events, and port and LAG utilization statistics.
- **Appendix A, WLAN Country Settings** — Provides information for configuring WLAN, including the country codes, power regulations, and frequency ranges.
- **Appendix B, Troubleshooting** — Provides basic troubleshooting for installing the device.

Intended Audience

This guide is intended for network administrators familiar with IT concepts and terminology.

Section 1. Device Description

This section contains a description of the D-Link DWS/DXS-3250 and D-Link DWS/DXS-3227/3227P, and contains the following topics:

- Viewing the Device
- Ports Description
- Cable Specifications
- LED Definitions
- Cable, Port, and Pinout Information
- Physical Dimensions

Viewing the Device

The devices described in this section are stackable Gigabit Ethernet Managed Switches. Device management is performed using an Embedded Web Server (EWS) or through a Command Line Interface (CLI). The device configuration is performed via an RS-232 interface.

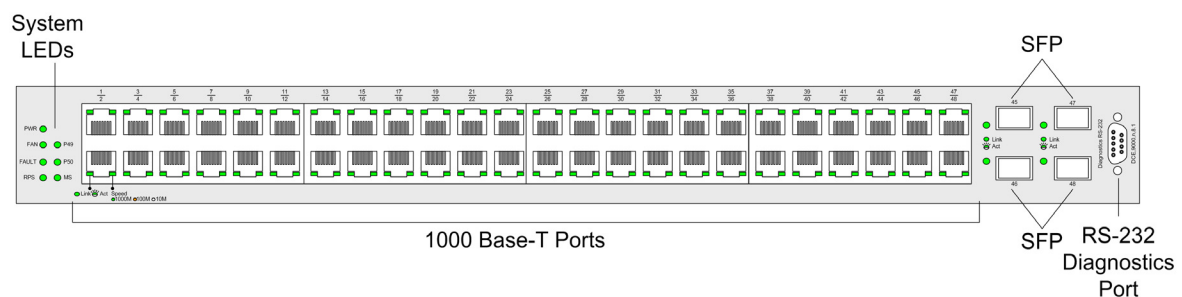
This section contains descriptions for the following:

- DXS-3250/DWS Front Panel
- DXS/DWS-3227 Front Panel
- DXS- 3227P Front Panel
- Back Panels

DXS-3250/DWS Front Panel

The D-Link DXS/DWS-3250 is a 48 port Gigabit Ethernet Managed Switch. The device contains 48 gigabit network ports and 4 SFP Ports on the front panel for network connectivity, and 2 stacking ports on the back panel. The following figure illustrates the DXS-3250 front panel.

Figure 1: DXS/DWS-3250 Front Panel



The device front panel is configured as follows:

- **48 Gigabit Ethernet ports** — RJ-45 ports designated as 10/100/1000Base-T . The RJ-45 ports are designated as ports Ports 1-48.
- **RS-232 Console port** — An asynchronous serial console port supporting the RS-232 electrical specification. The port is used to connect the device to the console managing the device.
- **4 SFP Ports** — There are four SFP port, which contains 1000Base-X (fiber) connections.

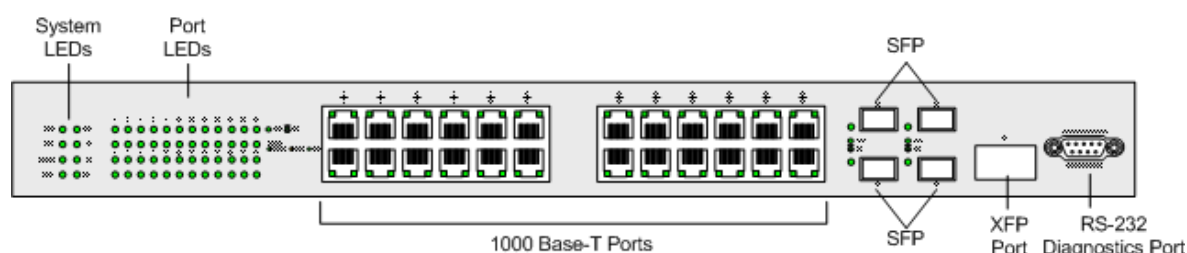
On the front panel there are the Port activity LEDs on each port with the system LEDs displayed separately.

DXS/DWS-3227 Front Panel

The D-Link DXS-3227 is a 24 port Gigabit Ethernet Managed Switch. The device contains 24 gigabit network ports, 4 SFP ports and 1XFP 10G port on the front panel for network connectivity, and 2 optional stacking or uplink module bays on the back panel.

The following figure illustrates the DXS-3227 front panel:

Figure 2: DXS/DWS-3227 Front Panel



The device front panel is configured as follows:

- **24 Gigabit Ethernet ports** — RJ-45 ports designated as 10/100/1000Base-T . The RJ-45 ports are designated as ports Ports 1-24.
- **RS-232 Console port** — An asynchronous serial console port supporting the RS-232 electrical specification. The port is used to connect the device to the console managing the device.
- **4 SFP Ports** — There are four SFP port, which contains 1000Base-X (fiber) connections.
- **XFP port** — Hot-swappable optical interface for 10 Gigabit, Fibre Channel, Gigabit Ethernet, and other applications.

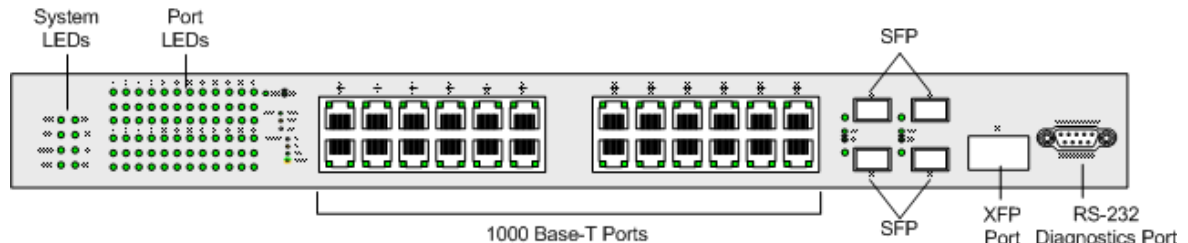
On the front panel there are the Port activity LEDs on each port with the system LEDs displayed separately.

DXS/DWS-3227P Front Panel

The D-Link DXS-3227P is a 24 port Gigabit Ethernet Managed Switch. The device contains 24 gigabit network ports, 4 SFP ports and 1XFP 10G port on the front panel for network connectivity, and 2 optional stacking or uplink module bays on the back panel. The DXS-3227P model also supports Power Over Ethernet.

The following figure illustrates the DXS-3227 front panel:

Figure 3: DXS/DWS-3227P Front Panel



The device front panel is configured as follows:

- **24 Gigabit Ethernet ports** — RJ-45 ports designated as 10/100/1000Base-T . The RJ-45 ports are designated as ports Ports 1-24.
- **RS-232 Console port** — An asynchronous serial console port supporting the RS-232 electrical specification. The port is used to connect the device to the console managing the device.
- **4 SFP Ports** — There are four SFP port, which contains 1000Base-X (fiber) connections.
- **XFP port** — Hot-swappable optical interface for 10 Gigabit and other applications.

On the front panel there are the Port activity LEDs on each port with the system LEDs displayed separately.

Back Panels

The following figures illustrate DXS-3250, DXS-3227 and DXS-3227P back panels:

Figure 4: DXS/DWS-3250 and DXS/DWS-3227 Back Panel

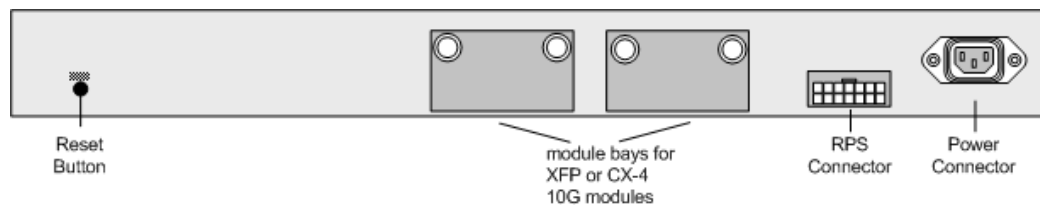
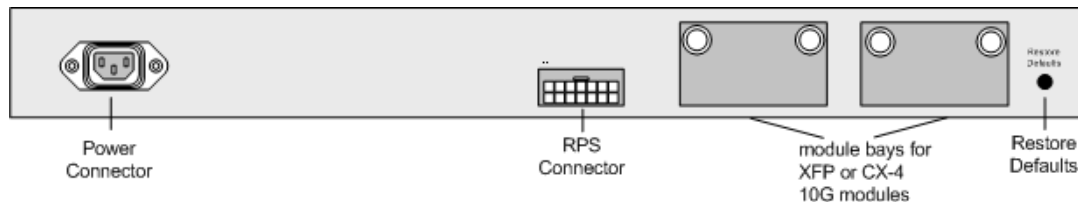


Figure 5: DXS/DWS-3227P Back Panel



The DXS-3200 series back panel is configured as follows:

- **Reset Button** — Resets the device. The Reset button does not extend beyond the device's front panel surface. This is to avoid accidental device resetting.
- **2 Stacking Connectors** — The devices provide two stacking 12 Link(XG) interface ports.
- **RPS Connector** — Redundant Power Supply (RPS) DC connector.
- **Power Connector** — AC power supply interface.

Ports Description

This section describes the device ports and includes the following topics:

- 1000Base-T Gigabit Ethernet Ports
- 10G XFP Fiber port
- CX-4 Copper Port
- SFP Ports
- Cable Specifications

1000Base-T Gigabit Ethernet Ports

The device contains a 1000 Base-TX Gigabit 24/48 port. The port is an RJ-45 port which supports half- and full-duplex mode 10/100/1000 Mbps.

10G XFP Fiber port

10Gigabit XFP fiber port. One fixed in DXS/DWS-3227/3227P models.

Optional Modules

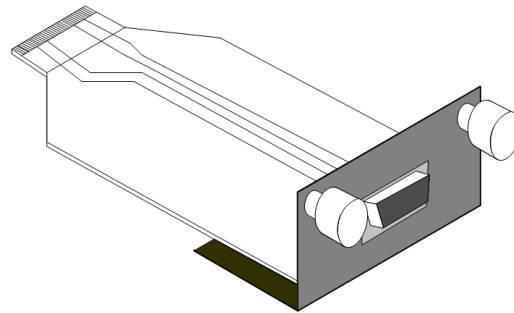
The 3200 series have module bays located on the back panel into which optional modules (DEM-411X and DEM-411XT) can be inserted and then provide additional 10Gigabit copper or fiber port.

CX-4 Copper Port

An optional 10Gigabit copper port. DEM-411T expansion module is inserted in one or two bays located on the back panel.

The following figure describes the DEM - 411T module used for a copper port:

Figure 6: CX-4 Expansion Module

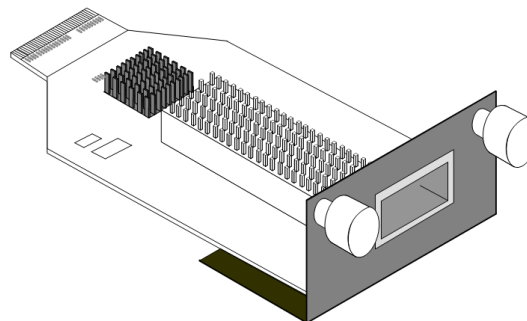


10G XFP Fiber port

An optional 10Gigabit fiber port that can be inserted to the modules bays located on the back panel.

The following figure describes the DEM - 411X module used for a fiber port: Transceivers can be purchased separately from D-Link.

Figure 7: XFP Expansion Module



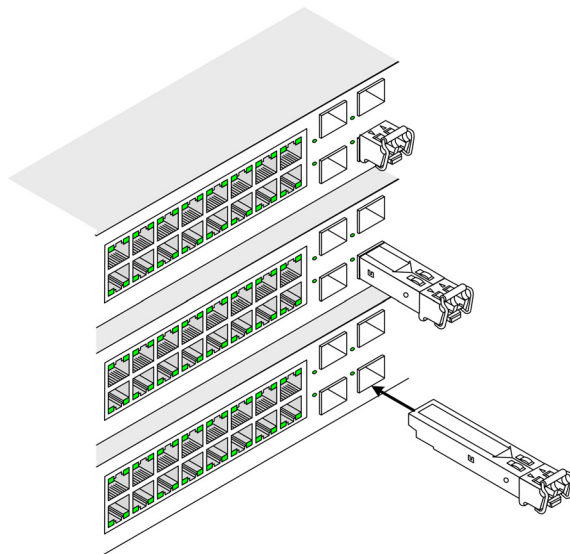
SFP Ports

Small Form Factor Pluggable (SFP) Optical Transceivers are integrated duplex data mini-GBIC links for bi-directional communication over multimode optical fiber, designed for high-speed Fiber Channel data links. The SFP port is designated as 1000Base-X.

The SFP (mini-GBIC) port can be removed and inserted as required. The following figure illustrates the mini-GBIC insertion.

The following figure illustrates how to insert an SFP into the device:

Figure 8: Inserting an SFP into the Device



RS-232 Console Port

The RS-232 port is an asynchronous serial console port supporting the RS-232 electrical specification. The port is used to connect the device to a console managing the device. This interface configuration is as follows:

- Eight data bits.
- One stop bit.
- No parity.
- Baud rate is 9600 (default). The user can change the rate from 115200 down to 9600 bps.
- Console speeds of 57600 and 115200.

Stacking Ports

The device has two optional stacking interface ports. One stacking port provides an Up connection, while the second provides a Down stacking connection. A 4X to 4X Infinidband Cable is used to connect devices in the stacking configuration.

The DEM - 411S Stacking kit includes:

- a) 0.5m CX-4 cable
- b) Two DEM - 411T modules

The following figure describes the DEM - 411S Stacking kit's components:

Figure 9: Stacking Kit (Optional)

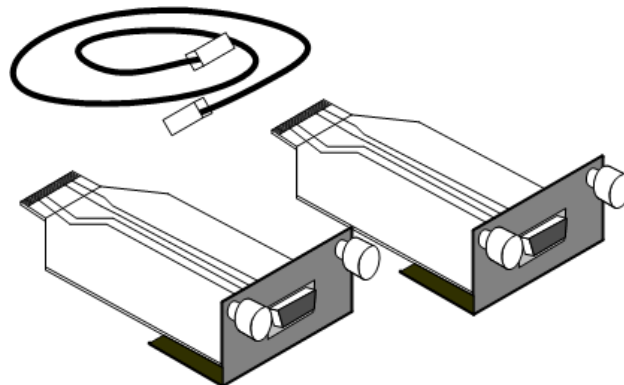
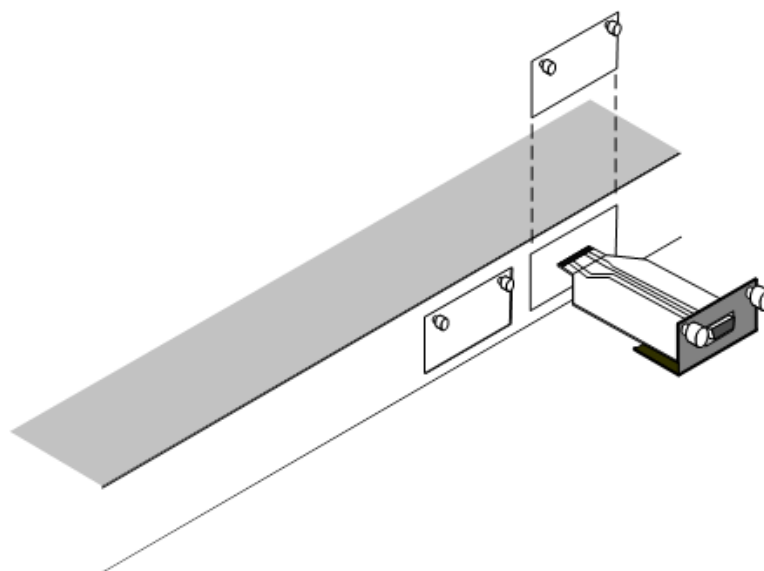


Figure 10: Inserting a Module Into a Device



To insert a module into a device:

1. Release bay cover bolts.
2. Remove bay cover.
3. Carefully Insert module into its proper slot.
4. Ensure that the module is inserted correctly.
5. Secure module bolts.

Cable Specifications

The following table contains the various cable specification for the DXS/DWS-3200 series:

Table 1: DXS-3250/DXS-3227P Cables and Optical Modules Specifications

Cable Type	Description
1000Base-T	UTP Cat. 5e (100 meters max.) UTP Cat. 5 (100 meters max.) EIA/TIA-568B 150-ohm STP (100 meters max.)
10G CX-4	10Gigabit copper port (Up to 15m)
1000BASE-LX	Single-mode fiber module (10Km)
1000BASE-SX	Multi-mode fiber module (550m)
1000BASE-LH	Single-mode fiber module (40km)
1000BASE-ZX	Single-mode fiber module (80km)
10Gigabit - XFP Please refer to the D-Link datasheet for DEM-421XT and DEM-422XT should there be any questions	Single/Multiple fiber XFP transceiver

LED Definitions

The device front panels contain Light Emitting Diodes (LED) that indicate the device status. The different LED types are as follows:

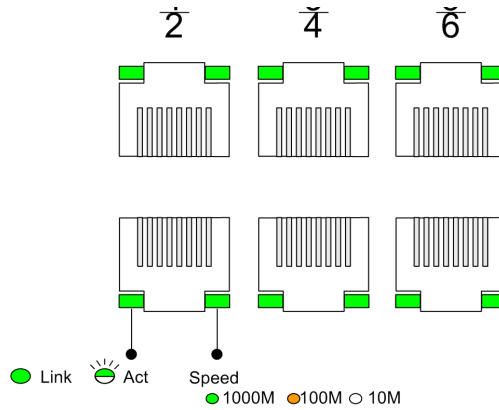
- **Port LEDs** — Indicate each port status.
- **SFP Ports** — Indicate SFP port status.
- **System** — Indicating the device power supply status.

Port LEDs

1000Base-T Gigabit Ethernet RJ-45 Port LEDs

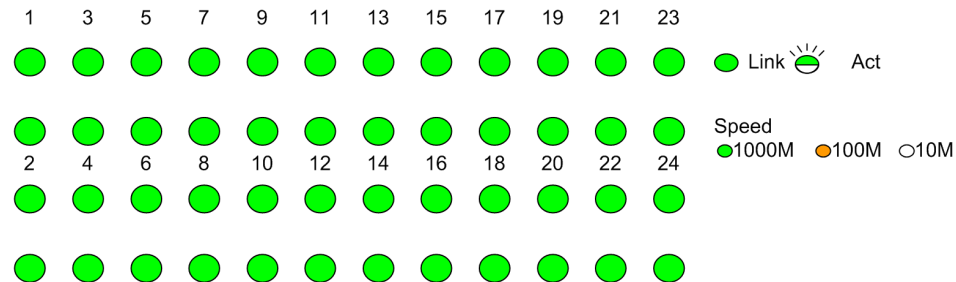
The LEDs on the three devices are differently indicated. The following figure illustrates the DXS-3250 port LEDs.

Figure 10: DXS-3250 1000Base-T Gigabit Ethernet RJ-45 Port LEDs



The DXS-3227 device has the LED indications on a LED panel on the left side of the device. The following figure illustrates the port LEDs:

Figure 11: DXS-3227 1000Base-T Gigabit Ethernet RJ-45 Port LEDs



The RJ-45 ports on both devices have two LEDs, one for speed, and one for Link /activity. The LED indications are described in the following table:

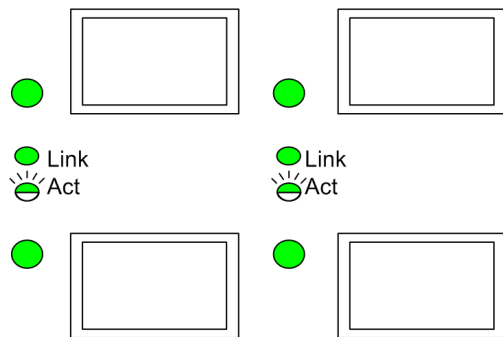
Table 2: 1000Base-T Gigabit Ethernet RJ-45 Port LED Indications

Port Description	LED Indication	Description
Speed	Green	A 1000-Mbps link is established on the port.
	Amber	A 100-Mbps link is established on the port.
	Off	A 10-Mbps link is established on the port.
Link/Activity LED	Green	A link is established on the port.
	Flashing Green	There is data transmission on the port.
	Off	No link is established on the port.

SFP LEDs

The following figure illustrates the port LEDs.

Figure 12: SFP LEDs



The Fiber ports each have one LED. The LED indications are described in the following table:

Table 3: SFP LED Indications

LED Indication	Description
Green	A link is established on the port.
Flashing Green	There is data transmission on the port.
Off	No link is established on the port.

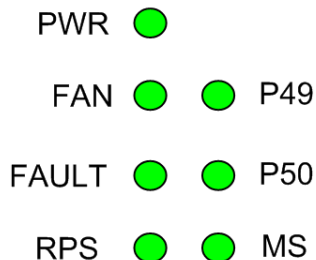
System LEDs

The three devices have different system LEDs.

DXS-3250

The system LEDs on the DXS-3250 device are on the left side of the device. The following figure illustrates the DXS-3250 system LEDs:

Figure 13: DXS-3250 System LEDs

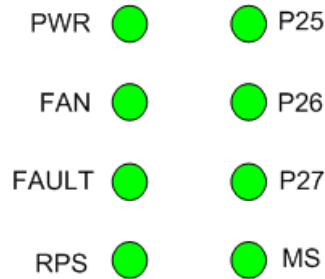


DXS/DWS-3227/3227P

The system LEDs are on the DXS/DWS-3227/3227P device in on the left side of the device.

The following figure illustrates the DXS/DWS-3227/3227P system LEDs:

Figure 14: DXS/DWS-3227/3227P LEDs



The LED indications are described in the following table:

Table 4: System's LED Indications

LED Description	LED Indication	Description
PWR	Green	The device is powered up.
	Off	The device is not powered up.
FAN	Red	Indicates a faulty fan.
	Off	All fans are functioning correctly.
Fault	Red Flashing	The device is currently running POST.
	Red	The device detected POST running error.
RPS	Green	The device is powered through the RPS.
	Off	The device is powered through the AC.
P49/P50 (DXS/DWS-3250) - Link/Act for XG port	Green	Link established on the port.
P25/P26/P27 (DXS/DWS-3227/3227P) - Link/Act for XG port	Green	Link established on the port.
	Green Flashing	There is data transmission on the port.
	Off	No link is established on the port.
MS	Red	Device is designated as the stack Master.
	Green	Device is designated as stack member.
	Off	Not a member of a stack (standalone).
PoE	Green	Power is provided at this port
	Off	Power is not provided at this port

Table 4: System's LED Indications

LED Description	LED Indication	Description
	Amber	An error is occurred at this port
	Off	There is no error at this port
	alternating Green and Amber	An error is occurred at this port

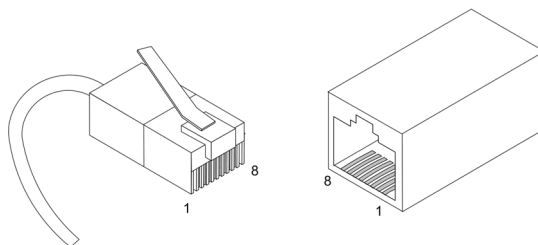
Cable, Port, and Pinout Information

This section describes the devices physical interfaces and provides information about cable connections. Stations are connected to the device ports through the physical interface ports on the front panel. For each station, the appropriate mode (Half/Full Duplex, Auto Negotiation) is set. The default is Auto Negotiation.

Pin Connections for the 10/100/1000 Ethernet Interface

The switching port can connect to stations wired in standard RJ-45 Ethernet station mode using straight cables. Transmission devices connected to each other use crossed cables. The following figure illustrates the pin allocation.

Figure 15: RJ-45 Pin Allocation

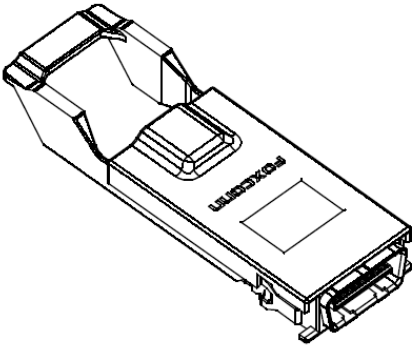


The following table describes the pin allocation:

Table 5: RJ-45 Pin Connections for 10/100/1000 Base-TX

Pin	Use
1	TxRx 1+
2	TxRx 1-
3	TxRx 2+
4	TxRx 2-
5	TxRx 3+
6	TxRx 3-
7	TxRx 4+
8	TxRx 4-

Figure 16: CX-4 Pin Allocation

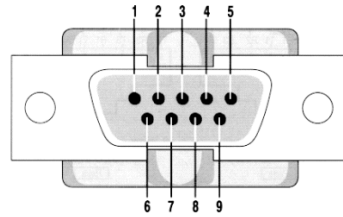


The following table describes the pin allocation

Table 6: CX-4 Port Pin Connections

Pin	Use
S1	Rx 0+
2	Rx 0-
3	Rx 1+
4	Rx 1-
5	Rx 2+
6	Rx 2-
7	Rx 3+
8	Rx 3-
9	Tx 3-
10	Tx 3+
11	Tx 2-
12	Tx 2+
13	Tx 1-
14	Tx 1+
15	Tx 0-
16	Tx 0+-

Figure 17: DB-9 Pin Allocation



The following table describes the pin allocation

Table 7: DB-9 Port Pin Connections

Pin	Use
1	N/A
2	RXD
3	TXD
4	N/A
5	GND
6	N/A
7	N/A
8	N/A
9	N/A

Physical Dimensions

The device has the following physical dimensions:

DXS/DWS - 3250 / DXS/DWS - 3227P

- Width: 440 mm (17.32 inch)
- Depth: 430mm (16.93 inch)
- Height: 44 mm (1.77 inch)

DXS/DWS - 3227

- Width: 440 mm (17.32 inch)
- Depth: 310 mm (12.20 inch)
- Height: 44 mm (1.77 inch)

This page is left blank intentionally.

Section 2. Mounting Device

This section contains information for installing the device, and includes the following sections:

- Preparing for Installation
- Installing the Device
- Connecting the Device
- Rack Installation

Preparing for Installation

This section provides an explanation for preparing the installation site, and includes the following topics:

- Installation Precautions
- Site Requirements
- Unpacking

Installation Precautions



Warnings

- The surface on which the switch is placed should be adequately secured to prevent it from becoming unstable and/or falling over.
- Ensure the power source circuits are properly grounded.
- Observe and follow service markings. Do not service any product except as explained in your system documentation. Opening or removing covers marked with a triangular symbol with a lightning bolt may cause electrical shock. These components are to be serviced by trained service technicians only.
- Ensure the power cable, extension cable, and/or plug is not damaged.
- Ensure the product is not exposed to water.
- Ensure the device is not exposed to radiators and/or heat sources.
- Do not push foreign objects into the device, as it may cause a fire or electric shock.
- Use the device only with approved equipment.
- Allow the product to cool before removing covers or touching internal equipment.
- Ensure the switch does not overload the power circuits, wiring, and over-current protection. To determine the possibility of overloading the supply circuits, add together the ampere ratings of all devices installed on the same circuit as the device being installed. Compare this total with the rating limit for the circuit. The maximum ampere ratings are usually printed on the switch, near their AC power connectors.



Cautions

- Ensure the air flow around the front, sides, and back of the switch is not restricted.
- Ensure the cooling vents are not blocked.
- Do not install the switch in an environment where the operating ambient temperature might exceed 40°C (104°F).

Site Requirements

The device is placed on a table-top. Before installing the unit, verify that the location chosen for installation meets the following site requirements.

- **General** — Ensure that the power supply is correctly installed.
- **Power** — The unit is installed within 1.5 m (5 feet) of a grounded, easily accessible outlet 100-250 VAC, 50-60 Hz.
- **Clearance** — There is adequate frontal clearance for operator access. Allow clearance for cabling, power connections and ventilation.
- **Cabling** — The cabling is routed to avoid sources of electrical noise such as radio transmitters, broadcast amplifiers, power lines and fluorescent lighting fixtures.
- **Ambient Requirements** — The ambient unit operating temperature range is 0 to 40°C (32 to 104°F) at a relative humidity of up to 95%, non-condensing. Verify that water or moisture cannot enter the device casing.

Unpacking

This section contains information for unpacking the device, and includes the following topics:

- Package Contents
- Unpacking Essentials

Package Contents

While unpacking the device, ensure that the following items are included:

- The device
- Four rubber feet with adhesive backing
- Rack kit
- An AC power cable
- Console RS-232 cable with DB-9 connector
- Documentation CD

Unpacking Essentials



Note

Before unpacking the device, inspect the package and report any evidence of damage immediately.

To unpack the device perform the following:

1. It is recommended to put on an ESD wrist strap and attach the ESD clip to a metal surface to act as ground. An ESD strap is not supplied with the device.
2. Place the container on a clean flat surface and cut all straps securing the container.
3. Open the container.
4. Carefully remove the device from the container and place it on a secure and clean surface.
5. Remove all packing material.
6. Inspect the product for damage. Report any damage immediately.

If any item is found missing or damaged, please contact your local D-Link reseller for replacement.

Installing the Device

The device can be installed on a flat surface or mounted in a rack. This section includes the following topics:

- Desktop or Shelf Installation
- Rack Installation

Desktop or Shelf Installation

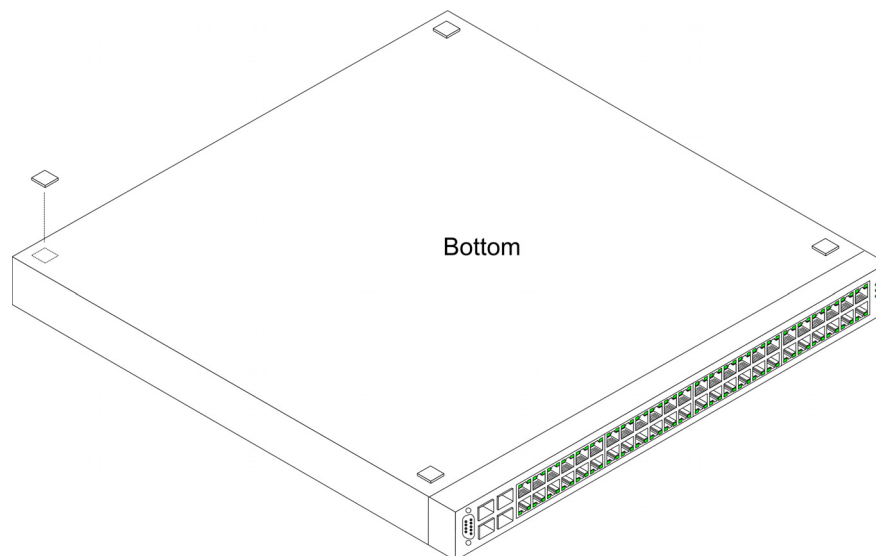
When installing the switch on a desktop or shelf, the rubber feet included with the device should first be attached. Attach these cushioning feet on the bottom at each corner of the device.

Ensure the surface is able to support the weight of the device and the device cables.

To install the device on a surface, perform the following:

1. Attach the rubber feet on the bottom of the device. The following figure illustrates the rubber feet installation on the device.

Figure 18: Installing Rubber Feet



2. Set device down on a flat surface, while leaving 2 inches on each side and 5 inches at the back.
3. Ensure that the device has proper ventilation by allowing adequate space for ventilation between the device and the objects around the device.

Rack Installation

The device can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install, the device the mounting brackets must first be attached on the devices's sides.



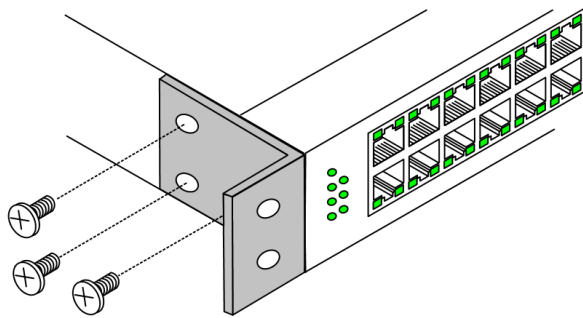
Notes

- Disconnect all cables from the unit before mounting the device in a rack or cabinet.
- When mounting multiple devices into a rack, mount the devices from the bottom up.

To install the device in a rack, perform the following:

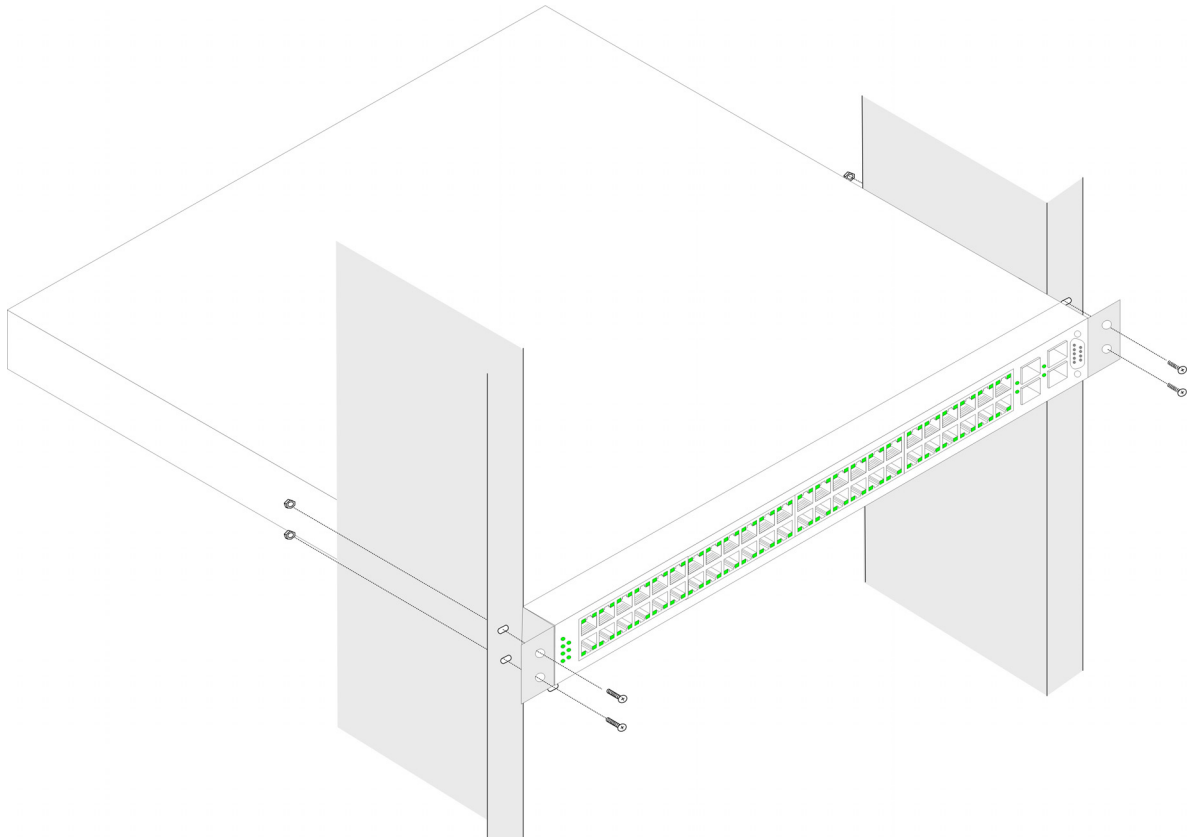
1. Place the supplied rack-mounting bracket on one side of the device ensuring the mounting holes on the device line up to the mounting holes on the rack mounting bracket. The following figure illustrates where to mount the brackets.

Figure 19: Attaching the Mounting Brackets



2. Insert the supplied screws into the rack mounting holes and tighten with a screwdriver.
3. Repeat the process for the rack-mounting bracket on the other side of the device.
4. Insert the unit into the 19-inch rack ensuring the rack-mounting holes on the device line up to the mounting hole on the rack. The following figure illustrates lining up and mounting the device in the rack.

Figure 20: Mounting Device in a Rack



5. Secure the unit to the rack with the rack screws (not provided). Fasten the lower pair of screws before the upper pair of screws. This ensures that the weight of the unit is evenly distributed during installation. Ensure that the ventilation holes are not obstructed.

Connecting the Device

This section describes how to connect the device, and includes the following sections:

- Connecting the Switch to a Terminal
- AC Power Connection

Connecting the Switch to a Terminal

The device is connected to a terminal through an console port on the front panel, which enables a connection to a terminal desktop system running terminal emulation software for monitoring and configuring the device.

The terminal must be a VT100 compatible terminal or a desktop or portable system with a serial port and running VT100 terminal emulation software.

To connect a terminal to the device Console port, perform the following:

1. Connect a cable to the terminal running VT100 terminal emulation software.
2. Ensure that the terminal emulation software is set as follows:
 - a) Select the appropriate port to connect to the device.
 - b) Set the data rate to 9600 baud.
 - c) Set the data format to 8 data bits, 1 stop bit, and no parity.
 - d) Set flow control to none.
 - e) Under Properties, select VT100 for Emulation mode.
 - f) Select **Terminal keys** for **Function**, **Arrow**, and **Ctrl** keys. Ensure that the setting is for Terminal keys (not Windows keys).



Note

When using HyperTerminal with Microsoft Windows 2000, ensure that you have Windows 2000 Service Pack 2 or later installed. With Windows 2000 Service Pack 2, the arrow keys function properly in HyperTerminal's VT100 emulation. Go to www.microsoft.com for information on Windows 2000 service packs.

3. Connect the cable to the console port on the device front panel.

AC Power Connection

To connect the power supply perform the following:

1. Using a 5-foot (1.5 m) standard power cable with safety ground connected, connect the power cable to the AC main socket located on the back panel.
2. Connect the power cable to a grounded AC outlet.
3. Confirm that the device is connected and operating by checking that the Power Supply LED on the front panel is green.

Section 3. Initial Configuration

This section describes the initial device configuration and includes the following topics:

- General Configuration Information
- Booting the Switch
- Configuration Overview
- Advanced Configuration
- Software Download and Reboot
- Configuring Stacking
- Startup Menu Functions

After completing all external connections, connect a terminal to the device to monitor the boot and other procedures. The order of installation and configuration procedures is illustrated in the following figure. For the initial configuration, the standard device configuration is performed. Other functions can be performed, but doing so suspends the installation process and causes a system reboot.

Performing other functions is described later in this section.

General Configuration Information

Your device has predefined features and setup configuration.

Auto-Negotiation

Auto-negotiation allows a device to advertise modes of operation and share information with another device that shares a point-to-point link segment. This automatically configures both devices to take maximum advantage of their abilities.

Auto-negotiation is performed completely within the physical layers during link initiation, without any additional overhead to either the MAC or higher protocol layers. Auto-negotiation allows the ports to do the following:

- Advertise their abilities
- Acknowledge receipt and understanding of the common modes of operation that both devices share
- Reject the use of operational modes that are not shared by both devices
- Configure each port for the highest-level operational mode that both ports can support

If connecting a port of the switch to the network interface card (NIC) of a terminal that does not support auto-negotiation or is not set to auto-negotiation, both the device port and the NIC must be manually set with the Web browser interface or CLI commands to the same speed and duplex mode.



Note

If the station on the other side of the link attempts to auto-negotiate with a port that is manually configured to full duplex, the auto-negotiation results in the station attempting to operate in half duplex. The resulting mismatch may lead to significant frame loss. This is inherent in the auto-negotiation standard.

Device Port Default Settings

The following table describes the device port default settings:

Table 8: Device Port Default Settings

Function	Default Settings
Port speed and mode	1000M Auto-negotiation
Port forwarding state	Enabled
Head of line blocking prevention	On (Enabled)
Flow Control	Off
Back Pressure	Off



Note

These default settings can be modified once the device is installed.

The following is an example for changing the port speed on port g1 using CLI commands:

```
Console(config)# interface ethernet 1
Console(config-if)# speed 100
```

The following is an example for enabling flow control on port g1 using CLI commands:

```
Console(config)# interface ethernet 1
Console(config-if)# flowcontrol on
```

The following is an example for enabling back pressure on port g1 using CLI commands.

```
Console(config)# interface ethernet 1
Console(config-if)# back-pressure
```

Booting the Switch

To boot the switch, perform the following:

1. Ensure that the device console is connected to a VT100 terminal device or VT100 terminal emulator.
2. Deactivate the AC power receptacle.
3. Connect the device to the AC receptacle.
4. Activate the AC power receptacle.

When the power is turned on with the local terminal already connected, the switch goes through Power On Self Test (POST). POST runs every time the device is initialized and checks hardware components to determine if the device is fully operational before completely booting. If a critical problem is detected, the program flow stops. If POST passes successfully, a valid executable image is loaded into RAM. POST messages are displayed on the terminal and indicate test success or failure.

As the switch boots, the bootup test first counts the device memory availability and then continues to boot. The following screen is an example of the displayed POST.

```
----- Performing the Power-On Self Test (POST) -----  
UART Channel Loopback Test.....PASS  
Testing the System SDRAM.....PASS  
Boot1 Checksum Test.....PASS  
Boot2 Checksum Test.....PASS  
Flash Image Validation Test.....PASS  
  
BOOT Software Version x.x.x.xx Built 07-Jan-200x 10:53:05  
Processor: xxxxxx xxxxx xxxx, xx MByte SDRAM.  
I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.  
  
Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

The boot process runs approximately 30 seconds.

The auto-boot message that appears at the end of POST (see the last lines) indicates that no problems were encountered during boot.

During boot, the Startup menu can be accessed if necessary to run special procedures. To enter the Startup menu, press **<Esc>** or **<Enter>** within the first two seconds after the auto-boot message is displayed. For information on the Startup menu, see "Startup Menu Functions."

If the system boot is not interrupted by pressing **<Esc>** or **<Enter>**, the system continues operation by decompressing and loading the code into RAM. The code starts running from RAM and the list of numbered system ports and their states (up or down) are displayed.



Note

The following screen is an example configuration. Items such as addresses, versions, and dates may differ for each device.

```
Preparing to decompress...

Decompressing SW from image-1
638000
OK
Running from RAM...

*****
*** Running SW Ver. x.x.x.x Date 11-Jan-200x Time 15:43:13 ***
*****

HW version is
Base Mac address is: 00:00:b0:24:11:80
Dram size is: xxM bytes
Dram first block size is: 47104K bytes
Dram first PTR is: 0x1200000
Flash size is: xM
Devices on SMI BUS:
-----
smi dev id = 16, dev type=0xd0411ab, dev revision=0x1

Device configuration:
Presteria based - Back-to-back system
Slot 1 - DB-DX240-24G HW Rev. xx.xx
Tapi Version: xx.x.x-x
Core Version: xx.x.x-x
01-Jan-200x 01:01:22 %INIT-I-InitCompleted: Initialization task is
completed

Console> 01-Jan-200x 01:01:23 %LINK-I-Up: e1
01-Jan-200x 01:01:23 %LINK-W-Down: e2
01-Jan-200x 01:01:23 %LINK-I-Up: Vlan 1
01-Jan-200x 01:01:23 %LINK-W-Down: e4
.
.
.
01-Jan-200x 01:01:23 %LINK-W-Down: e46
01-Jan-200x 01:01:23 %LINK-W-Down: e47
01-Jan-200x 01:01:23 %LINK-W-Down: e48
```

After the switch boots successfully, a system prompt appears (console>) and the local terminal can be used to begin configuring the switch. However, before configuring the switch, ensure that the software version installed on the device is the latest version. If it is not the latest version, download and install the latest version. See "Software Download and Reboot."

Configuration Overview

Before assigning a static IP address to the device, obtain the following information from the network administrator:

- A specific IP address allocated by the network administrator for the switch to be configured
- Network mask for the network

There are two types of configuration: Initial configuration consists of configuration functions with basic security considerations, whereas advanced configuration includes dynamic IP configuration and more advanced security considerations.

After making any configuration changes, the new configuration must be saved before rebooting. To save the configuration, enter the following CLI command:

```
Console# copy running-config startup-config
```

Initial Configuration

Initial configuration, which starts after the device has booted successfully, includes static IP address and subnet mask configuration, and setting user name and privilege level to allow remote management. If the device is to be managed from an SNMP-based management station, SNMP community strings must also be configured. The following configurations are completed:

- Static IP Address and Subnet Mask
- Static Route Configuration
- User Name
- SNMP Community strings

Static IP Address and Subnet Mask

IP interfaces can be configured on each port of the device. After entering the configuration command, it is recommended to check if a port was configured with the IP address by entering the “show ip interface” command.

The commands to configure the device are port specific.

To manage the switch from a remote network, a static route must be configured, which is an IP address to where packets are sent when no entries are found in the device tables. The configured IP address must belong to the same subnet as one of the device IP interfaces. To use the **ip route** command, the device mode must be changed from **switch** to **router**.

To configure a static route, enter the command at the system prompt as shown in the following configuration example where 101.101.101.101 is the specific management station, and 5.1.1.100 is the static route:

```
Console# configure
Console(config)# interface vlan 1
Console(config-if)# ip address 100.1.1.1 255.255.255.0
Console(config-if)# exit
Console# ip route 192.168.2.0/24 100.1.1.33
```



Note

100.1.1.33 is the IP address of the next hop that can be used to reach the management network 192.168.2.0.

```
Console# show ip interface
Proxy ARP is disabled

IP Address      I/F          Type          Directed
-----      -
100.1.1.1/24    vlan 1       static        disable
```

The above example is for **router** mode.

User Name

A user name is used to manage the device remotely, for example through SSH, Telnet, or the Web interface. To gain complete administrative (super-user) control over the device, the highest privilege (15) must be specified.



Note

Only the administrator (super-user) with the highest privilege level (15) is allowed to manage the device through the Web browser interface.

For more information about the privilege level, see the CLI Reference Guide.

The configured user name is entered as a login name for remote management sessions. To configure user name and privilege level, enter the command at the system prompt as shown in the configuration example:

```
Console> enable
Console# configure
Console(config)# username admin password lee privilege 15
```

SNMP Community Strings

Simple Network Management Protocol (SNMP) provides a method for managing network devices. Devices supporting SNMP run a local software (agent). The SNMP agents maintain a list of variables, used to manage the device. The variables are defined in the Management Information Base (MIB). The MIB presents the variables controlled by the agent. The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network.

Access rights to the SNMP agents are controlled by access strings and SNMP community strings.

The device is SNMP-compliant and contains an SNMP agent that supports a set of standard and private MIB variables. Developers of management stations require the exact structure of the MIB tree and receive the complete private MIBs information before being able to manage the MIBs.

All parameters are manageable from any SNMP management platform, except the SNMP management station IP address and community (community name and access rights). The SNMP management access to the switch is disabled if no community strings exist.



Note

The device switch is delivered with no community strings configured.

The following screen displays the default device configuration:

```
console# show snmp
Community-String      Community-Access      View name      IP address
-----
Community-String      Group name      IP address      Type
-----
Traps are enabled.
Authentication-failure trap is enabled.
Version 1,2 notifications
Target Address      Type      Community      Version      Udp      Filter      To      Retries
Port      name      Sec
-----
Version 3 notifications
Target Address      Type      Username      Security      Udp      Filter      To      Retries
Level      Port      name      Sec
-----
System Contact:
System Location:
```

The community-string, community-access, and IP address can be configured through the local terminal during the initial configuration procedure.

The SNMP configuration options for the Community String are as follows:

- Access rights options: ro (read only), rw (read-and-write) or su (super).
- An option to configure IP address or not: If an IP address is not configured, it means that all community members having the same community name are granted the same access rights.

Common practice is to use two community strings for the switch one (public community) with read-only access and the other (private community) with read-write access. The public string allows authorized management stations to retrieve MIB objects, while the private string allows authorized management stations to retrieve and modify MIB objects.

During initial configuration, it is recommended to configure the device according to the network administrator requirements, in accordance with using an SNMP-based management station.

To configure SNMP station IP address and community string(s) perform the following:

1. At the console prompt, enter the command **Enable**. The prompt is displayed as #.
2. Enter the command **configure** and press <Enter>.
3. In the configuration mode, enter the SNMP configuration command with the parameters including community name (private), community access right (read and write) and IP address, as shown in the following example:

```

console# configure
console(config)# snmp-server community priate rw 10.1.1.1 view bob1
console(config)# exit
console# show snmp
Community-String      Community-Access      View name      IP address
-----
      priate           read write          bob1           10.1.1.1
      private         read write          bob1           10.1.1.2

Community-String      Group name      IP address      Type
-----
Traps are enabled.
Authentication-failure trap is enabled.

Version 1,2 notifications
Target Address      Type      Community      Version      Udp      Filter      To      Retries
Port      name      Sec
-----
Version 3 notifications
Target Address      Type      Username      Security      Udp      Filter      To      Retries
Level      Port      name      Sec
-----
System Contact:
System Location:
    
```

This completes the initial configuration of the device from a local terminal. The configured parameters enable further device configuration from any remote location.

Advanced Configuration

This section provides information about dynamic allocation of IP addresses and security management based on the authentication, authorization, and accounting (AAA) mechanism, and includes the following topics:

- Configuring IP Addresses through DHCP
- Configuring IP Addresses through BOOTP
- Security Management and Password Configuration

When configuring/receiving IP addresses through DHCP and BOOTP, the configuration received from these servers includes the IP address, and may include subnet mask and default gateway.

Retrieving an IP Address From a DHCP Server

When using the DHCP protocol to retrieve an IP address, the device acts as a DHCP client. To retrieve an IP address from a DHCP server, perform the following steps:

1. Select and connect any port to a DHCP server or to a subnet that has a DHCP server on it, in order to retrieve the IP address.
2. Enter the following commands to use the selected port for receiving the IP address. In the following example, the commands are based on the port type used for configuration.
 - Assigning Dynamic IP Addresses:

```

console# configure
console(config)# interface ethernet 1
console(config-if)# ip address dhcp hostname <string>
    
```

The interface receives the IP address automatically.

1. To verify the IP address, enter the show IP interface command at the system prompt as shown in the following example.

```
Console# show ip interface

Gateway IP Address   Activity status   Type
-----
10.6.41.97          Active           Static

IP address          I?F              Type
-----
10.6.41.101/27     VLAN 1          Static
```



Notes

- The device configuration does not have to be deleted to retrieve an IP address for the DHCP server.
- When copying configuration files, avoid using a configuration file that contains an instruction to enable DHCP on an interface that connects to the same DHCP server, or to one with an identical configuration. In this instance, the switch retrieves the new configuration file and boots from it. The device then enables DHCP as instructed in the new configuration file, and the DHCP instructs it to reload the same file again.

Receiving an IP Address From a BOOTP Server

The standard BOOTP protocol is supported and enables the switch to automatically download its IP host configuration from any standard BOOTP server in the network. In this case, the device acts as a BOOTP client.

To retrieve an IP address from a BOOTP server:

1. Select and connect any port to a BOOTP server or subnet containing such a server, to retrieve the IP address.
2. At the system prompt, enter the delete startup configuration command to delete the startup configuration from flash. The device reboots with no configuration and in 60 seconds starts sending BOOTP requests. The device receives the IP address automatically.



Note

When the device reboot begins, any input at the ASCII terminal or keyboard automatically cancels the BOOTP process before completion and the device does not receive an IP address from the BOOTP server.

The following example illustrates the process:

```
Console> enable
Console# delete startup-config
Startup file was deleted
Console# reload
You haven't saved your changes. Are you sure you want to continue (y/n) [n]?
This command will reset the whole system and disconnect your current
session.Do you want to continue (y/n) [n]?
*****
/*the device reboots */
```

To verify the IP address, enter the show ip interface command. The device is now configured with an IP address.

Security Management and Password Configuration

System security is handled through the AAA (Authentication, Authorization, and Accounting) mechanism that manages user access rights, privileges, and management methods. AAA uses both local and remote user databases. Data encryption is handled through the SSH mechanism.

The system is delivered with no default password configured; all passwords are user-defined. If a user-defined password is lost, a password recovery procedure can be invoked from the Startup menu. The procedure is applicable for the local terminal only and allows a one-time access to the device from the local terminal with no password entered.

Configuring Security Passwords Introduction

The security passwords can be configured for the following services:

- Console
- Telnet
- SSH
- HTTP
- HTTPS

Passwords are user-defined.

When creating a user name, the default priority is "1," which allows access but not configuration rights. A priority of "15" must be set to enable access and configuration rights to the device. Although user names can be assigned privilege level 15 without a password, it is recommended to always assign a password. If there is no specified password, privileged users can access the Web interface with any password.

Configuring an Initial Console Password

To configure an initial console password, enter the following commands:

```
Console(config)# aaa authentication login default line
Console(config)# aaa authentication enable default line
Console(config)# line console
Console(config-line)# login authentication default
Console(config-line)# enable authentication default
Console(config-line)# password george
```

When initially logging on to a device through a console session, enter george at the password prompt.

When changing a device's mode to enable, enter george at the password prompt.

Configuring an Initial Telnet Password

To configure an initial Telnet password, enter the following commands:

```
Console(config)# aaa authentication login default line
Console(config)# aaa authentication enable default line
Console(config)# line telnet
Console(config-line)# login authentication default
Console(config-line)# enable authentication default
Console(config-line)# password bob
```

When initially logging onto a device through a Telnet session, enter bob at the password prompt.

When changing a device mode to enable, enter bob.

Configuring an Initial SSH password

To configure an initial SSH password, enter the following commands:

```
Console(config)# aaa authentication login default line
Console(config)# aaa authentication enable default line
Console(config)# line ssh
Console(config-line)# login authentication default
Console(config-line)# enable authentication default
Console(config-line)# password jones
```

When initially logging onto a device through a SSH session, enter "jones" at the password prompt.

When changing a device mode to enable, enter "jones".

Configuring an Initial HTTP Password

To configure an initial HTTP password, enter the following commands:

```
Console(config)# ip http authentication local
Console(config)# username admin password user1 level 15
```

Configuring an initial HTTPS Password

To configure an initial HTTPS password, enter the following commands:

```
Console(config)# ip https authentication local
Console(config)# username admin password user1 level 15
```

Enter the following commands once when configuring to use a console, a Telnet, or an SSH session in order to use an HTTPS session.

In the Web browser enable SSL 2.0 or greater for the content of the page to appear.

```
Console(config)# ip https server
Console(config)# crypto certificate 1 generate key-generate
Generating RSA private key, 1024 bit long modulus
Console(config)# ip https certificate 1
```

When initially enabling an http or https session, enter admin for user name and user1 for password.



Note

HTTP and HTTPS services require level 15 access and connect directly to the configuration level access.

Software Download and Reboot

Software Download through XModem

This section contains instructions for downloading device software (system and boot images) using XModem, which is a data transfer protocol for updating back-up configuration files.

To download a boot file using XModem:

1. Enter the command “xmodem:boot”. The switch is ready to receive the file via the XModem protocol and displays text similar to the following:

```
Console# copy xmodem:boot
Please download program using XMODEM.
console#
```

2. Specify the path of the source file within 20 seconds. If the path is not specified within 20 seconds, the command times out.

To download a software image file using XModem:

1. Enter the command “xmodem:image”. The switch is ready to receive the file via the XModem protocol.
2. Specify the path of the source file to begin the transfer process. The following is an example of the information that appears:

```
Console# copy xmodem:image
Please download program using XMODEM
console#
```

Software Download Through TFTP Server

This section contains instructions for downloading device software (system and boot images) through a TFTP server. The TFTP server must be configured before downloading the software.

The switch boots and runs when decompressing the system image from the flash memory area where a copy of the system image is stored. When a new image is downloaded, it is saved in the other area allocated for the additional system image copy.

On the next boot, the switch decompresses and runs the currently active system image unless chosen otherwise.

To download an image through the TFTP server:

1. Ensure that an IP address is configured on one of the device ports and pings can be sent to a TFTP server.
2. Ensure that the file to be downloaded is saved on the TFTP server (the DOS file).
3. Enter the command “show version” to verify which software version is currently running on the device. The following is an example of the information that appears:

```
Console# show version
SW version x.xx.xx (date xx-xxx-2004 time 13:42:41)Boot version
x.xx.x (date x-xxx-2003 time 15:12:20) HW version
```

4. Enter the command “show bootvar” to verify which system image is currently active. The following is an example of the information that appears:

```
Console# show bootvar
Images currently available on the Flash Image-1 active (selected for
next boot)Image-2 not active
Console#
```

5. Enter the command “copy tftp://{tftp address}/{file name}image” to copy a new system image to the device. When the new image is downloaded, it is saved in the area allocated for the other copy of system image (image-2, as given in the example). The following is an example of the information that appears:

```
Console# copy tftp://176.215.31.3/file1 image Accessing file file1 on
176.215.31.3...
Loading file1 from
176.215.31.3:!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy took 00:01:11 [hh:mm:ss]
```

Exclamation symbols indicate that a copying process is in progress. A period indicates that the copying process is timed out. Many periods in a row indicate that the copying process failed.

6. Select the image for the next boot by entering the boot system command. After this command, enter the command “show bootvar” to verify that the copy indicated as a parameter in the boot system command is selected for the next boot. The following is an example of the information that appears:

```
Console# boot system image-2
Console# sh bootvar
Images currently available on the Flash Image-1 active Image-2 not
active (selected for next boot)
```

If the image for the next boot is not selected by entering the boot system command, the system boots from the currently active image (image-1, as given in the example).

7. Enter the command “reload”. The following message is displayed:

```
Console# reload
This command will reset the whole system and disconnect your current
session.Do you want to continue (y/n) [n]?
```

8. Enter “Y” to reboot the switch.

Boot Image Download

Loading a new boot image from the TFTP server and programming it into the flash updates the boot image. The boot image is loaded when the switch is powered on.

To download a boot file through the TFTP server:

1. Ensure that an IP address is configured on one of the device ports and pings can be sent to a TFTP server.
2. Ensure that the file to be downloaded (the .rfb file) is saved on the TFTP server.
3. Enter the command “show version” to verify which boot version is currently running on the device. The following is an example of the information that appears:

```
Console# show version
SW version x.xx.xx (date xx-xxx-2004 time 13:42:41)Boot version
x.xx.xx (date xx-xx-2004 time 15:12:20)HW version xx.xx.xx (date xx-
xxx-2004 time 12:12:20)
```

4. Enter the command “copy tftp://{tftp address}/{file name} boot” to copy the boot image to the switch. The following is an example of the information that appears:

```
Console# copy tftp://176.215.31.3/6024_boot-10013.rfb
Erasing file
...done!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!Copy:393232 bytes copied in 00:00:05 [hh:mm:ss]
```


5. Enter the command “reload”. The following message is displayed:

```
Console# reload
This command will reset the whole system and disconnect your current
session. Do you want to continue (y/n) [n]?
```

6. Enter “Y” to reboot the switch.

Configuring Stacking

Configuring stacking is performed during the bootup process. To configure a device as part of a stack, the bootup process must be interrupted straight after the *Power On Self Test* (POST).

To configure the device for stacking, perform the following:

1. Ensure that the device console is connected to a VT100 terminal device or VT100 terminal emulator.
2. Deactivate the AC power receptacle.
3. Connect the device to the AC receptacle.
4. Activate the AC power receptacle.

When the power is turned on with the local terminal already connected, the switch goes through POST. POST runs every time the device is initialized and checks hardware components to determine if the device is fully operational before completely booting. If a critical problem is detected, the program flow stops. If POST passes successfully, a valid executable image is loaded into RAM. POST messages are displayed on the terminal and indicate test success or failure.

As the switch boots, the bootup test first counts the device memory availability and then continues to boot. The following screen is an example of the displayed POST.

```
----- Performing the Power-On Self Test (POST) -----
UART Channel Loopback Test.....PASS
Testing the System SDRAM.....PASS
Boot1 Checksum Test.....PASS
Boot2 Checksum Test.....PASS
Flash Image Validation Test.....PASS
BOOT Software Version x.x.x.xx Built 07-Jan-200x 10:53:05
Processor: xxxxxx xxxxx xxxx, xx MByte SDRAM.
I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.
Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

The boot process runs approximately 30 seconds.

The auto-boot message that appears at the end of POST (see the last lines) indicates that no problems were encountered during boot.

5. Suspend the startup process by pressing <Esc> or <Enter> within two seconds and the following message is displayed:

```
Autoboot in 2 seconds -press RETURN or Esc.to abort and enter prom.
```

The Startup Menu is displayed and contains the following configuration functions:

```
Startup Menu

[1]Download Software
[2]Erase Flash File
[3]Erase Flash Sectors
[4>Password Recovery Procedure
[5]Enter Diagnostic Mode
[6]Stack Menu
[7]Back Enter your choice or press 'ESC' to exit:
```

6. On the Startup Menu, press “6”.
The following Stack Menu is displayed:

```
Stack menu
[1] Set unit number in stack
[2] Change stacking ports
[3] Stack info
[4] Back
Enter your choice or press 'ESC' to exit:
```

7. To Set a unit number press “1” on the Stack Menu.
The following prompt is displayed:

```
Enter your choice or press 'ESC' to exit:
Unit number in stack: [0-8,0 marks standalone unit] 1

Stacking Ports List - 1 2
Change stacking ports.

Enter #1 stacking port (valid range 1-48 and 49-50) use 'k' to keep
current setting (port 1):49
Enter #2 stacking port (valid range 1-48 and 49-50) use 'k' to keep
current setting (port 2):50
==== Press Enter To Continue ====
```

8. Enter the first stacking port.
9. Enter the second stacking port.
10. Press **<Enter>**. The device is defined within the stack.
11. To change stacking ports press “2” on the Stack Menu.
The following prompt is displayed:

```
Enter your choice or press 'ESC' to exit:

Stacking Ports List - 1 2
Change stacking ports.

Enter #1 stacking port (valid range 1-48 and 49-50) use 'k' to keep
current setting (port 1):
k
Enter #2 stacking port (valid range 1-48 and 49-50) use 'k' to keep
current setting (port 2):
k
==== Press Enter To Continue ====
```

12. Enter the first stacking port.
13. Enter the second stacking port.
14. Press **<Enter>**. The device is defined within the stack.
15. For a stack info press “3” on the Stack Menu.
The following prompt is displayed:

```
Enter your choice or press 'ESC' to exit:

Stack Info:
-----
Unit stack ID - 1

Stacking Ports List - 49 50
==== Press Enter To Continue ====
```

16. From the Stack menu, press “4”. The Startup menu is displayed.
17. From the Startup menu, press “10”. The Startup menu is closed and the device continues the Startup process.



Note

Once the device is booted up and operational in the stack, the configuration can be modified through the Web or CLI.

Startup Menu Functions

Additional configuration functions can be performed from the Startup menu.

To display the Startup menu:

1. During the boot process, after the first part of the POST is completed press <Esc> or <Enter> within two seconds after the following message is displayed:

```
Autoboot in 2 seconds -press RETURN or Esc.to abort and enter prom.
```

The Startup menu is displayed and contains the following configuration functions:

```
Startup Menu

[1]Download Software
[2]Erase Flash File
[3]Erase Flash Sectors
[4>Password Recovery Procedure
[5]Enter Diagnostic Mode
[6]Stack Menu
[7]Back Enter your choice or press 'ESC' to exit:
```

The following sections describe the Startup menu options. If no selection is made within 25 seconds (default), the switch times out and the device continues to load normally.

Only technical support personnel can operate the Diagnostics Mode. For this reason, the **Enter Diagnostic Mode** option of the Startup menu is not described in this guide.

Download Software

Use the software download option when a new software version must be downloaded to replace corrupted files, update, or upgrade the system software.

To download software from the Startup menu:

1. On the Startup menu, press “1”.

The following prompt is displayed:

```
Downloading code using XMODEM
```

2. When using HyperTerminal, click **Transfer** on the HyperTerminal menu bar.
3. From the Transfer menu, click **Send File**. The **Send File** window is displayed.
4. Enter the file path for the file to be downloaded.
5. Ensure the protocol is defined as Xmodem.
6. Click **Send**.

The software is downloaded. Software downloading takes several minutes. The terminal emulation application, such as HyperTerminal, may display the progress of the loading process.

After software downloads, the device reboots automatically.

Erase FLASH File

In some cases, the device configuration must be erased. If the configuration is erased, all parameters configured via CLI, Web browser interface, or SNMP must be reconfigured.

To erase the device configuration:

1. From the Startup menu, press “2” within 6 seconds to erase flash file. The following message is displayed:

```
Warning! About to erase a Flash file.  
Are you sure (Y/N)?y
```

2. Press “Y”.



Note

Do not press <Enter>.

The following message is displayed.

```
Write Flash file name (Up to 8 characters, Enter for none.):config  
File config (if present) will be erased after system initialization  
=====Press Enter To Continue =====
```

3. Enter **config** as the name of the flash file. The configuration is erased and the device reboots.
4. Perform the switch’s initial configuration.

Erase FLASH Sectors

For troubleshooting purposes, the flash sectors may need to be erased. If the flash is erased, all software files must be downloaded and installed again.

To erase the FLASH:

1. From the Startup menu, press “3” within 6 seconds. The following message is displayed:

```
Warning! About to erase Flash Memory! FLASH size =16252928.blocks =64  
Are you sure (Y/N)
```

2. Confirm by pressing <Y>. The following message is displayed:

```
Enter First flash block (1 -63):
```

3. Enter the first flash block to be erased and press <Enter>. The following message is displayed:

```
Enter Last flash block (1 -63):
```

4. Enter the last flash block to be erased and press <Enter>. The following message is displayed:

```
Are you sure (Y/N)
```

5. Confirm by pressing <Y>. The following message is displayed:

```
Erasing flash blocks 1 -63: Done.
```

Password Recovery

If a password is lost, use the Password Recovery option on the Startup menu. The procedure enables the user to enter the device once without a password.

To recover a lost password for the local terminal only:

1. From the Startup menu, select “4” and press <Enter>. The password is deleted.
2. To ensure device security, reconfigure passwords for applicable management methods.

WLAN Licence Key

To upgrade a DXS- model into a DWS model with WLAN support, the user must enter a Licence key. The following section describes the procedures for entering a Licence Key.

As the switch boots, the bootup test first counts the device memory availability and then continues to boot. The following screen is an example of the displayed POST.

```
----- Performing the Power-On Self Test (POST) -----
UART Channel Loopback Test.....PASS
Testing the System SDRAM.....PASS
Boot1 Checksum Test.....PASS
Boot2 Checksum Test.....PASS
Flash Image Validation Test.....PASS
BOOT Software Version x.x.x.xx Built 07-Jan-200x 10:53:05
Processor: xxxxxx xxxxx xxxxx, xx MByte SDRAM.
I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.
Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

The boot process runs approximately 30 seconds.

The auto-boot message that appears at the end of POST (see the last lines) indicates that no problems were encountered during boot.

To enter a WLAN licence key perform the following:

1. Suspend the startup process by pressing <Esc> or <Enter> within two seconds and the following message is displayed:

```
Autoboot in 2 seconds -press RETURN or Esc.to abort and enter prom.
```

The Startup Menu is displayed and contains the following configuration functions:

```
Startup Menu
[1] Download Software
[2] Erase Flash File
[3] Password Recovery Procedure
[4] Enter Diagnostic Mode
[5] Set Terminal Baud-Rate
[6] Stack menu
[7] License menu
[8] Back
```

2. From the Startup Menu, press “7”.

The following Licence Menu is displayed:

```
License menu
[1] Add license
[2] Remove license
[3] Show license
[4] Back
Enter your choice or press 'ESC' to exit:
```

3. From the License Menu, press “1”.
The following prompt is displayed:

```
Enter licence:
```

4. Enter the licence key.
5. Press **<Enter>**
6. To remove a licence press “2” . The licence is removed (no prompt text appears).
7. To show a licence press “3”.
The following prompt is displayed:

```
Enter your choice or press 'ESC' to exit:
License number is:

N1-000000092948-25-0-A48D74999AC805DD

==== Press Enter To Continue ====
```

8. Press **<Escape>**

This page is left blank intentionally.

Section 4. Getting Started

This section provides an introduction to the user interface, and includes the following topics:

- Starting the D-Link Embedded Web Interface
- Understanding the D-Link Embedded Web Interface
- Using Screen and Table Options
- Resetting the Device
- Logging Off from the Device

Starting the D-Link Embedded Web Interface



Notes

- Disable the popup blocker before beginning device configuration using the EWS.

This section contains information on starting the D-Link Embedded Web interface. To access the D-Link user interface:

1. Open an Internet browser.
2. Ensure that pop-up blockers are disabled. If pop-up blockers are enable, edit, add, and device information messages may not open.
3. Enter the device IP address in the address bar and press Enter. The *Enter Network Password Page* opens:

Figure 21: Enter Network Password Page

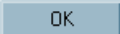
The screenshot shows a web browser window displaying the D-Link Embedded Web Interface. At the top, there is a blue header with the 'D-Link' logo. Below the header, the main content area is white. In the center, there is a grey box with the text 'Type in Username and Password, then click OK'. Below this text are two input fields: 'Username' and 'Password'. Below the input fields is a grey 'OK' button.

4. Enter your user name and password.



Notes

- The device is configured with a user name that is admin and a password that is blank, and can be configured without entering a password.
- Passwords are case sensitive.
- To operate the device, disable all pop-ups with a popup blocker.

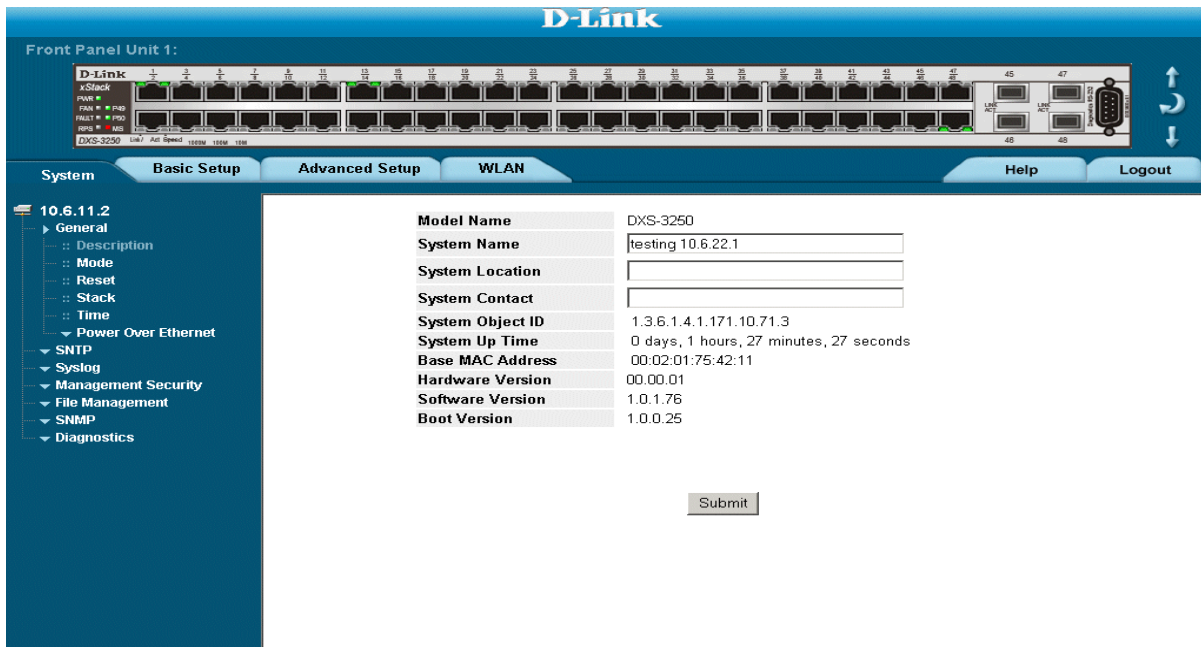
5. Click . The *D-Link Embedded Web Interface Home Page* opens:



Notes

- The screen captures in this Guide represent the 48 port device. The Web pages in the 24 port device may vary slightly.

Figure 22: D-Link Embedded Web Interface Home Page

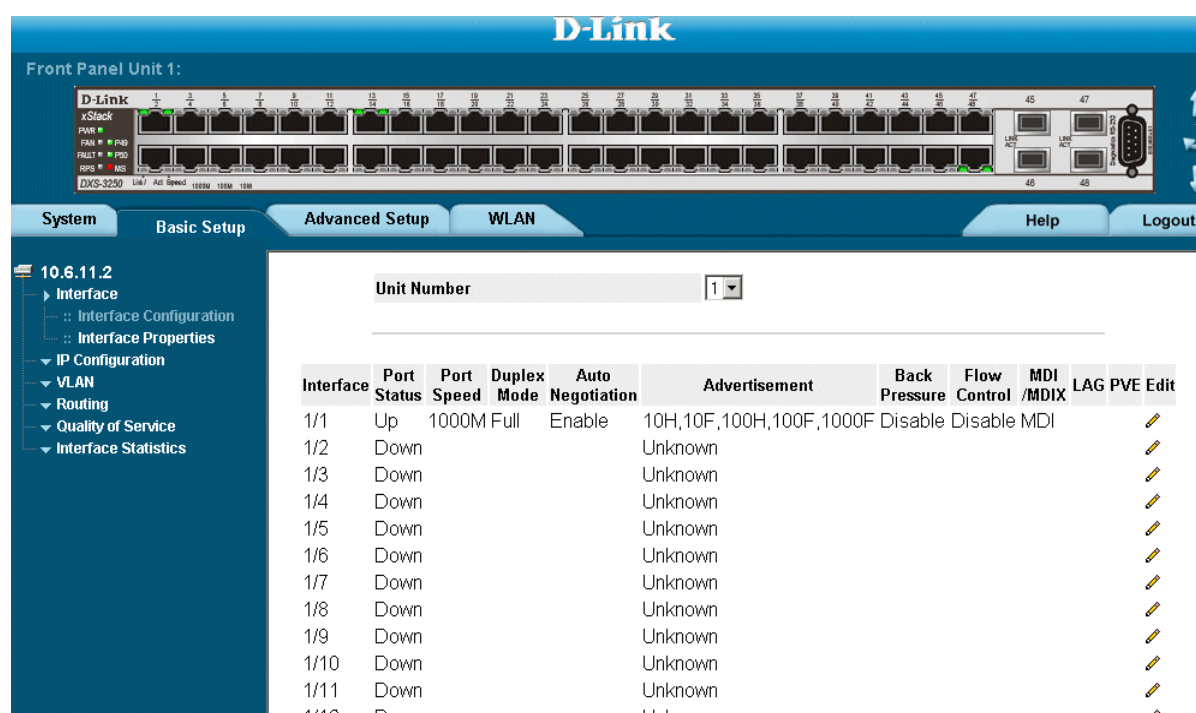


Understanding the D-Link Embedded Web Interface

The *D-Link Embedded Web Interface Home Page* contains the following views:

- **Port LED Indicators** — Located at the top of the home page, the port LED indicators provide a visual representation of the ports on the D-Link front panel.
- **Tab Area** — Located under the LED indicators, the tab area contains a list of the device features and their components.
- **Device View** — Located in the main part of the home page, the device view provides a view of the device, an information or table area, and configuration instructions.

Figure 23: D-Link Embedded Web Interface Components



The following table lists the user interface components with their corresponding numbers:

Table 9: Interface Components

View	Description
1 Tree View	Tree View provides easy navigation through the configurable device features. The main branches expand to display the sub-features.
2 Device View	Device View provides information about device ports, current configuration and status, table information, and feature components. Device View also displays other device information and dialog boxes for configuring parameters.

Table 9: Interface Components

View	Description
3 Tab Area	The Tab Area enables navigation through the different device features. Click the tabs to view all the components under a specific feature.
4 Zoom View	Provides a graphic of the device on which D-Link Web Interface runs.
5 D-Link Web Interface Information Tabs	Provide access to online help, and contain information about the EWS.

This section provides the following additional information:

- **Device Representation** — Provides an explanation of the D-Link user interface buttons, including both management buttons and task icons.
- **Using the D-Link Embedded Web Interface Management Buttons** — Provides instructions for adding, modifying, and deleting configuration parameters.

Device Representation

The *D-Link Embedded Web Interface Home Page* contains a graphical panel representation of the device.

Figure 24: Device Representation



Using the D-Link Embedded Web Interface Management Buttons

Configuration Management buttons and icons provide an easy method of configuring device information, and include the following:

Table 10: D-Link Web Interface Configuration Buttons









Button	Button Name	Description
	Clear Logs	Clears system logs.
	Create	Enables creation of configuration entries.
	Edit	Modifies configuration settings.
	Submit	Saves configuration changes to the device.
	Test	Performs cable tests.
	Query	Queries the device table.

Table 11: D-Link Web Interface Information Tabs

Tab	Tab Name	Description
	Help	Opens the online help.
	Logout	Opens the Logout page.

Using Screen and Table Options

D-Link contains screens and tables for configuring devices. This section contains the following topics:

- Adding Configuration Information
- Modifying Configuration Information
- Deleting Configuration Information

Adding Configuration Information

User-defined information can be added to specific D-Link Web Interface pages, by opening a new Add page. To add information to tables or D-Link Web Interface pages:

1. Open an D-Link Web Interface page.
2. Click **Create** . An add page opens, such as the *Add SNMP Interface Page*:

Figure 25: Add SNMP Interface



3. Define the fields.
4. Click **Submit** . The configuration information is saved, and the device is updated.

Modifying Configuration Information


1. Open The D-Link Embedded Web Interface page.
2. Select a table entry.
3. Click  . A modification page, such as the *IP Interface Settings Page* opens:

Figure 26: IP Interface Settings Page

IP Interface Settings

IP Address	10.6.25.174
<input checked="" type="radio"/> Network Mask	255.255.255.224
<input type="radio"/> Prefix Length	/27
Interface	<input type="radio"/> Port 1/1 <input type="radio"/> LAG 1 <input checked="" type="radio"/> VLAN 1
Type	DHCP

4. Modify the fields.
5. Click **Submit**. The fields are modified, and the information is saved to the device.

Deleting Configuration Information

1. Open The D-Link Embedded Web Interface page.
2. Select a table row.
3. Select the *Remove* checkbox.
4. Click **Submit**. The information is deleted, and the device is updated.

Resetting the Device

The *Reset* page enables resetting the device from a remote location.



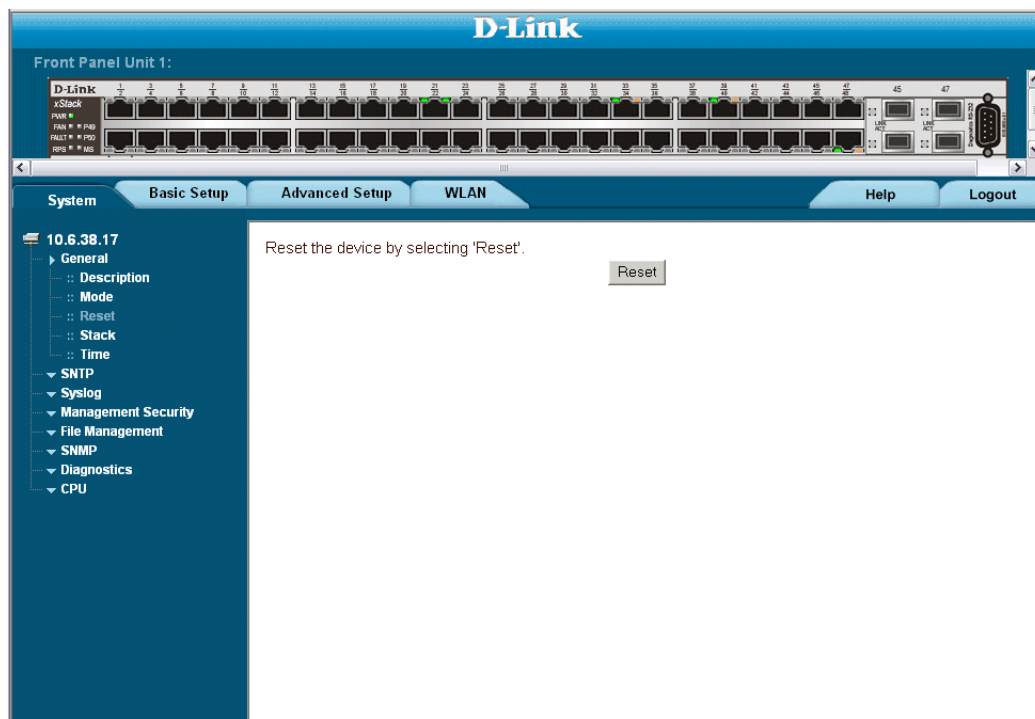
Note

To prevent the current configuration from being lost, save all changes from the running configuration file to the startup configuration file before resetting the device. For instructions, see *Copying Files*.

To reset the device:


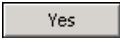
1. Click **System > General > Reset**. The *Reset* page opens.

Figure 27: Reset Page



2. Click **Reset Device**. A confirmation message is displayed.
3. Click **OK**. The device is reset, and a prompt for a user name and password is displayed.
4. Enter a user name and password to reconnect to the web Interface.

Logging Off from the Device

1. Click . The *Logout Page* opens.
2. Click . The *D-Link Embedded Web Interface Home Page* closes.

Section 5. Managing Device Information

This section contains information for setting general system information, and includes the following sections:

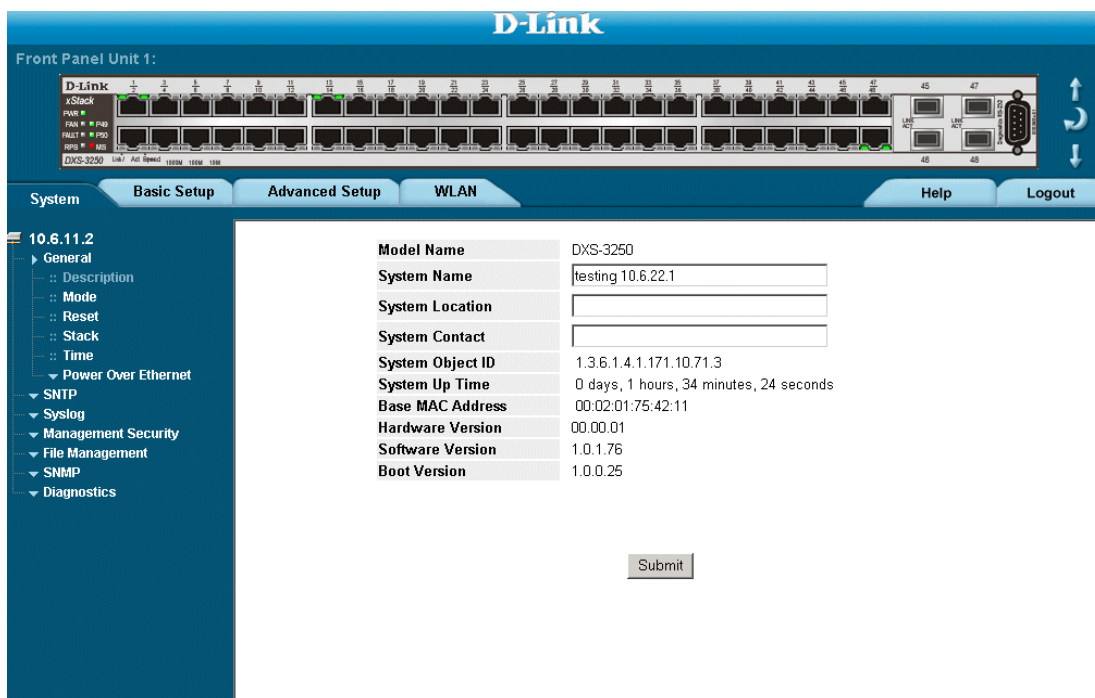
- Defining the System Description
- Defining Advanced System Settings

Defining the System Description

The *System Description Page* contains parameters for configuring general device information, including the system name, location, and contact, the system MAC Address, System Object ID, System Up Time, and MAC addresses, and both software, boot, and hardware versions. To define the general system information:

1. Click **System > General > Description**. The *System Description Page* opens:

Figure 28: System Description Page



The *System Description Page* contains the following fields:

- **Model Name** — Displays the device model number and name.
- **System Name** — Defines the user-defined device name. The field range is 0-160 characters.
- **System Location** — Defines the location where the system is currently running. The field range is 0-160 characters.
- **System Contact** — Defines the name of the contact person. The field range is 0-160 characters.

- **System Object ID** — Displays the vendor's authoritative identification of the network management subsystem contained in the entity.
- **System Up Time** — Displays the amount of time since the most recent device reset. The system time is displayed in the following format: Days, Hours, Minutes, and Seconds. For example, 41 days, 2 hours, 22 minutes and 15 seconds.
- **Base MAC Address** — Displays the device MAC address.
- **Hardware Version** — Displays the installed device hardware version number.
- **Software Version** — Displays the installed software version number.
- **Boot Version** — Displays the current boot version running on the device.

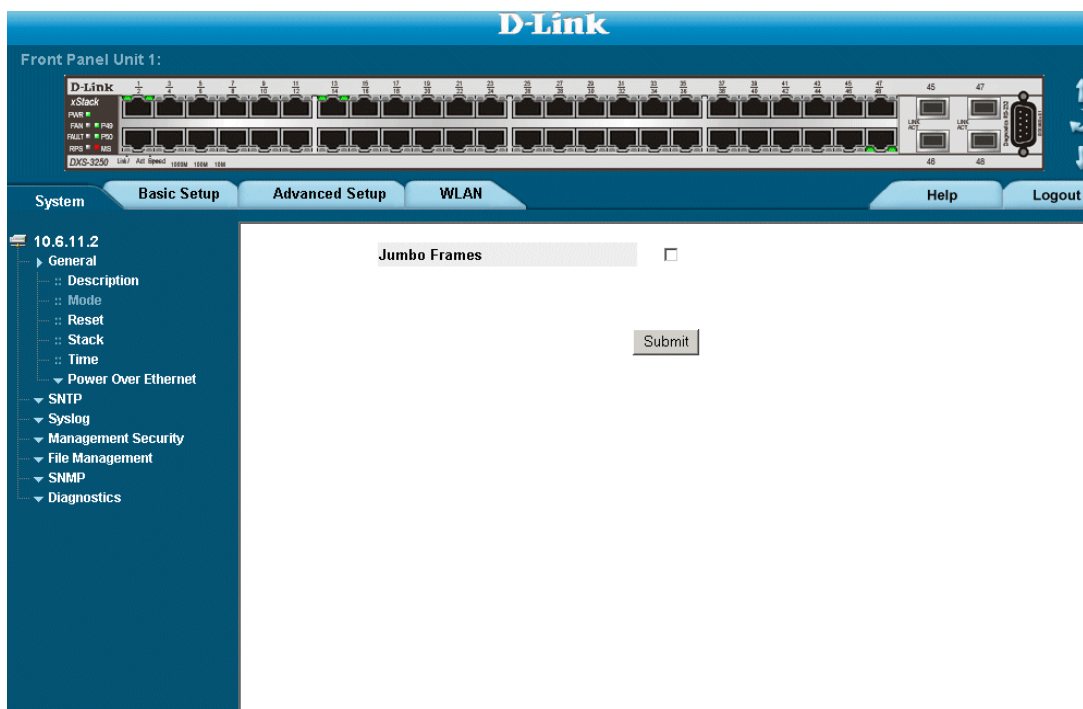
Defining Advanced System Settings

The *Mode Page* allows network managers to enable Jumbo Frames on the device. Jumbo Frames enable the transportation of identical data in fewer frames. This ensures less overhead, lower processing time, and fewer interruptions.

To define advanced system settings:

1. Click **System > General > Mode**. The *Mode Page* opens.

Figure 29: Mode Page



The *Mode Page* contains the following field:

- **Enable Jumbo Frames** — Indicates if Jumbo Frames are enabled on the device. Maximum packet length supported is 10Kb. The possible field values are:
 - *Checked* — Enables Jumbo Frames on the device.
 - *Unchecked* — Disables Jumbo Frames on the device.
2. Check the *Enable Jumbo Frames* field.
 3. Click **Submit**. Jumbo frames are enabled on the device.



Note

New settings will take effect only after resetting the device

This page is left blank intentionally.

Section 6. Managing Power over Ethernet Devices

Power over Ethernet (PoE) provides power to devices over existing LAN cabling, without updating or modifying the network infrastructure. Power over Ethernet removes the necessity of placing network devices next to power sources. Power over Ethernet can be used with:

- IP Phones
- Wireless Access Points
- IP Gateways
- PDAs
- Audio and video remote monitoring

Powered Devices are devices which receive power from the device power supplies, for example IP phones. Powered Devices are connected to the device via Ethernet ports.

PoE is enabled for the DXS-3227P only.

This section includes the following topics:

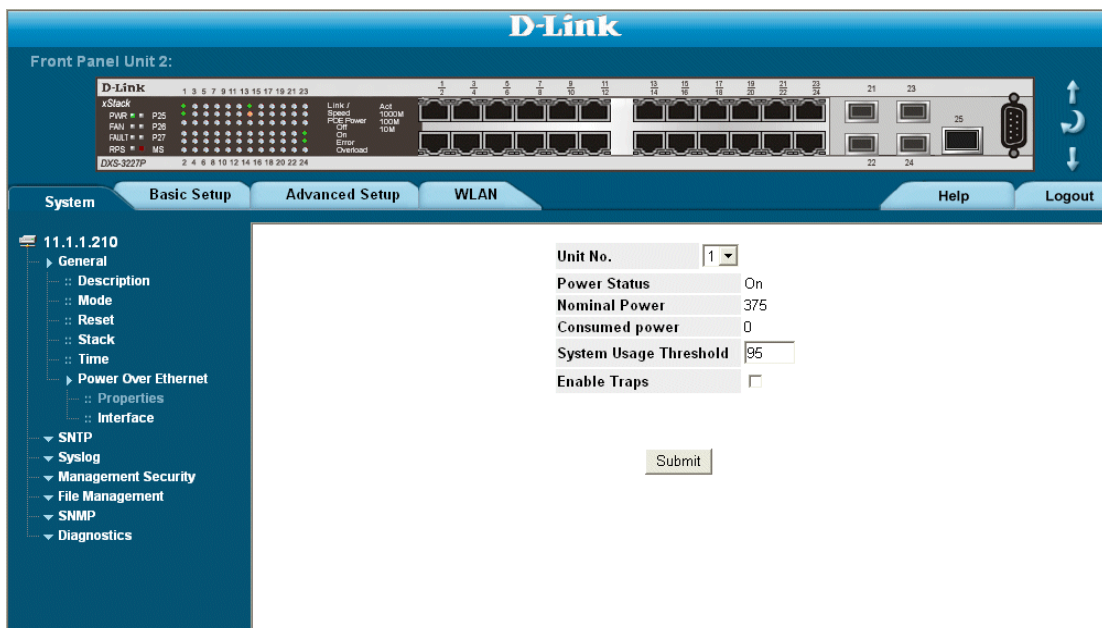
- Defining PoE System Information
- Displaying and Editing PoE System Information

Defining PoE System Information

The *PoE Properties Page* contains system PoE information for enabling PoE on the device, monitoring the current power usage, and enabling PoE traps. To enable PoE on the device:

1. Click the **System > Power over Ethernet > Properties** tab. The *PoE Properties Page* opens:

Figure 30: PoE Properties Page



The *PoE Properties Page* contains the following fields:

- **Unit No.** — Indicates the stacking member for which the POE is configured.
 - **Nominal Power** — Indicates the actual amount of power the device can supply. The field value is displayed in Watts.
 - **Power Status** — Indicates the inline power source status. The possible field values are:
 - *On* — Indicates that the power supply unit is functioning.
 - *Off* — Indicates that the power supply unit is not functioning.
 - *Faulty* — Indicates that the power supply unit is functioning, but an error has occurred. For example, a power overload or a short circuit.
 - **Consumed Power** — Indicates the amount of the power used by the device. The field value is displayed in Watts.
 - **System Usage Threshold** — Indicates the percentage of power consumed before an alarm is generated. The field value is 1-99 percent. The default is 95 percent.
 - **Enable Traps** — Indicate if PoE device traps are enabled. The possible field values are:
 - *Checked* — Enables PoE traps on the device.
 - *Unchecked* — Disables PoE traps on the device. This is the default value.
2. Modify the *Unit No.*, *Power Status*, and *Powered Device* fields.

3. Define the *Unit No.* and the *System Usage Threshold* field.
4. Check the *Traps* checkbox.
5. Click . The system PoE parameters are defined, and the device is updated.

Displaying and Editing PoE System Information

The *PoE Interface Page* displays system PoE information on the device, monitoring the current power usage, and enabling PoE traps. To display system PoE information on the device:

1. Click the **System > Power over Ethernet > Interface** tab. The *PoE Interface Page* opens:

Figure 31: PoE Interface Page

The screenshot shows the D-Link web interface for the PoE Interface Page. The top navigation bar includes 'System', 'Basic Setup', 'Advanced Setup', 'WLAN', 'Help', and 'Logout'. The left sidebar shows a tree view with 'Power Over Ethernet' expanded to 'Interface'. The main content area displays a table of PoE configurations for Unit No. 1.

Port	Admin Status	Oper. Status	Priority Level	Powered Device	Edit
1/1	Enable	Searching	Low		
1/2	Enable	Searching	Low		
1/3	Enable	Searching	Low		
1/4	Enable	Searching	Low		
1/5	Enable	Searching	Low		
1/6	Enable	Searching	Low		
1/7	Enable	Searching	Low		
1/8	Enable	Searching	Low		
1/9	Enable	Searching	Low		
1/10	Enable	Searching	Low		
1/11	Enable	Searching	Low		
1/12	Enable	Searching	Low		
1/13	Enable	Searching	Low		
1/14	Enable	Searching	Low		

The *PoE Interface Page* contains the following fields:

- **Unit No.** — Indicates the stacking member for which the POE is configured.
- **Port** — Indicates the specific interface for which PoE parameters are defined, and assigned to the powered interface connected to the selected port.
- **Admin Status** — Indicates the device PoE mode. The possible field values are:
 - *Auto* — Enables the Device Discovery protocol, and provides power to the device using the PoE module. The Device Discovery Protocol enables the device to discover Powered Devices attached to the device interfaces, and to learn their classification. This is the default settings.
 - *Never* — Disables the *Device Discovery* protocol, and stops the power supply to the device using the PoE module.
- **Operation Status** — Indicates if the port is enabled to work on PoE. The possible field values are:
 - *On* — Indicates the device is delivering power to the interface.
 - *Off* — Indicates the device is not delivering power to the interface.
 - *Test Fail* — Indicates the powered device test has failed. For example, a port could not be enabled and cannot be used to deliver power to the powered device.
 - *Testing* — Indicates the powered device is being tested. For example, a powered device is tested to confirm it is receiving power from the power supply.


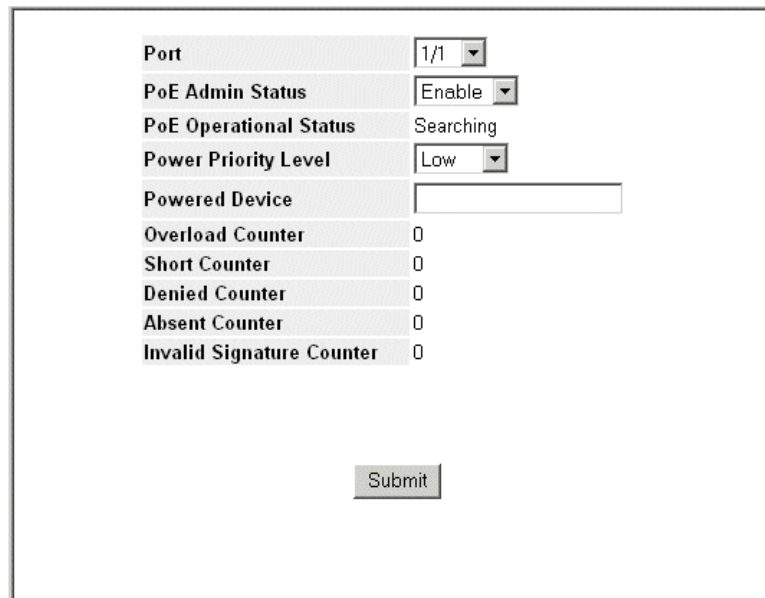
- *Searching* — Indicates that the device is currently searching for a powered device. Searching is the default PoE operational status.
 - *Fault* — Indicates that the device has detected a fault on the powered device. For example, the powered device memory could not be read.
 - **Priority Level** — Determines the port priority if the power supply is low. The port power priority is used if the power supply is low. The field default is low. For example, if the power supply is running at 99% usage, and port 1 is prioritized as high, but port 3 is prioritized as low, port 1 is prioritized to receive power, and port 3 may be denied power. The possible field values are:
 - *Low* — Defines the PoE priority level as low. This is the default level.
 - *High* — Defines the PoE priority level as high.
 - *Critical* — Defines the PoE priority level as Critical. This is the highest PoE priority level.
 - **Powered Device** — Provides a user-defined powered device description. The field can contain up to 24 characters.
2. Click  . The *PoE Interface Edit Page* opens:

Figure 32: PoE Interface Edit Page



Port	1/1
PoE Admin Status	Enable
PoE Operational Status	Searching
Power Priority Level	Low
Powered Device	
Overload Counter	0
Short Counter	0
Denied Counter	0
Absent Counter	0
Invalid Signature Counter	0

In addition to the fields in the *PoE Interface Page*, the *PoE Interface Edit Page* contains the following additional fields:

- **Overload Counter** — Indicates the total power overload occurrences.
- **Short Counter** — Indicates the total power shortage occurrences.
- **Denied Counter** — Indicates times the powered device was denied power.
- **Absent Counter** — Indicates the times the power supply was stopped to the powered device because the powered device was no longer detected.

- **Invalid Signature Counter** — Indicate the times an invalid signature was received. Signatures are the means by which the powered device identifies itself to the PSE. Signatures are generated during powered device detection, classification, or maintenance.
- 3. Modify the *PoE Admin Status*, *Power Priority Level*, and *Powered Device* fields.
- 4. Click . The system PoE parameters are edited, and the device is updated.

Section 7. Managing Stacking

Stacking provides multiple switch management through a single point as if all stack members are a single unit. All stack members are accessed through a single IP address through which the stack is managed. The stack is can be managed from the following:

- Web-based Interface
- SNMP Management Station
- Command Line Interface (CLI)

Devices support stacking up to eight units per stack, or can operate as stand-alone units.

During the Stacking setup, one switch is selected as the Stacking Master and another stacking member can be selected as the Secondary Master. All other devices are selected as stack members, and assigned a unique Unit ID.

Switch software is downloaded separately for each stack members. However, all units in the stack must be running the same software version.

Switch stacking and configuration is maintained by the Stacking Master. The Stacking Master detects and reconfigures the ports with minimal operational impact in the event of:

- Unit Failure
- Inter-unit Stacking Link Failure
- Unit Insertion
- Removing a Stacking Unit

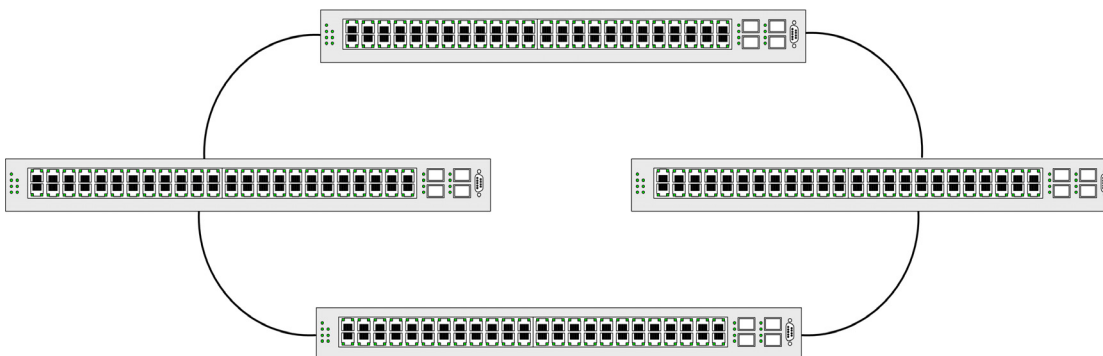
This section provides an introduction to the user interface, and includes the following topics:

- Understanding the Stack Topology
- Stacking Failover Topology
- Exchanging Stacking Members
- Switching the Stacking Master
- Configuring Stacking

Understanding the Stack Topology

The 32XX series Stacked devices operate in a Ring topology. A stacked Ring topology is where all devices in the stack are connected to each other forming a circle. Each stacked device accepts data and sends it to the device to which it is physically connected. The packet continues through the stack until it reaches the destination port. The system automatically discovers the optimal path on which to send traffic.

Figure 33: Stacking Ring Topology



Most difficulties incurred in Ring topologies occur when a device in the ring becomes non-functional, or a link is severed. In a stack, the system automatically switches to a Stacking Failover topology without any system downtime. An SNMP message is automatically generated, but no stack management action is required. However, the stacking link or stacking member must be repaired to ensure the stacking integrity.

After the stacking issues are resolved, the device can be reconnected to the stack without interruption, and the Ring topology is restored.

Stacking Failover Topology

If a failure occurs in the stacking topology, the stack reverts to Stacking Failover Topology. In the Stacking Failover topology, devices operate in a chain formation. The Stacking Master determines where the packets are sent. Each unit is connected to two neighboring devices, except for the top and bottom units.

Stacking Members and Unit ID

Stacking Unit IDs are essential to the stacking configuration. The stacking operation is determined during the boot process. The Operation Mode is determined by the Unit ID selected during the initialization process. For example, if the user selected stand-alone mode, the device boots as a stand-alone device.

The device units are shipped with the default Unit ID of the stand-alone unit. If the device is operating as a stand-alone unit, all stacking LEDs are off. Once the user selects a different Unit ID, the default Unit ID not erased, and remains valid, even if the unit is reset.

Unit ID 1 and Unit ID 2 are reserved for Master enabled units. Unit IDs 3 to 8 can be defined for stack members.

When the Master unit boots or when inserting or removing a stack member, the Master unit initiates a stacking discovering process.



Notes

- If two members are discovered with the same Unit ID the stack continues to function, however only the unit with the older join time joins the stack. A message is sent to the user, notifying that a unit failed to join the stack.

Removing and Replacing Stacking Members

Stacking member 1 and Stacking member 2 are Stacking Master enabled units. Unit 1 and Unit 2 are either designated as Master Unit or Secondary Master Unit. The Stacking Master assignment is performed during the configuration process. One Master enabled stack member is elected Master, and the other Master enabled stack member is elected Secondary Master, according to the following decision process:

- If only one Stacking Master enabled unit is present, it is elected Master.
- If two Stacking Masters enabled stacking members are present, and one has been manually configured as the Stacking Master, the manually configured member is elected Stacking Master.
- If two Master enabled units are present and neither has been manually configured as the Stacking Master, the one with the longer up-time is elected Stacking Master.
- If the two Master enabled stacking members are the same age, Unit 1 is elected Stacking Master.



Notes

- Two stacking member are considered the same age if they were inserted within the same ten minute interval.

For example, Stack member 2 is inserted in the first minute of a ten-minute cycle, and Stack member 1 is inserted in fifth minute of the same cycle, the units are considered the same age. If there are two Master enabled units that are the same age, then Unit 1 is elected master.

The Stacking Master and the Secondary Master maintain a Warm Standby. The Warm Standby ensures that the Secondary Master takes over for the Stacking Master if a failover occurs. This guarantees that the stack continues to operate normally.

During the Warm Standby, the Master and the Secondary Master are synchronized with the static configuration only. When the Stacking Master is configured, the Stacking Master must synchronize the Stacking Secondary Master. The Dynamic configuration is not saved, for example, dynamically learned MAC addresses are not saved.

Each port in the stack has a specific Unit ID, port type, and port number, which is part of both the configuration commands and the configuration files. Configuration files are managed only from the device Stacking Master, including:

- Saving to the FLASH
- Uploading Configuration files to an external TFTP Server
- Downloading Configuration files from an external TFTP Server

Whenever a reboot occurs, topology discovery is performed, and the master learns all units in the stack. Unit IDs are saved in the unit and are learned through topology discovery. If a unit attempts to boot without a selected Master, and the unit is not operating in stand-alone mode, the unit does not boot.

Configuration files are changed only through explicit user configuration. Configuration files are not automatically modified when:

- Units are Added
- Units are Removed
- Units are reassigned Unit IDs

- Units toggle between Stacking Mode and Stand-alone Mode

Each time the system reboots, the Startup Configuration file in the Master unit is used to configure the stack. If a stack member is removed from the stack, and then replaced with a unit with the same Unit ID, the stack member is configured with the original device configuration. Only ports which are physically present are displayed in the D-Link Web Management Interface home page, and can be configured through the web management system. Non-present ports are configured through the CLI or SNMP interfaces.

Exchanging Stacking Members

If a stack member with the same Unit ID replaces an existing Unit ID with the same Unit ID, the previous device configuration is applied to the inserted stack member. If the new inserted device has either more than or less ports than the previous device, the relevant port configuration is applied to the new stack member. For example:

Switching the Stacking Master

The Secondary Master replaces the Stacking Master if the following events occur:

- The Stacking Master fails or is removed from the stack.
- Links from the Stacking Master to the stacking members fails.
- A soft switchover is performed with either via web interface or the CLI.

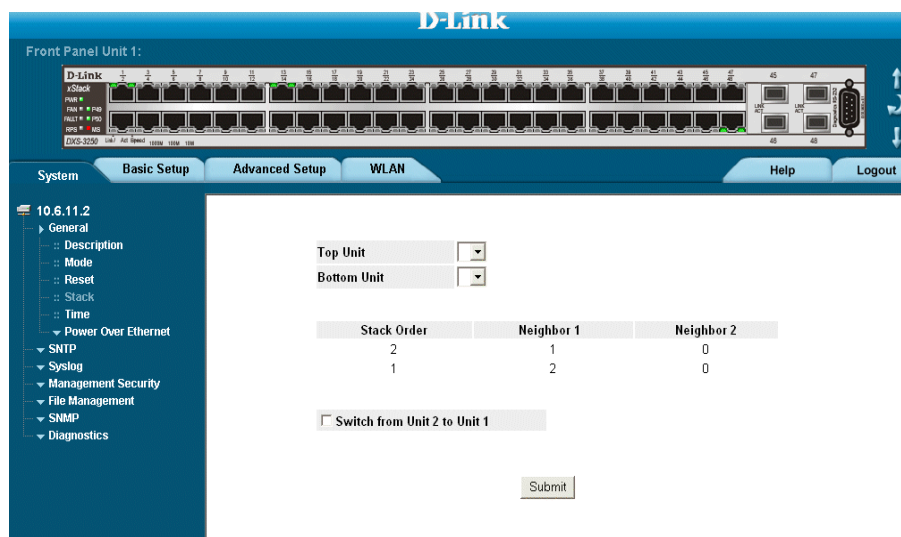
Switching between the Stacking Master and the Secondary Master results in a limited service loss. Any dynamic tables are relearned if a failure occurs. The running configuration file is synchronized between Stacking Master and the Secondary Master, and continues running on the Secondary Master.

Configuring Stacking

The *Stack Page* allows network managers to either reset the entire stack or a specific device. Device configuration changes that are not saved before the device is reset are not saved. If the Stacking Master is reset, the entire stack is reset. To open the *Stack Page*:

- Click **System > General** tab. The *Stack Page* opens.

Figure 34: Stack Page



The *Stack Page* contains the following fields:

- **Top Unit**— Indicates the top most stacking member's number. Possible values are Master and 1-8.
- **Bottom Unit** — Indicates the lower most stacking member's number. Possible values are Master and 1-8.
- **Stack Order** — Displays the stacking unit order based on the Unit IDs.
- **Neighbor 1** — Displays the selected stacking unit's neighbor.
- **Neighbor 2** — Displays the selected stacking unit's neighbor.
- **Switch Stack Control from Unit 2 to Unit 1** — Changes the stack control from the Backup Master to the Stack Master. The possible field values are:
 - *Checked* — Enables switching the stack control to the Stack Master.
 - *Unchecked* — Maintains the current stacking control.

Switching Between Stack Masters:

1. Open the *Stack Page*.
2. Check the *Switch Stack Control from Unit 1 to Unit 2* check box.
3. Click **Submit**. A confirmation message displays.

This page is left blank intentionally.

Section 8. Configuring Device Security

This section provides access to security pages that contain fields for setting security parameters for ports, device management methods, users, and server security. This section contains the following topics:

- Configuring Management Security
- Configuring Network Security

Configuring Management Security

This section provides information for configuring device management security. This section includes the following topics:

- Configuring Authentication Methods
- Configuring Passwords

Configuring Authentication Methods

This section provides information for configuring device authentication methods. This section includes the topics:

- Defining Access Profiles
- Defining Profile Rules
- Defining Authentication Profiles
- Mapping Authentication Methods
- Defining RADIUS Settings

Defining Access Profiles

Access profiles are profiles and rules for accessing the device. Access to management functions can be limited to user groups. User groups are defined for interfaces according to IP addresses or IP subnets. Access profiles contain management methods for accessing and managing the device. The device management methods include:

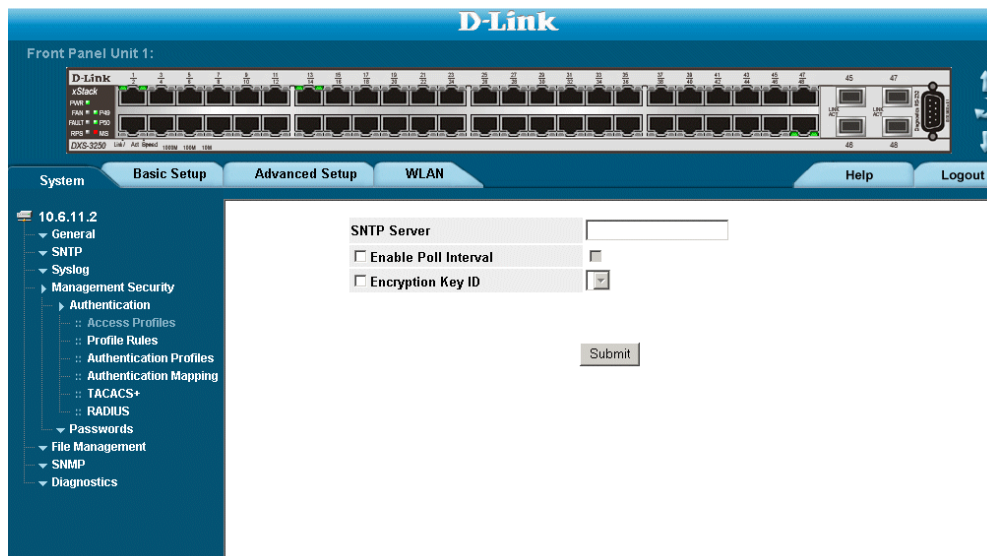
- All
- Telnet
- Secure Telnet (SSH)
- HTTP
- Secure HTTP (HTTPS)
- SNMP

Management access to different management methods may differ between user groups. For example, User Group 1 can access the switch module only via an HTTPS session, while User Group 2 can access the switch module via both HTTPS and Telnet sessions. The *Access Profile Page* contains the currently configured access profiles and their activity status.

Assigning an access profile to an interface denies access via other interfaces. If an access profile is assigned to any interface, the device can be accessed by all interfaces. To configure access profiles:

1. Click **System > Management Security > Authentication > Access Profiles**. The *Access Profile Page* opens.

Figure 35: Access Profile Page



The *Access Profile Page* contains the following fields:

- **Access Profile Name** — Defines the access profile name. The access profile name can contain up to 32 characters.
- **Current Active Active Profile** — Defines the access profile currently active.
- **Remove** — Removes the selected access profile. The possible field values are:
 - *Checked* — Removes the selected access profile. Access Profiles cannot be removed when Active.

- *Unchecked* — Maintains the access profiles.
2. Click . The *Add Access Profile Page* opens:

Figure 36: Add Access Profile Page

The screenshot shows the 'Add Access Profile' page with the following fields and options:

- Access Profile Name:** Text input field.
- Rule Priority:** Text input field.
- Management Method:** Dropdown menu with 'All' selected.
- Interface:** Checkbox.
- Source IP Address:** Checkbox.
- Action:** Dropdown menu with 'Permit' selected.
- Port:** Radio button and dropdown menu.
- LAG:** Radio button and dropdown menu.
- VLAN:** Radio button and dropdown menu.
- Network Mask:** Radio button and text input field.
- Prefix Length:** Radio button and text input field.

A 'Submit' button is located at the bottom center of the form.

In addition to the fields in the *Access Profile Page*, the *Add Access Profile Page* contains the following fields:

- **Access Profile Name** — Defines the access profile name. The access profile name can contain up to 32 characters.
- **Rule Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis. The rule priorities are assigned in the *Profile Rules Page*.
- **Management Method** — Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
 - *All* — Assigns all management methods to the rule.
 - *Telnet* — Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
 - *Secure Telnet (SSH)* — Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
 - *HTTP* — Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
 - *Secure HTTP (HTTPS)* — Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
 - *SNMP* — Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.
- **Interface** — Defines the interface on which the access profile is defined. The possible field values are:
 - *Port* — Specifies the port on which the access profile is defined.
 - *LAG* — Specifies the LAG on which the access profile is defined.
 - *VLAN* — Specifies the VLAN on which the access profile is defined.

- **Source IP Address** — Defines the interface source IP address to which the access profile applies. The *Source IP Address* field is valid for a subnetwork.
3. Define the *Access Profile Name*, *Rule Priority*, *Management Method*, *Interface*, *Source IP Address*, *Network Mask* or *Prefix Length*, and *Action* fields.
 4. Click . The access profile is created, and the device is updated.

Defining Profile Rules

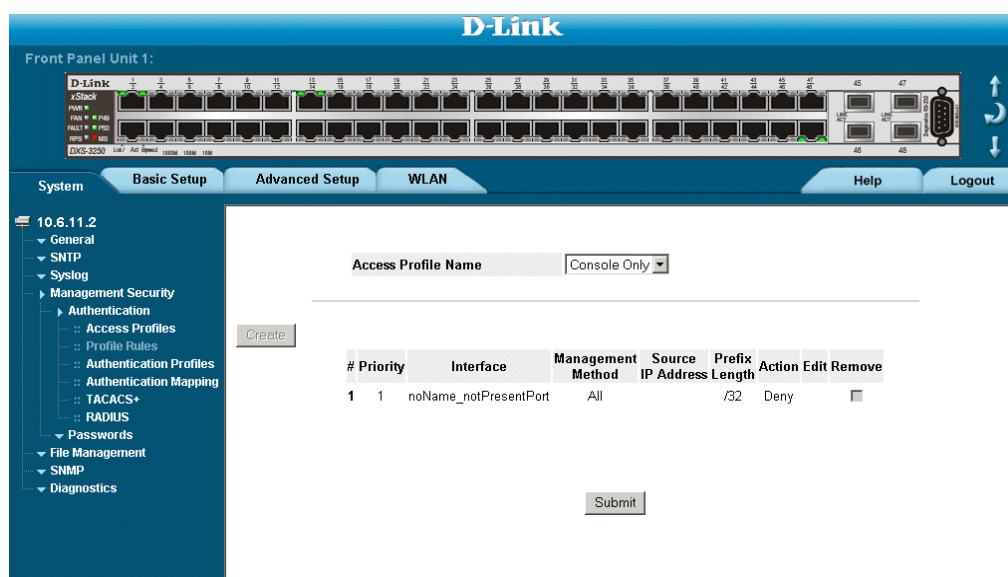
Access profiles can contain up to 128 rules that determine which users can manage the switch module, and by which methods. Users can also be blocked from accessing the device. Rules are composed of filters including:

- Rule Priority
- Interface
- Management Method
- Source IP Address
- Prefix Length
- Forwarding Action

The rule order is essential as packets are matched on a first-fit basis. To define profile rules:

1. Click **System > Management Security > Authentication > Profile Rules**. The *Profile Rules Page* opens.

Figure 37: Profile Rules Page



The *Profile Rules Page* contains the following fields:

- **Access Profile Name** — Displays the access profile to which the rule is attached.
- **Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis.
- **Interface** — Indicates the interface type to which the rule applies. The possible field values are:
 - *Port* — Attaches the rule to the selected port.
 - *LAG* — Attaches the rule to the selected LAG.
 - *VLAN* — Attaches the rule to the selected VLAN.
- **Management Method** — Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
 - *All* — Assigns all management methods to the rule.

- *Telnet* — Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
 - *Secure Telnet (SSH)* — Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
 - *HTTP* — Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
 - *Secure HTTP (HTTPS)* — Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
 - *SNMP* — Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.
 - **Source IP Address** — Defines the interface source IP address to which the rule applies.
 - **Prefix Length** — Defines the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
 - **Action** — Defines the action attached to the rule. The possible field values are:
 - *Permit* — Permits access to the device.
 - *Deny* — Denies access to the device. This is the default.
 - **Remove** — Removes rules from the selected access profiles. The possible field values are:
 - *Checked* — Removes the selected rule from the access profile.
 - *Unchecked* — Maintains the rules attached to the access profile.
2. Click **Create**. The *Add Profile Rule Page* opens:



Figure 38: Add Profile Rule Page

The screenshot shows the 'Add Profile Rule' configuration page. The form includes the following fields and options:

- Access Profile Name:** A text input field.
- Priority:** A text input field.
- Management Method:** A dropdown menu currently set to 'All'.
- Interface:** A checkbox.
- Port, LAG, VLAN:** Radio buttons for selecting the management interface.
- Source IP Address:** A text input field.
- Network Mask, Prefix Length:** Radio buttons and a text input field for specifying IP address criteria.
- Action:** A dropdown menu currently set to 'Permit'.
- Submit:** A button at the bottom right of the form.

3. Define the *Access Profile Name*, *Priority*, *Management Method*, *Interface*, *Source IP Address*, *Network Mask* or *Prefix Length*, and *Action* fields.
4. Click **Submit**. The profile rule is added to the access profile, and the device is updated.

To modify a Profile Rule:

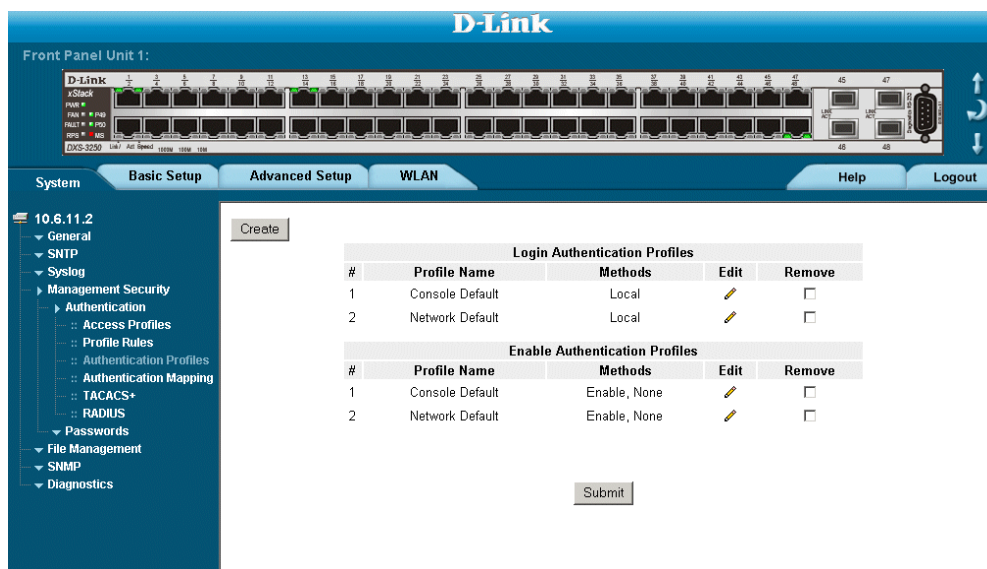
1. Click **System > Management Security > Authentication > Profile Rules**. The *Access Profile Page* opens
2. Click . The *Profile Rules Setting Page* opens:
3. Modify the fields.
4. Click . The profile rule is modified, and the device is updated.

Defining Authentication Profiles

Authentication profiles allow network administrators to assign authentication methods for user authentication. User authentication can be performed either locally or on an external server. User authentication occurs in the order the methods are selected. If the first authentication method is not available, the next selected method is used. For example, if the selected authentication methods are RADIUS and Local, and the RADIUS server is not available, then the user is authenticated locally. To define Authentication profiles:

1. Click **System > Management Security > Authentication > Authentication Profiles**. The *Authentication Profile Page* opens.

Figure 39: Authentication Profile Page



The *Authentication Profile Page* contains the following fields:

- **Profile Name** — Contains a list of user-defined authentication profile lists to which user-defined authentication profiles are added.
- **Methods** — Defines the user authentication methods. The possible field values are:
 - *None* — Assigns no authentication method to the authentication profile.
 - *Local* — Authenticates the user at the device level. The device checks the user name and password for authentication.
 - *RADIUS* — Authenticates the user at the RADIUS server. For more information, see “Defining RADIUS Settings.”
 - *Line* — Authenticates the user using a line password.
 - *Enable* — Authenticates the user using an enable password.
 - *TACACS+* — Authenticates the user at the TACACS+
- **Remove** — Removes the selected authentication profile. The possible field values are:
 - *Checked* — Removes the selected authentication profile.
 - *Unchecked* — Maintains the authentication profiles.

2. Click **Create**. The *Add Authentication Profile Page* opens.

Figure 40: Add Authentication Profile Page

Add Authentication Profile

Profile Method Login Enable

Profile Name

Authentication Method

Optional Methods		Selected Methods
Local	←	
None		
RADIUS	→	
Line		

3. Define the *Profile Method*, *Profile Name* and *Authentication Methods* fields.
4. Click **Submit**. The authentication profile is defined, and the device is updated.

To modify an authentication profile:


1. Click **System > Management Security > Authentication > Authentication Profiles**. The *Authentication Profile Page* opens.

Authentication Profile Settings

Profile Name

Authentication Method

Optional Methods		Selected Methods
Line	←	Local
Enable		
RADIUS	→	
TACACS+		

2. Click . The *Authentication Profile Settings Page* opens:
3. Select an authentication method from the *Optional Methods* list.
4. Click **Submit**. The authentication method is selected, and the device is updated.

Mapping Authentication Methods

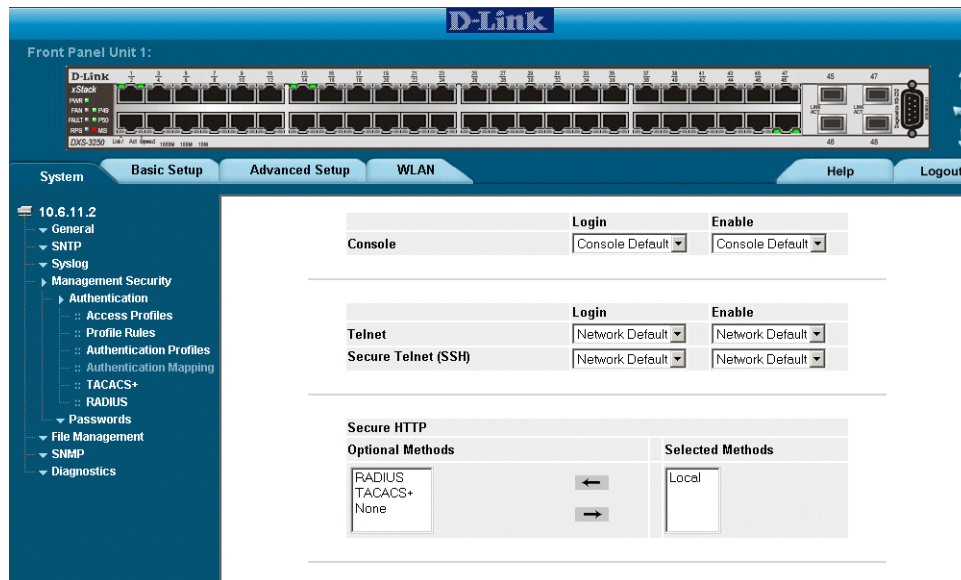
After authentication profiles are defined, they can be applied to management access methods. For example, console users can be authenticated by Authentication Profile List 1, while Telnet users are authenticated by Authentication Method List 2.

Authentication methods are selected using arrows. The order in which the methods are selected is the order by which the authentication methods are used.

To map authentication methods:

1. Click **System > Management Security > Authentication > Authentication Mapping**. The *Authentication Mapping Page* opens.

Figure 41: Authentication Mapping Page



The *Authentication Mapping Page* contains the following fields:

- **Console** — Indicates that Authentication profiles are used to authenticate console users.
- **Telnet** — Indicates that Authentication profiles are used to authenticate Telnet users.
- **Secure Telnet (SSH)** — Indicates that Authentication profiles are used to authenticate Secure Shell (SSH) users. SSH provides clients secure and encrypted remote connections to a device.
- **Secure HTTP** — Indicates that Authentication methods used for Secure HTTP access. Possible field values are:

- *None* — Indicates that no authentication method is used for access.
 - *RADIUS* — Indicates that authentication occurs at the RADIUS server.
 - *TACACS+* — Indicates that authentication occurs at the TACACS+
 - *Local* — Indicates that authentication occurs locally.
 - **HTTP** — Indicates that Authentication methods are used for HTTP access. Possible field values are:
 - *None* — Indicates that no authentication method is used for access.
 - *RADIUS* — Indicates that Authentication occurs at the RADIUS server.
 - *TACACS+* — Indicates that authentication occurs at the TACACS+
 - *Local* — Indicates that authentication occurs locally.
1. Define the *Console*, *Telnet*, and *Secure Telnet (SSH)* fields.
 2. Map the authentication method in the *Secure HTTP* selection box.
 3. Map the authentication method in the *HTTP* selection box.
 4. Click . The authentication mapping is saved, and the device is updated.

Defining RADIUS Settings

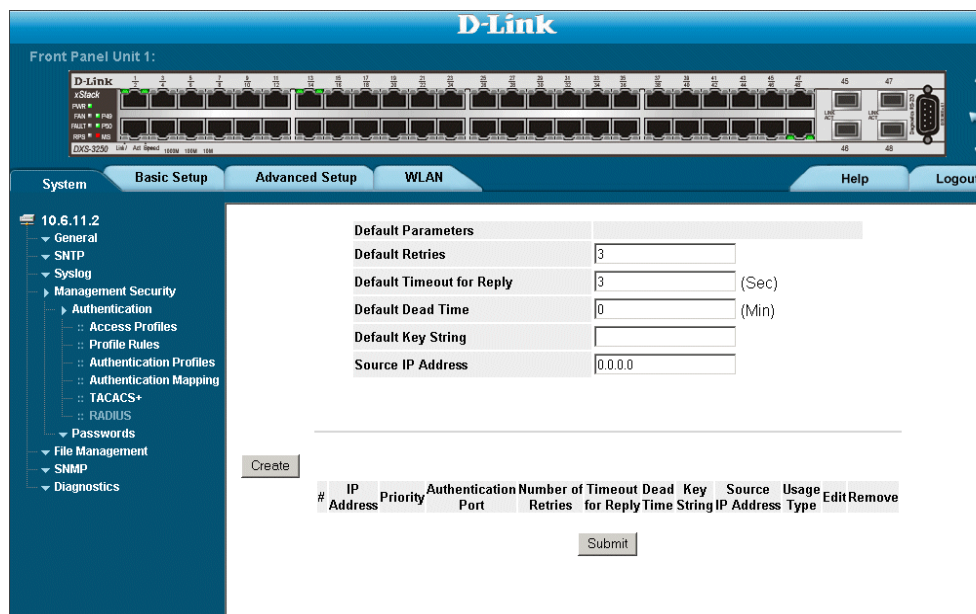
Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. RADIUS servers provide a centralized authentication method for web access.

The default parameters are user-defined, and are applied to newly defined RADIUS servers. If new default parameters are not defined, the system default values are applied to newly defined RADIUS servers.

To configure RADIUS servers:

1. Click **System > Management Security > Authentication > RADIUS**. The *RADIUS Page* opens:

Figure 42: RADIUS Page



The *RADIUS Page* contains the following fields:

- **Retries** — Defines the number of transmitted requests sent to the RADIUS server before a failure occurs. Possible field values are 1-10. The default value is 3.
- **Timeout for Reply** — Defines the amount of time (in seconds) the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. Possible field values are 1-30. The default value is 3.
- **Dead Time** — Defines the default amount of time (in minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. The default value is 0.
- **Key String** — Defines the default key string used for authenticating and encrypting all RADIUS-communications between the device and the RADIUS server. This key must match the RADIUS encryption.
- **Source IP Address** — Defines the default IP address of a device accessing the RADIUS server.

The *RADIUS Page* also contains the following fields:

- **IP Address** — Lists the RADIUS server IP addresses.
- **Priority** — Displays the RADIUS server priority. The possible values are 1-65535, where 1 is the highest value. The RADIUS server priority is used to configure the server query order.

- **Authentication Port** — Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812.
 - **Number of Retries** — Defines the number of transmitted requests sent to the RADIUS server before a failure occurs. The possible field values are 1-10. Three is the default value.
 - **Timeout for Reply** — Defines the amount of time (in seconds) the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. The possible field values are 1-30. Three is the default value.
 - **Dead Time** — Defines the amount of time (in minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. The default is 0 minutes.
 - **Key String** — Defines the default key string used for authenticating and encrypting all RADIUS-communications between the device and the RADIUS server. This key must match the RADIUS encryption.
 - **Source IP Address** — Defines the source IP address that is used for communication with RADIUS servers.
 - **Usage Type** — Specifies the RADIUS server authentication type. The default value is *All*. The possible field values are:
 - *Log in* — Indicates the RADIUS server is used for authenticating user name and passwords.
 - *802.1X* — Indicates the RADIUS server is used for 802.1X authentication.
 - *All* — Indicates the RADIUS server is used for authenticating user names and passwords, and 802.1X port authentication.
 - **Remove**— Removes a RADIUS server. The possible field values are:
 - *Checked* — Removes the selected RADIUS server.
 - *Unchecked* — Maintains the RADIUS servers.
2. Click **Create**. The *Add Radius Server Page* opens:

Figure 43: Add Radius Server Page

Add RADIUS Server

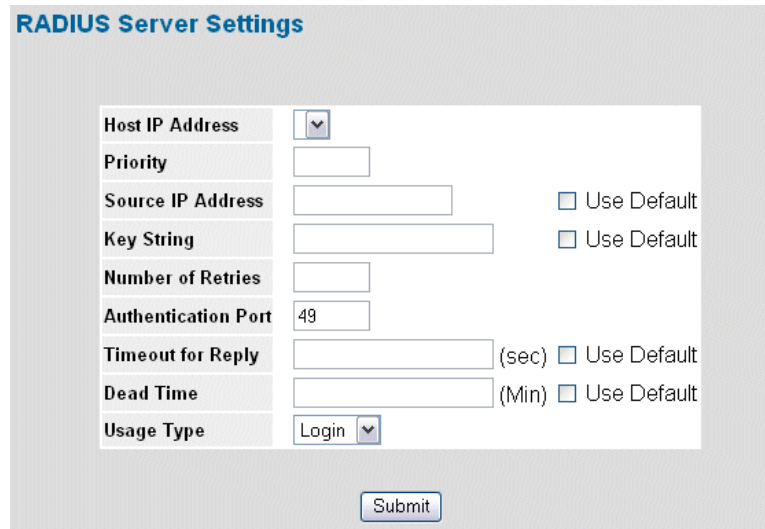
Host IP Address	<input type="text"/>	
Priority	<input type="text" value="0"/>	
Authentication Port	<input type="text" value="1812"/>	
Number of Retries	<input type="text" value="Default"/>	<input checked="" type="checkbox"/> Use Default
Timeout for Reply	<input type="text" value="Default"/> (Sec)	<input checked="" type="checkbox"/> Use Default
Dead Time	<input type="text" value="Default"/> (Min)	<input checked="" type="checkbox"/> Use Default
Key String	<input type="text"/> (Alpha Numeric)	<input type="checkbox"/> Use Default
Source IP Address	<input type="text" value="Default"/>	<input checked="" type="checkbox"/> Use Default
Usage Type	<input type="text" value="All"/>	

3. Define the fields.
4. Click **Submit**. The RADIUS server is added, and the device is updated.

To edit RADIUS Server Settings:

1. Click **System > Management Security > Authentication > RADIUS**. The *RADIUS Page* opens.
2. Click . The *RADIUS Server Settings Page* opens:

Figure 44: RADIUS Server Settings Page



RADIUS Server Settings	
Host IP Address	<input type="text"/>
Priority	<input type="text"/>
Source IP Address	<input type="text"/> <input type="checkbox"/> Use Default
Key String	<input type="text"/> <input type="checkbox"/> Use Default
Number of Retries	<input type="text"/>
Authentication Port	49
Timeout for Reply	<input type="text"/> (sec) <input type="checkbox"/> Use Default
Dead Time	<input type="text"/> (Min) <input type="checkbox"/> Use Default
Usage Type	Login <input type="text"/>

3. Define the *Host IP Address*, *Priority*, *Source IP Address*, *Key String*, *Number of Retries*, *Authentication Port*, *Timeout for Reply*, *Dead Time*, and *Usage Type* fields.
4. Click . The RADIUS server settings are saved, and the device is updated.

Defining TACACS+ Authentication

Terminal Access Controller Access Control System (TACACS+) provides centralized security user access validation. The system supports up-to 4 TACACS+ servers.

TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes. TACACS+ provides the following services:

- **Authentication** — Provides authentication during login and via user names and user-defined passwords.
- **Authorization** — Performed at login. Once the authentication session is completed, an authorization session starts using the authenticated user name.

The TACACS+ protocol ensures network integrity through encrypted protocol exchanges between the client and TACACS+ server.

The TACACS+ default parameters are user-assigned defaults. The default settings are applied to newly defined TACACS+ servers. If default values are not defined, the system defaults are applied to the new TACACS+ new servers.

To define TACACS+ authentication settings:

1. Click **System > Management Security > Authentication > TACACS+**. The *TACACS+ Page* opens.

Figure 45: TACACS+ Page

The screenshot shows the D-Link web interface for configuring TACACS+ authentication. The left sidebar contains a navigation tree with 'Management Security' expanded to 'Authentication' and 'TACACS+'. The main content area is titled 'Default Parameters' and contains three input fields: 'Source IP Address' (0.0.0.0), 'Key String' (empty), and 'Timeout for Reply' (5 Sec). Below these fields is a 'Create' button and a table with columns: '#', 'Host IP Address', 'Priority', 'Source IP Address', 'Authentication Port', 'Timeout for Reply', 'Single Connection', 'Status', 'Edit', and 'Remove'. A 'Submit' button is located below the table.

The **Default Parameters** section contains the following fields:

- **Source IP Address** — Defines the default device source IP address used for the TACACS+ session between the device and the TACACS+ server.
- **Key String** — Defines the default authentication and encryption key for TACACS+ communication between the device and the TACACS+ server.
- **Timeout for Reply** — Defines the default time that passes before the connection between the device and the TACACS+ times out. The default is 5.

The TACACS+ Page also contains the following fields:

- **Host IP Address** — Defines the TACACS+ Server IP address.
- **Priority** — Defines the order in which the TACACS+ servers are used. The field range is 0-65535. The default is 0.
- **Source IP Address** — Defines the device source IP address used for the TACACS+ session between the device and the TACACS+ server.
- **Authentication Port (0-65535)** — Defines the port number via which the TACACS+ session occurs. The default port is port 49.
- **Timeout for Reply**— Defines the amount of time in seconds that passes before the connection between the device and the TACACS+ times out. The field range is 1-1000 seconds.
- **Single Connection** — Maintains a single open connection between the device and the TACACS+ server. The possible field values are:
 - *Checked* — Enables a single connection.
 - *Unchecked* — Disables a single connection.
- **Status** — Indicates the connection status between the device and the TACACS+ server. The possible field values are:
 - *Connected* — Indicates there is currently a connection between the device and the TACACS+ server.
 - *Not Connected* — Indicates there is not currently a connection between the device and the TACACS+ server.
- **Remove** — Removes TACACS+ server. The possible field values are:
 - *Checked* — Removes the selected TACACS+ server.
 - *Unchecked* — Maintains the TACACS+ servers.

2. Click **Create**. The TACACS+ Page opens.

Figure 46: Add TACACS+ Host Page

Add TACACS Host

Host IP Address

Priority

Source IP Address Use Default

Key String Use Default

Authentication Port

Timeout for Reply (sec) Use Default

Single Connection

3. Define the *Host IP Address*, *Priority*, *Source IP Address*, *Key String*, *Authentication Port*, *Timeout for Reply*, and *Single Connection*.

4. Click **Submit**. The TACACS+ server is defined, and the device is updated.

To edit a TACACS+ server settings:


1. Click **System > Management Security > Authentication > TACACS+**. The *TACACS+ Page* opens.
2. Select TACACS+ server entry.
3. Click . The *Add TACACS+ Host Page* opens.

Figure 47: TACACS+ Host Settings Page

TACACS Host Settings

Host IP Address	<input type="text" value="10.6.41.108"/>	
Priority	<input type="text" value="5"/>	
Source IP Address	<input type="text" value="Default"/>	<input checked="" type="checkbox"/> Use Default
Key String	<input type="text" value="Default"/>	<input checked="" type="checkbox"/> Use Default
Authentication Port	<input type="text" value="49"/>	
Timeout for Reply	<input type="text" value="Default"/> (sec)	<input checked="" type="checkbox"/> Use Default
Status	Not Connected	
Single Connection	<input checked="" type="checkbox"/>	

4. Define the fields.
5. Click . The TACACS+ host settings are saved, and the device is updated.

Configuring Passwords

This section contains information for defining device passwords, and includes the following topics.

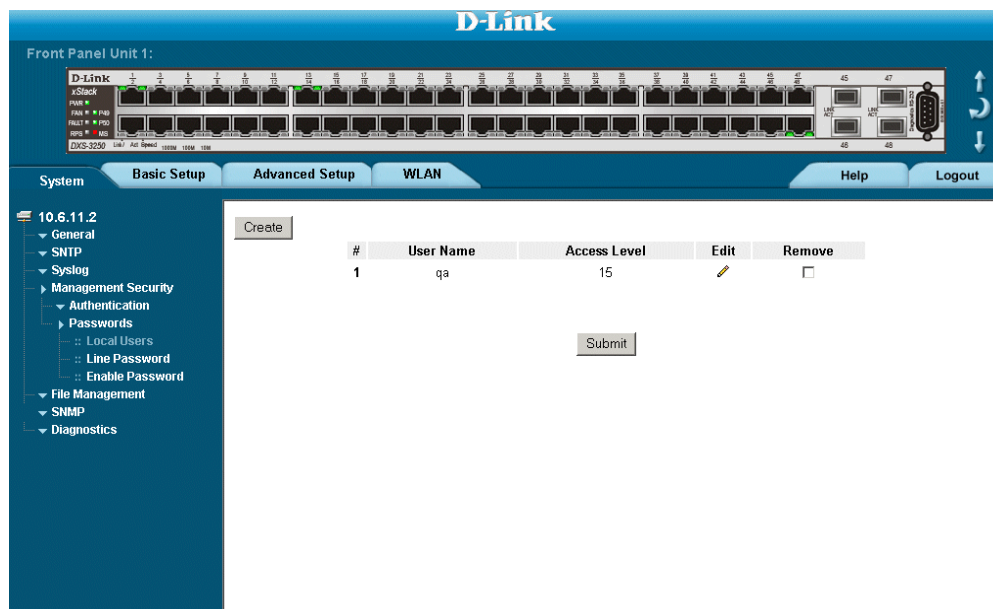
- Defining Local Users
- Defining Line Passwords
- Defining Enable Passwords

Defining Local Users

Network administrators can define users, passwords, and access levels for users using the *Local User Page*. To define local users:

1. Click **System > Management Security > Passwords > Local Users**. The *Local User Page* opens:

Figure 48: Local User Page




The *Local User Page* contains the following fields:

- **User Name** — Displays the user name.
- **Access Level** — Displays the user access level. The lowest user access level is 1 and the highest is 15. Users with access level 15 are Privileged Users.
- **Remove** — Removes the user from the *User Name* list. The possible field values are:
 - *Checked* — Removes the selected local user.
 - *Unchecked* — Maintains the local users.

2. Click **Create**. The *Add Local User Page* opens:

Figure 49: Add Local User Page



In addition to the fields in the *Local User Page*, the *Add Local User Page* contains the following fields:

- **User Name** — Defines the user name.
- **Access Level** — Define the user access level. The lowest user access level is 1 and the highest is 15. Users with access level 15 are Privileged Users.
- **Password** — Defines the local user password. Local user passwords can contain up to 159 characters.
- **Confirm Password** — Verifies the password.

To edit the settings for a local user:


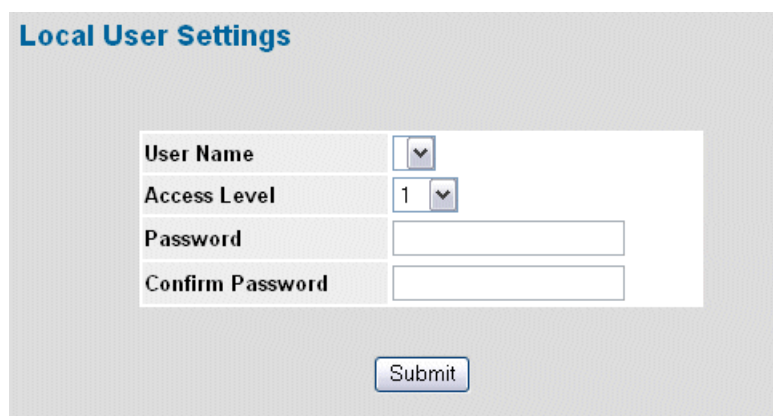

1. Click **System > Management Security > Passwords > Local Users**. The *Local User Page* opens.
2. Click  . The *Local User Settings Page* opens:

Figure 50: Local User Settings Page



3. Define the *User Name*, *Access Level*, *Password*, and *Confirm Password* fields.
4. Click  . The local user passwords settings are saved, and the device is updated.

Defining Line Passwords

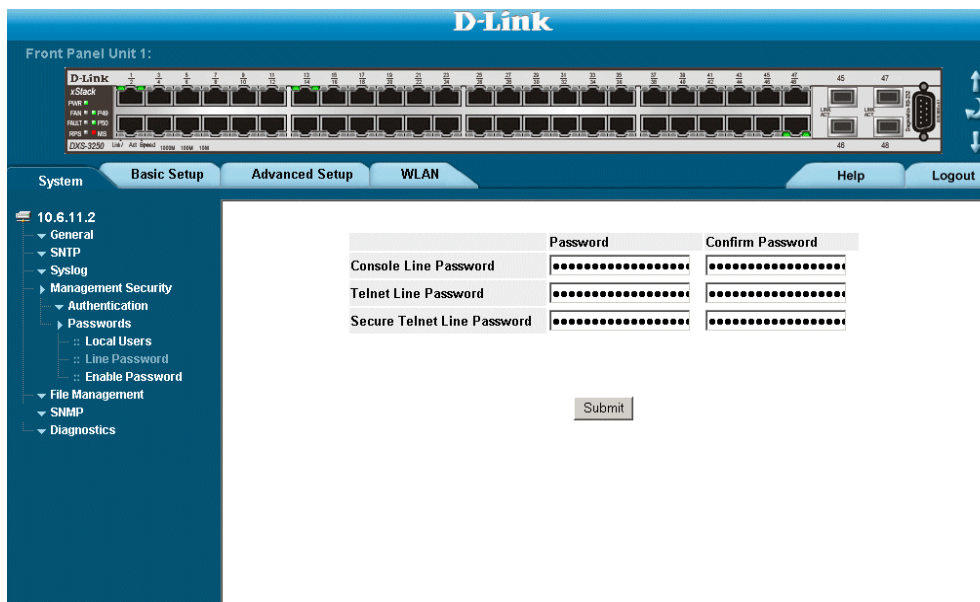
Network administrators can define line passwords in the *Line Password Page*. After the line password is defined, a management method is assigned to the password. The device can be accessed using the following methods:

- Console Passwords
- Telnet Line Passwords
- Secure Telnet Line Passwords

To define line passwords:

1. Click **System > Management Security > Passwords > Line Password**. The *Line Password Page* opens:

Figure 51: Line Password Page



The *Line Password Page* contains the following fields:

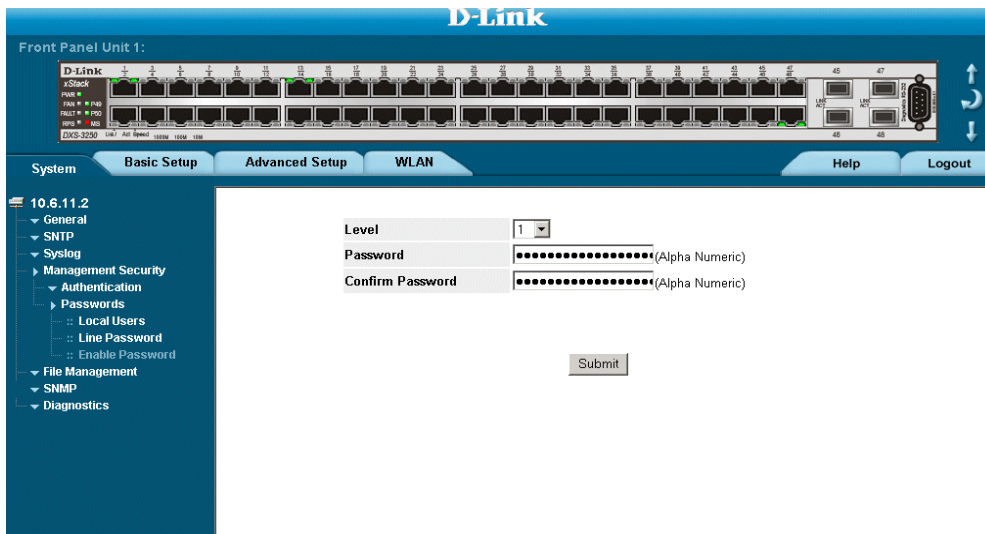
- **Console Line Password** — Defines the line password for accessing the device via a Console session. Passwords can contain a maximum of 159 characters.
 - **Telnet Line Password** — Defines the line password for accessing the device via a Telnet session. Passwords can contain a maximum of 159 characters.
 - **Secure Telnet Line Password** — Defines the line password for accessing the device via a secure Telnet session. Passwords can contain a maximum of 159 characters.
2. Define the *Console Line Password*, *Telnet Line Password*, and *Secure Telnet Line Password* fields.
 3. Redefine the *Confirm Password* field for each of the passwords defined in the previous steps to verify the passwords.
 4. Click **Submit**. The line passwords are saved, and the device is updated.

Defining Enable Passwords

The *Enable Password Page* sets a local password for a particular access level. To enable passwords:

1. Click **System > Management Security > Passwords > Enable Password**. The *Enable Password Page* opens:

Figure 52: Enable Password Page



The *Enable Password Page* contains the following fields:

- **Level** — Defines the access level associated with the enable password. Possible field values are 1-15.
 - **Password** — Defines the enable password.
 - **Confirm Password** — Confirms the new enable password. The password appears in the * * * * * format.
2. Define the *Select Enable Access Level*, *Password*, and *Confirm Password* fields.
 3. Click **Submit**. The enable password is defined, and the device is updated.

Configuring Network Security

Network security manages both access control lists and locked ports. This section contains the following topics:

- Network Security Overview
- Defining Network Authentication Properties
- Defining Port Authentication
- Configuring Traffic Control

Network Security Overview

This section provides an overview of network security and contains the following topics:

- Port-Based Authentication
- Advanced Port-Based Authentication

Port-Based Authentication

Port-based authentication authenticates users on a per-port basis via an external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the RADIUS server using the *Extensible Authentication Protocol* (EAP). Port-based authentication includes:

- **Authenticators** — Specifies the device port which is authenticated before permitting system access.
- **Supplicants** — Specifies the host connected to the authenticated port requesting to access the system services.
- **Authentication Server** — Specifies the server that performs the authentication on behalf of the authenticator, and indicates whether the supplicant is authorized to access system services.

Port-based authentication creates two access states:

- **Controlled Access** — Permits communication between the supplicant and the system, if the supplicant is authorized.
- **Uncontrolled Access** — Permits uncontrolled communication regardless of the port state.

The device currently supports port-based authentication via RADIUS servers.

Advanced Port-Based Authentication

Advanced port-based authentication enables multiple hosts to be attached to a single port. Advanced port-based authentication requires only one host to be authorized for all hosts to have system access. If the port is unauthorized, all attached hosts are denied access to the network.

Advanced port-based authentication also enables user-based authentication. Specific VLANs in the device are always available, even if specific ports attached to the VLAN are unauthorized. For example, Voice over IP does not require authentication, while data traffic requires authentication. VLANs for which authorization is not required can be defined. Unauthenticated VLANs are available to users, even if the ports attached to the VLAN are defined as authorized.

Advanced port-based authentication is implemented in the following modes:

- **Single Host Mode** — Allows port access only to the authorized host.
- **Multiple Host Mode** — Multiple hosts can be attached to a single port. Only one host must be authorized for all hosts to access the network. If the host authentication fails, or an EAPOL-logoff message is received, all attached clients are denied access to the network.
- **Guest VLANs** — Provides limited network access to authorized ports. If a port is denied network access via port-based authorization, but the Guest VLAN is enabled, the port receives limited network access. For exam-

ple, a network administrator can use Guest VLANs to deny network access via port-based authentication, but grant Internet access to unauthorized users.

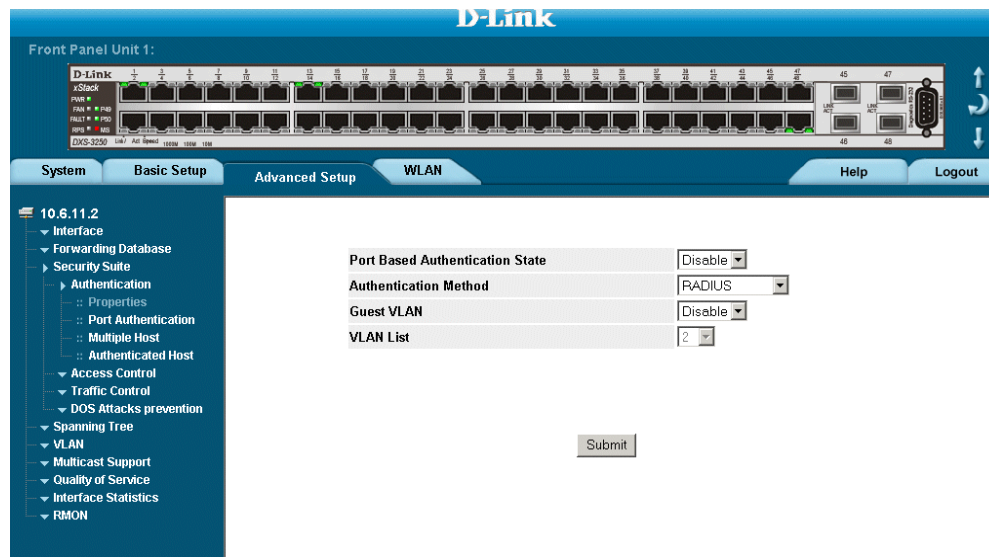
- **Unauthenticated VLANs** — Are available to users, even if the ports attached to the VLAN are defined as unauthorized.

Defining Network Authentication Properties

The *Network Authentication Properties Page* allows network managers to configure network authentication parameters. In addition, Guest VLANs are enabled from the *Network Authentication Properties Page*. To define the network authentication properties:


1. Click **Advanced Setup > Security Suite > Authentication > Properties**. The *Network Authentication Properties Page* opens.

Figure 53: Network Authentication Properties Page



The *Network Authentication Properties Page* contains the following fields:

- **Port-based Authentication State** — Indicates if Port Authentication is enabled on the device. The possible field values are:
 - *Enable* — Enables port-based authentication on the device.
 - *Disable* — Disables port-based authentication on the device.
- **Authentication Method** — Specifies the authentication method used for port authentication. The possible field values are:
 - *RADIUS, None* — Provides port authentication, first using the RADIUS server. If the port is not authenticated, then no authentication method is used, and the session is permitted.
 - *RADIUS* — Provides port authentication using the RADIUS server.
 - *None* — Indicates that no authentication method is used to authenticate the port.
- **Guest VLAN** — Specifies whether the Guest VLAN is enabled on the device. The possible field values are:
 - *Enable* — Enables using a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in the *VLAN List* field.
 - *Disable* — Disables port-based authentication on the device. This is the default.

- **VLAN List** — Contains a list of VLANs. The Guest VLAN is selected from the VLAN list.
2. Define the Port-based *Authentication State*, *Authentication Method*, *Guest VLAN*, and *VLAN List* fields.
 3. Click . The network authentication properties are set, and the device is updated.

Defining Port Authentication

The *Port Authentication Page* allows network managers to configure port-based authentication global parameters. To define the port-based authentication global properties:

1. Click **Advanced Setup > Security Suite > Authentication > Port Authentication**. The *Port Authentication Page* opens.

Figure 54: Port Authentication Page

#	Port	User Name	Admin Port Control	Current Port Control	Guest Vlan	Enable Periodic Reauthentication	Reauthentication Period	Authenticator State	Quiet Period	Resending EAP
1	1/1		Force Authorized	Authorized	Disable	False	3600	Force Authorized	60	30
2	1/2		Force Authorized	Authorized*	Disable	False	3600	Initialize	60	30
3	1/3		Force Authorized	Authorized*	Disable	False	3600	Initialize	60	30
4	1/4		Force Authorized	Authorized*	Disable	False	3600	Initialize	60	30
5	1/5		Force Authorized	Authorized*	Disable	False	3600	Initialize	60	30
6	1/6		Force Authorized	Authorized*	Disable	False	3600	Initialize	60	30
7	1/7		Force Authorized	Authorized*	Disable	False	3600	Initialize	60	30
8	1/8		Force Authorized	Authorized*	Disable	False	3600	Initialize	60	30
9	1/9		Force Authorized	Authorized*	Disable	False	3600	Initialize	60	30

The *Port Authentication Page* contains the following fields:

- **Copy from Entry Number** — Copies port authentication information from the selected port.
- **to Row Number(s)** — Copies port authentication information to the selected port.
- **Unit No.** — Indicates the stacking member for which the port authentication details are displayed.
- **Port** — Displays a list of interfaces on which port-based authentication is enabled.
- **User Name** — Displays the supplicant user name.
- **Admin Port Control** — Displays the admin port authorization state.
- **Current Port Control** — Displays the current port authorization state.
- **Guest Vlan** — Displays the current Guest VLAN state. Disable is the default value.
- **Enable Periodic Reauthentication** — Permits immediate port reauthentication. The possible field values are:
 - *Enable* — Enables immediate port reauthentication. This is the default value.
 - *Disable* — Disables port reauthentication.
- **Reauthentication Period** — Displays the time span (in seconds) in which the selected port is reauthenticated. The field default is 3600 seconds.
- **Authenticator State** — Displays the current authenticator state.

- **Quiet Period** — Defines the time (in seconds) after an authentication failure (for example, a wrong password) before the switch tries to authenticate the client again. The default value is 60 seconds. During this time the switch acts as defined in the 'Action on Violation' parameter (may forward, drop the packets from the client or shut down the port).
- **Resending EAP** — Defines the amount of time (in seconds) that lapses before EAP requests are resent. The field default is 30 seconds.
- **Max EAP Requests** — Displays the total amount of EAP requests sent. If a response is not received after the defined period, the authentication process is restarted. The field default is 2 retries.
- **Supplicant Timeout** —
- **Server Timeout**—
- **Termination Cause** — Indicates the reason for which the port authentication was terminated.

2. Click  . The *Port Authentication Settings Page* opens:

Figure 55: Port Authentication Settings Page

Port Authentication Settings

Port	2
User Name	
Admin Port Control	forceAuthorized
Guest VLAN ID	None
Make Guest VLAN	Disable
Enable Periodic Reauthentication	<input type="checkbox"/>
Reauthentication Period	3600
Reauthenticate Now	<input type="checkbox"/>
Authenticator State	Initialize
Quiet Period	60
Resending EAP	30
Max EAP Requests	2
Supplicant Timeout	30
Server Timeout	30
Termination Cause	Port re-initialize

3. Modify the fields.

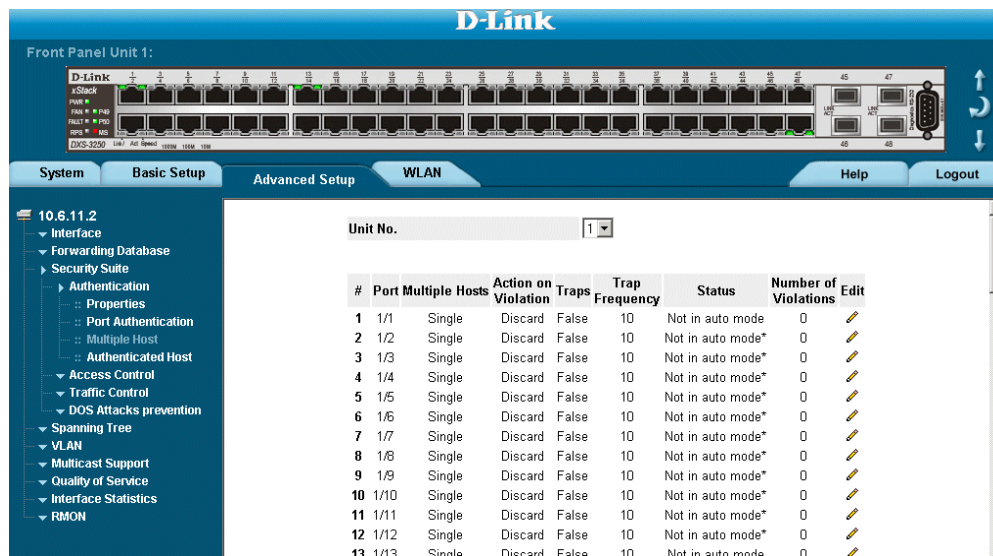
4. Click . The port authentication settings are defined, and the device is updated.

Configuring Multiple Hosts

The *Multiple Host Page* allows network managers to configure advanced port-based authentication settings for specific ports and VLANs. For more information on advanced port-based authentication, see *Advanced Port-Based Authentication*. To define the network authentication global properties:

1. Click **Advanced Setup > Security Suite > Authentication > Multiple Host**. The *Multiple Host Page* opens.

Figure 56: Multiple Host Page



The *Multiple Host Page* contains the following fields:

- **Unit No.** — Indicates the stacking member for which the multiple host details are displayed.
- **Port** — Displays the port number for which advanced port-based authentication is enabled.
- **Multiple Hosts** — Indicates whether multiple hosts are enabled. Multiple hosts must be enabled in order to either disable the ingress-filter, or to use port-lock security on the selected port. The possible field values are:
 - *Multiple* — Multiple hosts are enabled.
 - *Disable* — Multiple hosts are disabled.
- **Action on Violation** — Defines the action to be applied to packets arriving in single-host mode, from a host whose MAC address is not the supplicant MAC address. The possible field values are:
 - *Forward* — Forwards the packet.
 - *Discard* — Discards the packets. This is the default value.
 - *Shutdown* — Discards the packets and shuts down the port. The port remains shut down until reactivated, or until the device is reset.
- **Traps** — Indicates if traps are enabled for Multiple Hosts. The possible field values are:
 - *True* — Indicates that traps are enabled for Multiple hosts.
 - *False* — Indicates that traps are disabled for Multiple hosts.
- **Trap Frequency** — Defines the time period by which traps are sent to the host. The Trap Frequency (1-1000000) field can be defined only if multiple hosts are disabled. The default is 10 seconds.

- **Status** — Indicates the host status. If there is an asterisk (*), the port is either not linked or is down. The possible field values are:
 - *Unauthorized* — Indicates that either the port control is Force Unauthorized and the port link is down, or the port control is Auto but a client has not been authenticated via the port.
 - *Not in Auto Mode* — Indicates that the port control is Forced Authorized, and clients have full port access.
 - *Single-host Lock* — Indicates that the port control is Auto and a single client has been authenticated via the port.
 - *No Single Host* — Indicates that Multiple Host is enabled.
- **Number of Violations** — Indicates the number of packets that arrived on the interface in single-host mode, from a host whose MAC address is not the supplicant MAC address.


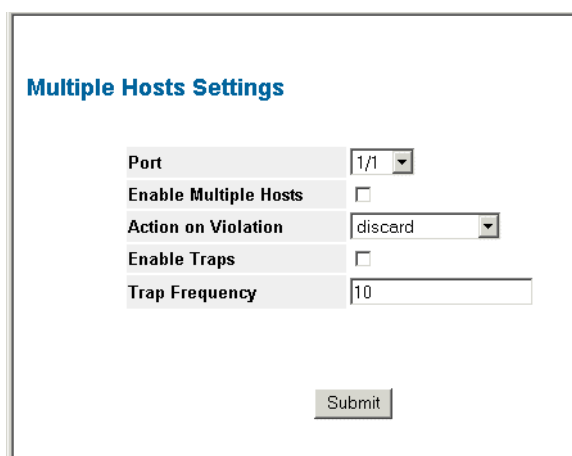
2. Click  . The Multiple Host Settings Page opens:

Figure 57: Multiple Host Settings Page



Port	1/1
Enable Multiple Hosts	<input type="checkbox"/>
Action on Violation	discard
Enable Traps	<input type="checkbox"/>
Trap Frequency	10

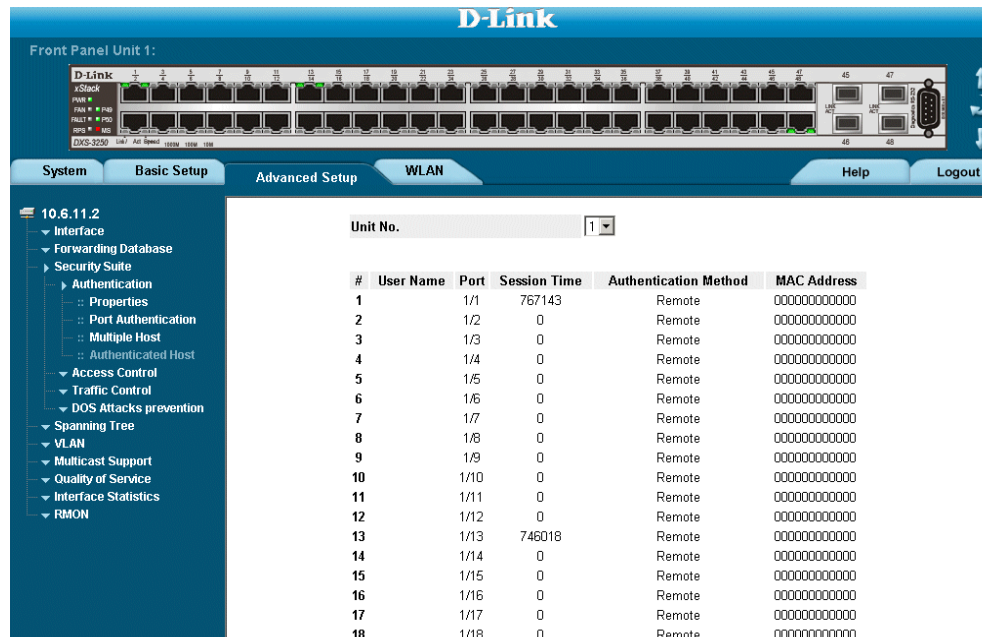
3. Modify the *Port*, *Enable Multiple Hosts*, *Action on Violation*, *Enable Traps*, and *Trap Frequency* fields.
4. Click . The multiple host settings are modified, and the device is updated.

Defining Authentication Hosts

The *Authenticated Host Page* contains a list of authenticated users. To define authenticated users:

1. Click **Advanced Setup > Security Suite > Authentication > Authenticated Host**. The *Authenticated Host Page* opens:

Figure 58: Authenticated Host Page



The *Authenticated Host Page* contains the following fields:

- **User Name** — Lists the supplicants that were authenticated, and are permitted on each port.
- **Port** — Displays the port number.
- **Session Time** — Displays the amount of time (in seconds) the supplicant was logged on the port.
- **Authentication Method** — Displays the method by which the last session was authenticated. The possible field values are:
 - *Remote* — 802.1x authentication is not used on this port (port is forced-authorized).
 - *None* — The supplicant was not authenticated.
 - *RADIUS* — The supplicant was authenticated by a RADIUS server.
- **MAC Address** — Displays the supplicant MAC address.

Configuring Traffic Control

This section contains information for managing both port security and storm control, and includes the following topics:

- Managing Port Security
- Enabling Storm Control

Managing Port Security

Network security can be increased by limiting access on a specific port only to users with specific MAC addresses. The MAC addresses can be dynamically learned or statically configured. Locked port security monitors both received and learned packets that are received on specific ports. Access to the locked port is limited to users with specific MAC addresses. These addresses are either manually defined on the port, or learned on that port up to the point when it is locked. When a packet is received on a locked port, and the packet D-Link source MAC address is not tied to that port (either it was learned on a different port, or it is unknown to the system), the protection mechanism is invoked, and can provide various options. Unauthorized packets arriving at a locked port are either:

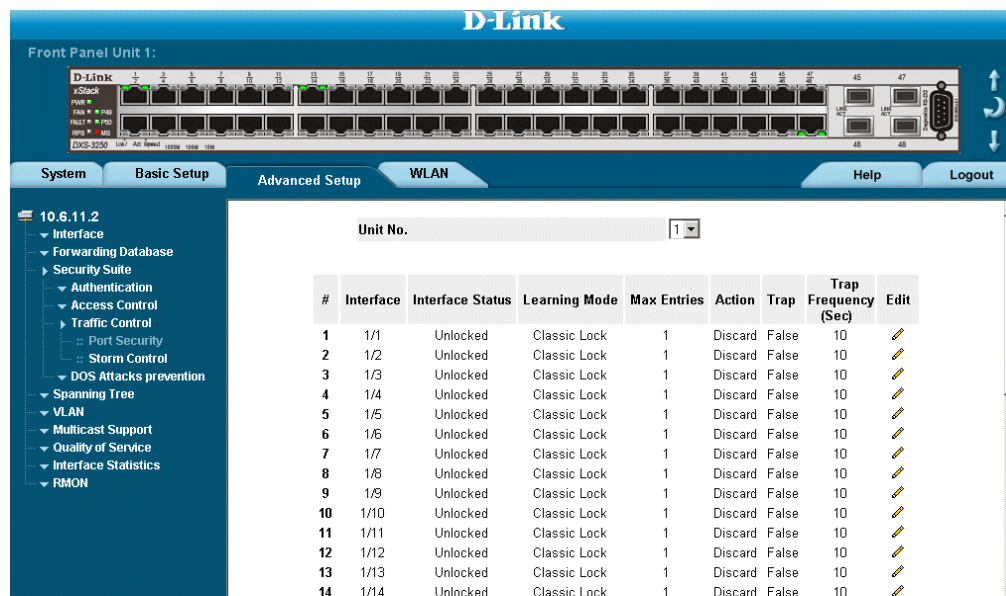
- Forwarded
- Discarded with no trap
- Discarded with a trap
- Shuts down the port.

Locked port security also enables storing a list of MAC addresses in the configuration file. The MAC address list can be restored after the device has been reset.

Disabled ports are activated from the *Port Security Page*. To define port security:

1. Click **Advanced Setup > Security Suite > Traffic Control > Port Security**. The *Port Security Page* opens.

Figure 59: Port Security Page



The *Port Security Page* contains the following fields:

- **Interface** — Displays the port or LAG name.
- **Interface Status** — Indicates the host status. The possible field values are:
 - *Unauthorized* — Indicates that the port control is Force Unauthorized, the port link is down or the port control is Auto, but a client has not been authenticated via the port.


- *Not in Auto Mode* — Indicates that the port control is Forced Authorized, and clients have full port access.
 - *Single-host Lock* — Indicates that the port control is Auto and a single client has been authenticated via the port.
 - **Learning Mode** — This mode has 2 value options: 'Classic Lock' and 'Limited Dynamic Lock'. Classic Lock - immediately lock the port from learning new MAC Addresses. Limited Dynamic Lock - this parameter depends on the 'Max Entries' parameter value
 - **Max Entries** — Number of MAC addresses which the port learns until the Limited Dynamic Lock parameter locks it.
 - **Action** — Indicates the action to be applied to packets arriving on a locked port. The possible field values are:
 - *Forward* — Forwards packets from an unknown source without learning the MAC address.
 - *Discard* — Discards packets from any unlearned source. This is the default value.
 - *Shutdown* — Discards packets from any unlearned source and shuts down the port. The port remains shut down until reactivated, or until the device is reset.
 - **Trap** — Enables traps when a packet is received on a locked port. The possible field values are:
 - Checked — Enables traps.
 - Unchecked — Disables traps.
 - **Trap Frequency (Sec)** — The amount of time (in seconds) between traps. The default value is 10 seconds.
2. Click  . The *Port Security Settings Page* opens:

Figure 60: Port Security Settings Page

Interface Table Settings

Interface	<input checked="" type="radio"/> Port <input type="radio"/> LAG
Lock Interface	<input type="checkbox"/>
Learning Mode	Classic Lock
Max Entries	1
Action on Violation	discard
Enable Trap	<input type="checkbox"/>
Trap Frequency	10

3. Modify the fields.
4. Click . The port security settings are defined, and the device is updated.

Enabling Storm Control

Storm control limits the amount of Multicast and Broadcast frames accepted and forwarded by the device. When Layer 2 frames are forwarded, Broadcast, and Multicast frames are flooded to all ports on the relevant VLAN. This occupies bandwidth, and loads all nodes on all ports.

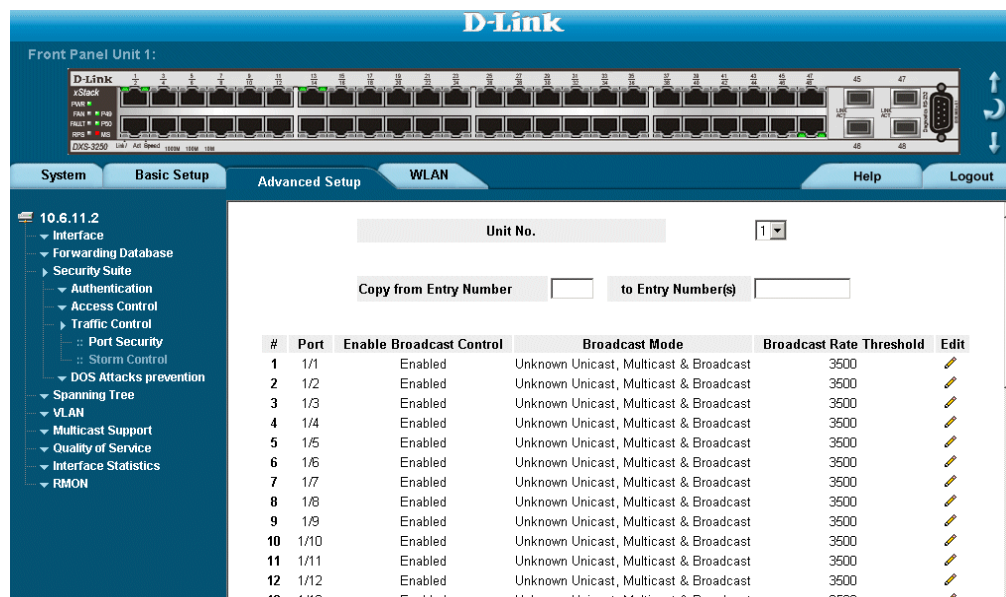
A Broadcast Storm is a result of an excessive amount of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, straining network resources or causing the network to time out.

Storm control is enabled for all Gigabit ports by defining the packet type and the rate the packets are transmitted. The system measures the incoming Broadcast and Multicast frame rates separately on each port, and discards the frames when the rate exceeds a user-defined rate.

The *Storm Control Page* provides fields for configuring broadcast storm control. To enable storm control:

1. Click **Advanced Setup > Security Suite > Traffic Control > Storm Control**. The *Storm Control Page* opens.

Figure 61: Storm Control Page



The *Storm Control Page* contains the following fields:

- **Unit No.** — Indicates the stacking unit for which the storm control information is displayed.
- **Copy from Entry No.** — Copies the storm control parameters from the selected port.
- **To Entry Numbers** — Copies the storm control parameters to the selected port.
- **Port** — Indicates the port from which storm control is enabled. The possible field values are:
 - *Enable* — Enables storm control on the selected port.
 - *Disable* — Disables storm control on the selected port.
- **Broadcast Control** — Indicates if forwarding Broadcast packet types on the interface.
- **Broadcast Mode** — Specifies the Broadcast mode currently enabled on the device. The possible field values are:


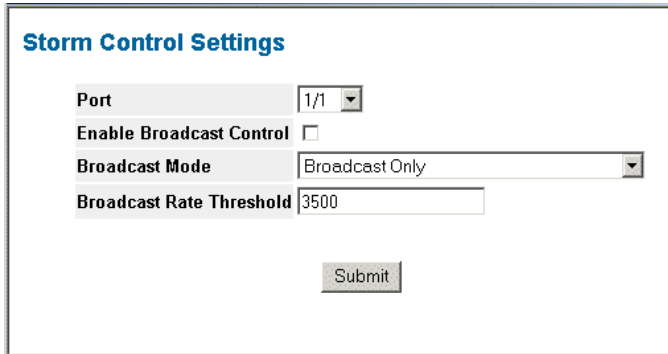
- *Unknown Unicast, Multicast & Broadcast* — Counts Unicast, Multicast, and Broadcast traffic.
 - *Multicast & Broadcast* — Counts Broadcast and Multicast traffic together.
 - *Broadcast Only* — Counts only Broadcast traffic.
 - **Broadcast Rate Threshold** — Indicates the maximum rate (kilobits per second) at which unknown packets are forwarded. The range is 70-1,000,000. The default value is zero. All values are rounded to the nearest 64 Kbps. If the field value is under 64 Kbps, the value is rounded up to 64 Kbps, with the exception of the value zero.
2. Click  . The *Storm Control Settings Page* opens:

Figure 62: Storm Control Settings Page



Storm Control Settings


Port 1/1

Enable Broadcast Control

Broadcast Mode Broadcast Only

Broadcast Rate Threshold 3500

Submit

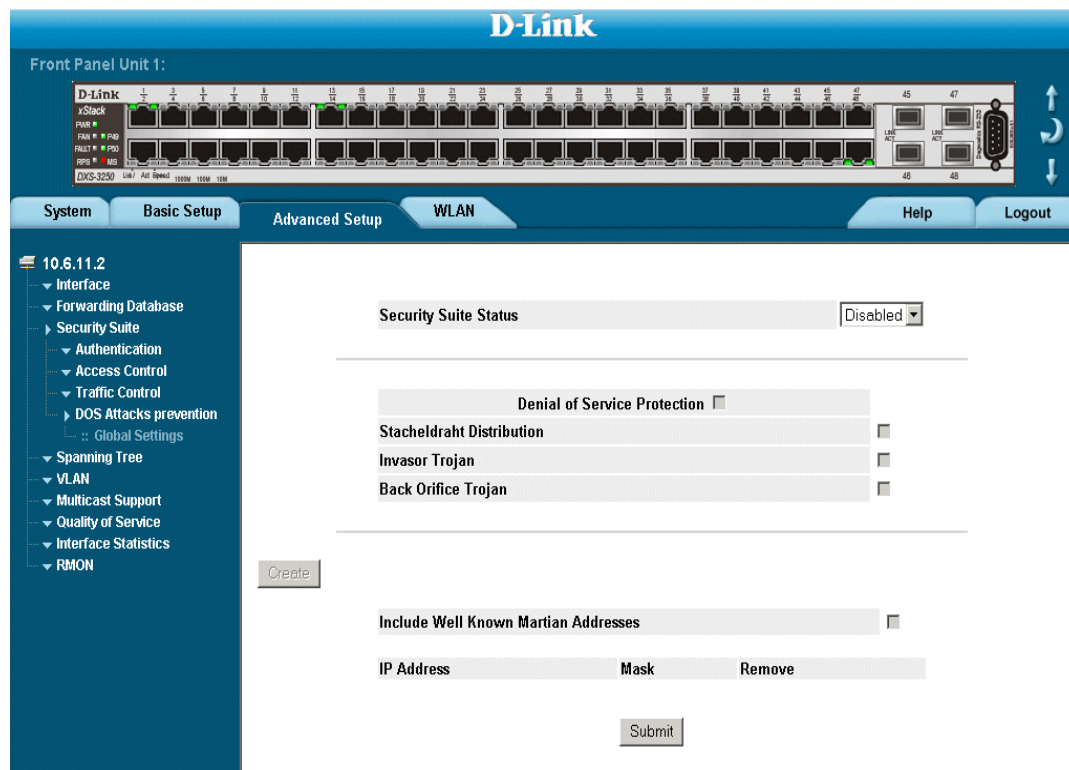
3. Modify the *Port*, *Enable Broadcast Control*, *Broadcast Mode*, and *Broadcast Rate Threshold* fields.
4. Click  . Storm control is enabled on the device.

Defining DOS Protection Security

Denial of Service (DOS) protection provides Security Suite for DWS/DXS-3200 systems allows administrators to match, discard, and redirect packets based on packet header values. Packets which are redirected are analyzed for viruses and Trojans. To enable DOS attack on the system:

1. Click **Advanced Setup > Security Suite > DOS Attacks > Global Settings**. The *DOS Attacks Global Settings Page* opens.

Figure 63: DOS Attacks Global Settings Page



The *DOS Attacks Global Settings Page* contains the following fields:

- **Security Suite Status** — Indicates if DOS security is enabled on the device. The possible field values are:
 - *Enable* — Enables DOS security.
 - *Disable* — Disables DOS security on the device. This is the default value.
- **Denial of Service Protection** — Indicates if service is enabled. If the service protection is disabled, the *Stacheldraht Distribution*, *Invasor Trojan*, and *Back Office Trojan* fields are disabled.
- **Stacheldraht Distribution** — Discard TCP packets with source TCP port equal to 16660
- **Invasor Trojan** — Discard TCP packets with destination TCP port equal to 2140 and source TCP port equal to 1024.
- **Back Orifice Trojan** — Discard UDP packets with destination UDP port equal to 31337 and source UDP port equal to 1024.

- **Include Well Known Martian Addresses** — Indicates that packets arriving from Martian addresses are dropped. When enabled, the following IP addresses are included:
 - 0.0.0.0/8 (except 0.0.0.0/32), 127.0.0.0/8
 - 192.0.2.0/24 , 224.0.0.0/4
 - 240.0.0.0/4 (except 255.255.255.255/32)
 - **IP Address** — Displays the IP addresses for which DOS attack is enabled.
 - **Mask** — Displays the Mask for which DOS attack is enabled.
 - **Remove** — Removes selected IP addresses from the Service Protection list. The possible field values are:
 - *Checked* — Removes the selected IP address and mask.
 - *Unchecked* — Maintains IP addresses and IP masks.
2. Click **Create**. The *Add Martian Addresses Page* opens:

Figure 64: Add Martian Addresses Page

Add Martian Addresses

IP Address Select from Known Martian Addresses 10.0.0.0/8 New IP Address

Mask Prefix Length

3. Define the fields.
4. Click **Submit**. DOS attack is defined, and the device is updated.

Section 9. Configuring Ports

The *Interface Configuration Page* contains fields for defining port parameters.

To define port parameters:

1. Click **Basic Setup > Interface > Interface Configuration**. The *Interface Configuration Page* opens.

Figure 65: Interface Configuration Page

Front Panel Unit 1:

D-Link

System Basic Setup Advanced Setup WLAN Help Logou

10.6.11.2

- Interface
 - Interface Configuration
 - Interface Properties
- IP Configuration
- VLAN
- Routing
- Quality of Service
- Interface Statistics

Unit Number: 1

Interface	Port Status	Port Speed	Duplex Mode	Auto Negotiation	Advertisement	Back Pressure	Flow Control	MDI	LAG	PVE	Edit
1/1	Up	1000M	Full	Enable	10H,10F,100H,100F,1000F	Disable	Disable	MDI			
1/2	Down				Unknown						
1/3	Down				Unknown						
1/4	Down				Unknown						
1/5	Down				Unknown						
1/6	Down				Unknown						
1/7	Down				Unknown						
1/8	Down				Unknown						
1/9	Down				Unknown						
1/10	Down				Unknown						
1/11	Down				Unknown						
1/12	Down				Unknown						

The Interface Configuration Ports Table contains the following fields:

- **Unit No.** — Indicates the stacking member for which the port information is displayed.
- **Interface** — Displays the port number.
- **Port Status** — Indicates whether the port is currently operational or non-operational. The possible field values are:
 - *Up* — Indicates the port is currently operating.
 - *Down* — Indicates the port is currently not operating.
- **Port Speed** — Displays the configured rate for the port. The port type determines what speed setting options are available. Port speeds can only be configured when auto negotiation is disabled. The possible field values are:
 - *10* — Indicates the port is currently operating at 10 Mbps.
 - *100* — Indicates the port is currently operating at 100 Mbps.
 - *1000* — Indicates the port is currently operating at 1000 Mbps.

- *10000* — Indicates the port is currently operating at 10000 Mbps.
- **Duplex Mode** — Displays the port duplex mode. This field is configurable only when auto negotiation is disabled, and the port speed is set to 10M or 100M. This field cannot be configured on LAGs. The possible field values are:
 - *Full* — The interface supports transmission between the device and its link partner in both directions simultaneously.
 - *Half* — The interface supports transmission between the device and the client in only one direction at a time.
- **Auto Negotiation** — Displays the auto negotiation status on the port. Auto negotiation is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode, and flow control abilities to its partner.
- **Advertisement** — Defines the auto negotiation setting the port advertises. The possible field values are:
 - *Max Capability* — Indicates that all port speeds and duplex mode settings are accepted.
 - *10 Half* — Indicates that the port advertises for a 10 Mbps speed port and half duplex mode setting.
 - *10 Full* — Indicates that the port advertises for a 10 Mbps speed port and full duplex mode setting.
 - *100 Half* — Indicates that the port advertises for a 100 Mbps speed port and half duplex mode setting.
 - *100 Full* — Indicates that the port advertises for a 100 Mbps speed port and full duplex mode setting.
 - *1000 Full* — Indicates that the port advertises for a 1000 Mbps speed port and full duplex mode setting.
- **Back Pressure** — Displays the back pressure mode on the Port. Back pressure mode is used with half duplex mode to disable ports from receiving messages.
- **Flow Control** — Displays the flow control status on the port. Operates when the port is in full duplex mode.
- **MDI/MDIX** — Displays the MDI/MDIX status on the port. Hubs and switches are deliberately wired opposite the way end stations are wired, so that when a hub or switch is connected to an end station, a straight through Ethernet cable can be used, and the pairs are matched up properly. When two hubs or switches are connected to each other, or two end stations are connected to each other, a crossover cable is used to ensure that the correct pairs are connected. The possible field values are:
 - *Auto* — Use to automatically detect the cable type.
 - *MDI (Media Dependent Interface)* — Use for end stations.
 - *MDIX (Media Dependent Interface with Crossover)* — Use for hubs and switches.
- **LAG** — Indicates whether the port is part of a *Link Aggregation Group* (LAG).

The Interface Configuration LAG table contains the following fields:

- **PVE** — Displays the PVE group to which the port is configured.

2. Click  . The *Port or LAG Interface Settings Page* opens:



Note

In addition to the fields in the *Interface Configuration Page*, the *Port or LAG Configuration Settings Page* includes the **Reactivate Suspended Port** or **Reactivate Suspended Lag** fields. Select **Reactivate Suspended Port** or **Reactivate Suspended Lag** fields to return a suspended port or LAG to active status.

Figure 66: Port Configuration Settings Page

Port Configuration Settings

Port	1/1
Admin Status	Up
Current Port Status	Up
Reactivate Suspended Port	<input type="checkbox"/>
Operational Status	Active
Admin Speed	1000M
Current Port Speed	1000M
Admin Duplex	Full
Current Duplex Mode	Full
Auto Negotiation	Enable
Current Auto Negotiation	Enable
Admin Advertisement	<input checked="" type="checkbox"/> Max Capability <input type="checkbox"/> 10 Half <input type="checkbox"/> 10 Full <input type="checkbox"/> 100 Half <input type="checkbox"/> 100 Full
Current Advertisement	10 Half 10 Full 100 Half 100 Full 1000 Full
Neighbor Advertisement	1000 Full
Back Pressure	Enable
Current Back Pressure	Disable
Flow Control	Disable
Current Flow Control	Disable
MDI/MDIX	AUTO
Current MDI/MDIX	MDI
PVE	None
LAG	

Submit

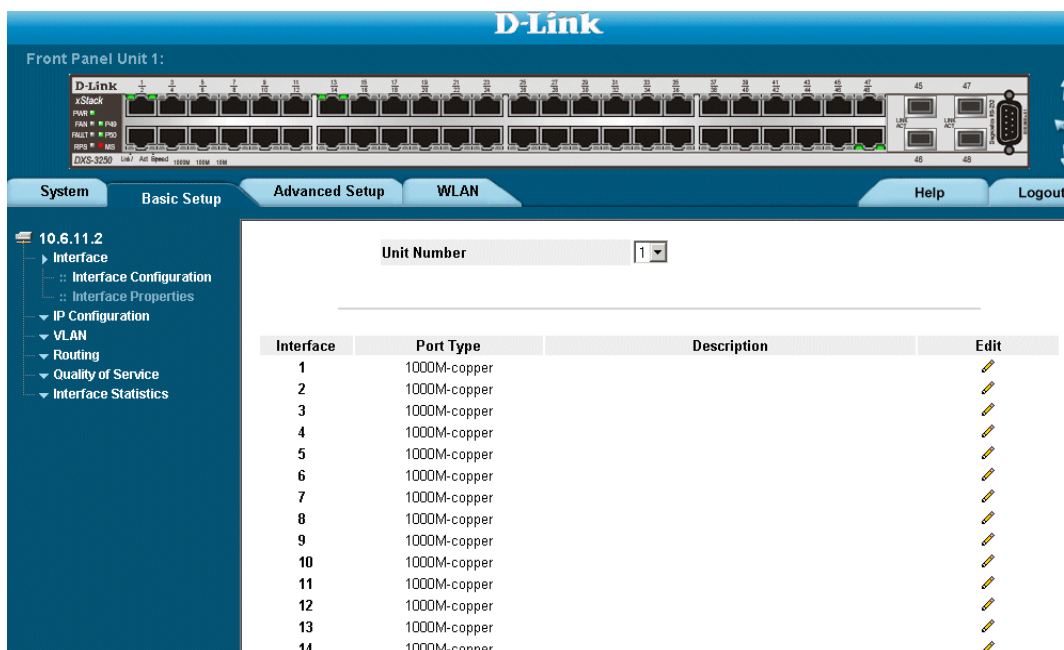
3. Modify the fields.
4. Click **Submit**. The parameters are saved, and the device is updated.

Viewing Port Properties

The *Interface Properties Page* contains fields for defining port parameters. To define port parameters:

1. Click **Basic Setup > Interface > Interface Properties**. The *Interface Properties Page* opens:

Figure 67: Interface Properties Page



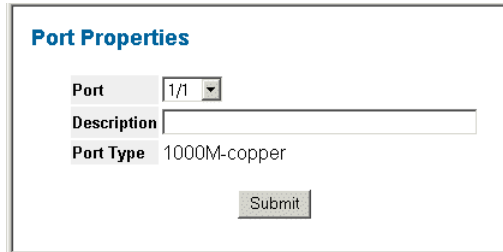
The *Interface Properties Page* contains the following fields:

- **Unit No** — Indicates the stacking member for which the port information is displayed.
- **Interface** — Displays the port number.
- **Port Type** — Displays the port type. The possible field values are:
 - Copper — Indicates the port has a copper port connection.
 - Fiber — Indicates the port has a fiber optic port connection.
- **Description** — Provides a user-defined port description

To edit the port properties:

2. Click . The *Port Properties Page* opens:

Figure 68: Port Properties Page



Port Properties

Port 1/1

Description

Port Type 1000M-copper

Submit

3. Define the *Port* and *Description* fields.
4. Click **Submit**. The interface properties are modified, and the device is updated.

This page is left blank intentionally.

Section 10. Aggregating Ports

Link Aggregation optimizes port usage by linking a group of ports together to form a single LAG. Aggregating ports multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

The device supports both static LAGs and *Link Aggregation Control Protocol* (LACP) LAGs. LACP LAGs negotiate aggregating port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them. Ensure the following:

- All ports within a LAG must be the same media type.
- A VLAN is not configured on the port.
- The port is not assigned to a different LAG.
- Auto-negotiation mode is not configured on the port.
- The port is in full-duplex mode.
- All ports in the LAG have the same ingress filtering and tagged modes.
- All ports in the LAG have the same back pressure and flow control modes.
- All ports in the LAG have the same priority.
- All ports in the LAG have the same transceiver type.
- The device supports up to 64 LAGs, with eight ports in each LAG.
- Ports can be configured as LACP ports only if the ports are not part of a previously configured LAG.
- Ports added to a LAG lose their individual port configuration. When ports are removed from the LAG, the original port configuration is applied to the ports.

This section contains the following topics:

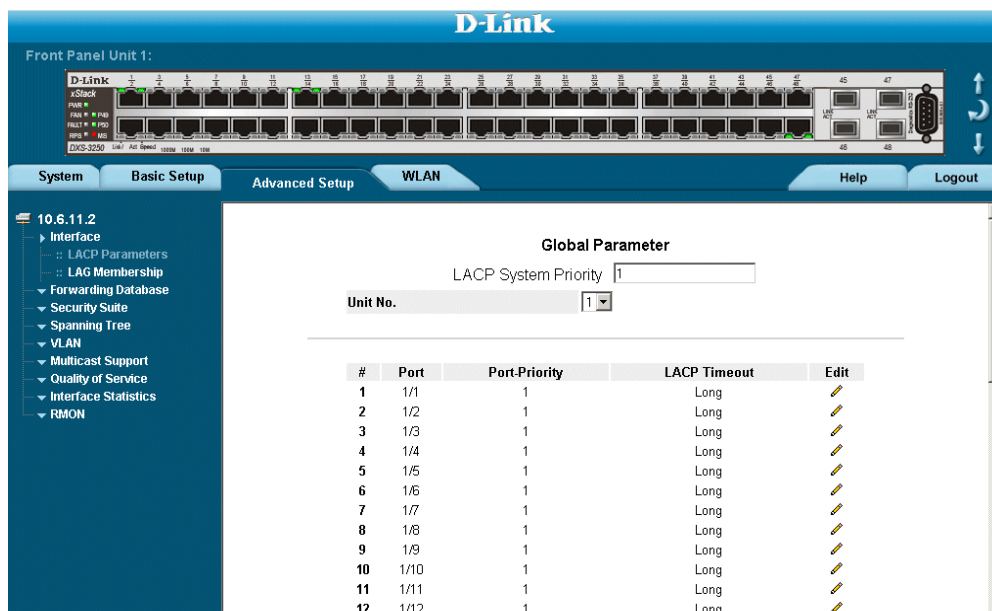
- Configuring LACP

Configuring LACP

LAG ports can contain different media types if the ports are operating at the same speed. Aggregated links can be set up manually or automatically established by enabling LACP on the relevant links. Aggregate ports can be linked into link-aggregation port-groups. Each group is comprised of ports with the same speed. The *LACP Parameters Page* contains fields for configuring LACP LAGs. To configure LACP for LAGs:

1. Click **Advanced Setup > Interface > LACP Parameters** tab. The *LACP Parameters Page* opens:

Figure 69: LACP Parameters Page

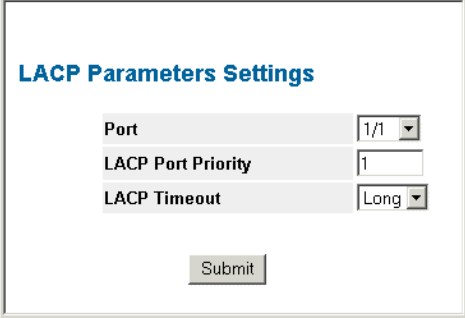


The *LACP Parameters Page* contains the following fields:

- **LACP System Priority** — Specifies system priority value. The field range is 1-65535. The field default is 1.
- **Unit No.** — Displays the stacking member for which the LAG parameters are defined.
- **Port** — Displays the port number to which timeout and priority values are assigned.
- **Port-Priority** — Displays the LACP priority value for the port. The field range is 1-65535.
- **LACP Timeout** — Displays the administrative LACP timeout.

2. Click . The *LACP Parameters Settings Page* opens:

Figure 70: LACP Parameters Settings Page



LACP Parameters Settings

Port	1/1
LACP Port Priority	1
LACP Timeout	Long

Submit

3. Edit the *Port Priority* and *LACP Timeout* fields.
4. Click . The LACP settings are saved, and the device is updated

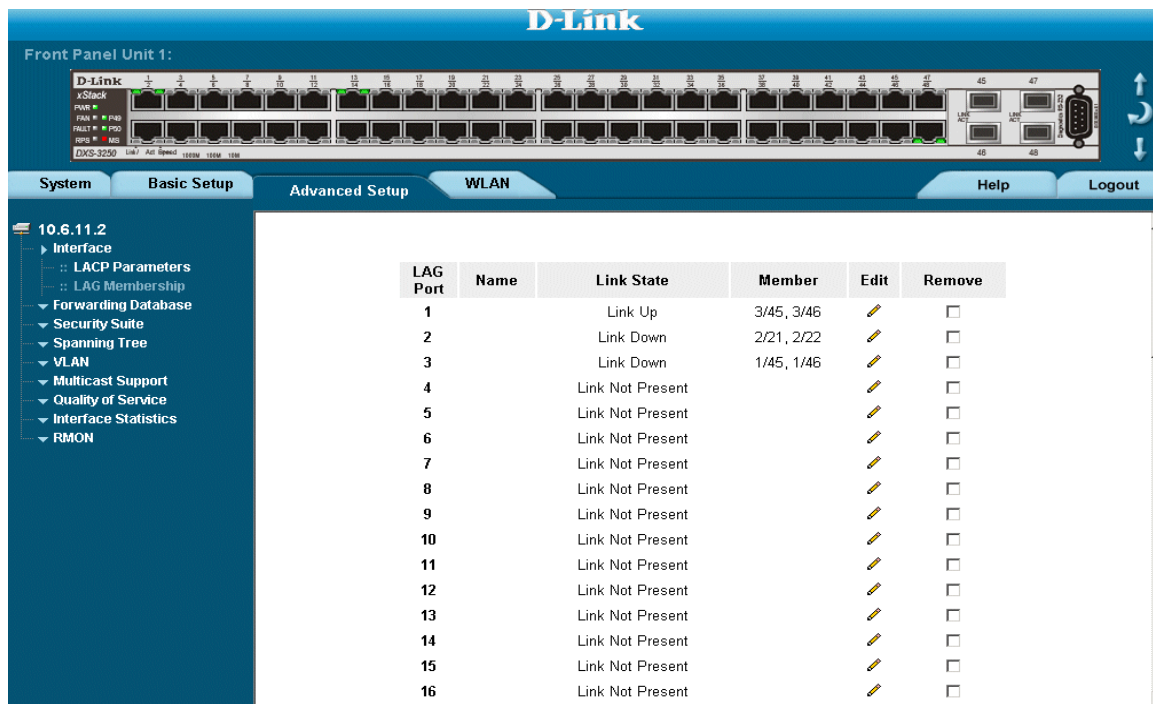
Defining LAG Members

The *LAG Membership Page* contains fields for configuring parameters for configured LAGs.

To define LAG parameters:


1. Click **Advanced Setup > Interface > LAG Membership**. The *LAG Membership Page* opens.

Figure 71: LAG Membership Page



The *LAG Membership Page* contains the following fields:

- **LAG Port** — Displays the ports which can be assigned to the LAG.
- **Name** — Indicates the LAG name.
- **Link State** — Displays the link operational status.
- **Members** — Displays the ports which are currently configured to the LAG.
- **Remove** — Removes the LAG. The possible field values:
 - *Checked* — Removes the selected LAG.
 - *Unchecked* — Maintains the LAGs.

2. Click . The LAG membership settings are saved, and the device is updated.

Section 11. Configuring VLANs

VLANs are logical subgroups with a Local Area Network (LAN) which combine user stations and network devices into a single unit, regardless of the physical LAN segment to which they are attached. VLANs allow network traffic to flow more efficiently within subgroups. VLANs use software to reduce the amount of time it takes for network changes, additions, and moves to be implemented.

VLANs have no minimum number of ports, and can be created per unit, per device, or through any other logical connection combination, since they are software-based and not defined by physical attributes.

VLANs function at Layer 2. Since VLANs isolate traffic within the VLAN, a Layer 3 router working at a protocol level is required to allow traffic flow between VLANs. Layer 3 routers identify segments and coordinate with VLANs. VLANs are Broadcast and Multicast domains. Broadcast and Multicast traffic is transmitted only in the VLAN in which the traffic is generated.

VLAN tagging provides a method of transferring VLAN information between VLAN groups. VLAN tagging attaches a 4-byte tag to packet headers. The VLAN tag indicates to which VLAN the packets belong. VLAN tags are attached to the VLAN by either the end station or the network device. VLAN tags also contain VLAN network priority information.

Combining VLANs and GARP (Generic Attribute Registration Protocol) allows network managers to define network nodes into Broadcast domains.

This section contains the following topics:

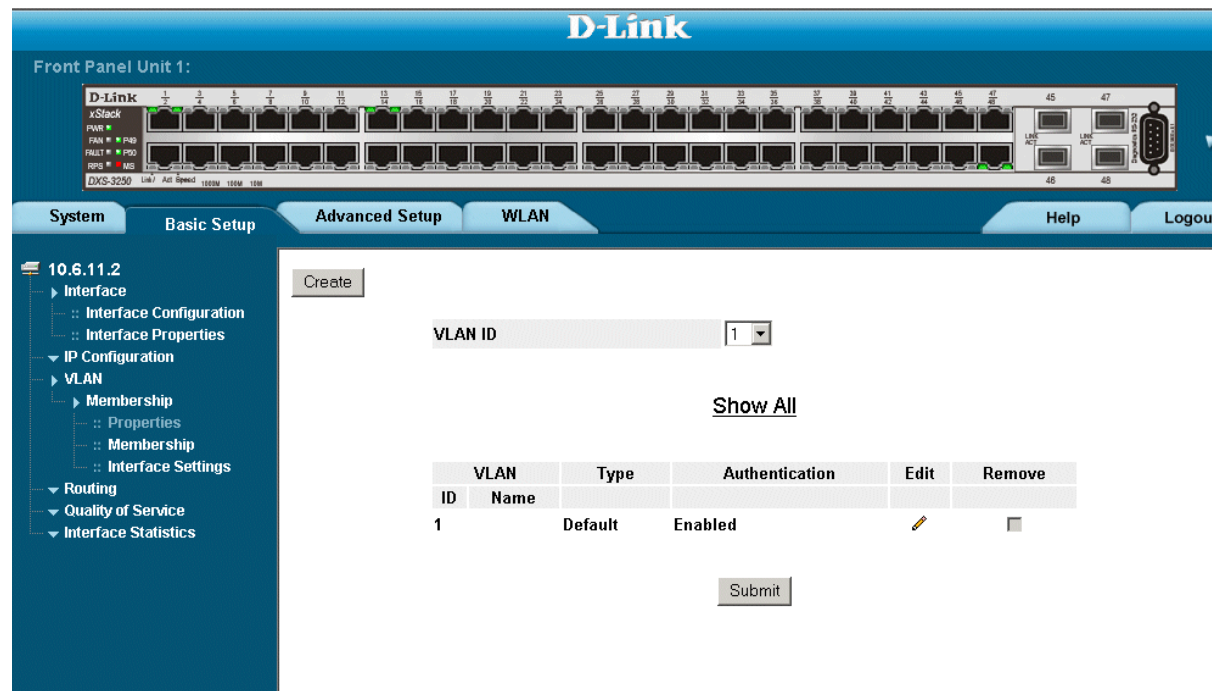
- Defining VLAN Properties
- Defining VLAN Membership
- Defining VLAN Interface Settings
- Configuring GARP
- Configuring Multicast VLANs

Defining VLAN Properties

The *VLAN Properties Page* provides information and global parameters for configuring and working with VLANs. To define VLAN properties:

1. Click **Basic Setup > VLAN > Membership > Properties**. The *VLAN Properties Page* opens.

Figure 72: VLAN Properties Page

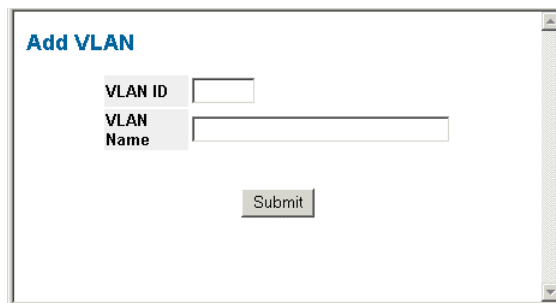


The *VLAN Properties* page contains the following fields:

- **VLAN ID** — Contains a drop-down list of the currently configured VLAN IDs.
- **Show All** — Displays all currently configured VLANs.
- **VLAN ID** — Displays the VLAN ID.
- **Name** — Displays the user-defined VLAN name.
- **Type**— Displays the VLAN type. The possible field values are:
 - *Dynamic* — Indicates the VLAN was dynamically created through GARP.
 - *Static* — Indicates the VLAN is user-defined.
 - *Default* — Indicates the VLAN is the default VLAN.
- **Authentication**— Indicates whether unauthorized users can access a Guest VLAN. The possible field values are:
 - *Enable* — Enables unauthorized users to use the Guest VLAN.
 - *Disable* — Disables unauthorized users from using the Guest VLAN.

- **Remove**— Removes VLANs. The possible field values are:
 - *Checked* — Removes the selected VLAN.
 - *Unchecked* — Maintains VLANs.
2. Click **Create**. The *Add VLAN* page opens:

Figure 73: Add VLAN Page



The screenshot shows a web form titled "Add VLAN". It contains two input fields: "VLAN ID" and "VLAN Name". Below the fields is a "Submit" button. The form is enclosed in a window-like border with a scrollbar on the right side.

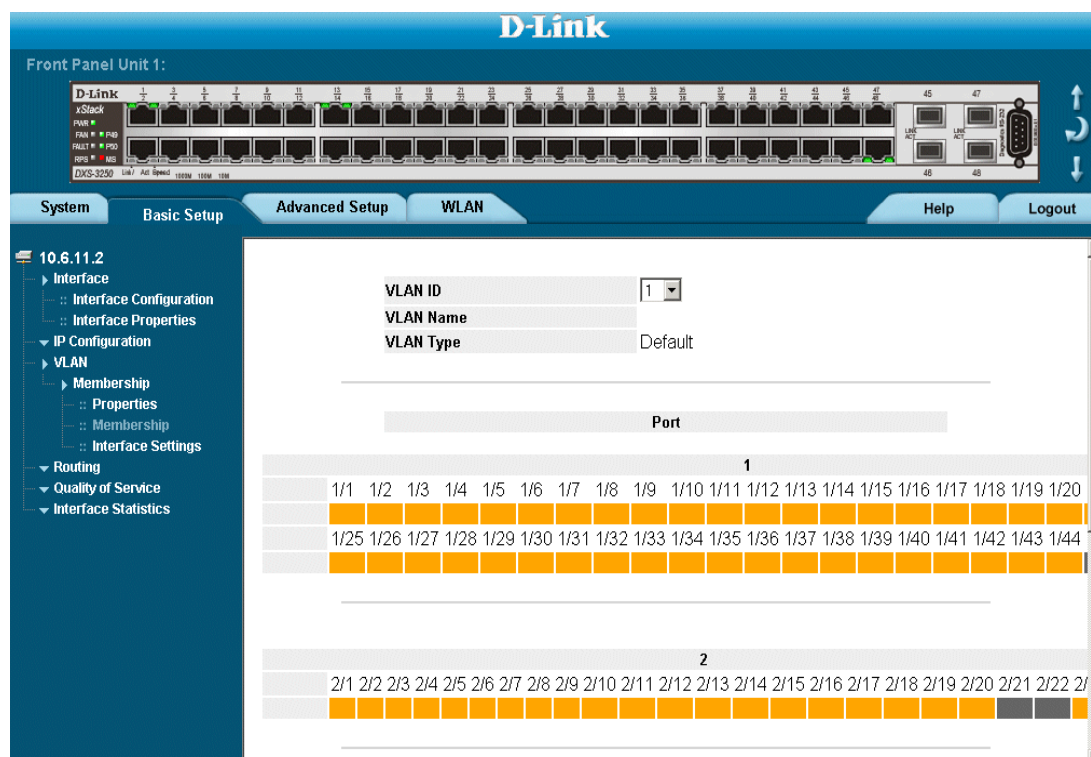
3. Define the *VLAN ID* and *VLAN Name* fields.
4. Click **Submit**. The *VLAN ID* is defined, and the device is updated.

Defining VLAN Membership

The *VLAN Membership Page* contains a table that maps VLAN parameters to ports. Ports are assigned VLAN membership by toggling through the Port Control settings. To define VLAN membership:

1. Click **Basic Setup > VLAN > Membership > Membership**. The *VLAN Membership Page* opens.

Figure 74: VLAN Membership Page



The *VLAN Membership Page* contains the following fields:

- **VLAN ID** — Displays the user-defined VLAN ID.
- **VLAN Name** — Displays the name of the VLAN
- **VLAN Type**— Indicates the VLAN type. The possible field values are:
 - *Dynamic* — Indicates the VLAN was dynamically created through GARP.
 - *Static* — Indicates the VLAN is user-defined.
 - *Default* — Indicates the VLAN is the default VLAN.
- **Port** — Indicates the port membership.
- **LAG** — Indicates the LAG membership.
- **Untagged (Brown)** — Indicates the interface is an untagged VLAN member. Packets forwarded by the interface are untagged.
- **Tagged (Blue)** — Indicates the interface is a tagged member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.

- **Include (Green)** — Includes the port in the VLAN.
- **Exclude (Red)** — Excludes the interface from the VLAN. However, the interface can be added to the VLAN through GARP.
- **Forbidden (Purple)** — Denies the interface VLAN membership, even if GARP indicates the port is to be added.

Defining VLAN Interface Settings

The *VLAN Interface Settings Page* contains fields for managing ports that are part of a VLAN. The *Port Default VLAN ID (PVID)* is configured on the *VLAN Interface Settings Page*. All untagged packets arriving at the device are tagged with the port PVID. To define VLAN interfaces:

1. Click **Basic Setup > VLAN > Membership > Interface Settings**. The *VLAN Interface Settings Page* opens.

Figure 75: VLAN Interface Settings Page

#	Interface	Interface VLAN Mode	Multicast TV VLAN	PVID	Frame Type	Ingress Filtering	Reserved VLAN	Edit
1	1/1	Trunk		1	Admit All	Enable		
2	1/2	Trunk		1	Admit All	Enable		
3	1/3	Trunk		1	Admit All	Enable		
4	1/4	Trunk		1	Admit All	Enable		
5	1/5	Trunk		1	Admit All	Enable		
6	1/6	Trunk		1	Admit All	Enable		
7	1/7	Trunk		1	Admit All	Enable		
8	1/8	Trunk		1	Admit All	Enable		
9	1/9	Trunk		1	Admit All	Enable		
10	1/10	Trunk		1	Admit All	Enable		
11	1/11	Trunk		1	Admit All	Enable		
12	1/12	Trunk		1	Admit All	Enable		
13	1/13	Trunk		1	Admit All	Enable		
14	1/14	Trunk		1	Admit All	Enable		
15	1/15	Trunk		1	Admit All	Enable		

The *VLAN Interface Settings Page* contains the following fields:

- **Interface** — Displays the port number included in the VLAN.
- **Interface VLAN Mode** — Displays the port mode. The possible values are:
 - *General* — Indicates the port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full IEEE802.1q mode).
 - *Access* — Indicates a port belongs to a single untagged VLAN. When a port is in Access mode, the packet types which are accepted on the port cannot be designated. Ingress filtering cannot be enabled or disabled on an access port.
 - *Trunk* — Indicates the port belongs to VLANs in which all ports are tagged, except for one port that can be untagged.
 - *Customer* — Assigns an interface to a VLAN based on the host source MAC address connected to the interface.
- **Multicast TV VLAN** — indicates the CPE VLAN which is mapped to the Multicast TV VLAN.
- **PVID** — Assigns a VLAN ID to untagged packets. The possible values are 1-4094. VLAN 4095 is defined as per standard and industry practice as the Discard VLAN. Packets classified to the Discard VLAN are dropped.
- **Frame Type** — Specifies the packet type accepted on the port. The possible field values are:
 - *Admit Tag Only* — Only tagged packets are accepted on the port.



- *Admit All* — Both tagged and untagged packets are accepted on the port.
 - **Ingress Filtering**— Indicates whether ingress filtering is enabled on the port. The possible field values are:
 - *Enable* — Enables ingress filtering on the device. Ingress filtering discards packets that are defined to VLANs of which the specific port is not a member.
 - *Disable* — Disables ingress filtering on the device.
 - **Reserve VLAN** — Indicates the VLAN selected by the user to be the reserved VLAN if not in use by the system.
2. Select a port.
 3. Click  . The *VLAN Interface Settings Page* opens:

Figure 76: VLAN Interface Settings Page

VLAN Port's Settings

Port Interface	1
Port VLAN Mode	Access
Enable Multicast TV VLAN	
PVID	1
Frame Type	Admit All
Ingress Filtering	Enable
Current Reserved VLAN	
Reserve VLAN for Internal Use	

4. Define the fields.
5. Click  . The VLAN interface settings are modified, and the device is updated.

Configuring GARP

This section contains information for configuring *Generic Attribute Registration Protocol* (GARP). This section includes the following topics:

- Defining GARP
- Defining GVRP

Defining GARP

Generic Attribute Registration Protocol (GARP) protocol is a general-purpose protocol that registers any network connectivity or membership-style information. GARP defines a set of devices interested in a given network attribute, such as VLAN or multicast address. When configuring GARP, ensure the following:

- The leave time must be greater than or equal to three times the join time.
- The leave-all time must be greater than the leave time.
- Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, the GARP application does not operate successfully.

To define GARP on the device:

1. Click **Advanced Setup > VLAN > GARP > GARP Parameters**. The *GARP Parameters Page* opens:

Figure 77: GARP Parameters Page

The screenshot shows the D-Link web interface for configuring GARP parameters. The navigation menu on the left includes System, Basic Setup, Advanced Setup, and WLAN. The 'Advanced Setup' menu is expanded to show 'VLAN' > 'GARP' > 'GARP Parameters'. The main content area displays a table with the following data:

#	Interface	Join Timer	Leave Timer	Leave All Timer	Edit
1	1	200	600	10000	
2	2	200	600	10000	
3	3	200	600	10000	
4	4	200	600	10000	
5	5	200	600	10000	
6	6	200	600	10000	
7	7	200	600	10000	
8	8	200	600	10000	
9	9	200	600	10000	
10	10	200	600	10000	
11	11	200	600	10000	
12	12	200	600	10000	

At the top of the table, there is a 'Copy from Entry Number' field and a 'to Entry Number(s)' field.

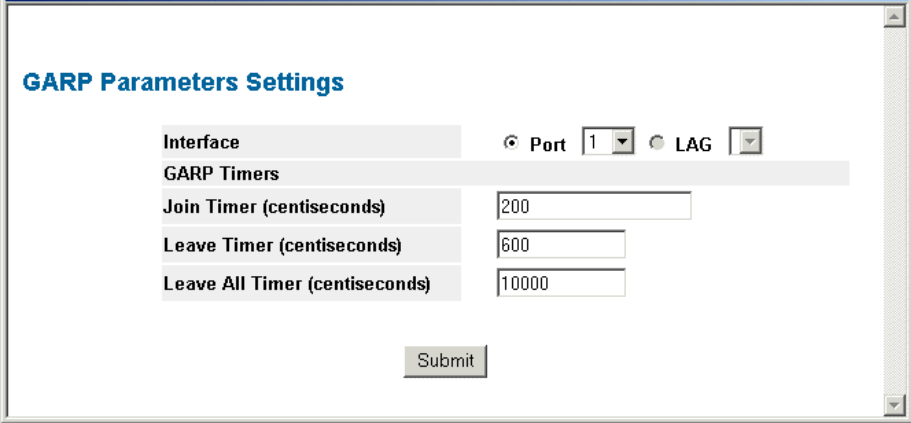
The *GARP Parameters Page* contains the following fields:

- **Unit No.** — Displays the stacking member for which the GARP parameters are displayed.
- **Copy from Entry Number** — Indicates the row number from which GARP parameters are copied.
- **To Row Number** — Indicates the row number to which GARP parameters are copied.
- **Interface** — Displays the port or LAG on which GARP is enabled.

- **Join Timer**— Indicates the amount of time, in centiseconds, that PDUs are transmitted. The default value is 20 centiseconds.
- **Leave Timer**— Indicates the amount of time lapse, in centiseconds, that the device waits before leaving its GARP state. Leave time is activated by a Leave All Time message sent/received, and cancelled by the Join message received. Leave time must be greater than or equal to three times the join time. The default value is 60 centiseconds.
- **Leave All Timer** — Indicates the amount of time lapse, in centiseconds, that all device waits before leaving the GARP state. The leave all time must be greater than the leave time. The default value is 1000 centiseconds.

2. Click  . The *GARP Parameters Settings Page* opens:

Figure 78: GARP Parameters Settings Page



GARP Parameters Settings

Interface Port 1 LAG

GARP Timers

Join Timer (centiseconds)

Leave Timer (centiseconds)

Leave All Timer (centiseconds)

3. Modify the *Interface*, *Join Timer (centiseconds)*, *Leave Timer (centiseconds)*, and *Leave All Timer (centiseconds)* fields.
4. Click . The GARP parameters are defined, and the device is updated.

Defining GVRP

GARP VLAN Registration Protocol (GVRP) is specifically provided for automatic distribution of VLAN membership information among VLAN-aware bridges. GVRP allows VLAN-aware bridges to automatically learn VLANs to bridge ports mapping, without having to individually configure each bridge and register VLAN membership. To define GARP. To define GVRP on the device:

1. Click **Advanced Setup > VLAN > GARP > GVRP Parameters**. The *GVRP Parameters Page* opens:

Figure 79: GVRP Parameters Page

The screenshot shows the D-Link web interface for the GVRP Parameters page. The left sidebar contains a navigation tree with 'VLAN' expanded and 'GVRP Parameters' selected. The main content area shows the 'GVRP Global Status' set to 'Disable'. Below this is a 'Copy from Entry Number' field and a 'to Entry Number(s)' field. A table lists 12 interfaces with their respective GVRP states and dynamic VLAN creation settings.

#	Interface	GVRP State	Dynamic VLAN Creation	GVRP Registration	Edit
1	1	Disabled	Enabled	Enabled	
2	2	Disabled	Enabled	Enabled	
3	3	Disabled	Enabled	Enabled	
4	4	Disabled	Enabled	Enabled	
5	5	Disabled	Enabled	Enabled	
6	6	Disabled	Enabled	Enabled	
7	7	Disabled	Enabled	Enabled	
8	8	Disabled	Enabled	Enabled	
9	9	Disabled	Enabled	Enabled	
10	10	Disabled	Enabled	Enabled	
11	11	Disabled	Enabled	Enabled	
12	12	Disabled	Enabled	Enabled	

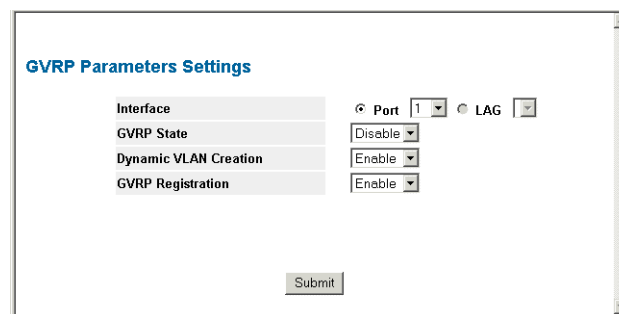
The *GVRP Parameters Page* is divided into port and LAG parameters. The field definitions are the same. The *GVRP Parameters Page* contains the following fields:


- **Unit No.** — Displays the stacking member for which the GVRP parameters are displayed.
- **GVRP Global Status** — Indicates if GVRP is enabled on the device. The possible field values are:
 - *Enable* — Enables GVRP on the selected device.
 - *Disable* — Disables GVRP on the selected device.
- **Copy from Entry Number** — Indicates the row number from which GARP parameters are copied.
- **To Row Number** — Indicates the row number to which GARP parameters are copied.
- **Interface** — Displays the port on which GVRP is enabled.
- **GVRP State** — Indicates if GVRP is enabled on the port. The possible field values are:
 - *Enable* — Enables GVRP on the selected port.
 - *Disable* — Disables GVRP on the selected port.

- **Dynamic VLAN Creation** — Indicates if Dynamic VLAN creation is enabled on the interface. The possible field values are:
 - *Enable* — Enables Dynamic VLAN creation on the interface.
 - *Disable* — Disables Dynamic VLAN creation on the interface.
- **GVRP Registration** — Indicates if VLAN registration through GVRP is enabled on the device. The possible field values are:
 - *Enable* — Enables GVRP registration on the device.
 - *Disable* — Disables GVRP registration on the device.

2. Click  . The *GVRP Parameters Settings Page* opens:

Figure 80: GVRP Parameters Settings Page



3. Define the *GVRP State*, *Dynamic VLAN Creation*, and *GVRP Registration* fields.
4. Click  . The GVRP Interface parameters are sent, and the device is updated.

Configuring Multicast VLANs

Network Manager can enhance Multicast TV services by catapulting networking into the next generation of IT services by combining cable television, VoIP, and high speed inter-net connections via a single cable. Triple Play service ensure that Layer 2 isolation between subscribers remains intact.

Service provider packets sent to the subscriber arrive from the following VLAN types:

- Subscriber VLANs
- Multicast TV VLANs

Each subscriber on a network maintains a Customer Premise Equipment Multi-Connect (CPE MUX) box. The MUX boxes directs network traffic from uplink ports to MUX access ports. MUX access ports are based on VLAN tags located in packet headers. Service provider's packets are tagged twice. Each packet has an internal tag and an external tag. The external tag indicates if the packet arrived from a Multicast TV VLAN or from a subscriber's VLAN. The internal tag indicates the port within the VLAN to which the packet is addressed.

The VLAN tag identifies:

- The media service type, including:
 - Internet
 - TV
 - Phone
- The service provider

This section includes the following topics:

Defining VLAN Groups

VLAN groups increase network flexibility and portability. For example, network users grouped by MAC address can log on to the network from multiple locations without moving between VLANs.

VLANs can be grouped by MAC address, Subnets, and Protocols. Once a user logs on, the system attempts to classify the user by MAC address. If the user cannot be classified by MAC address, the system attempts to classify the user by Subnet. If the subnet classification is unsuccessful, the system attempts to classify the user by protocol. If the protocol classification is unsuccessful, the user is classified by PVID.

This section contains the following sections:

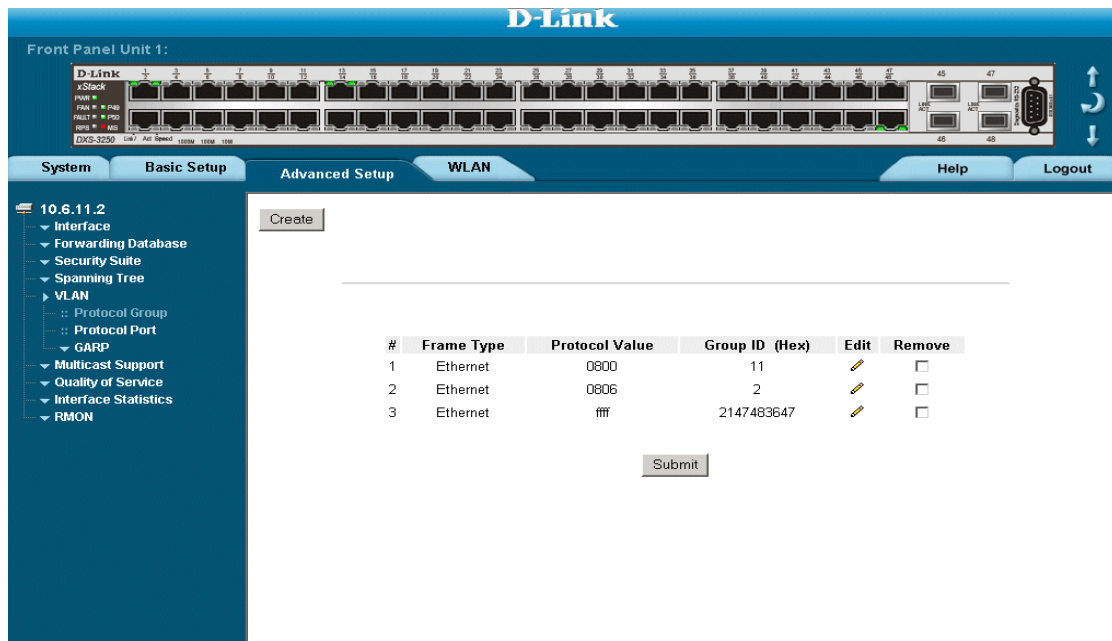
- Defining Protocol Based VLANs
- Defining VLAN Protocol Ports

Defining Protocol Based VLANs

The *Protocol Group Page* contains information regarding protocol names and the VLAN Ethernet type. Interfaces can be classified as a specific protocol based interface. The classification places the interface into a protocol group. To define protocol based VLANs:

1. Click **Advanced Setup > VLAN > Protocol Group**. The *Protocol Group Page* opens:

Figure 81: Protocol Group Page

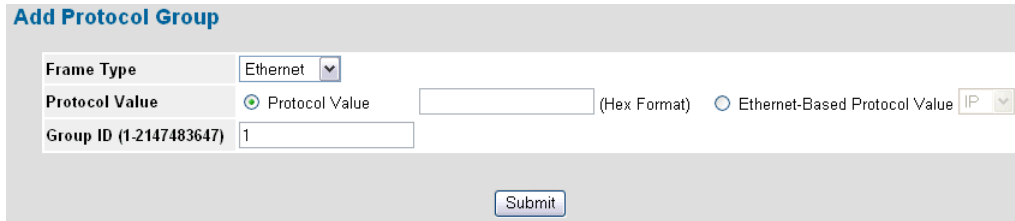


The *Protocol Group Page* contains the following fields:

- **Frame Type** — The packet type. Possible field values are **Ethernet**, **RFC1042**, and **LLC Other**.
- **Protocol Value** — User-defined protocol name.
- **Group ID** — ID number assigned to frames containing specified protocol value The possible field range is 1 - 2147483647.
- **IP Address** – Defines the IP address assigned to the VLAN group.

- **Prefix** – Defines the IP address's prefix. The possible field range is 0-32.
2. Click **Create**. The *Add Protocol Group* opens.

Figure 82: Add Protocol Group



The screenshot shows a web interface titled "Add Protocol Group". It contains three main input fields: "Frame Type" with a dropdown menu set to "Ethernet"; "Protocol Value" with a radio button selected for "Protocol Value" and an empty text box, and another radio button for "Ethernet-Based Protocol Value" with a dropdown menu set to "IP"; and "Group ID (1-2147483647)" with a text box containing the number "1". A "Submit" button is located at the bottom center of the form.

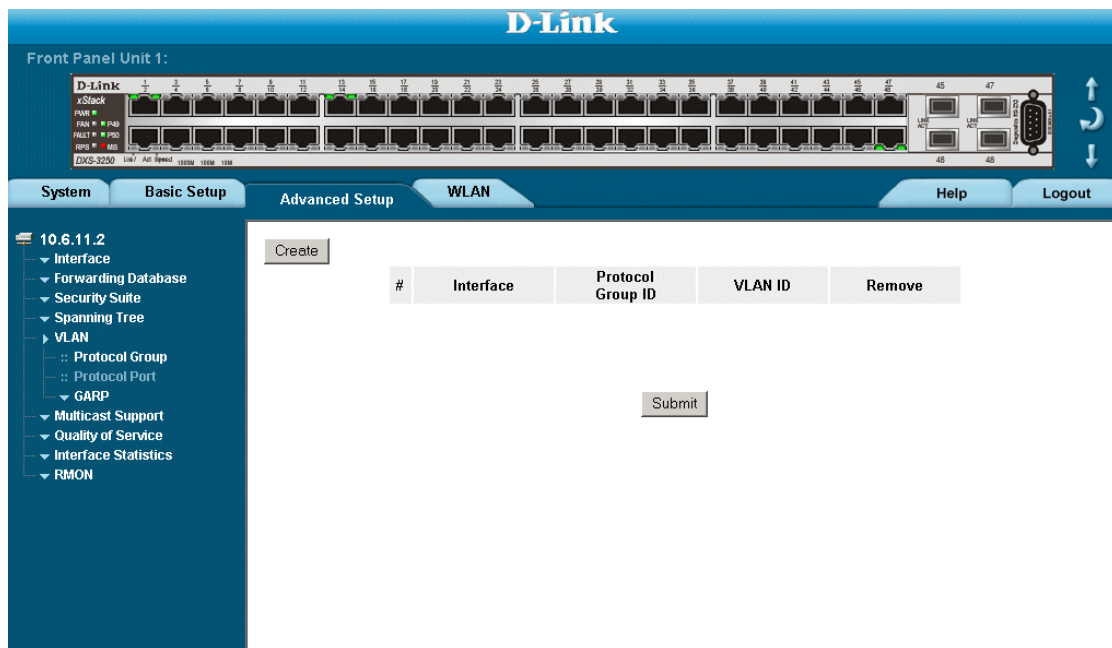
3. Define the fields.
4. Click **Submit**. The Protocol based VLAN group is defined, and the device is updated.

Defining VLAN Protocol Ports

The Protocol Group Page adds interfaces to Protocol groups. To define VLAN protocol ports:

1. Click **Advanced Setup > VLAN > Protocol Port**. The *VLAN Protocol Port Page* opens.

Figure 83: VLAN Protocol Port Page



The *VLAN Protocol Port Page* contains the following fields:

- **Interface** - Indicates the interfaces to which the protocol group is added. The possible field values are:
- **Protocol Group ID** – Defines the Protocol group ID to which the interface is added. Protocol group IDs are defined in the Protocol Group Table.
- **VLAN ID (1-4095)** – Attaches the interface to a user-defined VLAN ID. The VLAN ID is defined on the Create a New VLAN page. Protocol ports can either be attached to a VLAN ID or a VLAN name.
- **Remove** – Removes the port assignment from a VLAN or protocol group. The possible field values are:
 - *Checked* – Removes the selected interface from the protocol group.
 - *Unchecked* – Maintains the interface within the protocol group

2. Click . The *VLAN Protocol Port Setting Page* opens.

Figure 84: VLAN Protocol Port Setting Page

Add Protocol Port

Interface	<input checked="" type="radio"/> Port <input type="text" value="1"/>	<input type="radio"/> LAG <input type="text" value=""/>
Group ID	<input type="text" value=""/>	
VLAN ID	<input checked="" type="radio"/> <input type="text" value="1"/>	<input type="radio"/> <input type="text" value=""/>
VLAN Name	<input type="text" value=""/>	


3. Define the fields.
4. Click . The Protocol based VLAN port is defined, and the device is updated.
5. Click . The *Protocol Group Settings Page* opens:

Figure 85: Protocol Group Settings Page

Protocol Group Settings

Frame Type	Ethernet
Protocol Value	1193
Group ID (Hex)	<input type="text" value="1"/>

6. Define the fields.
7. Click . The GVRP Interface parameters are sent, and the device is updated.

Section 12. Defining WLAN

A *Wireless Local Area Network (WLAN)* is a technology that provides network services using radio waves. WLAN provides wireless network service connections to all users within a defined service area. D-Link DXS3200/DWS3200 product line contains a wired side, with one or more access points. WLAN users are connected to the network via the access points.

D-Link WLAN feature requires a licence key. The DWS series devices are preconfigured with a license for 10 access points, however, the DXS series devices require a license key. For more information about obtaining a 10-APs or 25APs licences key, contact Sales Department for how to purchase a wireless license key. Please have the MAC address of the switch(es) that you wish to upgrade handy as this information is required for wireless upgrade.

The D-Link DXS-3200 series provides a total solution to wireless networking. Wireless networking provides greater flexibility and freedom for network users.

This section includes the following topics:

- Defining WLAN System Properties
- Defining WLAN Access Points
- Configuring WLAN Radio Settings
- Viewing WLAN Statistics

Defining WLAN System Properties

This section contains information for configuring and viewing general WLAN parameters, and includes the following topics:

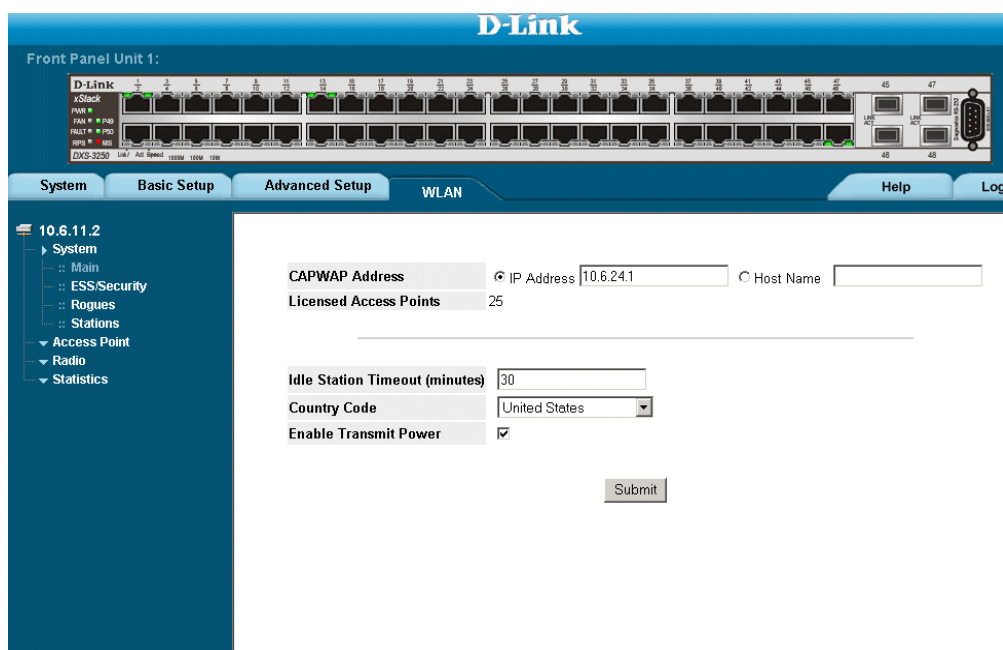
- Enabling WLAN
- Defining WLAN Security
- Viewing WLAN Rogues
- Viewing WLAN Stations

Enabling WLAN

The *WLAN Main Configuration Page* provides information for starting and enabling WLAN. To begin configuring the wireless network:

1. Click **WLAN > System > Main**. The *WLAN Main Configuration Page* opens:

Figure 86: WLAN Main Configuration Page



The *WLAN Main Configuration Page* contains the following fields:

- **CAPWAP Address** — Defines the *Control And Provisioning of Wireless Access Points* (CAPWAP) interface. The CAPWAP address is used to send traffic from access points to the controller. The possible field values are:
 - *IP Address* — Indicates the IP address that is assigned as the CAPWAP address.
 - *Host Name* — Indicates the host name to which the CAPWAP address is assigned.
- **Licensed Access Points** — Indicates the maximum number of licensed access points which can be connected to the device. The possible values are 10 - 25.

- **Idle Station Timeout** — Indicates the amount of time (minutes) that elapses before an idle station is timed out. Idle stations that are timed out must login to the system. The default value is 30 minutes.
 - **Country Code** — Defines the country code by which WLAN settings are set. The default is United States. For the complete list of country codes and settings, see *Appendix A, WLAN Country Settings*.
 - **Enable Transmit Power** — enables/disables global tx-power on the switch
2. Define the fields.
 3. Click . The wireless network is enabled, and the device is updated.

Defining WLAN Security

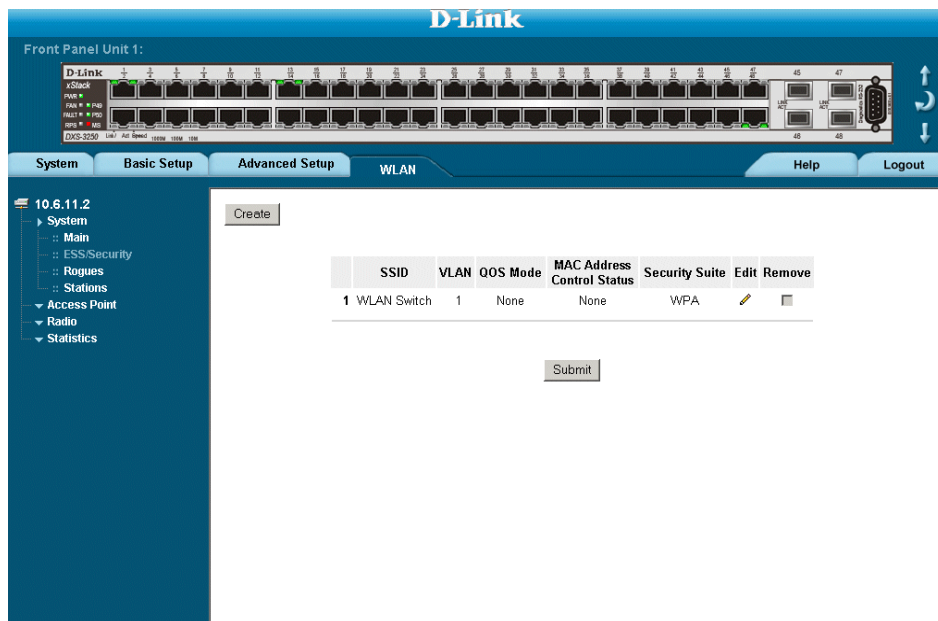
The *ESS Security Page* provides information for configuring *Extended Service Sets* (ESS). ESS are the primary method of organizing access points, security, and VLANs in a WLAN network. An ESS is a group of access points that share the same Service Set Identification (SSID).

APs announce their ESS membership by SSID parameter via Beacon frames. When stations roam between the same ESS APs, stations remain connected to the same wired network domain. Since the station remains in the same broadcast domain and IP subnet, the station retains the same IP address while roaming between the same ESS APs.

To configure ESS security:

1. Click **WLAN > System > ESS/Security**. The *ESS Security Page* opens:

Figure 87: ESS Security Page



The *ESS Security Page* contains the following fields:

- **SSID** — Displays the *Service Set Identifier* SSID for the ESS. SSIDs act as a password when a mobile device attempts to connect to the BSS. SSIDs differentiate between WLANs, therefore all access points and devices which comprise the specific WLAN must have the same SSID. Devices not providing a unique SSID are denied network access. Each SSID must be unique, and can contain up-to 32 characters.

- **VLAN** — Displays the VLAN mapped to the ESS. The default is VLAN 1.
- **QoS Mode** — Indicates if QoS is enabled for the ESS. The possible field values are:
 - *None* — Indicates that QoS is not enabled for ESS.
 - *WMM* — Indicates that QoS is enabled for Wi-Fi Multimedia (EDCF).
- **Mac Address Control Status** — Indicates if MAC Address can be filtered for the ESS. The possible field values are:
 - *Disabled* — Indicates that filtering MAC addresses for the ESS is disabled. Station MAC addresses can be located under the MAC Address Control List but no action is taken until the status is changed to Permit. This is the default value.
 - *Permit* — Enables filtering MAC addresses for the ESS. The system *accepts* packets only from wireless stations having specific MAC addresses located on the MAC Control List of a specific ESS ID.
 - *None* — Enables filtering MAC addresses for the ESS. The system *rejects* packets only from wireless stations having specific MAC addresses located on the MAC Control List of a specific ESS ID.
- **Security Suite** — Indicates if security suites are enabled for the ESS. Security Suites provide access authentication and encryption. Wireless stations can be assigned to a VLAN based on security suite supported by the station. The possible field values are:
 - *Secured* — Enables security suites in the ESS.
 - *Disabled* — Disables security suites in the ESS. This is the default value.
- **Remove** — Removes ESS. ESS number 1 cannot be removed. The possible field values are:
 - *Checked* — Removes the selected ESS.
 - *Unchecked* — Maintains the current ESS.

2. Click . The *Create ESS Configuration Page* opens

Figure 88: Create ESS Configuration Page

Create ESS Configuration

ESS Index 2

ESS Name (SSID)

* In order to config ESS you may use the ESS edit screen

In addition to the field in the *ESS Security Page*, the *Create ESS Configuration Page* contains the following additional fields:

- **Enable MAC Address Control** — Indicates if MAC address filtering is enabled on the ESS. MAC address can be filtered when the MAC address attempts to access the ESS. MAC address filtering protects the system from intruders, for example, Wi-Fi phones, which do not support WPA Address list is configured per ESS Central configuration in the switch for all APs in the ESS. The system consults the MAC address list when an station attempts connecting to the WLAN network. The possible field values are:
 - *Checked* — Enables filtering MAC addresses.
 - *Unchecked* — Disables filtering MAC addresses. This is the default value.
 - **MAC Address Control Action** — Indicates the action applied to packets with MAC addresses that have been filtered. The possible field values are:
 - *Deny* — Denies WLAN access to packets originating from the listed MAC address. This is the default value.
 - *Permit* — Permits WLAN access to packets originating from the listed MAC address.
3. Define the fields.
 4. Click . The ESS is defined, and the device is updated.

To edit ESS settings:

1. Click **WLAN > System > ESS/Security**. The *ESS Security Page* opens.
2. Click  . The *ESS Settings Page* opens:

Figure 89: ESS Settings Page

The screenshot shows the 'ESS Settings Page' configuration interface. At the top, there are three fields: 'ESS Name (SSID)' with the value 'WLAN Switch', 'Load Balancing' set to 'Disable', and 'QoS Mode' set to 'None'. Below these is a 'Type' section with several options: 'Open' (unchecked), 'WEP (802.1x Disabled)' (unchecked), 'WEP KEY' (radio buttons for 'Ascii' and 'Hex', with 'Ascii' selected), 'WEP (802.1x Enabled)' (unchecked), 'WPA' (checked, dropdown set to 'WPA'), 'WPA-PSK' (empty text field), 'WPA2' (unchecked, dropdown), and 'WPA2-PSK' (empty text field). To the right of these options are five 'VLAN' dropdown menus, all set to '1'. A note below states: 'The RADIUS server may override the VLAN assignment.' At the bottom, there is a 'MAC Address Control List' section with a 'Disable' dropdown. Below this is a list box (currently empty) and two buttons: 'Remove Selected MAC Address' and 'Add'. The 'Add' button has radio buttons for 'New MAC Address' (selected) and 'Select from List'.

In addition to the field in the *ESS Security Page*, the *ESS Settings Page* contains the following additional fields:

- **Load Balancing** — Indicates if load balancing type enabled for the wireless network. The possible field values are:
 - *Disable* — Indicates that load balancing is not enabled for the wireless network. If load balancing is not enabled, the system autonomously provides services to stations. However, this may result in uneven stations distribution between AP.
 - *At Association* — Enables load balancing with the associated station. Stations can be moved to an adjacent access point when load balancing is set to *At Association*. Services are assigned when the stations associate with the access point. If there is a access point which is not as busy, the station to access point association is rejected.
 - *Periodically* — Enables load balancing to occur at a fixed time period. Stations are moved to less busy APs in the ESS based on load balancing periods.
 - **Open** — Enables open system authentication without encryption.
 - **WEP (802.1x Disabled)** — Enables WEP but with 802.1x authentication disabled.
 - **WEP (802.1x Enabled)** — Indicates that *Wired Equivalent Privacy (WEP)* is the selected WLAN security method. WEP provides the same security level as a wired LAN. WEP encrypts data over radio waves during the packet transmission. WEP keys are 40 bit or 104 bit encryption keys.
 - **WEP Key** — Indicates the WEP encryption key type,. the possible field values are:
 - *ASCII* — Indicate the WEP key is in ASCII format.
 - *Hex* — Indicate the WEP key is in Hex format.
 - **WPA** — Indicates that *Wi-Fi Protected Access (WPA)* is the selected WLAN security method. WPA is based on WEP, but provides enhanced encryption using *Temporal Key Integrity Protocol (TKIP)*. In addition, WEP improves authentication using EAP. EAP ensures that only authorized network users access the network though secure encryption systems.
 - **WPA2** — Indicates that *Wi-Fi Protected Access 2 (WPA)* is the selected WLAN security method. WPA2 with 802.1x authenticates WLAN users and dynamically generate keys.
 - **WPA2-PSK** —Indicates that WPA2-PSK is the selected WLAN security method. WPA2-PSK improves system security by encrypting signals at a higher bitrates.
3. Define the fields.
 4. Click . The ESS settings are saved, and the device is updated.

Viewing WLAN Rogues

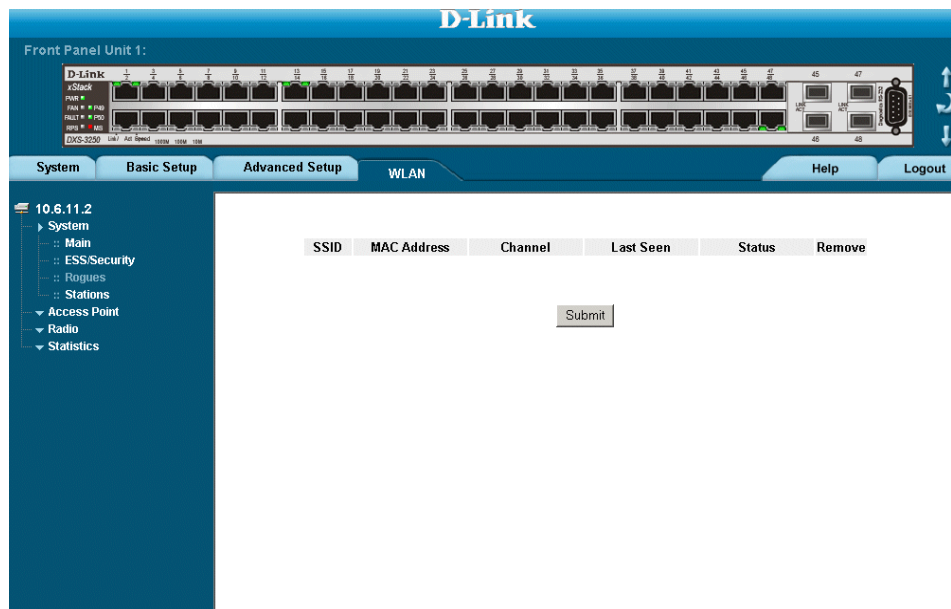
Rogue AP is an unauthorized Access Point that presents potential security threat. When connected to a corporate network, the AP roguis, as a result of security breaches, may allow access to corporate network for unauthorized parties.

The 32xx supports Rogue AP detection and Containment. The Rogue AP detection detects rogue AP and neutralizes it. This is done by APs that are connected to the 32xx switch and are continuously scanning WLAN frequencies. The AP may perform scanning while serving WLAN stations. It can also be configured to only perform scanning with no WLAN service. When the APs report detects, using the UI, neighbors to the WLAN switch, the detected neighbors in the rogue AP list can be displayed to the operator and allow to manually approve the neighbor ,or, initiate rogue AP containment.

The AP containment is done by disrupting the rogue BSS operation. The AP continuously sends de-authenticate frames to the rogue BSS. The frames are sent to a broadcast address and receive BSSID of the offender. As a result, stations associated with the rogue AP will be disconnected to avoid further potential damage. To view WLAN rogues:

- Click **WLAN > System >Rogues**. The *WLAN Rogues Page* opens:

Figure 90: WLAN Rogues Page



The *WLAN Rogues Page* contains the following fields:

- **SSID** — Displays the access point Service Set Identifier (SSID) associated with the rogue. The SSID is the name of the ESS to which the transceiver belongs.
- **MAC Address** — Displays the MAC address associated with the rogue WLAN device.
- **Channel** — Displays the access point channel used from which the rogue is transmitting.
- **Last Seen** — Indicates the last time the rogue was detected on wireless network.
- **Status** —Displays the Rogue status. The possible field values are:
 - *New* — Indicates that the SSID is newly discovered.

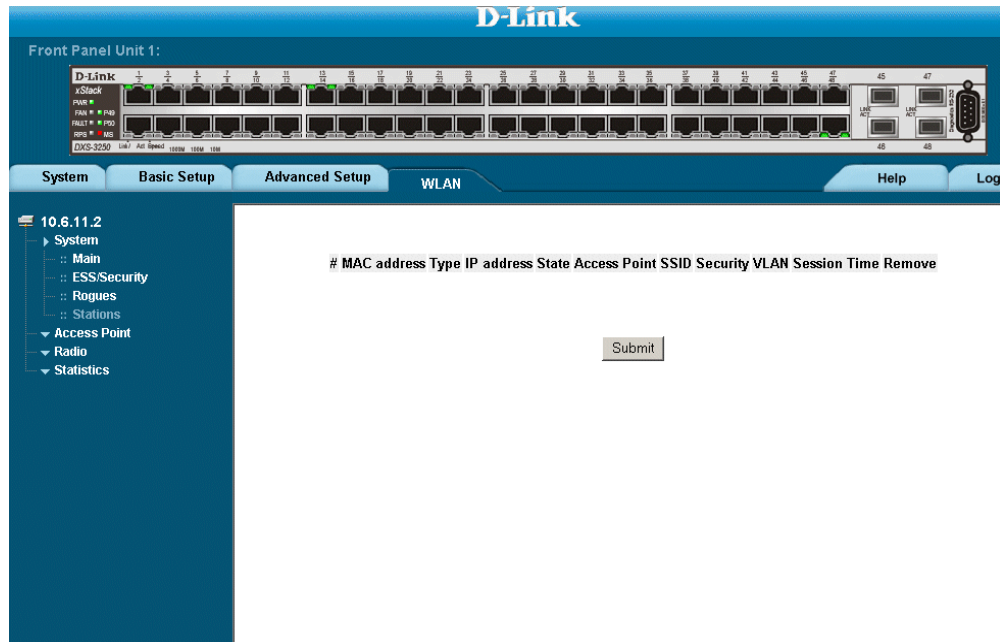
- *Mitigate* — Indicates that a disassociation instruction is sent for the SSID.
- *Known* — Indicates that the SSID is already known to the system.
- **Remove** — Removes detected rogue AP. The possible field values for:
 - *Checked* — Removes the selected rogue APs
 - *Unchecked* — Maintains the rogue APs.

Viewing WLAN Stations

The *Monitor WLAN Stations Page* provides information to network manager regarding the stations associated with the access point. To view the WLAN stations:

1. Click **WLAN > System > Stations**. The *Monitor WLAN Stations Page* opens:

Figure 91: Monitor WLAN Stations Page



The *Monitor WLAN Stations Page* contains the following fields:

- **MAC Address**— Displays the MAC address attached to the WLAN station.
- **Type** — Indicates the radio type associated to the station – can be either 802.11g or 802.11a.
- **IP Address**— Displays the WLAN station’s IP address.
- **State** — Indicates the station’s current status. The possible field values are:
 - *Associated* — Indicates that the station is currently associated with the wireless network but has not been authorized and authenticated.
 - *Authorized* — Indicates that the station is currently in the authorization process and waiting for authentication.
 - *Authenticated* — Indicates that the station has been authenticated.
- **Access Point** — Displays the access point associated with the wireless station.
- **SSID** — Displays the SSID associated with the wireless network.
- **Security** — Displays the SSID security type or types, associated with the wireless network.
- **VLAN** — Displays the security VLAN associated with the wireless network.
- **Session Time** — Indicates the amount of time the station has been connected to the access point.
- **Remove** — Disassociates the station and remove it from the list. The possible field values for:
 - *Checked* — Removes the selected WLAN stations

- *Unchecked* — Maintains the WLAN stations.

Defining WLAN Access Points

Access Points act as communication hubs for wireless networks. In addition, access points provide both encryption and bridging between 802.11 and ethernet points. Access points also extend the physical size of wireless networks. When several access points are grouped, they allow network users to roam. Access Points contain the parameters:

- **IP Addresses** — A unique IP address must be assigned to each Access Point.
- **Radio Channels** — Prevent access points from interfering with each other.
- **Transmit power** — Reduces the access point numbers and the system cost by maximizes the wireless range.
- **Service Set Identifier (SSID)** — Defines the user WLAN name. The SSID establishes and maintains wireless connectivity.
- **Data Rate** — Indicates the rate at which data is transferred. The default wireless data rates are 1, 2, 5.5, and 11Mbps. The data rate can help ensure the link quality between the client device and the access point.
- **Beacon Interval** — Indicates the access point beacon transmission rates. For example, if the interval is set to 20ms, then 20 beacons are sent per second.
- **Request-to-Send (RTS)/ Clear-to-Send (CTS)** — Reduces collisions when multiple stations are within a specific common access point range but outside range of each other.
- **Encryption** — Encrypts WLAN data packets.
- **Authentication** — Provides authentication via a RADIUS server for access points.

The farther a device is from the access point determines the strength of the signal the device receives. The system supports up-to 25 simultaneous access points. Each access point supports up-to 50 stations. This section includes the following topics:

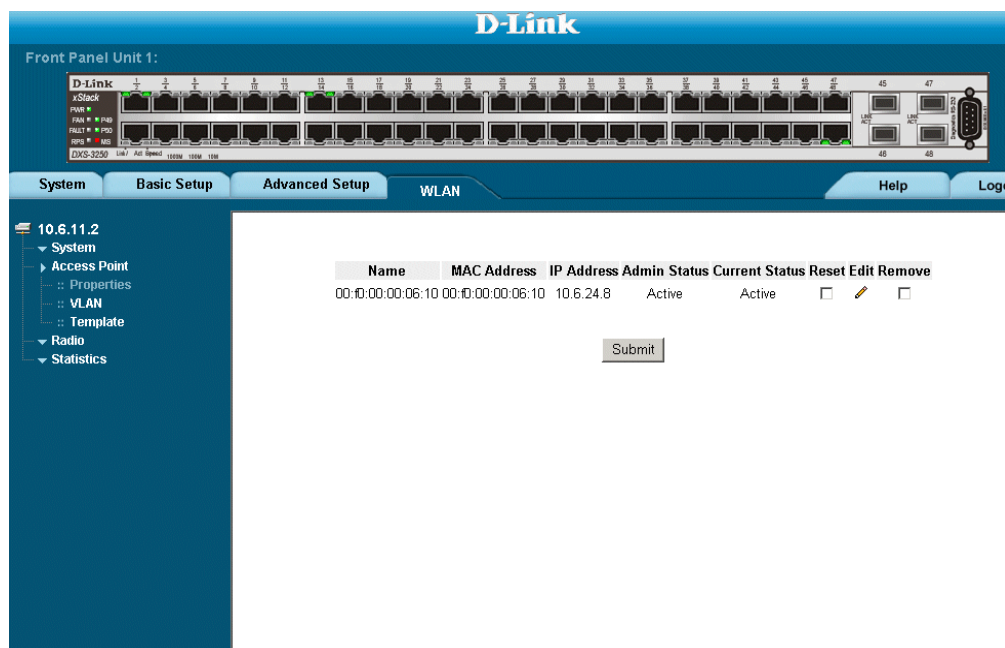
- Defining WLAN Access Point Properties
- Configuring WLAN VLANs
- Configuring WLAN Template Settings

Defining WLAN Access Point Properties

The *WLAN Access Point Properties Page* displays information regarding the currently configured WLAN stations, including the SSID, the access point MAC address, the current access point status, and the discovery time. Ensure that the *Wireless Controller Software (WCS)* has been activated. To view the WLAN access point properties:

1. Click **WLAN > Access Point > Properties**. The *WLAN Access Point Properties Page* opens:

Figure 92: WLAN Access Point Properties Page



The *WLAN Access Point Properties Page* contains the following fields:

- **Name** — Displays the user-defined access point name.
- **MAC Address** — Displays the MAC Address assigned to the access point.
- **IP Address** — Displays the IP Address assigned to the access point.
- **Admin Status** — Displays the selected access point's administration status. The possible field values are:
 - *Active* — Indicates that the access point is currently active.
 - *Not Active* — Indicates that the AP has not been accessed.
- **Current Status** — Displays the selected access point transceiver's status. The possible field values are:
 - *Discovered* — Indicates that the access point was discovered, but was not activated by the user.
 - *Activating* — Indicates the access point is currently being activated.
 - *Initializing* — Indicates the access point transceiver's is currently active.
 - *Error* — Indicates that a error has occurred at the access point link.
 - *No Connection* — Indicates that there is not currently a connection with the access point.
- **Reset** — Resets WLAN access points. The possible field values are:
 - *Checked* — Resets the selected access points.

- *Unchecked* — Maintains the access points.
- **Remove** — Removes access points. The possible field values are:
 - *Checked* — Removes the selected access point.
 - *Unchecked* — Maintains the current access points.

Adding a New Access point


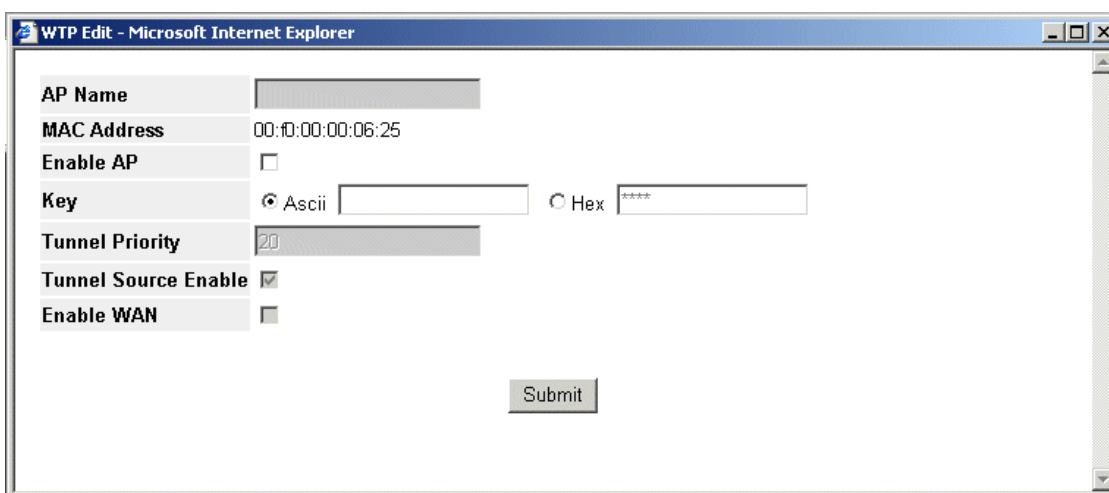
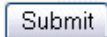
1. Connect the AP to the switch. The switch discovers the AP.
2. Click  . The *WTP edit* screen opens:

Figure 93: WTP Edit Screen



The *WTP Edit* screen contains the following fields:

- **AP Name** — Indicates the AP name (Max. 32 alphanumeric symbols)
- **Enable AP** — Enables/Disables the AP
- **Key** — Indicates the WEP encryption key type, the possible field values are:
 - *ASCII* — Indicates the WEP key is in ASCII format.
 - *Hex* — Indicates the WEP key is in Hex format.
- **Tunnel Priority** — Used to configure the AP priority for VLAN tunneling.
- **Tunnel Source Enable** — Indicates that AP is enabled as a VLAN source via a tunnel.
- **Enable WAN** — Accommodates certain timing constraints in the communication to a remotely connected AP separated by a WAN link or the Internet. To disable WAN support, use the no form of this command..

3. Select the Enable AP check box.
4. Select the key type.
5. Click  . The AP is activated.

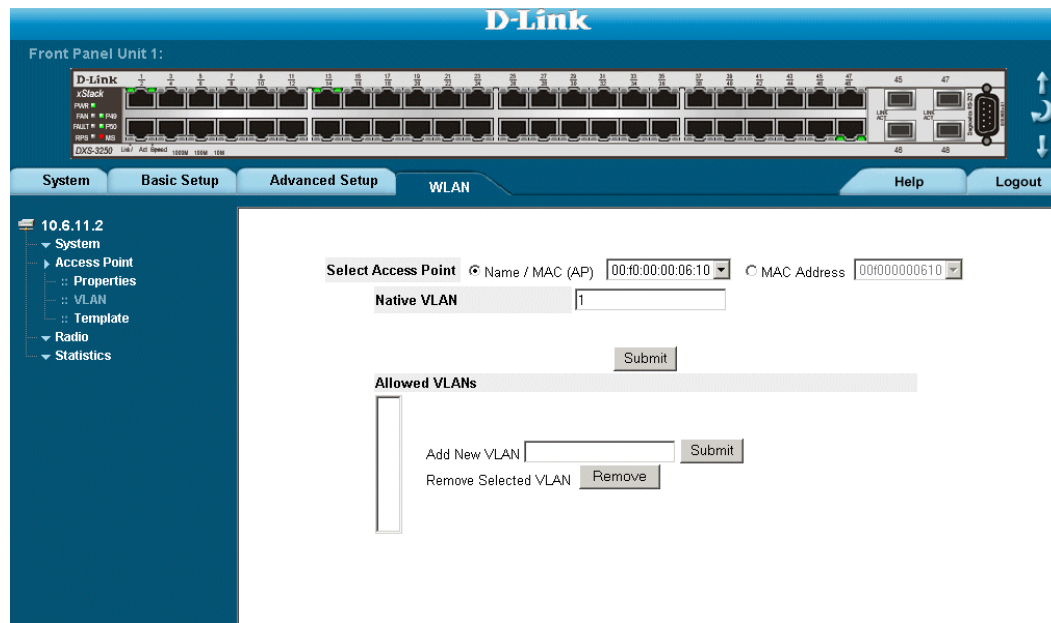
The WTP Edit Screen is also used for editing existing APs.

Configuring WLAN VLANs

The *WLAN Access Point VLANs Page* allows network managers to configure VLANs from access points. The switch provides VLAN ID of the station. The AP VLAN ID is stored per station basis in the AP tags frames. To define WLAN VLANs:

1. Click **WLAN > Access Point > VLAN**. The *WLAN Access Point VLANs Page* opens:

Figure 94: WLAN Access Point VLANs Page



The *WLAN Access Point VLANs Page* contains the following fields:

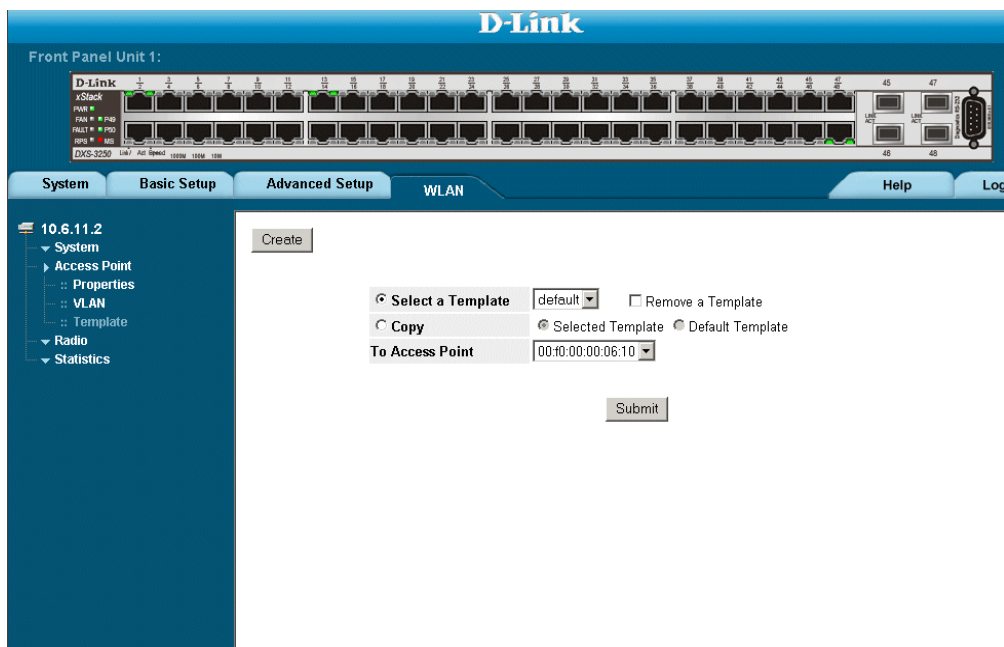
- **Select Access Point** — Contains a list of either the user-defined access points or the MAC address assigned to wireless networks. The possible field values.
 - *Name (AP)* — Contains the access points which can be assigned to a WLAN VLAN.
 - *Mac Address* — Contains the MAC Address which can be assigned to a WLAN VLAN.
 - **Native VLAN** — Defines the VLAN to which the access port or MAC address is defined.
 - **Add New VLAN** — Adds a new VLAN to the wireless network.
 - **Remove Selected VLAN** — Removes a VLAN from the wireless network.
2. Select the access point type.
 3. Define the Native VLAN field.
 4. Remove or Add VLANs using the arrows.
 5. Click . The WLAN VLAN is defined, and the device is updated.

Configuring WLAN Template Settings

The WLAN Templates Page allows network managers to define WLAN templates. Templates contains the Basic Service Set parameters, and can be applied to access points. To define WLAN templates:

1. Click **WLAN > Access Points > Templates**. The WLAN Templates Page opens:

Figure 95: WLAN Template Page



The *WLAN Template Page* contains the following fields:

- **Select a Template** — Contains a list of user-defined WLAN templates which can be applied to an access points. WLAN template names can contain up-to 32 characters.
- **Remove a Template** — Removes user-defined WLAN templates. The possible field values are:
 - *Checked* — Removes the selected WLAN template.
 - *Unchecked* — Maintains the selected WLAN template. This is the default value.
- **Copy** — Copies a previously defined WLAN template to a selected access point. The possible field values are:
 - *Selected Template* — Indicates that a user-defined template is applied to the access point.
 - *Default Template* — Indicates that the default template is applied to the access point.
- **To access point** — Copies the template to the selected access point.

2. Click **Create**. The *Create WLAN Template Page* opens:

Figure 96: Create WLAN Template Page

Template Name	<input type="text"/>
Enable Wide Area Support	<input type="checkbox"/>
Enable Console Logging	<input type="checkbox"/>
Default L2 Vlan	<input type="text" value="0"/>
Enable Tunnel	<input type="checkbox"/>

The *Create WLAN Template Page* contains the following fields:

- **Template Name** — Defines the WLAN template name. Template names can contain up-to 32 characters.
 - **Enable Wide Area Support** — Enables using remote access points which are connect by Wide Area Networks (WAN) or the internet. The possible field values are:
 - *Checked* — Enable WAN support.
 - *Unchecked* — Disables WAN support. This is the default value.
 - **Enable Console Logging** — Indicates that recording WLAN events in the console log is enabled. The possible field values are:
 - *Checked* — Enables logging WLAN events.
 - *Unchecked* — Disables logging WLAN events. This is the default value.
 - **Default L2 VLAN** — Defines the Layer 2 default VLAN.
 - **Enable Tunnel** — Enables using an access point in a VLAN. The possible field values are:
 - *Checked* — Enables using an access point in a VLAN.
 - *Unchecked* — Disables using an access point in a VLAN. This is the default value.
3. Define the *Template Name*, *Enable Wide Area Support*, *Enable Console Logging*, *Default L2 VLAN*, and *Enable Tunnel* fields.
 4. Click . The template is created, and the device is updated.

Configuring WLAN Radio Settings

Access Points can have up-to two radio interfaces. However, each radio interface is configured and controlled separately. Radio interfaces inherit the common configuration parameters from the ESS configuration. This section contains information for defining WLAN Radio settings, and includes the following topics:

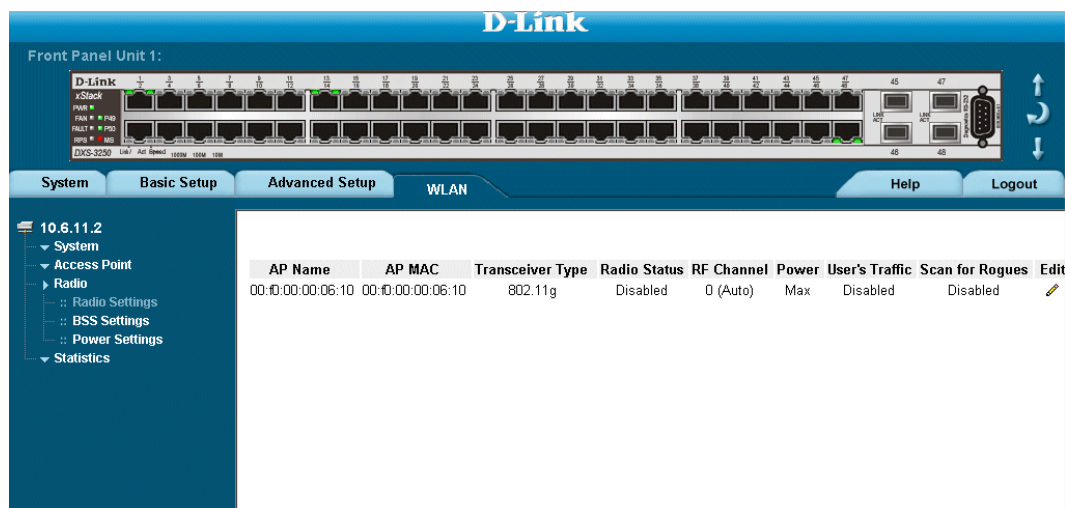
- Defining WLAN Radio Settings
- Defining BSS Settings
- Defining WLAN Power Settings

Defining WLAN Radio Settings

IWLAN communications are transmitted via radio waves. The *Radio Settings Page* allows network managers to configure WLAN Radio settings for transmitting WLAN communications. To configure the:



1. Click **WLAN > Radio > Radio Settings**. The *Radio Settings Page* opens:

Figure 97: Radio Settings Page



The *Radio Settings Page* contains the following fields:

- **AP Name** — Display the specific access point to which the radio settings are assigned.
- **AP MAC** — Display the MAC address assigned to the access point.
- **Transceiver Type** — Indicates the radio transceiver type. The possible field values are:
 - *A* — Indicates the radio type is 802.1a.
 - *G* — Indicates the radio type is 802.1g.
- **Radio Status** — Indicates the Radio transmitter/transceiver status. The possible field values are:
 - *Enabled* — Indicates that the interface radio is enabled.
 - *Disabled* — Indicates that the interface radio is disabled.
- **RF Channel** — Indicates the Radio Frequency channel from which the transmissions are sent.
- **Power** — Indicates the country's power setting. For a complete listing of the each country's power regulations, see *Appendix A, WLAN Country Settings*. The possible field values are:
 - *Max* — Defines a Maximum power setting relative to the selected country's device power regulations.

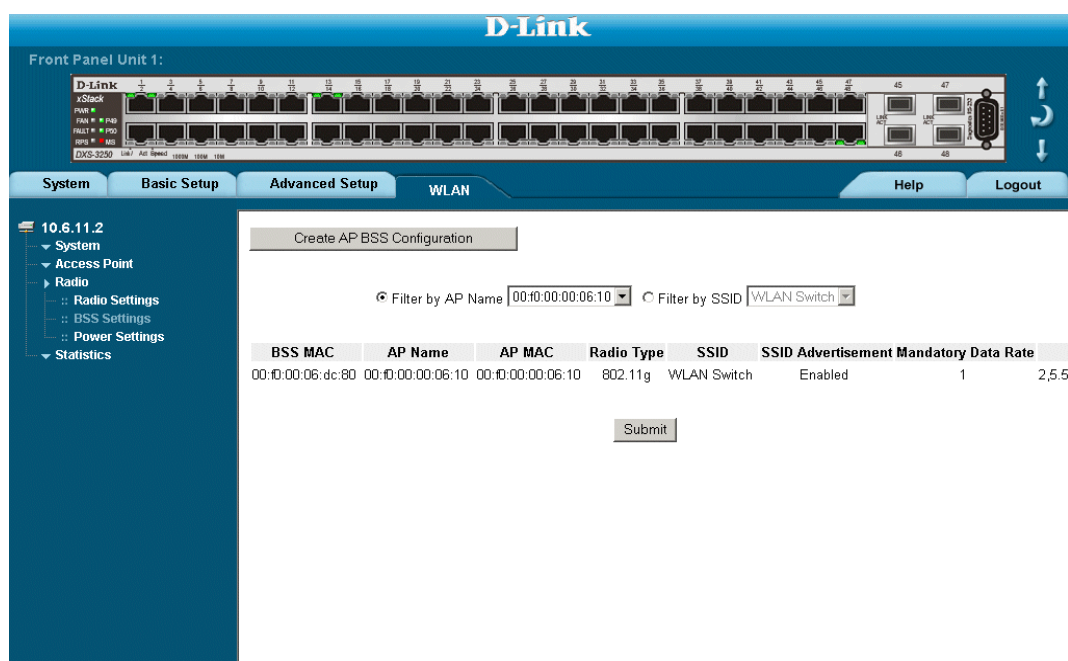
- *Half* — Defines half of the maximum power relative to the selected country's device power regulations.
 - *Quarter* — Defines a quarter of the maximum power relative to the selected country's device power regulations.
 - *Eighth* — Defines an eighth of the maximum power relative to the selected country's device power regulations.
 - *Minimum* — Sets the power to the minimum power settings relative to the selected country's device power regulations.
 - **Auto Adjust Signal Strength** — Adjusts the transmit power of APs, so the signal strength heard at the second-closest access point is as close as possible to the target signal-strength configured by the wlan tx-power auto signal-strength global configuration command. Auto Transmit Power can be enabled only when rogue detection is enabled
 - **User's Traffic** — Determines if user traffic is enabled for this radio. The possible field values are:
 - *Enable* — Enables user traffic on the radio frequency. This is the default value.
 - *Disable* — Disables user traffic on the radio frequency.
 - **Scan for Rogues** — Indicates the rogue scanning status. The possible field values are:
 - *Enabled* — Indicates that rogue scanning is enabled.
 - *Disabled* — Indicates that rogue scanning is disabled.
2. Click  . The *Modify Radio Setting Page* opens.
 3. Modify the fields.
 4. Click  . The radio settings are modified, and the device is updated.

Defining BSS Settings

The *BSS Settings Page* allows network managers to define *Basic Service Sets* (BSS). BSS are a set of stations that directly communicate with each other. The logical connection between the WLAN stations determines a set, not the station location. To configuring BSS:

1. Click **WLAN > Radio > BSS Settings**. The *BSS Settings Page* opens:

Figure 98: BSS Settings Page



The *BSS Settings Page* contains the following fields:

- **Filter by AP name** — Filters the Basic Service Set by access point name.
- **Filter by SSID** — Filters the Basic Service set by SSID.
- **BSS MAC** — Displays the BSS MAC address assigned access point.
- **AP Name** — Displays the access point attached to the BSS.
- **AP MAC** — Displays the AP MAC address assigned access point.
- **Radio Type** — Displays the radio type attached to the BSS. The possible field values are:
 - *802.11a* — Indicates the radio type attached to the BSS is an 802.1a radio.
 - *802.11g* — Indicates the radio type attached to the BSS is an 802.1g radio.
- **SSID** — Displays the SSID.
- **SSID Advertisement** — Indicates if advertising SSID in beacons is enabled. The possible field values are:
 - *Enable* — Enables advertising SSID in beacons, and responding to SSID probe requests. This is the default value.
 - *Disable* — Disables SSID advertisement requests.
- **Mandatory Data Rate** — Displays the rate at which non-Unicast traffic must be forwarded in the WLAN. Each rate is represented in Kbps. The possible field values are:

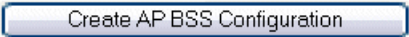
- 1 — Indicates non-Unicast traffic is transferred at 1000 Kbps.
 - 2 — Indicates non-Unicast traffic is transferred at 2000 Kbps.
 - 5.5 — Indicates non-Unicast traffic is transferred at 5500 Kbps.
 - 6 — Indicates non-Unicast traffic is transferred at 6000 Kbps.
 - 9 — Indicates non-Unicast traffic is transferred at 9000 Kbps.
 - 11 — Indicates non-Unicast traffic is transferred at 11000 Kbps.
 - 12 — Indicates non-Unicast traffic is transferred at 12000 Kbps.
 - 18 — Indicates non-Unicast traffic is transferred at 18000 Kbps.
 - 24 — Indicates non-Unicast traffic is transferred at 24000 Kbps.
 - 36 — Indicates non-Unicast traffic is transferred at 36000 Kbps.
 - 48 — Indicates non-Unicast traffic is transferred at 48000 Kbps.
 - 54 — Indicates non-Unicast traffic is transferred at 54000 Kbps.
 - **Optional Data Rate**— Indicates the rate at which Unicast traffic is forwarded. The possible field values are:
 - 1 — Indicates Unicast traffic is transferred at 1000 Kbps.
 - 2 — Indicates Unicast traffic is transferred at 2000 Kbps.
 - 5.5 — Indicates Unicast traffic is transferred at 5500 Kbps.
 - 6 — Indicates Unicast traffic is transferred at 6000 Kbps.
 - 9 — Indicates Unicast traffic is transferred at 9000 Kbps.
 - 11 — Indicates Unicast traffic is transferred at 11000 Kbps.
 - 12 — Indicates Unicast traffic is transferred at 12000 Kbps.
 - 18 — Indicates Unicast traffic is transferred at 18000 Kbps.
 - 24 — Indicates Unicast traffic is transferred at 24000 Kbps.
 - 36 — Indicates Unicast traffic is transferred at 36000 Kbps.
 - 48 — Indicates Unicast traffic is transferred at 48000 Kbps.
 - 54 — Indicates Unicast traffic is transferred at 54000 Kbps.
2. Click . The *Create AP BSS Configuration Page* opens:

Figure 99: Create AP BSS Configuration Page

AP MAC	00f000000615
Radio Type	802.11a
SSID	Gili_R
Enable BSS	<input checked="" type="checkbox"/>
Enable SSID Advertisement	<input checked="" type="checkbox"/>
Supported Data Rates	6 Optional
	9 Optional
	12 Optional
	18 Optional
	24 Optional
	36 Optional
	48 Optional
54 Optional	

3. Define the fields.

4. Click . The AP BSS configuration is saved, and the device is updated.

To modify BSS settings:

1. Click **WLAN > Configuration > Radio > BSS Settings**. The *BSS Settings Page* opens.

2. Click  . The *Edit BSS Settings Page* opens:

Figure 100: Edit BSS Settings Page

AP MAC	00:f0:00:00:06:15
Radio Type	802.11a
SSID	Gili_R
Enable BSS	<input checked="" type="checkbox"/>
Enable SSID Advertisement	<input checked="" type="checkbox"/>
Supported Data Rates	6 Mandatory
	9 Optional
	12 Optional
	18 Optional
	24 Optional
	36 Optional
	48 Optional
54 Optional	

In addition to the fields in the *BSS Settings* page, the *Create BSS Settings* page contains the following fields:

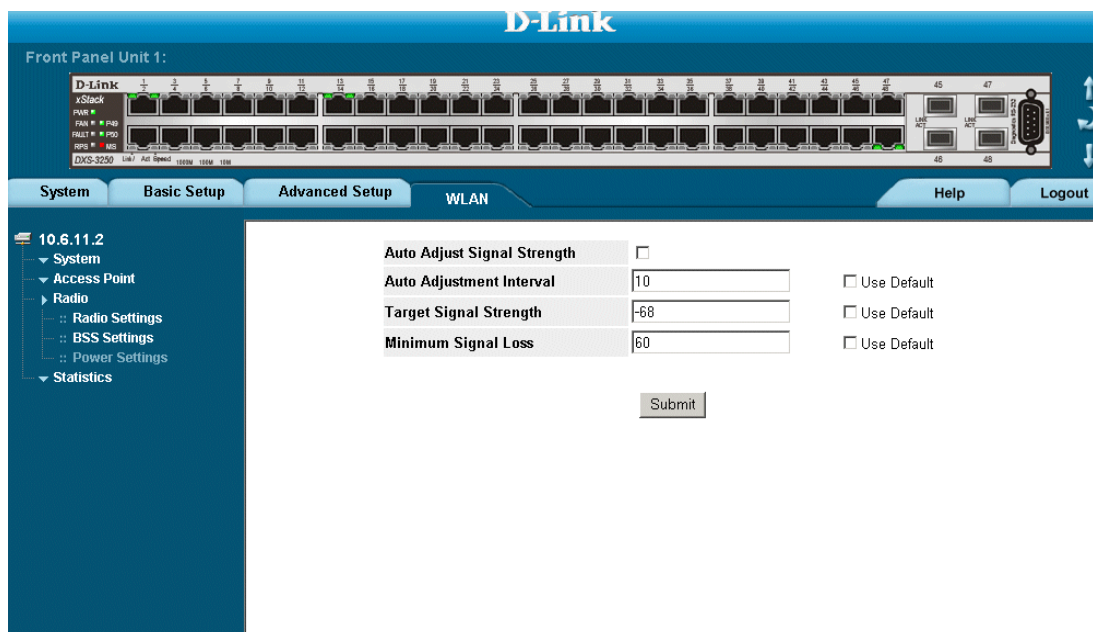
- **Enable SSID Advertisement** — Indicates if SSID advertisement is enabled.
 - **Supported Data Rates** — Indicates which data rates are supported, and in what capacity. The rates are in MBits per second and include the rates 6, 9, 12, 18, 24, 36, 48 and 54. The possible values are:
 - *Mandatory* — Rate must be supported.
 - *Optional* — Rate can be supported, but is not compulsory.
 - *Not Allowed* — Rate is not supported,
3. Modify the fields.
 4. Click . The BSS settings are saved, and the device is updated.

Defining WLAN Power Settings

The *WLAN Radio Power Settings Page* allows network managers to define WLAN radio power settings. To define WLAN radio power settings:

1. Click **WLAN > Radio > Power Settings**. The *WLAN Radio Power Settings Page* opens:

Figure 101: WLAN Radio Power Settings Page



The *WLAN Radio Power Settings Page* contains the following fields:

- **Auto Adjust Signal Strength** — Enables adjusting the target signal strength received by closest access point. The possible field values are:
 - *Checked* — Enables automatic signal adjustments.
 - *Unchecked* — Disables automatic signal adjustments.
- **Auto Adjustment Interval** — Reconfigures the automatic power transmissions time periods.
- **Use Default** — Enables using the default *Auto Adjustment Interval* value. The possible field values are:
 - *Checked* — Enables the device *Auto Adjustment Interval* adjustment default value.
 - *Unchecked* — Disables the device *Auto Adjustment Interval* adjustment default value.
- **Target Signal Strength** — Configure the target signal strength received by closest access point in *Decibel Miliwatts* (dBm). The possible field range is -40 - -80. The field default is -68.
- **Use Default** — Enables using the default *Target Signal Strength* value. The possible field values are:
 - *Checked* — Enables the device *Target Signal Strength* default value.
 - *Unchecked* — Disables the device *Target Signal Strength* default value.
- **Minimum Signal Loss** — Defines the signal range by which access points are defined as too close. This helps eliminates signal interference. The possible field range is -20 - -80. The field default is -60.
- **Use Default** — Enables using the default *Minimum Signal Loss* value. The possible field values are:
 - *Checked* — Enables the device *Minimum Signal Loss* default value.

- *Unchecked* — Disables the device *Minimum Signal Loss* default value.
2. Define the fields.
 3. Click . The WLAN power settings are saved, and the device is updated.

Viewing WLAN Statistics

This section contains information for viewing WLAN statistics, and includes the following topics:

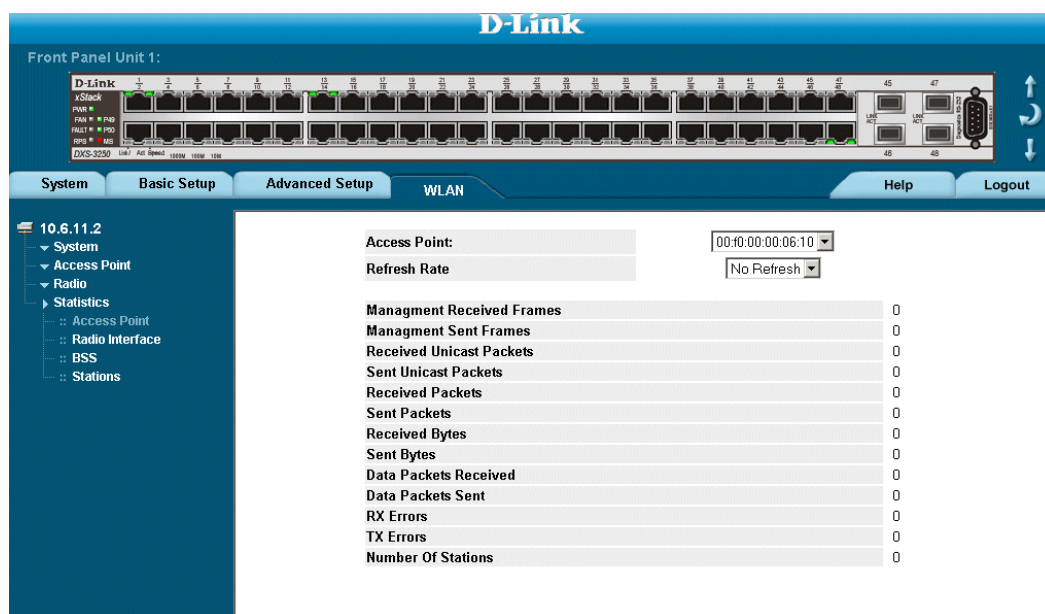
- Viewing Access Point Statistics
- Viewing Radio Interfaces Statistics
- Viewing BSS Statistics
- Viewing WLAN Stations

Viewing Access Point Statistics

The *WLAN Access Points Statistics Page* contains information for viewing and monitoring the WLAN Access points. To view access points information:

1. Click **WLAN > Statistics > Access Points**. The *WLAN Access Points Statistics Page* opens:

Figure 102: WLAN Access Points Statistics Page



The *WLAN Access Points Statistics Page* contains the following fields:

- **Access Point** — Contains a list of access points for which the WLAN statistics are displayed.
- **Refresh Rate** — Defines the amount of time that passes before the statistics are refreshed. The possible field values are:
 - *15 Sec* — Indicates that the statistics are refreshed every 15 seconds.
 - *30 Sec* — Indicates that the statistics are refreshed every 30 seconds.
 - *60 Sec* — Indicates that the statistics are refreshed every 60 seconds.
 - *No Refresh* — Indicates that the statistics are not refreshed.
- **Management Received Frames** — Displays the number of management packets that were received on the access point.

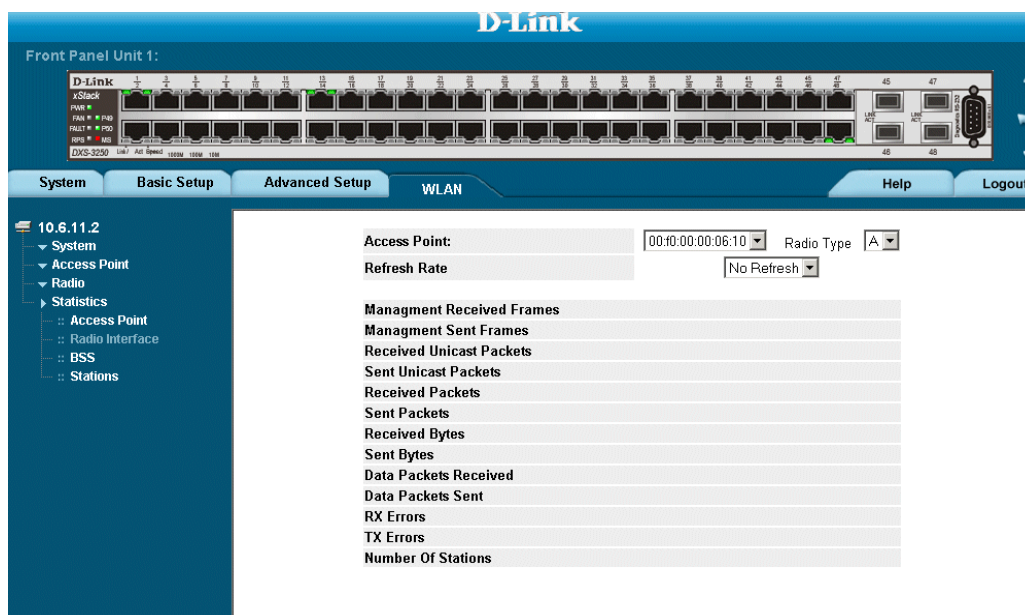
- **Management Sent Frames** — Displays the number of management packets that were sent from the access point.
 - **Received Unicast Packets** — Displays the number of Unicast frames that were received on the access point.
 - **Sent Unicast Packets** — Displays the number of Unicast frames that were sent from the access point.
 - **Received Packets** — Displays the number of packets that were received on the access point.
 - **Sent Packets** — Displays the number of sent that were sent from the access point.
 - **Received Bytes** — Displays the number of bytes that were received on the access point.
 - **Sent Bytes** — Displays the number of bytes that were sent from the access point.
 - **Data Packets Received** — Displays the number of data packets that were received on the access point.
 - **Data Packets Sent** — Displays the number of data that were sent from the access point.
 - **Rx Errors** — Displays the number of packets with errors that were sent from the access point.
 - **Tx Errors** — Displays the number of packets were with errors from the access point.
 - **Number of Stations** — Displays the number of stations attached to the access point.
2. Select a station and refresh time, the station statistics are displayed.

Viewing Radio Interfaces Statistics

The *WLAN Radio Interface Statistics Page* contains information for helping network administrators to manage radio transmission statistics. To open the *WLAN Radio Interface Statistics Page*:

1. Click **WLAN > Statistics > Radio Interface**. The *WLAN Radio Interface Statistics Page* opens:

Figure 103: WLAN Radio Interface Statistics Page



The *WLAN Radio Interface Statistics Page* contains the following fields:

- **Access Point** — Contains a list of access points for which the radio WLAN statistics are displayed.
- **Radio Type** — Displays the radio type. The possible field values are:
 - A — Indicates the radio type is 802.1a.
 - G — Indicates the radio type is 802.1g.
- **Refresh Rate** — Defines the amount of time that passes before the statistics are refreshed. The possible field values are:
 - 15 Sec—Indicates that the statistics are refreshed every 15 seconds.
 - 30 Sec—Indicates that the statistics are refreshed every 30 seconds.
 - 60 Sec—Indicates that the statistics are refreshed every 60 seconds.
 - No Refresh—Indicates that the statistics are not refreshed.
- **Management Received Frames** — Displays the amount of management packets received on the interface.
- **Management Sent Frames** — Displays the amount of management packets sent from interface.
- **Received Unicast Packets** — Displays the amount of Unicast packets received on the interface.
- **Sent Unicast Packets** — Displays the amount of Unicast packets sent from interface.
- **Received Packets** — Displays the amount of packets received on the interface.
- **Sent Packets** — Displays the amount of packets sent from interface.
- **Received Bytes** — Displays the amount of bytes received on the interface.

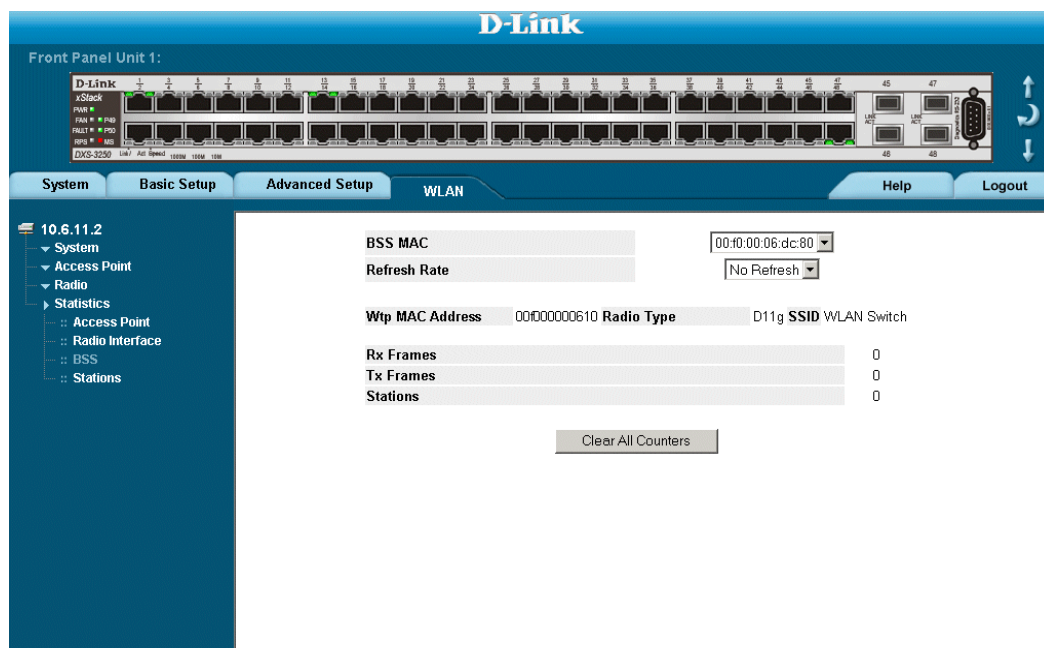
- **Sent Bytes** — Displays the amount of bytes sent from interface.
 - **Data Packets Received** — Displays the amount of management data packets received on the interface.
 - **Data Packets Sent** — Displays the amount of data packets sent from interface.
 - **Rx Errors** — Displays the number of packets with errors that were sent from the interface.
 - **Tx Errors** — Displays the number of packets were with errors from the interface.
 - **Number of Stations** — Displays the number of stations attached to the interface.
2. Select a station and refresh time, the station statistics are displayed.

Viewing BSS Statistics

The *BSS Information Page* allows network managers to monitor Basic Service Set activity. To view BSS statistics:

1. Click **WLAN > Monitor > BSS**. The *BSS Information Page* opens:

Figure 104: BSS Information Page



The *BSS Information Page* contains the following fields:

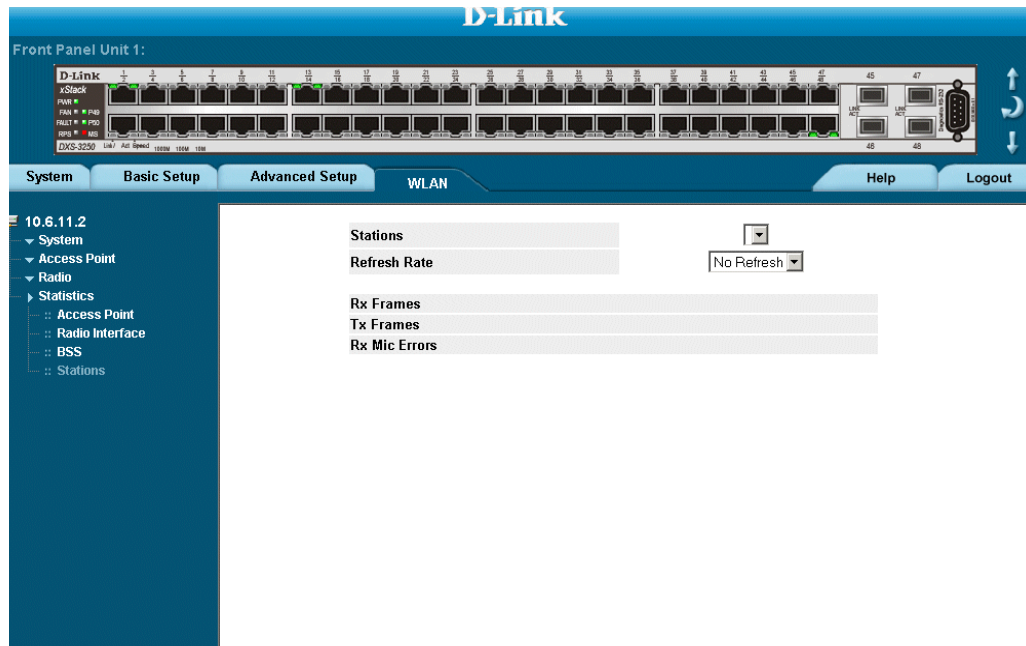
- **BSS MAC** — Indicates the Basic Service Set for which the WLAN information is displayed.
 - **Refresh Rate** — Defines the amount of time that passes before the statistics are refreshed. The possible field values are:
 - *15 Sec*—Indicates that the statistics are refreshed every 15 seconds.
 - *30 Sec*—Indicates that the statistics are refreshed every 30 seconds.
 - *60 Sec*—Indicates that the statistics are refreshed every 60 seconds.
 - *No Refresh*—Indicates that the statistics are not refreshed.
 - **Wtp MAC Address** — Displays the Wtp MAC address.
 - **Radio Type** — Displays the WLAN radio type.
 - **SSID** — Displays the SSID attached to the BSS.
 - **Rx Frames** — Displays the number of packets with errors that were sent from the interface.
 - **Tx Frames** — Displays the number of packets with errors from the interface.
 - **Stations** — Displays the number of stations attached to the BSS.
2. Select a station and refresh time, the station statistics are displayed.

Viewing WLAN Stations

The *WLAN Stations Statistics Page* contains statistics regarding WLAN stations. To view WLAN station statistics:

1. Click **WLAN > Statistics > Stations**. The *WLAN Stations Statistics Page* opens:

Figure 105: WLAN Stations Statistics Page



The *WLAN Stations Statistics Page* contains the following fields:

- **Stations** — Contains a drop-down list of the WLAN stations for which statistics can be displayed.
 - **Refresh Rate** — Defines the amount of time that passes before the statistics are refreshed. The possible field values are:
 - **15 Sec**—Indicates that the statistics are refreshed every 15 seconds.
 - **30 Sec**—Indicates that the statistics are refreshed every 30 seconds.
 - **60 Sec**—Indicates that the statistics are refreshed every 60 seconds.
 - **No Refresh**—Indicates that the statistics are not refreshed.
 - **Rx Frames**— Displays the number of packets received on the port.
 - **Tx Frames**— Displays the number of packets sent from the port.
 - **Rx Mic Errors** — Displays the number of MIC frames received on the port.
2. Select a station and refresh time, the station statistics are displayed.

Section 13. Configuring IP Information

This section provides information for defining device IP addresses, and includes the following topics:

- Configuring IP Interfaces
- Configuring Domain Name Servers

Configuring IP Interfaces

This section contains information for defining IP interfaces, and includes the following sections:

- Defining IP Addresses
- Defining Default Gateways
- Configuring DHCP
- Configuring ARP

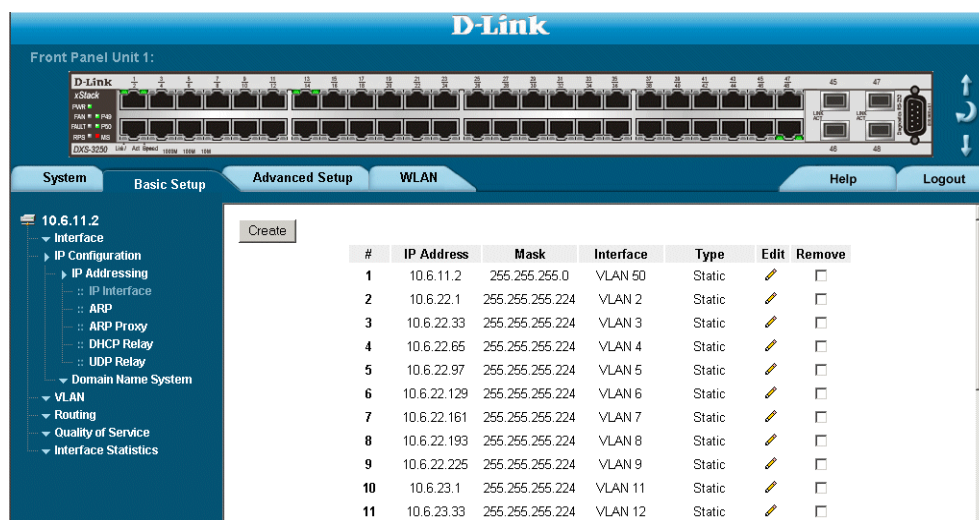
Defining IP Addresses

The *IP Interface Page* contains fields for assigning IP addresses. Packets are forwarded to the default IP when frames are sent to a remote network. The configured IP address must belong to the same IP address subnet of one of the IP interfaces.

To define an IP interface:

1. Click **Basic Setup > IP Configuration > IP Addressing > IP Interface**. The *IP Interface Page* opens:

Figure 106: IP Interface Page



The *IP Interface Page* contains the following fields:

- **IP Address** — Displays the currently configured IP address.
- **Mask** — Displays the currently configured IP address mask.
- **Interface** — Displays the interface used to manage the device.
 - *Dynamic* — Indicates that the IP address is dynamically created.
 - *Static* — Indicates the IP address is a static IP address.
- **Type** — Indicates if the IP address has been configured statically or added dynamically.
- **Remove** — Removes the selected IP address from the interface. The possible field values are:
 - *Checked* — Removes the IP address from the interface.
 - *Unchecked* — Maintains the IP address assigned to the Interface.

2. Click **Create**. The *Add IP Interface Page* opens:

Figure 107: Add IP Interface Page

Add IP Interface

Source IP Address

Network Mask

Prefix Length

Interface Port 1/1 LAG VLAN 1

Submit

3. Define the *Source IP Address*, *Network Mask* or *Prefix Length*, and *Interface* fields.
4. Click **Submit**. The IP configuration fields are saved, and the device is updated.

To modify an IP interface:


1. Click **Basic Setup > IP Configuration > IP Addressing > IP Interface**. The *IP Interface Page* opens.
2. Click . The *IP Interface Settings Page* opens:

Figure 108: IP Interface Settings Page

IP Interface Settings

IP Address

Network Mask

Prefix Length

Interface Port 1/1 LAG VLAN 1

Type

Submit

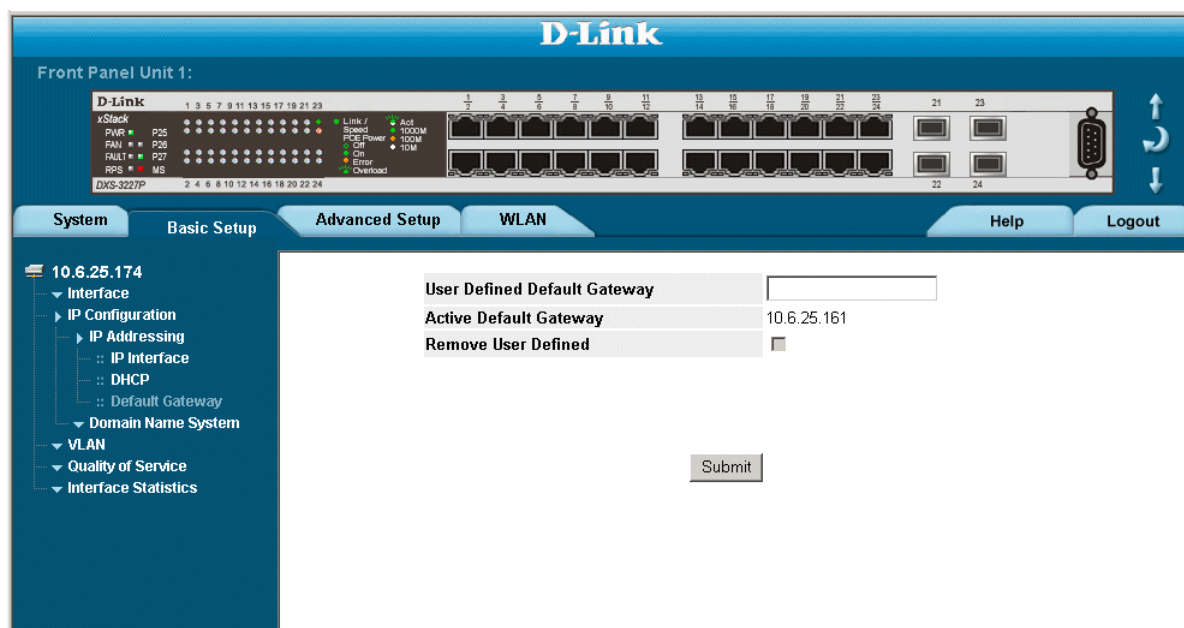
3. Modify the *Source IP Address*, *Network Mask* or *Prefix Length*, and *Interface* fields.
4. Click **Submit**. The IP Interface is modified, and the device is updated.

Defining Default Gateways

Packets are forwarded to the default IP when frames are sent to a remote network via the default gateway. The configured IP address must belong to the same subnet of one of the IP interfaces. To define a default gateway:

1. Click **Basic Setup > IP Configuration > IP Addressing > Default Gateway**. The *Default Gateway Page* opens:

Figure 109: Default Gateway Page



The *Default Gateway Page* contains the following fields:

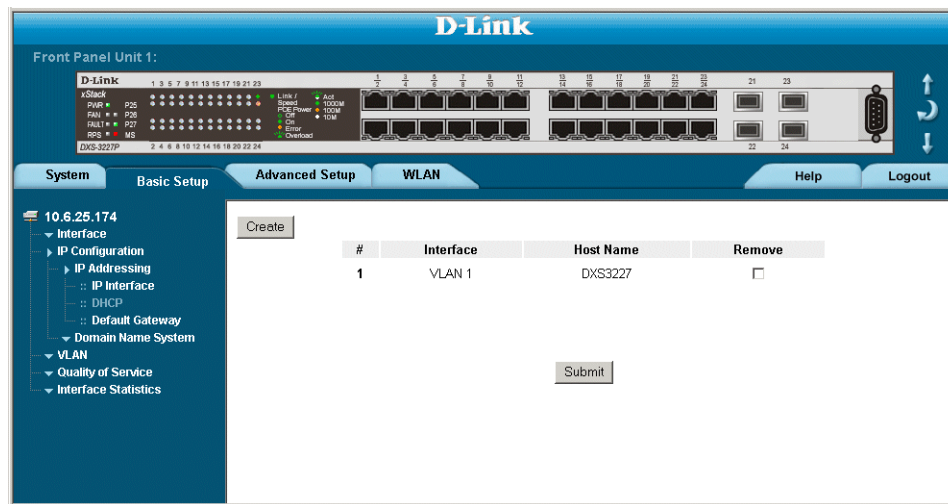
- **User Defined Default Gateway** — Defines the default gateway IP address.
 - **Active Default Gateway** — Indicates if the default gateway is active. The possible field values are:
 - **Remove User Defined** — Removes the default gateway. The possible field values are:
 - *Checked* — Removes the selected default gateway.
 - *Unchecked* — Maintains the default gateway.
2. Enter an IP address in the *User Defined Default Gateway* field.
 3. Click **Submit**. The device's default gateway is defined, and the device is updated.

Configuring DHCP

The *Dynamic Host Configuration Protocol* (DHCP) assigns dynamic IP addresses to devices on a network. DHCP ensures that network devices can have a different IP address every time the device connects to the network. To define a DHCP Interface:

1. Click **Basic Setup > IP Configuration > IP Addressing > DHCP**. The *DHCP Page* opens:

Figure 110: DHCP Page



The *DHCP Page* contains the following fields:

- **Interface** — Displays the IP address of the interface which is connected to the DHCP server.
- **Host Name** — Displays the system name.
- **Remove** — Removes DHCP interfaces. The possible field values are:
 - *Checked* — Removes the selected DHCP interface.
 - *Unchecked* — Maintains the DHCP interfaces.

2. Click **Create**. The *Add DHCP IP Interface Page* opens:

Figure 111: Add DHCP IP Interface Page

Add DHCP IP Interface

Interface Port LAG VLAN

Host Name

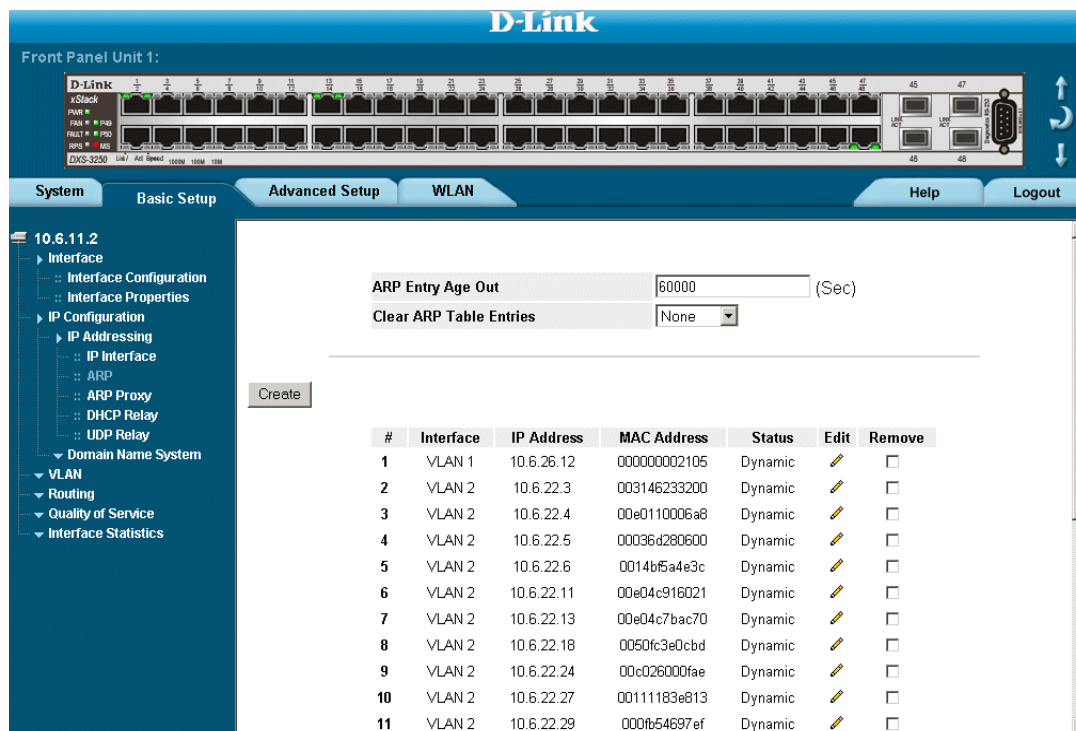
3. Define the *Interface* and *Host Name* fields.
4. Click . The DHCP interface is added, and the device is updated.

Configuring ARP

The *Address Resolution Protocol* (ARP) converts IP addresses into physical addresses, and maps the IP address to a MAC address. ARP allows a host to communicate with other hosts only when the IP address of its neighbors is known. To define ARP information:

1. Click **Basic Setup > IP Configuration > IP Addressing > ARP**. The *ARP Page* opens:

Figure 112: ARP Page



The *ARP Page* contains the following fields:

- **ARP Entry Age Out** — Specifies the amount of time (in seconds) that passes between *ARP Table* entry requests. Following the *ARP Entry Age* period, the entry is deleted from the table. The range is 1 - 4000000. The default value is 60000 seconds.
- **Clear ARP Table Entries** — Specifies the types of ARP entries that are cleared. The possible values are:
 - *None* — Maintains the ARP entries.
 - *All* — Clears all ARP entries.
 - *Dynamic* — Clears only dynamic ARP entries.
 - *Static* — Clears only static ARP entries.
- **Interface** — Displays the interface type for which ARP parameters are displayed. The possible field values are:
 - *Port* — Indicates the port for which ARP parameters are defined.
 - *LAG* — Indicates the LAG for which ARP parameters are defined.

- **VLAN** — Indicates the VLAN for which ARP parameters are defined.
 - **IP Address** — Indicates the station IP address, which is associated with the MAC address filled in below.
 - **MAC Address** — Displays the station MAC address, which is associated in the ARP table with the IP address.
 - **Status** — Displays the ARP table entry type. Possible field values are:
 - *Dynamic* — Indicates the ARP entry is learned dynamically.
 - *Static* — Indicates the ARP entry is a static entry.
 - **Remove** — Removes a specific ARP entry. The possible field values are:
 - *Checked* — Removes the selected ARP entries.
 - *Unchecked* — Maintains the current ARP entries.
2. Define the *ARP Entry Age Out* and *Clear ARP Table Entries* fields.
 3. Click **Submit**. The ARP parameters are defined, and the device is updated.
- To create a new ARP entry:
1. Click **Basic Setup > IP Configuration > IP Addressing > ARP**. The *ARP Page* opens.
 2. Click **Create**. The *ARP Settings Page* opens:

Figure 113: ARP Settings Page

ARP Settings

Interface	<input type="radio"/> Port <input type="text" value="1"/>	<input type="radio"/> LAG <input type="text" value=""/>	<input type="radio"/> VLAN <input type="text" value="1"/>
IP Address	<input type="text" value="0.0.0.0"/>		
MAC Address	<input type="text" value=""/>		

3. Define the *fields*.
4. Click **Submit**. The ARP interface is added, and the device is updated.

Configuring Domain Name Servers

Domain Name System (DNS) converts user-defined domain names into IP addresses. Each time a domain name is assigned, the DNS service translates the name into a numeric IP address. For example, **www.ipexample.com** is translated into 192.87.56.2. DNS servers maintain databases of domain names and their corresponding IP addresses.

This section contains the following topics:

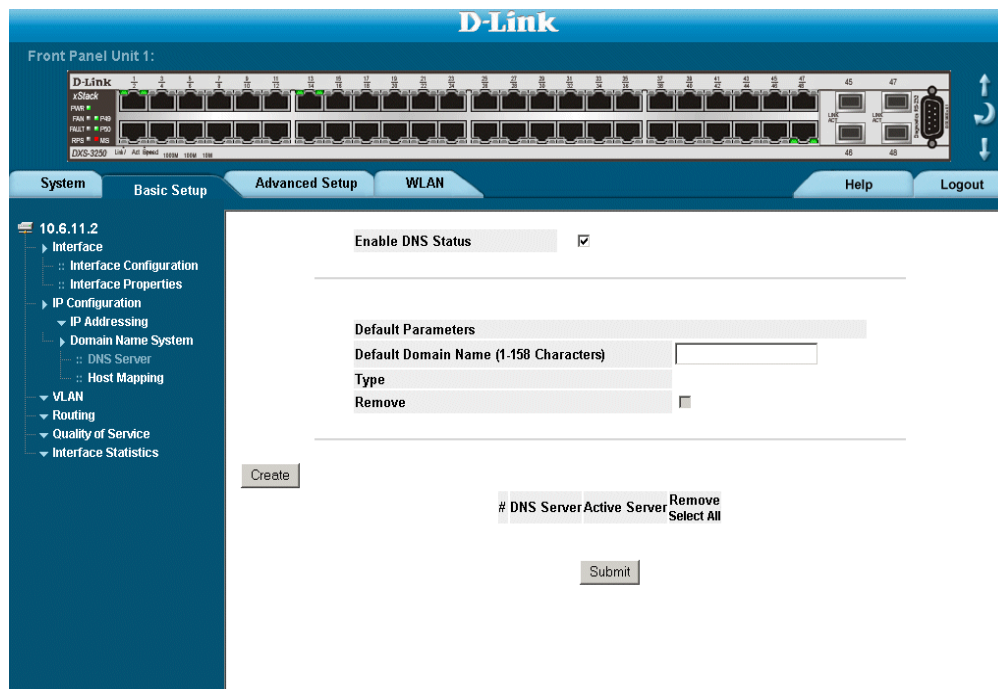
- Defining DNS Servers
- Defining DNS Host Mapping

Defining DNS Servers

The *DNS Server Page* contains fields for enabling and activating specific DNS servers. To enable a DNS server:

1. Click **Basic Setup > IP Configuration > Domain Name System > DNS Server**. The *DNS Server Page* opens:

Figure 114: DNS Server Page



The *DNS Server Page* contains the following fields:

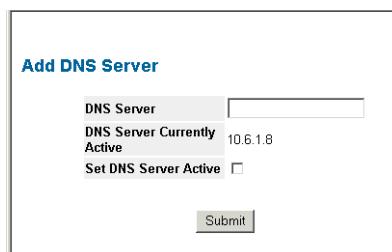
- **Enable DNS** — Enables translating the DNS names into IP addresses. The possible field values are:
 - *Checked* — Translates the domains into IP addresses.
 - *Unchecked* — Disables translating domains into IP addresses.
- **Default Domain Name (1 -158 Characters)** — Specifies the user-defined DNS server name.
- **Type** — Displays the IP address type. The possible field values are:

- *Dynamic* — The IP address is dynamically created.
 - *Static* — The IP address is a static IP address.
 - **Remove** — Removes DNS servers. The possible field values are:
 - *Checked* — Removes the selected DNS server
 - *Unchecked* — Maintains the current DNS server list.
 - **DNS Server** — Displays the DNS server IP address. DNS servers are added in the *Add DNS Server Page*.
 - **Active Server**— Specifies the DNS server that is currently active.
 - **Remove**—
 - *Checked* — Removes the selected server
 - *Unchecked* — Maintains the current server list.
2. Select *Enable DNS Status*.
 3. Define the *Default Domain Name* and *Active Server* fields.
 4. Click **Submit**. The DNS server is enabled, and the device is updated.

To add a new DNS Server:

1. Click **Basic Setup > IP Configuration > Domain Name System > DNS Server**. The *DNS Server Page* opens.
2. Click **Create**. The *Add DNS Server Page* opens:

Figure 115: Add DNS Server Page



Add DNS Server

DNS Server	<input type="text"/>
DNS Server Currently Active	10.6.1.8
Set DNS Server Active	<input type="checkbox"/>

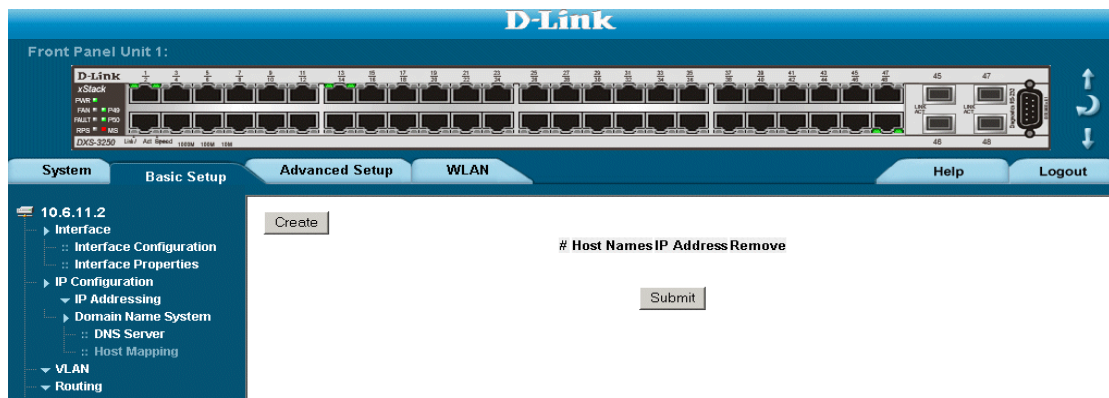
3. Define the *DNS Server*, *DNS Server Currently Active*, and *Set DNS Server Active* fields.
4. Click **Submit**. The DNS server is added, and the device is updated.

Defining DNS Host Mapping

The *DNS Host Mapping Page* provides information for defining DNS Host Mapping. To define DNS host mapping:

1. Click **Basic Setup > IP Configuration > Domain Name System > Host Mapping**. The *DNS Host Mapping Page* opens:

Figure 116: DNS Host Mapping Page

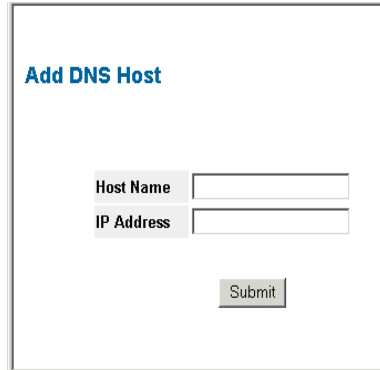


The *DNS Host Mapping Page* contains the following fields:

- **Host Names** — Displays a user-defined default domain name. When defined, the default domain name is applied to all unqualified host names. The *Host Name* field can contain up to 158 characters.
- **IP Address** — Displays the DNS host IP address.
- **Remove** — Removes default domain names. The possible field values are:
 - *Checked* — Removes the selected DNS host.
 - *Unchecked* — Maintains the current DNS host mapping list.

2. Click **Create**. The *Add DNS Host Page* opens:

Figure 117: Add DNS Host Page



The screenshot shows a web form titled "Add DNS Host" in blue text. Below the title are two input fields: "Host Name" and "IP Address", each with a corresponding text box. Below these fields is a "Submit" button.

3. Define the *Host Name* and *IP Address* fields.
4. Click **Submit**. The DNS host is added, and the device is updated.

Section 14. Defining the Forwarding Database and Static Routes

Packets addressed to destinations stored in either the Static or Dynamic databases are immediately forwarded to the port. The Dynamic MAC Address Table can be sorted by interface, VLAN, or MAC Address, whereas MAC addresses are dynamically learned as packets from sources that arrive at the device. Static addresses are configured manually.

An address becomes associated with a port by learning the port from the frame's source address, but if a frame that is addressed to a destination MAC address is not associated with a port, that frame is flooded to all relevant VLAN ports. To prevent the bridging table from overflowing, a dynamic MAC address, from which no traffic arrives for a set period, is erased.

This section contains information for defining both static and dynamic forwarding database entries, and includes the following topics:

- Defining Static Forwarding Database Entries
- Defining Dynamic Forwarding Database Entries
- Configuring Routing

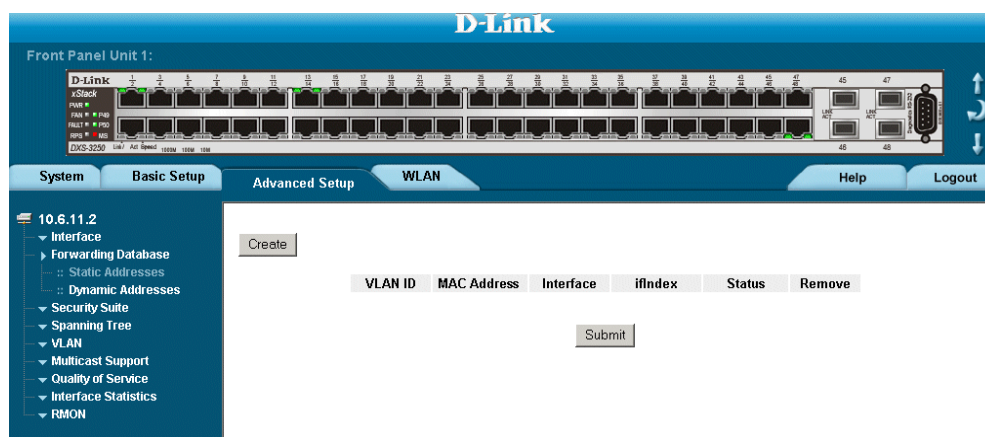
Defining Static Forwarding Database Entries

The *Forwarding Database Static Addresses Page* contains parameters for defining the age interval on the device. To prevent static MAC addresses from being deleted when the device is reset, ensure that the port attached to the MAC address is locked.

To configure the static forwarding database:

1. Click **Advanced Setup > Forwarding Database > Static Addresses**. The *Forwarding Database Static Addresses Page* opens.

Figure 118: Forwarding Database Static Addresses Page



The *Forwarding Database Static Addresses Page* contains the following fields:

- **VLAN ID** — Displays the VLAN ID number to which the entry refers.
- **MAC Address** — Displays the MAC address to which the entry refers.
- **Interface** — Displays the interface to which the entry refers:
 - **Port** — The specific port number to which the forwarding database parameters refer.
 - **LAG** — The specific LAG number to which the forwarding database parameters refer.
- **ifIndex** — Displays the interface to which the entry refers.
- **Status** — Displays how the entry was created. The possible field values are:
 - *Secure* — The MAC Address is defined for locked ports.
 - *Permanent* — The MAC address is permanent.
 - *Delete on Reset* — The MAC address is deleted when the device is reset.
 - *Delete on Timeout* — The MAC address is deleted when a timeout occurs.
- **Remove** — Removes the entry. The possible field values are:
 - *Checked* — Removes the selected entry.
 - *Unchecked* — Maintains the current static forwarding database.



Note

To prevent static MAC addresses from being deleted when the device is reset, make sure that the port attached to the MAC address is locked.

To add a new static forwarding database entry:

1. Click **Advanced Setup > Forwarding Database > Static Addresses**. *The Forwarding Database Static Addresses Page* opens.
2. Click **Create**. The Add Forwarding Database Page opens:

Figure 119: Add Forwarding Database Page

Add Forwarding Database

Interface Port 1/1 LAG

MAC Address

VLAN ID 1

VLAN Name

Status Permanent

Submit

3. Define the *Interface*, *MAC Address*, *VLAN ID* or *VLAN Name*, and *Status* fields.
4. Click **Submit**. The forwarding database information is modified, and the device is updated.

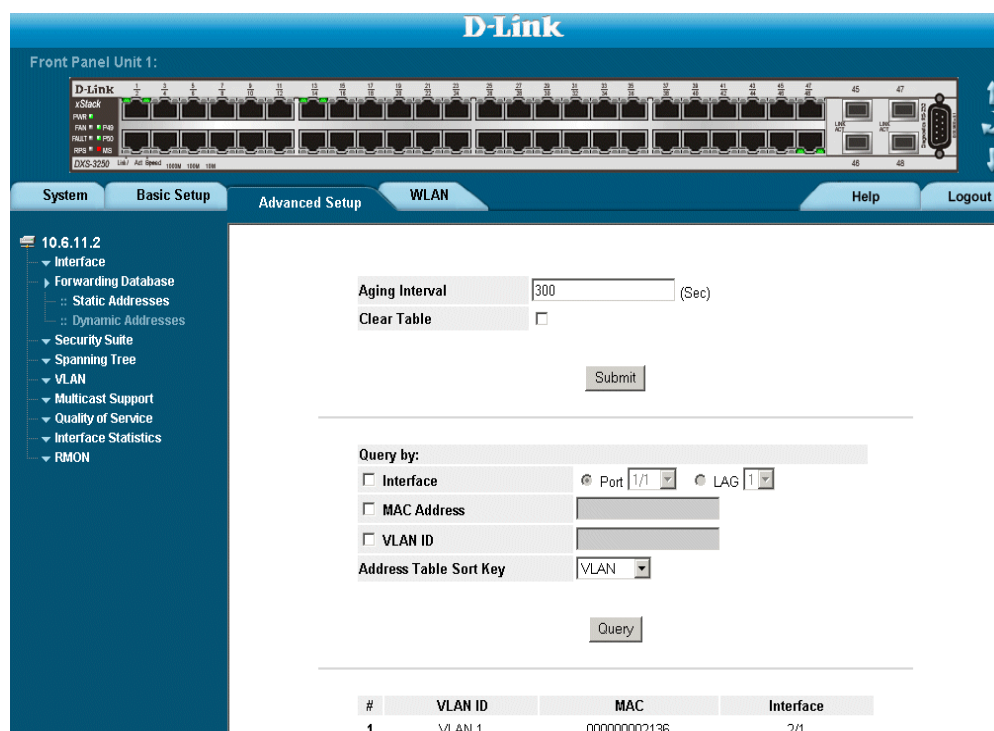
Defining Dynamic Forwarding Database Entries

The *Dynamic Addresses Page* contains parameters for querying information in the Dynamic MAC Address Table, including the interface type, MAC addresses, VLAN, and table storing. The Dynamic MAC Address table contains information about the aging time before a dynamic MAC address is erased, and includes parameters for querying and viewing the Dynamic MAC Address table. The Dynamic MAC Address table contains address parameters by which packets are directly forwarded to the ports. The Dynamic Address Table can be sorted by interface, VLAN, and MAC Address.

To configure the Dynamic MAC Address table:

1. Click **Advanced Setup > Forwarding Database > Dynamic Addresses**. The *Dynamic Addresses Page* opens.

Figure 120: Dynamic Addresses Page



The *Dynamic Addresses Page* contains the following fields:

- **Aging Interval (secs)** — Specifies the amount of time the MAC Address remains in the Dynamic Address Table before it times out. The default value is 300 seconds.
- **Clear Table** — Clears the current Address Table entries.
- **Query by:** — Sorts the addresses table by:
 - *Interface* — Displays the interface to for which the dynamic address is defined.
 - *MAC Address* — Specifies the MAC address for which the table is queried.
 - *VLAN ID* — Specifies the VLAN ID for which the table is queried.

- **Address Table Sort Key** —Specifies the means by which the Dynamic MAC Address Table is sorted. The address table can be sorted by address, VLAN, or interface.

2. Define the fields.

3. Click . The *Dynamic Address Aging* field is defined, and the device is updated.

To query the Dynamic MAC Address Table:

1. Click **Advanced Setup > Forwarding Database > Dynamic Addresses**. The *Dynamic Addresses Page* opens.

2. Select a *port*, *MAC Address*, and *VLAN ID*.

3. Select an *Address Table Sort Key*.

4. Click . The Dynamic MAC Address Table is queried, and the results are displayed.

Configuring Routing

Once the switch has been defined as a router, statics route can be defined. Network managers can define up to 32 static IP routes. To configure an IP static route:

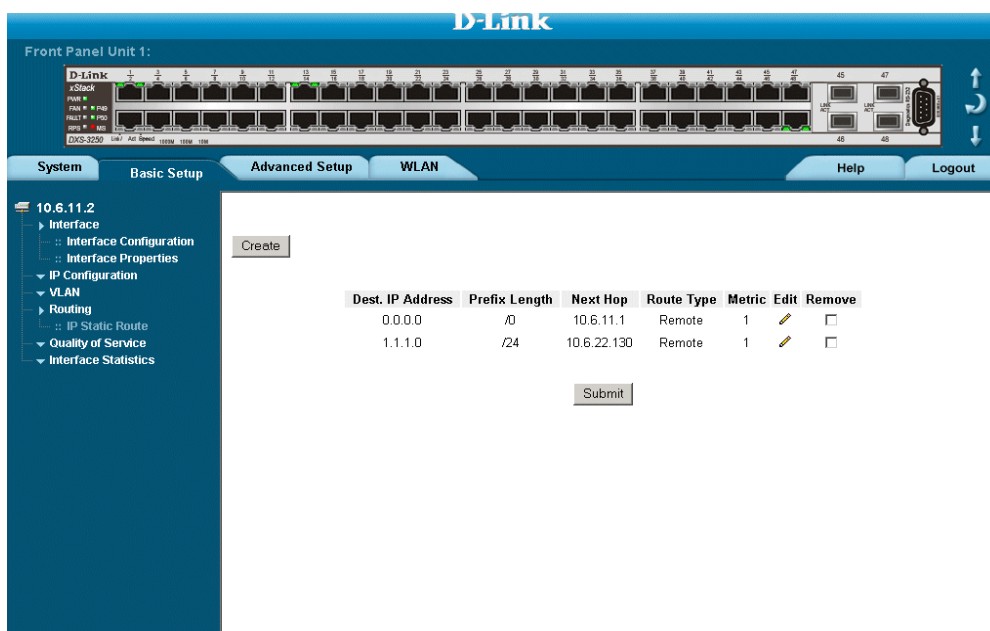


Note

For configuring the switch as a router, please refer to the D-Link CLI WLAN CLI Reference Guide

1. Click **Basic Setup > Routing > IP Static Route**. *The IP Static Route Page opens.*

Figure 121: IP Static Route Page



The *IP Static Route Page* contains the following fields:

- **Dest. IP Address** — Defines the destination IP address.
- **Prefix Length** — Defines the IP route prefix for the destination IP. The prefix length must be preceded by a forward slash (/).
- **Next Hop** — Indicates the next hop's IP address or IP alias on the route.
- **Route Type** — Defines the route type. The possible field values are:
 - *Reject* — Rejects the route, and stops routing to the destination network via all gateways.
 - *Remote* — Indicates the route is a remote path.
 - *Local* — Indicates the route is a local path.
- **Metric** — Indicates the administrative distance to the next hop. The default value is 1.
- **Remove** — Removes the user-defined route. The possible field values are:
 - *Checked* — Deletes the user-defined route.
 - *Unchecked* — Maintains the user-defined routes. This is the default value.

2. Click . The *Add IP Static Route* page opens:
3. Define the fields.
4. Click . The IP static route is defined and the device is updated.

Section 15. Configuring Spanning Tree

Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP also provides a single path between end stations on a network, eliminating loops.

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency.

The device supports the following STP versions:

- **Classic STP** — Provides a single path between end stations, avoiding and eliminating loops. For more information on configuring Classic STP, see *Defining Classic Spanning Tree*.
- **Rapid STP** — Detects and uses network topologies that provide faster convergence of the spanning tree, without creating forwarding loops. For more information on configuring Rapid STP, see *Defining Rapid Spanning Tree*.
- **Multiple STP** — Provides various load balancing scenarios. For example, if port A is blocked in one STP instance, the same port can be placed in the *Forwarding State* in another STP instance. For more information on configuring Multiple STP, see *Defining Multiple Spanning Tree*.

This section contains the following topics:

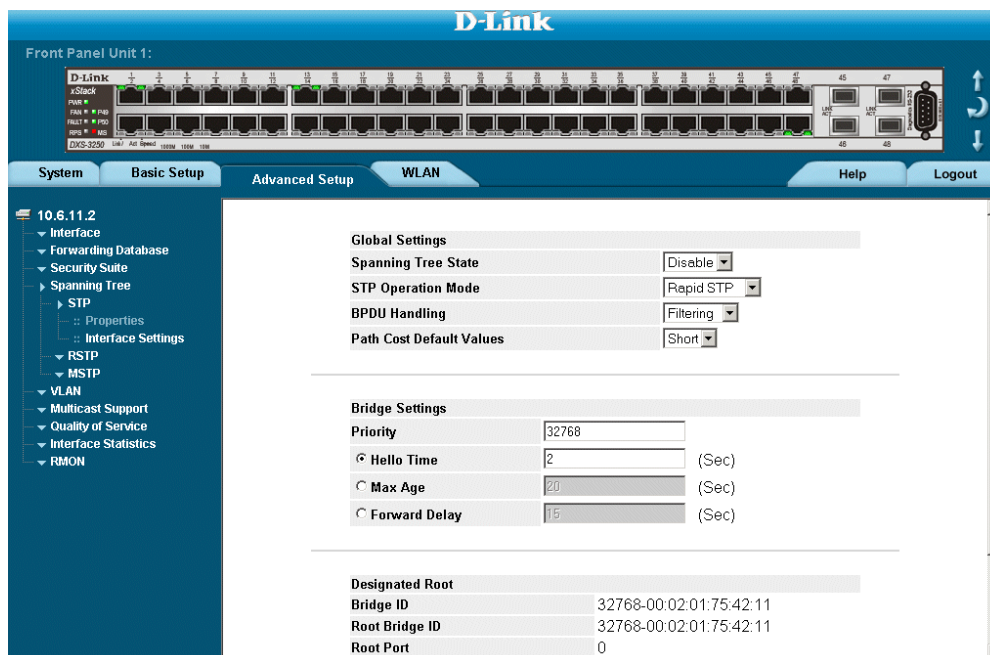
- Defining Classic Spanning Tree
- Defining STP on Interfaces
- Defining Rapid Spanning Tree
- Defining Multiple Spanning Tree

Defining Classic Spanning Tree

The *STP Properties Page* contains parameters for enabling STP on the device. To enable STP on the device:

1. Click **Advanced Setup > Spanning Tree > STP > Properties**. The *STP Properties Page* opens:

Figure 122: STP Properties Page



The *STP Properties Page* contains the following fields:

- **Spanning Tree State** — Indicates whether STP is enabled on the device. The possible field values are:
 - *Enable* — Enables STP on the device.
 - *Disable* — Disables STP on the device.
- **STP Operation Mode** — Specifies the STP mode that is enabled on the device. The possible field values are:
 - *Classic STP* — Enables Classic STP on the device. This is the default value.
 - *Rapid STP* — Enables Rapid STP on the device.
 - *Multiple STP* — Enables Multiple STP on the device.
- **BPDU Handling** — Determines how BPDU packets are managed when STP is disabled on the port or device. BPDUs are used to transmit spanning tree information. The possible field values are:
 - *Filtering* — Filters BPDU packets when spanning tree is disabled on an interface. This is the default value.
 - *Flooding* — Floods BPDU packets when spanning tree is disabled on an interface.
- **Path Cost Default Values** — Specifies the method used to assign default path cost to STP ports. The possible field values are:

- *Short* — Specifies 1 through 65,535 range for port path cost. This is the default value.
 - *Long* — Specifies 1 through 200,000,000 range for port path cost. The default path cost assigned to an interface varies according to the selected method (*Hello Time*, *Max Age*, or *Forward Delay*).
 - **Priority (0-65535)** — Specifies the bridge priority value. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the device with the lowest priority value becomes the Root Bridge. The default value is 32768. The port priority value is provided in increments of 4096.
 - **Hello Time (1-10)** — Specifies the device Hello Time. The Hello Time indicates the amount of time in seconds a Root Bridge waits between configuration messages. The default is 2 seconds.
 - **Max Age (6-40)** — Specifies the device Maximum Age Time. The Maximum Age Time is the amount of time in seconds a bridge waits before sending configuration messages. The default Maximum Age Time is 20 seconds.
 - **Forward Delay (4-30)** — Specifies the device Forward Delay Time. The Forward Delay Time is the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. The default is 15 seconds.
 - **Bridge ID** — Identifies the Bridge priority and MAC address.
 - **Root Bridge ID** — Identifies the Root Bridge priority and MAC address.
 - **Root Port** — Indicates the port number that offers the lowest cost path from this bridge to the Root Bridge. This field is significant when the bridge is not the Root Bridge. The default is zero.
 - **Root Path Cost** — The cost of the path from this bridge to the Root Bridge.
 - **Topology Changes Counts** — Specifies the total amount of STP state changes that have occurred.
 - **Last Topology Change** — Indicates the amount of time that has elapsed since the bridge was initialized or reset, and the last topographic change that occurred. The time is displayed in a day-hour-minute-second format, such as 2 days 5 hours 10 minutes and 4 seconds.
2. Select *Enable* in the *Spanning Tree State* field.
 3. Select an STP type in the *STP Operation Mode* field.
 4. Define the *BPDU Handling* and *Path Cost Default Values* fields.
 5. Select either the *Hello Time*, *Max Age*, or *Forward Delay* field.
 6. Click . STP is enabled, and the device is updated.

Defining STP on Interfaces

Network administrators can assign STP settings to specific interfaces using the *STP Interface Page*. The Global LAGs section displays the STP information for Link Aggregated Groups. To assign STP settings to an interface:

1. Click **Advanced Setup > Spanning Tree > STP > Interface Settings**. The *STP Interface Page* opens:

Figure 123: STP Interface Page

#	Port	STP	Port Fast	Root Guard	Port State	Port Role	Speed	Path Cost	Priority	Designated Bridge ID	Designated Port ID	Designated Cost	Forward Transitions	LAC
1	1/1	Enable	Auto	Disable	Disabled	Disable	1000M	4	128	N/A	N/A	N/A	N/A	
2	1/2	Enable	Auto	Disable	Disabled	Disable	1000M	100	128	N/A	N/A	N/A	N/A	
3	1/3	Enable	Auto	Disable	Disabled	Disable	1000M	100	128	N/A	N/A	N/A	N/A	
4	1/4	Enable	Auto	Disable	Disabled	Disable	1000M	100	128	N/A	N/A	N/A	N/A	
5	1/5	Enable	Auto	Disable	Disabled	Disable	1000M	100	128	N/A	N/A	N/A	N/A	
6	1/6	Enable	Auto	Disable	Disabled	Disable	1000M	100	128	N/A	N/A	N/A	N/A	
7	1/7	Enable	Auto	Disable	Disabled	Disable	1000M	100	128	N/A	N/A	N/A	N/A	
8	1/8	Enable	Auto	Disable	Disabled	Disable	1000M	100	128	N/A	N/A	N/A	N/A	
9	1/9	Enable	Auto	Disable	Disabled	Disable	1000M	100	128	N/A	N/A	N/A	N/A	
10	1/10	Enable	Auto	Disable	Disabled	Disable	1000M	100	128	N/A	N/A	N/A	N/A	
11	1/11	Enable	Auto	Disable	Disabled	Disable	1000M	100	128	N/A	N/A	N/A	N/A	
12	1/12	Enable	Auto	Disable	Disabled	Disable	1000M	100	128	N/A	N/A	N/A	N/A	
13	1/13	Enable	Auto	Disable	Disabled	Disable	1000M	4	128	N/A	N/A	N/A	N/A	
14	1/14	Enable	Auto	Disable	Disabled	Disable	1000M	100	128	N/A	N/A	N/A	N/A	
15	1/15	Enable	Auto	Disable	Disabled	Disable	1000M	100	128	N/A	N/A	N/A	N/A	
16	1/16	Enable	Auto	Disable	Disabled	Disable	1000M	100	128	N/A	N/A	N/A	N/A	

The *STP Interface Page* contains the following fields:

- **Port** — The interface for which the information is displayed.
- **STP Status** — Indicates if STP is enabled on the port. The possible field values are:
 - *Enabled* — Indicates that STP is enabled on the port.
 - *Disabled* — Indicates that STP is disabled on the port.
- **Root Guard** — Prevents devices outside the network core from being assigned the spanning tree root.
- **Port Fast** — Indicates if Fast Link is enabled on the port. If Fast Link mode is enabled for a port, the *Port State* is automatically placed in the *Forwarding* state when the port link is up. Fast Link optimizes the STP protocol convergence. STP convergence can take 30-60 seconds in large networks.
- **Port State** — Displays the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:
 - *Disabled* — Indicates that STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
 - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses. Blocking is displayed when Classic STP is enabled.
- **Port Role** — Indicates the port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:


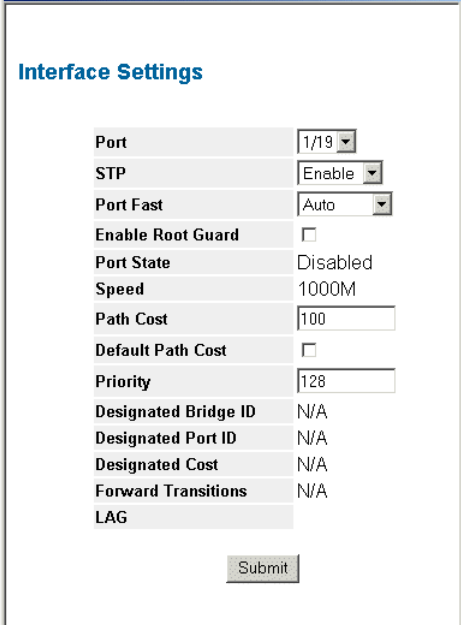
- *Root* — Provides the lowest cost path to forward packets to root switch.
 - *Designated* — Indicates that the port or LAG via which the designated switch is attached to the LAN.
 - *Alternate* — Provides an alternate path to the root switch from the root interface.
 - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
 - *Disabled* — Indicates the port is not participating in the Spanning Tree.
- **Speed** — Indicates the speed at which the port is operating.
 - **Path Cost** — Indicates the port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path is re-routed.
 - **Priority** — Priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority value is between 0 -240. The priority value is determined in increments of 16.
 - **Designated Bridge ID** — Indicates the bridge priority and the MAC Address of the designated bridge.
 - **Designated Port ID** — Indicates the selected port D-Link priority and interface.
 - **Designated Cost** — Indicates the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
 - **Forward Transitions** — Indicates the number of times the port has changed from *Forwarding* state to *Blocking* state.
 - **LAG** — Indicates the LAG to which the port belongs.
2. Click  . The *STP Interface Settings Page* opens:

Figure 124: STP Interface Settings Page



Port	1/19
STP	Enable
Port Fast	Auto
Enable Root Guard	<input type="checkbox"/>
Port State	Disabled
Speed	1000M
Path Cost	100
Default Path Cost	<input type="checkbox"/>
Priority	128
Designated Bridge ID	N/A
Designated Port ID	N/A
Designated Cost	N/A
Forward Transitions	N/A
LAG	

Submit

3. Select *Enable* in the *STP* field.

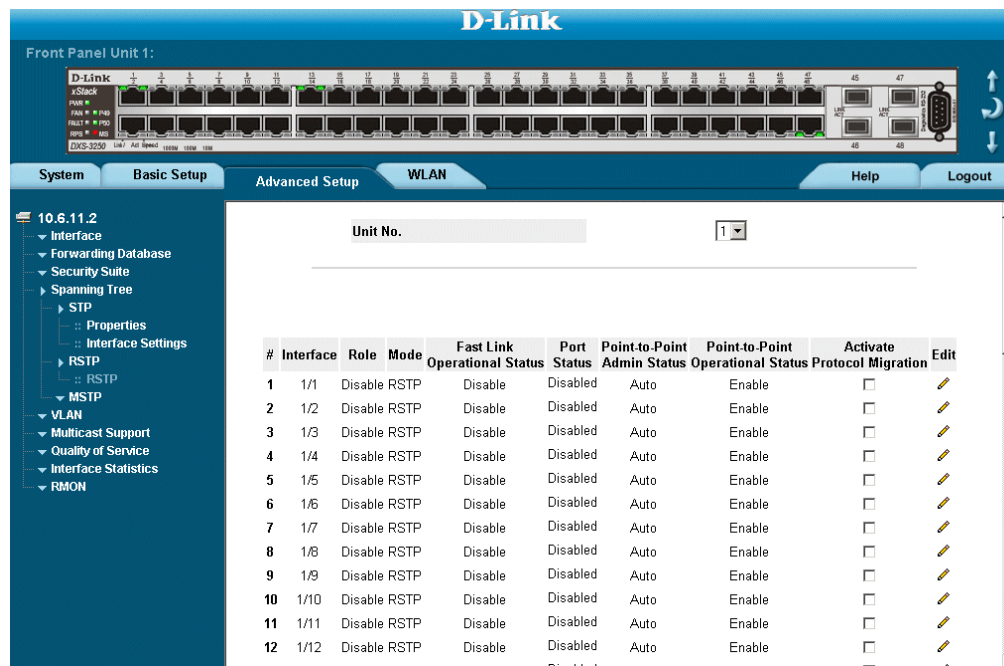
4. Define the *Fast Link*, *Enable Root Guard*, *Path Cost*, *Default Path Cost*, and *Priority* fields.
5. Click . STP is enabled on the interface, and the device is updated.

Defining Rapid Spanning Tree

While Classic STP prevents Layer 2 forwarding loops in a general network topology, convergence can take between 30-60 seconds. This time may delay detecting possible loops and propagating status topology changes. *Rapid Spanning Tree Protocol (RSTP)* detects and uses network topologies that allow a faster STP convergence without creating forwarding loops. The Global System LAG information displays the same field information as the ports, but represent the LAG RSTP information. To define RSTP on the device:

1. Click **Advanced Setup > Spanning Tree > RSTP > RSTP**. The *RSTP Page* opens:

Figure 125: RSTP Page



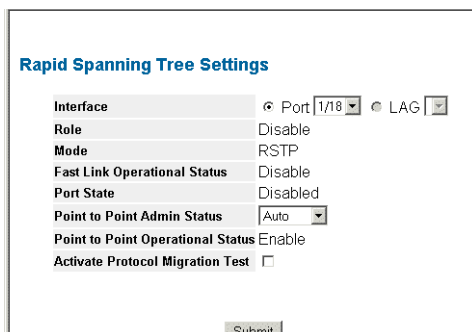
The *RSTP Page* contains the following fields:


- **Unit No.** — Indicates the stacking member for which the STP interface parameters are displayed.
- **Interface** — Displays the port or LAG on which Rapid STP is enabled.
- **Role** — Displays the port role assigned by the STP algorithm to provide to STP paths. The possible field values are:
 - *Root* — Provides the lowest cost path to forward packets to the root switch.
 - *Designated* — The port or LAG through which the designated switch is attached to the LAN.
 - *Alternate* — Provides an alternate path to the root switch from the root interface.
 - *Backup* — Provides a backup path the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link, or when a LAN has two or more connections connected to a shared segment.
 - *Disabled* — The port is not participating in the Spanning Tree.
- **Mode**—Displays the current STP mode. The STP mode is selected in the *STP Properties Page*. The possible field values are:

- *STP* — Classic STP is enabled on the device.
- *Rapid STP* — Rapid STP is enabled on the device.
- *Multiple STP* — Multiple STP is enabled on the device.
- **Fast Link Operational Status** — Indicates whether Fast Link is enabled or disabled for the port or LAG. If Fast Link is enabled for a port, the port is automatically placed in the forwarding state.
- **Point-to-Point Admin Status** — Indicates whether a point-to-point link is established, or if the device is permitted to establish a point-to-point link. The possible field values are:
 - *Enable* — The device is permitted to establish a point-to-point link, or is configured to automatically establish a point-to-point link. To establish communications over a point-to-point link, the originating PPP first sends *Link Control Protocol* (LCP) packets to configure and test the data link. After a link is established and optional facilities are negotiated as needed by the LCP, the originating PPP sends *Network Control Protocol* (NCP) packets to select and configure one or more network layer protocols. When each of the chosen network layer protocols has been configured, packets from each network layer protocol can be sent over the link. The link remains configured for communications until explicit LCP or NCP packets close the link, or until some external event occurs. This is the actual switch port link type. It may differ from the administrative state.
 - *Disable* — Disables point-to-point link.
- **Point-to-Point Operational Status** — Displays the point-to-point operating state.
- **Activate Protocol Migration** — Indicates whether sending Link Control Protocol (LCP) packets to configure and test the data link is enabled. The possible field values are:
 - *Checked* — Protocol Migration is enabled.
 - *Unchecked* — Protocol Migration is disabled.

2. Click  . The *RSTP Settings Page* opens:

Figure 126:RSTP Settings Page



3. Define the *Interface*, *Point-to-Point Admin Status* and *Activate Protocol Migration* fields.
4. Click  . RSTP is defined for the interface, and the device is updated.

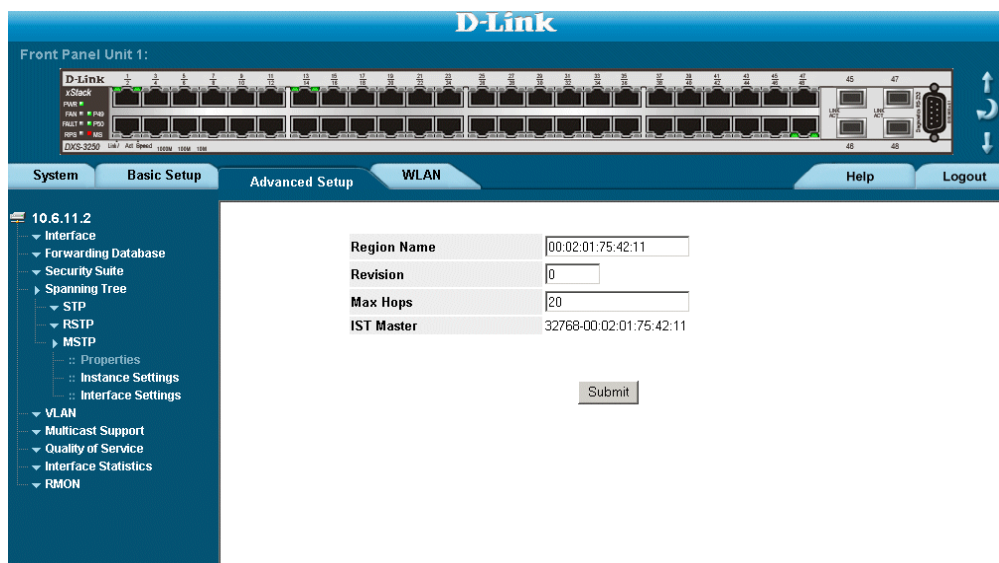
Defining Multiple Spanning Tree

Multiple Spanning Tree (MSTP) provides differing load balancing scenarios. For example, while port A is blocked in one STP instance, the same port can be placed in the *Forwarding* state in another STP instance. The *MSTP*

Properties Page contains information for defining global MSTP settings, including region names, MSTP revisions, and maximum hops. To define MSTP:

1. Click **Advanced Setup > Spanning Tree > MSTP > Properties**. The *MSTP Properties Page* opens:

Figure 127: MSTP Properties Page



The *MSTP Properties Page* contains the following fields:

- **Region Name** — User-defined STP region name.
 - **Revision** — An unsigned 16-bit number that identifies the revision of the current MSTP configuration. The revision number is required as part of the MSTP configuration. The possible field range is 0-65535.
 - **Max Hops** — Specifies the total number of hops that occur in a specific region before the BPDU is discarded. Once the BPDU is discarded, the port information is aged out. The possible field range is 1-40. The field default is 20 hops.
 - **IST Master** — Identifies the Spanning Tree Master instance. The IST Master is the specified instance root.
2. Define the *Region Name*, *Revision*, and *Max Hops* fields.
 3. Click **Submit**. The MSTP properties are defined, and the device is updated.

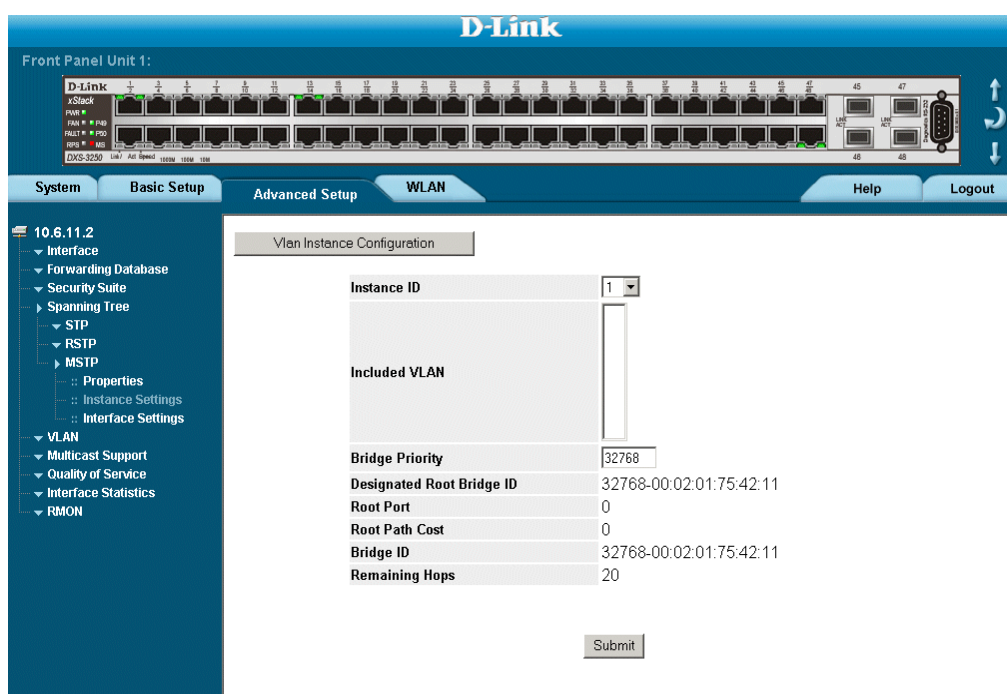
Defining MSTP Instance Settings

MSTP maps VLANs into STP instances. Packets assigned to various VLANs are transmitted along different paths within *Multiple Spanning Tree Regions* (MST Regions). Regions are one or more Multiple Spanning Tree bridges by which frames can be transmitted. In configuring MSTP, the MST region to which the device belongs is defined. A configuration consists of the name, revision, and region to which the device belongs.

Network administrators can define the MSTP instance settings using the *MSTP Instance Settings Page*. To define MSTP instance settings:

1. Click **Advanced Setup > Spanning Tree > MSTP > Instance Settings**. The *MSTP Instance Settings Page* opens:

Figure 128: MSTP Instance Settings Page



The *MSTP Instance Settings Page* contains the following fields:

- **Instance ID** — Specifies the VLAN group to which the interface is assigned.
- **Included VLAN** — Maps the selected VLANs to the selected instance. Each VLAN belongs to one instance.
- **Bridge Priority** — Specifies the selected spanning tree instance device priority. The field range is 0-61440
- **Designated Root Bridge ID** — Indicates the ID of the bridge with the lowest path cost to the instance ID.
- **Root Port** — Indicates the selected instance's root port.
- **Root Path Cost** — Indicates the selected instance's path cost.
- **Bridge ID** — Indicates the bridge ID of the selected instance.
- **Remaining Hops** — Indicates the number of hops remaining to the next destination.

2. Click **Vlan Instance Configuration**. The *MSTP Instance Configuration Table* opens:

Figure 129: MSTP Instance Configuration Table

	VLAN	Instance ID (0-15)
1	VLAN 1	<input type="text" value="0"/>
2	VLAN 2	<input type="text" value="0"/>
3	VLAN 3	<input type="text" value="0"/>
4	VLAN 4	<input type="text" value="0"/>
5	VLAN 5	<input type="text" value="0"/>
6	VLAN 6	<input type="text" value="0"/>
7	VLAN 7	<input type="text" value="0"/>
8	VLAN 8	<input type="text" value="0"/>
9	VLAN 9	<input type="text" value="0"/>
10	VLAN 10	<input type="text" value="0"/>
11	VLAN 11	<input type="text" value="0"/>
12	VLAN 12	<input type="text" value="0"/>
13	VLAN 13	<input type="text" value="0"/>
14	VLAN 14	<input type="text" value="0"/>
15	VLAN 15	<input type="text" value="0"/>
16	VLAN 16	<input type="text" value="0"/>
17	VLAN 17	<input type="text" value="0"/>
18	VLAN 18	<input type="text" value="0"/>

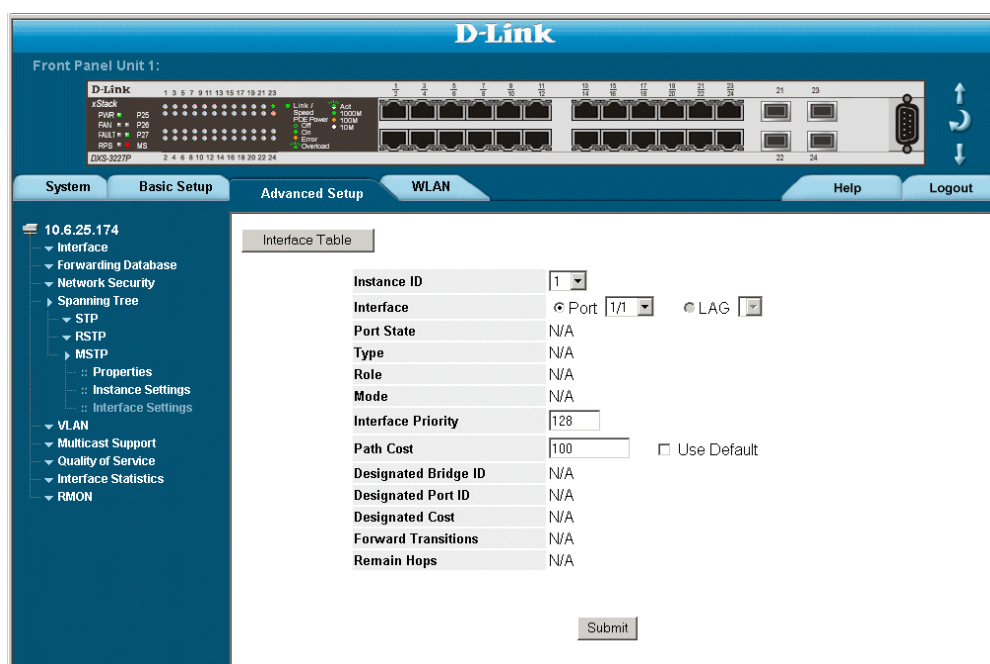
3. Define the *Instance ID* field.
4. Click **Submit**. The MSTP Instances are assigned, and the device is updated.

Defining MSTP Interface Settings

Network Administrators can assign MSTP Interface settings in the *MSTP Instance Settings Page*. To define MSTP interface settings:

1. Click **Advanced Setup > Spanning Tree > MSTP > Interface Settings**. The *MSTP Interface Settings Page* opens:

Figure 130: MSTP Interface Settings Page



The *MSTP Interface Settings Page* contains the following fields:

- **Instance ID** — Lists the MSTP instances configured on the device. Possible field range is 0-15.
- **Interface** — Displays the interface for which the MSTP settings are displayed. The possible field values are:
 - *Port* — Specifies the port for which the MSTP settings are displayed.
 - *LAG* — Specifies the LAG for which the MSTP settings are displayed.
- **Port State**— Indicates whether the port is enabled for the specific instance. The possible field values are:
 - *Enabled* — Enables the port for the specific instance.
 - *Disabled* — Disables the port for the specific instance.
- **Type** — Indicates whether the port is a Boundary or Master port. The possible field values are:
 - *Boundary Port* — Indicates that the port is a Boundary port. A Boundary port attaches MST bridges to LANs in an outlying region. If the port is a Boundary port, this field also indicates whether the device on the other side of the link is working in RSTP or STP mode
 - *Master Port* — Indicates the port is a master port. A Master port provides connectivity from a MSTP region to the outlying CIST root.
- **Role** — Indicates the port role assigned by the STP algorithm to provide to STP paths. The possible field values are:

- *Root* — Provides the lowest cost path to forward packets to the root device.
 - *Designated* — Indicates the port or LAG through which the designated device is attached to the LAN.
 - *Alternate* — Provides an alternate path to the root device from the root interface.
 - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link or when a LAN has two or more connections connected to a shared segment.
 - *Disabled* — Indicates the port is not participating in the Spanning Tree.
 - **Mode** — Indicates the STP mode by which STP is enabled on the device. The possible field values are:
 - *Classic STP* — Classic STP is enabled on the device. This is the default value.
 - *Rapid STP* — Rapid STP is enabled on the device.
 - *Multiple STP* — Multiple STP is enabled on the device.
 - **Interface Priority** — Defines the interface priority for the specified instance. The default value is 128.
 - **Path Cost** — Indicates the port contribution to the Spanning Tree instance. The range should always be 1-200,000,000.
 - **Designated Bridge ID** — Displays the ID of the bridge that connects the link or shared LAN to the root.
 - **Designated Port ID** — Displays the ID of the port on the designated bridge that connects the link or the shared LAN to the root.
 - **Designated Cost** — Indicates that the default path cost is assigned according to the method selected on the Spanning Tree Global Settings page.
 - **Forward Transitions** — Indicates the number of times the LAG State has changed from a *Forwarding* state to a *Blocking* state.
 - **Remain Hops** — Indicates the hops remaining to the next destination.
2. Click Interface Table . The *MSTP Interface Table* opens.

This page is left intentionally.

Section 16. Configuring Multicast Forwarding

This section contains information for configuring Multicast forwarding and Multicast TV, and includes the following sections:

- Defining IGMP Snooping
- Defining Multicast Bridging Groups
- Defining Multicast Forward All Settings
- Configuring Multicast TV

Defining IGMP Snooping

When IGMP Snooping is enabled globally, all IGMP packets are forwarded to the CPU. The CPU analyzes the incoming packets and determines:

- Which ports want to join which Multicast groups.
- Which ports have Multicast routers generating IGMP queries.
- Which routing protocols are forwarding packets and Multicast traffic.

Ports requesting to join a specific Multicast group issue an IGMP report, specifying that Multicast group is accepting members. This results in the creation of the Multicast filtering database.

To enable IGMP Snooping:

1. Click **Advanced Setup > Multicast Support > IGMP Snooping**. The *IGMP Snooping Page* opens:

Figure 131: IGMP Snooping Page

#	VLAN ID	IGMP Snooping Status	Auto Learn	Host Timeout	MRouter Timeout	Leave Timeout	Edit
1	1	Enabled	Enabled	260	300	10	
2	2	Enabled	Enabled	260	300	10	
3	3	Enabled	Enabled	260	300	10	
4	4	Enabled	Enabled	260	300	10	
5	5	Enabled	Enabled	260	300	10	
6	6	Enabled	Enabled	260	300	10	
7	7	Enabled	Enabled	260	300	10	
8	8	Enabled	Enabled	260	300	10	
9	9	Enabled	Enabled	260	300	10	
10	10	Enabled	Enabled	260	300	10	
11	11	Enabled	Enabled	260	300	10	

The *IGMP Snooping Page* contains the following fields:

- **Enable IGMP Snooping Status** — Indicates if IGMP Snooping is enabled on the device. IGMP Snooping can be enabled only if Bridge Multicast Filtering is enabled. The possible field values are:
 - *Checked* — Enables IGMP Snooping on the device.
 - *Unchecked* — Disables IGMP Snooping on the device.
- **VLAN ID** — Specifies the VLAN ID.
- **IGMP Snooping Status** — Indicates if IGMP snooping is enabled on the VLAN. The possible field values are:
 - *Enable* — Enables IGMP Snooping on the VLAN.
 - *Disable* — Disables IGMP Snooping on the VLAN.


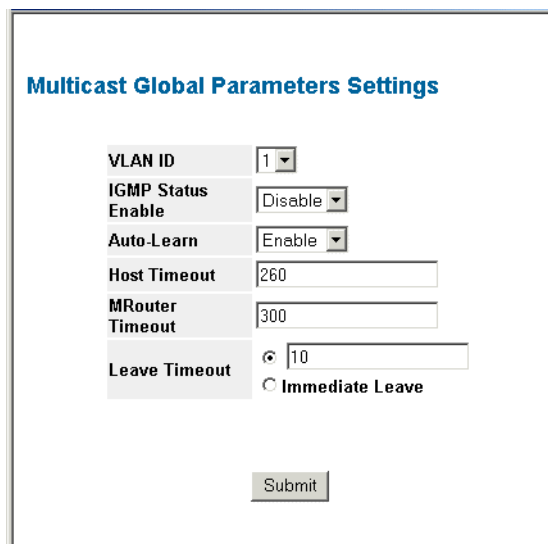
- **Auto Learn** — Indicates if Auto Learn is enabled on the device. If Auto Learn is enabled, the devices automatically learns where other Multicast groups are located. Enables or disables Auto Learn on the Ethernet device. The possible field values are:
 - *Enable* — Enables auto learn
 - *Disable* — Disables auto learn.
 - **Host Timeout** — Indicates the amount of time host waits to receive a message before timing out. The default time is 260 seconds.
 - **MRouter Timeout** — Indicates the amount of the time the Multicast router waits to receive a message before it times out. The default value is 300 seconds.
 - **Leave Timeout** — Indicates the amount of time the host waits, after requesting to leave the IGMP group and not receiving a Join message from another station, before timing out. If a Leave Timeout occurs, the switch notifies the Multicast device to stop sending traffic The Leave Timeout value is either user-defined, or an immediate leave value. The default timeout is 10 seconds.
2. Check the *Enable IGMP Snooping Status* checkbox.
 3. Click . The *Multicast Global Parameters Settings Page* opens:

Figure 132: Multicast Global Parameters Settings Page



Multicast Global Parameters Settings

VLAN ID

IGMP Status Enable

Auto-Learn

Host Timeout

MRouter Timeout

Leave Timeout 10 Immediate Leave

4. Modify the *VLAN ID*, *IGMP Status Enable*, *Auto Learn*, *Host Timeout*, *MRouter Timeout*, and *Leave Timeout* fields.
5. Click . The IGMP global parameters are sent, and the device is updated.

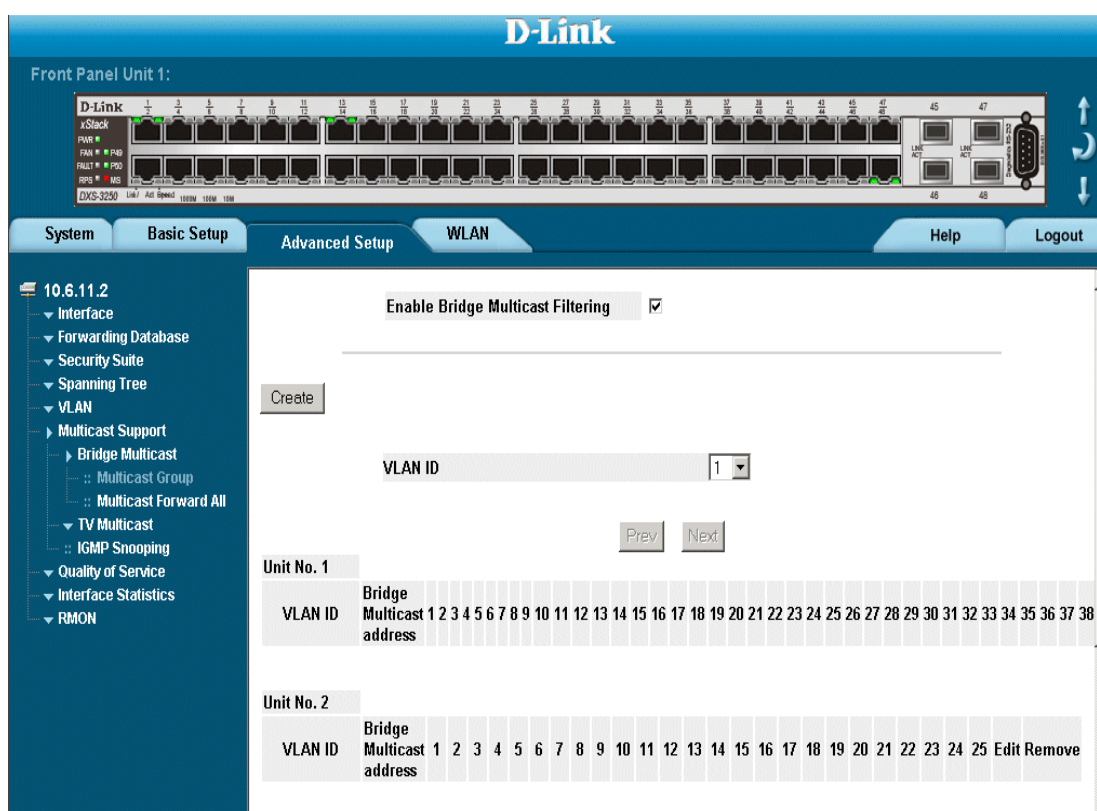
Defining Multicast Bridging Groups

The *Multicast Group Page* displays the ports and LAGs attached to the Multicast service group in the Ports and LAGs tables. The Port and LAG tables also reflect the manner in which the port or LAGs joined the Multicast group. Ports can be added either to existing groups or to new Multicast service groups. The *Multicast Group Page* permits new Multicast service groups to be created. The *Multicast Group Page* also assigns ports to a specific Multicast service address group.

To define Multicast groups:

1. Click **Advanced Setup > Multicast Support > Bridge Multicast > Multicast Group**. The *Multicast Group Page* opens:

Figure 133: Multicast Group Page



The *Multicast Group Page* contains the following information:

- **Enables Bridge Multicast Filtering** — Indicate if bridge Multicast filtering is enabled on the device. The possible field values are:
 - *Checked* — Enables Multicast filtering on the device.
 - *Unchecked* — Disables Multicast filtering on the device. If Multicast filtering is disabled, Multicast frames are flooded to all ports in the relevant VLAN. Disabled is the default value.
- **VLAN ID** — Identifies a VLAN and contains information about the Multicast group address.
- **Bridge Multicast Address** — Identifies the Multicast group MAC address/IP address.

- **Ports** — Displays Port that can be added to a Multicast service.

The following table contains the IGMP port and LAG members management settings:

Table 12: IGMP Port/LAG Members Table Control Settings

Port Control	Definition
D	Dynamically joins ports/LAG to the Multicast group in the Current Row.
S	Attaches the port to the Multicast group as static member in the Static Row. The port/LAG has joined the Multicast group statically in the Current Row.
F	Forbidden ports are not included the Multicast group, even if IGMP snooping designated the port to join a Multicast group.
N	None. The port is not part of a Multicast group.

2. Click . The *Add Multicast Group Page* opens:

Figure 134: Add Multicast Group Page

The screenshot displays the configuration page for adding a multicast group. At the top, there are three input fields: 'VLAN ID' with a dropdown menu showing '1', 'Bridge IP Multicast' with a text box and '(X.X.X.X)' placeholder, and 'Bridge Mac Multicast' with an empty text box. Below these is a section titled 'Unit No1' containing a grid of 29 columns (ports) and three rows (N, F, S). The 'N' row is highlighted in blue, 'F' in grey, and 'S' in brown. Each cell in the grid contains a radio button. Below the grid is a 'LAG' section with three rows (N, F, S) and a 'Submit' button at the bottom center.

3. Define the *VLAN ID*, *Bridge Multicast IP Address*, and *Bridge Multicast MAC Address* fields.
4. Select ports to join the Multicast group.
5. Define the Multicast port settings.
6. Click . The Multicast group is defined, and the device is updated.

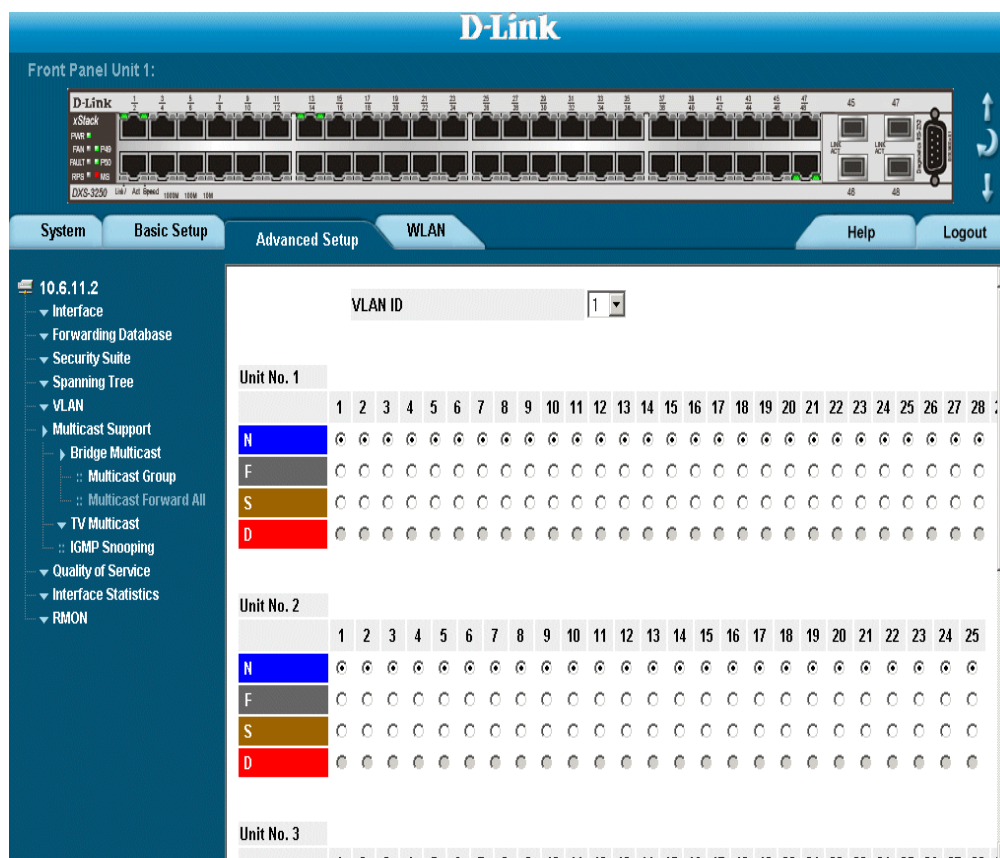
Defining Multicast Forward All Settings

The Bridge Multicast Forward All page contains fields for attaching ports or LAGs to a device that is attached to a neighboring Multicast router/switch. Once IGMP Snooping is enabled, Multicast packets are forwarded to the appropriate port or VLAN. Unless LAGs are defined, only a Multicast Forward All table displays.

To define Multicast forward all settings:

1. Click **Advanced Setup > Multicast Support > Bridge Multicast > Multicast Forward All**. The *Multicast Forward All Page* opens:

Figure 135: Multicast Forward All Page



The *Multicast Forward All Page* contains the following fields:

- **VLAN ID** — Displays the VLAN for which Multicast parameters are displayed.
- **Ports/LAG** — Ports that can be added to a Multicast service.

The following table summarizes the Multicast settings which can be assigned to ports in the *Multicast Forward All Page*.

Table 13: Bridge Multicast Forward All Router/Port Control Settings Table

Port Control	Definition
D	Attaches the port to the Multicast router or switch as a dynamic port.
S	Attaches the port to the Multicast router or switch as a static port.
F	Forbidden.
N	None the port is not attached.

2. Select a VLAN in the *VLAN ID* drop-down box.
3. Define the VLAN port settings.
4. Click . The Multicast forward all settings are defined, and the device is updated.

Configuring Multicast TV

Multicast TV allows subscribers to join the same Multicast stream, even if the subscribers are not members of the same VLAN, eliminating television traffic duplication. Ports which receive Multicast Transmissions, or *Receiver Ports*, can be defined in any VLAN, and not just in the Multicast VLAN. Receiver ports can only receive Multicast transmissions, they cannot initiate a Multicast TV transmission. Multicast TV source ports must be a Multicast VLAN members. This section contains the following topics:

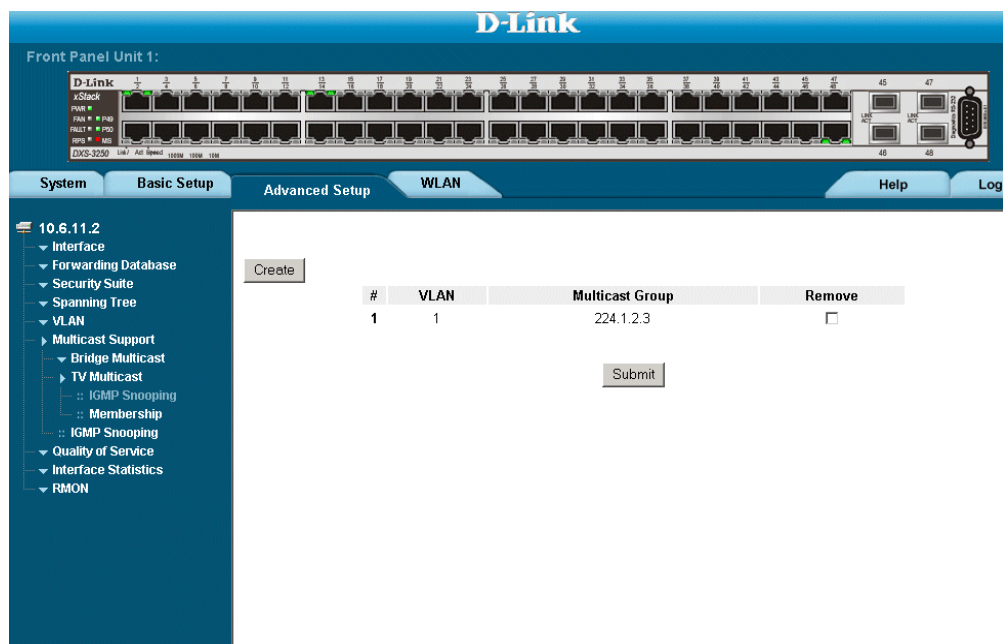
- Defining IGMP Snooping for Multicast TV
- Viewing Multicast TV Members

Defining IGMP Snooping for Multicast TV

IGMP messages are used to indicate which ports are requesting to join or leave the Multicast group. The *Multicast TV IGMP Snooping Page* page allows network administrators to define IGMP Snooping for Multicast TV groups. To define IGMP Snooping for Multicast TV:

1. Click **Advanced Setup > Multicast Support > TV Multicast > IGMP Snooping** The *Multicast Forward All Page* opens:

Figure 136: Multicast TV IGMP Snooping Page



The *Multicast TV IGMP Snooping Page* contains the following fields:

- **VLAN** — Defines the VLAN attached to the for which the IGMP Snooping mapping is defined.
- **Multicast Group** — Defines the Multicast group IP addressed mapped to the VLAN.
- **Remove** — Removes Multicast TV IGMP mappings. The possible field values are:
 - *Checked* — Removes the specific IGMP mapping from the selected VLAN.
 - *Unchecked* — Maintains the IGMP mapping.

- Click . The *Add IGMP Snooping Mapping Page* opens.

Figure 137: Add IGMP Snooping Mapping Page

Add IGMP Snooping Mapping

VLAN	<input type="text" value="1"/>
Multicast Group	<input type="text" value="224.2.1.3"/>

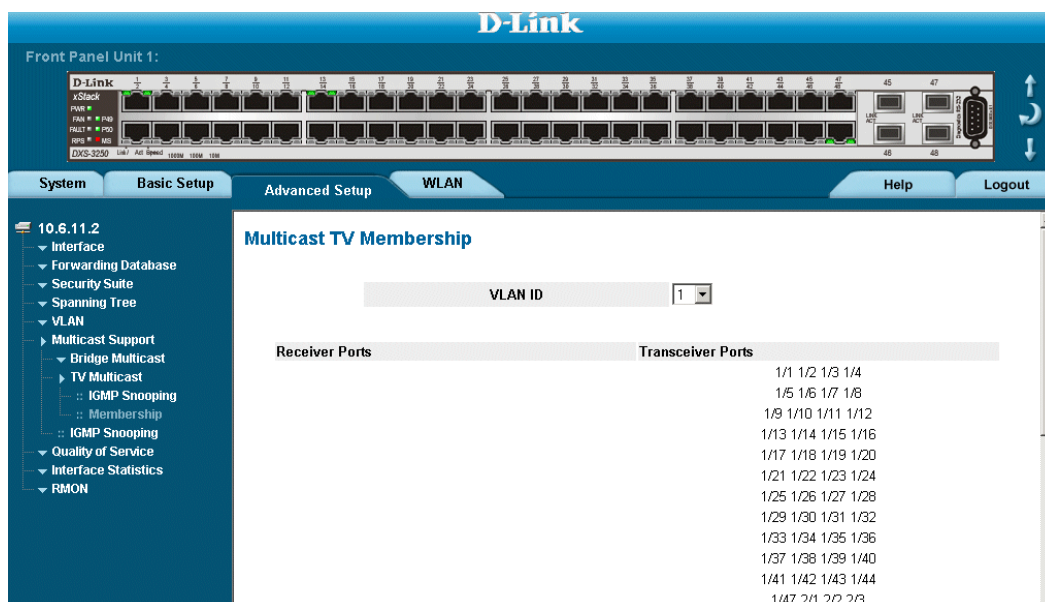
- Define the *VLAN* and *Multicast Group* fields.
- Click . IGMP Snooping is defined for Multicast TV groups, and the device is updated.

Viewing Multicast TV Members

The *Multicast TV Membership Page* allows network managers to display the ports associated with a Multicast TV VLAN. Ports and trunks are assigned to Multicast VLAN in the *IP Interface Page*. To define Multicast TV Members:

1. Click **Advanced Setup > Multicast Support > TV Multicast > Membership** The *Multicast TV Membership Page* opens:

Figure 138: Multicast TV Membership Page



The *Multicast TV Membership Page* contains the following fields:

- **VLAN ID**— Indicates the Multicast VLAN ID to which the source ports and receiver ports are members.
 - **Receiver Ports** — Indicates the port on which Multicast TV transmissions are received.
 - **Transceiver Ports** — Indicates the source port from which the Multicast TV transmission originates. The source port is learned through the IGMP messages.
2. Select a VLAN, the Multicast TV membership for the selected VLAN is displayed.

Section 17. Configuring SNMP

Simple Network Management Protocol (SNMP) provides a method for managing network devices. The device supports the following SNMP versions:

- SNMP version 1
- SNMP version 2c
- SNMP version 3

SNMP v1 and v2c

The SNMP agents maintain a list of variables, which are used to manage the device. The variables are defined in the Management Information Base (MIB). The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network. Access rights to the SNMP agents are controlled by access strings.

SNMP v3

SNMP v3 applies access control and a new traps mechanism. In addition, User Security Model (USM) parameters are defined for SNMPv3, including:

- **Authentication** — Provides data integrity and data origin authentication.
- **Privacy** — Protects against the disclosure of message content. Cipher Block-Chaining (CBC) is used for encryption. Either authentication is enabled on a SNMP message, or both authentication and privacy are enabled on a SNMP message. However, privacy cannot be enabled without authentication.
- **Timeliness** — Protects against message delay or message redundancy. The SNMP agent compares incoming message to the message time information.
- **Key Management** — Defines key generation, key updates, and key use.

The device supports SNMP notification filters based on Object IDs (OIDs). OIDs are used by the system to manage device features.

SNMP v3 supports the following features:

- Security
- Feature Access Control
- Traps

The device generates the following traps:

- Copy trap

This section contains the following topics:

- Configuring SNMP Security
- Configuring SNMP Notifications

Configuring SNMP Security

This section contains information for configuring SNMP security parameters, and contains the following topics:

- Defining SNMP Security
- Defining SNMP Views
- Defining SNMP Group Profiles

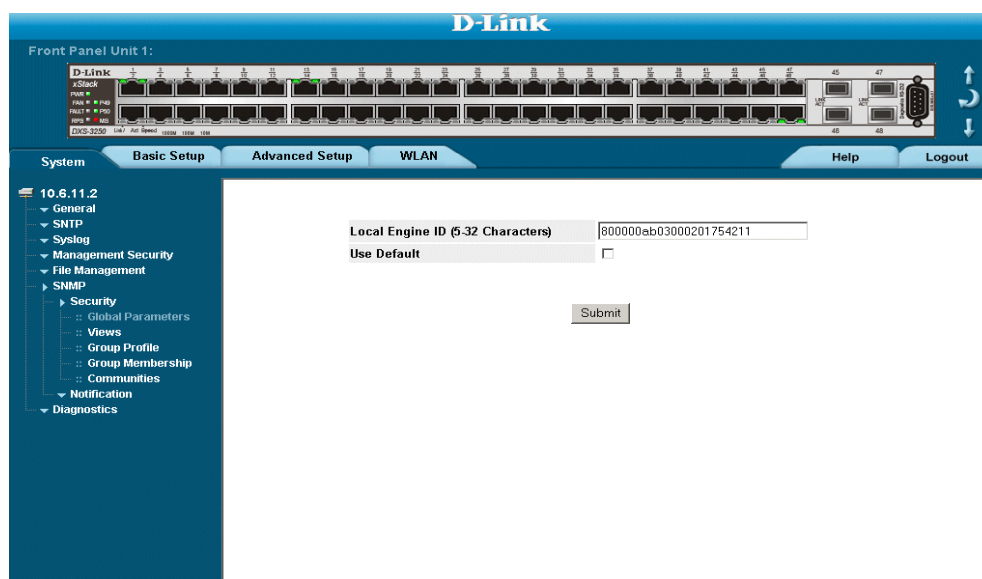
- Defining SNMP Group Members
- Defining SNMP Communities

Defining SNMP Security

The *SNMP Security Global Parameters Page* permits the enabling of both SNMP and Authentication notifications. To define the SNMP security parameters:

1. Click **System > SNMP > Security > Global Parameters**. The *SNMP Security Global Parameters Page* opens:

Figure 139: SNMP Security Global Parameters Page



The *SNMP Security Global Parameters Page* contains the following fields:

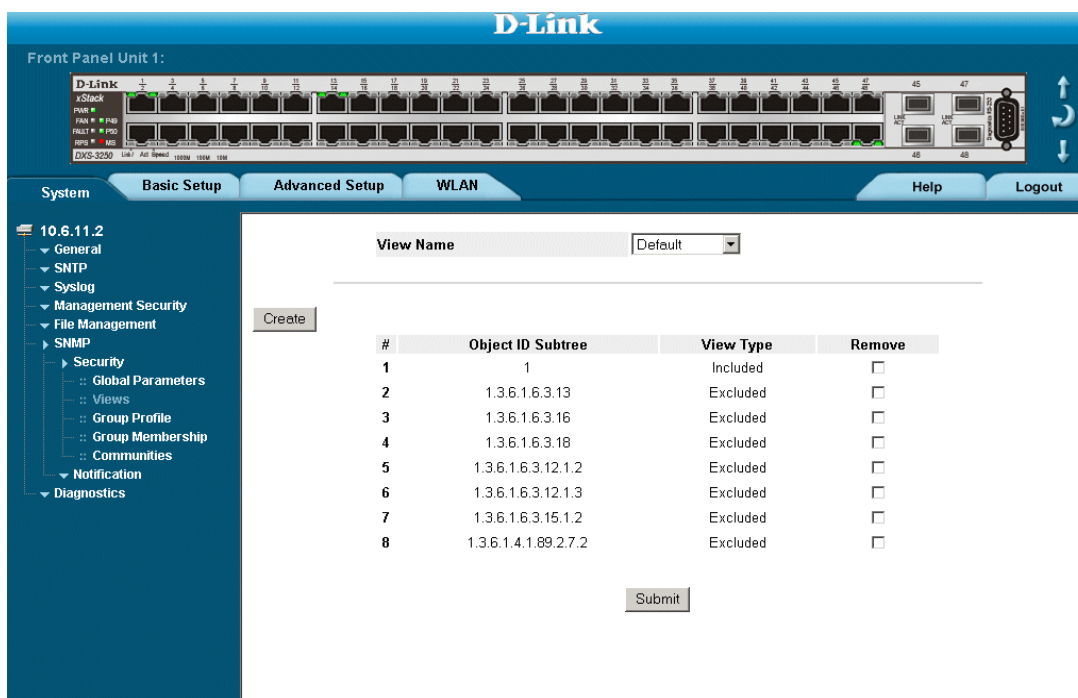
- **Local Engine ID (0-32 Characters)**— Displays the local device Engine ID. The field value is a hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or a colon. The Engine ID must be defined before SNMPv3 is enabled. Select a default Engine ID that is comprised of an Enterprise number and the default MAC address.
 - **Use Default** — Uses the device-generated Engine ID. The default Engine ID is based on the device MAC address and is defined per standard as:
 - *First 4 octets* — first bit = 1, the rest is IANA Enterprise number.
 - *Fifth octet* — Set to 3 to indicate the MAC address that follows.
 - *Last 6 octets* — MAC address of the device.
2. Define the *Local Engine ID* and *Use Default* fields.
 3. Click **Submit**. The SNMP global security parameters are set, and the device is updated.

Defining SNMP Views

SNMP Insert space views provide or block access to device features or portions of features. For example, a view can be defined which provides that SNMP group A has *Read Only* (R/O) access to Multicast groups, while SNMP group B has *Read-Write* (R/W) access to Multicast groups. Feature access is granted via the MIB name or MIB Object ID. To define SNMP views:

1. Click **System > SNMP > Security > Views**. The *SNMP Security Views Page* opens:

Figure 140: SNMP Security Views Page

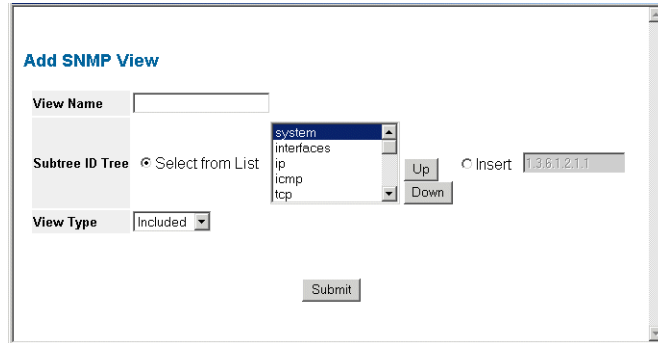


The *SNMP Security Views Page* contains the following fields:

- **View Name** — Displays the user-defined views. The view name can contain a maximum of 30 alphanumeric characters.
- **Object ID Subtree** — Displays the device feature OID included in or excluded from the selected SNMP view.
- **View Type** — Indicates whether the defined OID branch will be included in or excluded from the selected SNMP view.
- **Remove** — Deletes the currently selected view. The possible field values are:
 - *Checked* — Removes the selected view.
 - *Unchecked* — Maintains the list of views.

2. Click **Create**. The *Add SNMP View Page* opens:

Figure 141: Add SNMP View Page



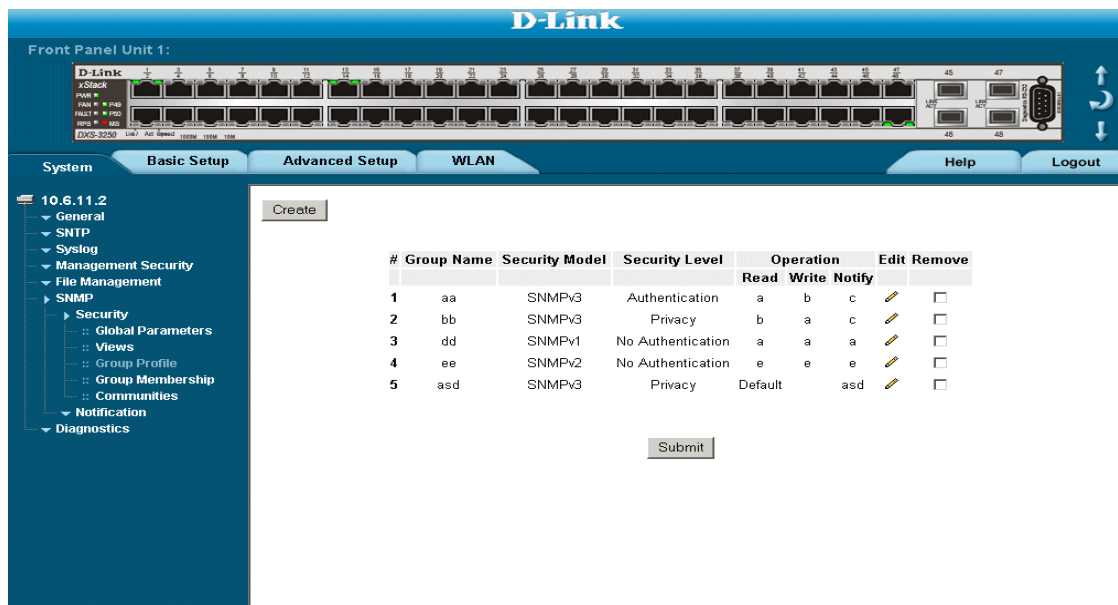
3. Define the *View Name* field.
4. Define the view using **Up** and **Down**.
5. Define the *View Type* field.
6. Click **Submit**. The view is defined, and the device is updated.

Defining SNMP Group Profiles

The *SNMP Group Profile Page* provides information for creating SNMP groups, and assigning SNMP access control privileges to SNMP groups. Groups allow network managers to assign access rights to specific features, or feature aspects. To define an SNMP group:

1. Click **System > SNMP > Security > Group Profile**. The *SNMP Group Profile Page* opens:

Figure 142: SNMP Group Profile Page



The *SNMP Group Profile Page* contains the following fields:

- **Group Name** — Displays the user-defined group to which access control rules are applied. The field range is up to 30 characters.
- **Security Model** — Defines the SNMP version attached to the group. The possible field values are:
 - *SNMPv1* — SNMPv1 is defined for the group.
 - *SNMPv2c* — SNMPv2c is defined for the group.
 - *SNMPv3* — SNMPv3 is defined for the group.
- **Security Level** — Defines the security level attached to the group. Security levels apply to SNMPv3 only. The possible field values are:
 - *No Authentication* — Indicates that neither the Authentication nor the Privacy security levels are assigned to the group.
 - *Authentication* — Authenticates SNMP messages, and ensures that the SNMP message's origin is authenticated.
 - *Privacy* — Encrypts SNMP messages.
- **Operation** — Defines the group access rights. The possible field values are:
 - *Read* — Management access is restricted to read-only, and changes cannot be made to the assigned SNMP view.


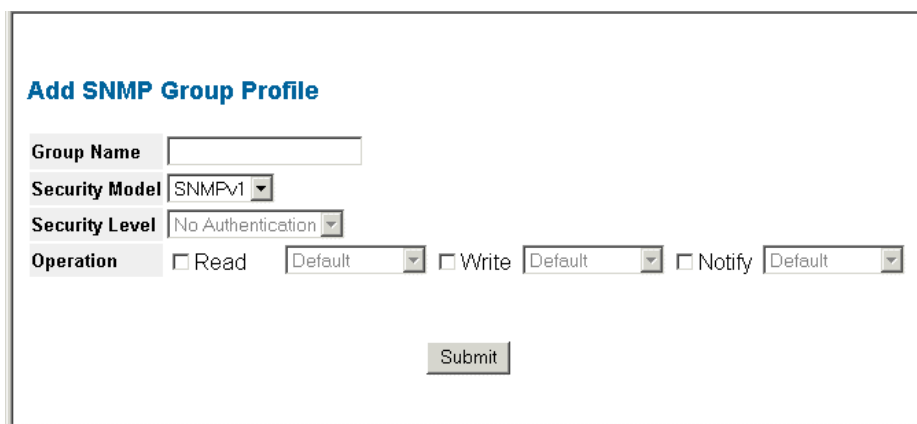
- *Write* — Management access is read-write and changes can be made to the assigned SNMP view.
 - *Notify* — Sends traps for the assigned SNMP view.
 - **Remove** — Removes SNMP groups. The possible field values are:
 - *Checked* — Removes the selected SNMP group.
 - *Unchecked* — Maintains the SNMP groups.
2. Click . The *Add SNMP Group Profile Page* opens:

Figure 143: Add SNMP Group Profile Page



Add SNMP Group Profile

Group Name

Security Model

Security Level

Operation Read Write Notify



3. Define the *Group Name*, *Security Model*, *Security Level*, and *Operation* fields.
4. Click . The SNMP group profile is added, and the device is updated.
- To modify SNMP Group Settings:
1. Click **System > SNMP > Security > Group Profile**. The *SNMP Group Profile Page* opens.
 2. Click . The *SNMP Group Profile Settings Page* opens:

Figure 144: SNMP Group Profile Settings Page

SNMP Group Profile Settings

Query Access Control Configuration						
Group Name	t3					
Security Model	SNMPv1					
Security Level	No Authentication					
Operation	<input checked="" type="checkbox"/> Read	Default	<input type="checkbox"/> Write	Default	<input type="checkbox"/> Notify	Default

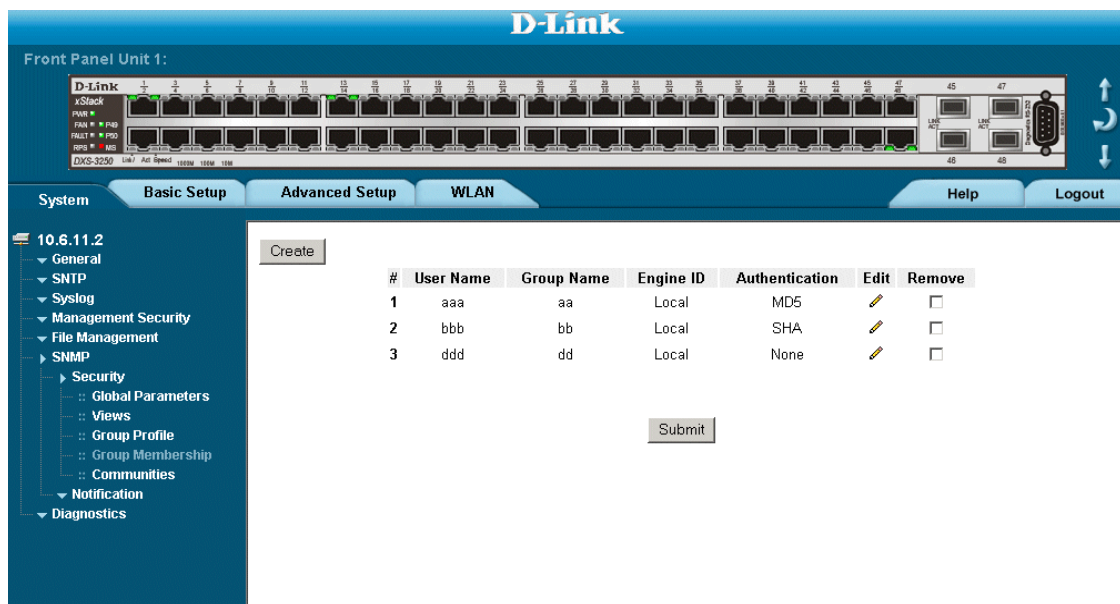
3. Modify the fields.
4. Click . The SNMP group profile is modified, and the device is updated.

Defining SNMP Group Members

The *SNMP Group Membership Page* enables assigning system users to SNMP groups, as well as defining the user authentication method.

1. Click **System > SNMP > Security > Group Membership**. The *SNMP Group Membership Page* opens:

Figure 145: SNMP Group Membership Page



The *SNMP Group Membership Page* contains the following fields:

- **User Name** — Contains a list of user-defined user names. The field range is up to 30 alphanumeric characters.
- **Group Name** — Contains a list of user-defined SNMP groups. SNMP groups are defined in the *SNMP Group Profile Page*.
- **Engine ID** — Displays either the local or remote SNMP entity to which the user is connected. Changing or removing the local SNMP Engine ID deletes the SNMPv3 user database.
 - *Local* — Indicates that the user is connected to a local SNMP entity.
 - *Remote* — Indicates that the user is connected to a remote SNMP entity. If the Engine ID is defined, remote devices receive inform messages.
- **Authentication** — Displays the method used to authenticate users. The possible field values are:
 - *MD5 Key* — Users are authenticated using the HMAC-MD5 algorithm.
 - *SHA Key* — Users are authenticated using the HMAC-SHA-96 authentication level.
 - *MD5 Password* — The HMAC-MD5-96 password is used for authentication. The user should enter a password.
 - *SHA Password* — Users are authenticated using the HMAC-SHA-96 authentication level. The user should enter a password.
 - *No Authentication* — No user authentication is used.


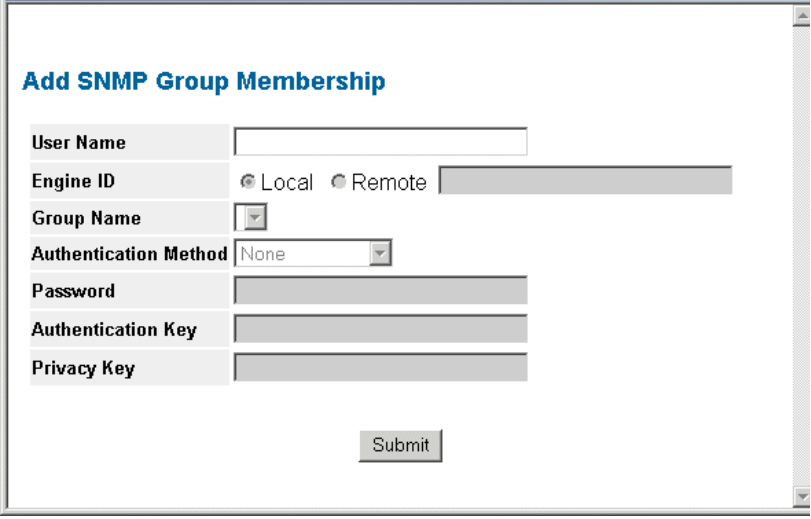

- **Remove** — Removes users from a specified group. The possible field values are:
 - *Checked* — Removes the selected user.
 - *Unchecked* — Maintains the list of users.
2. Click . The *Add SNMP Group Membership Page* opens:

Figure 146: Add SNMP Group Membership Page



In addition to the fields in the *SNMP Group Membership Page*, the *Add SNMP Group Membership Page* contains the following fields:

- **Authentication Method** — Defines the SNMP Authentication Method.
 - **Password** — Defines the password for the group member
 - **Authentication Key** — Defines the HMAC-MD5-96 or HMAC-SHA-96 authentication level. The authentication and privacy keys are entered to define the authentication key. If only authentication is required, 16 bytes are defined. If both privacy and authentication are required, 32 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or a colon.
 - **Privacy Key** — Defines the privacy key (LSB). If only authentication is required, 20 bytes are defined. If both privacy and authentication are required, 36 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon.
3. Define the *User Name*, *Group Name*, *Engine ID*, *Authentication Method*, *Password*, *Authentication Key*, and *Privacy Key* fields.
 4. Click . The SNMP group membership is modified, and the device is updated.

To modify SNMP Group Membership Settings:


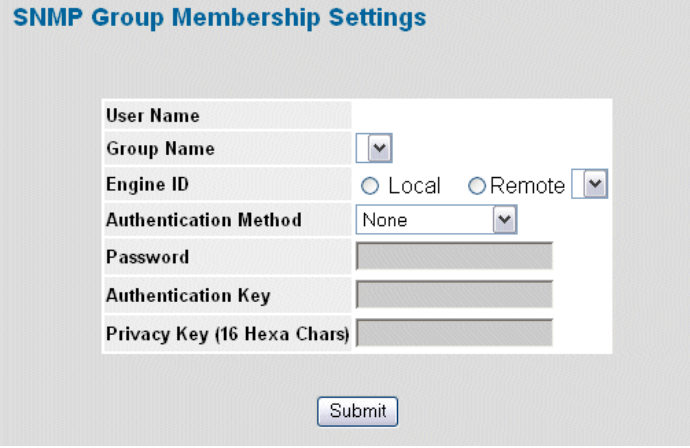

1. Click **System > SNMP > Security > Group Membership**. The *SNMP Group Membership Page* opens.
2. Click . The *SNMP Group Membership Settings Page* opens:

Figure 147: SNMP Group Membership Settings Page



The image shows a web form titled "SNMP Group Membership Settings". The form contains the following fields and controls:

- User Name:** A text input field.
- Group Name:** A dropdown menu.
- Engine ID:** Radio buttons for "Local" and "Remote", followed by a dropdown menu.
- Authentication Method:** A dropdown menu with "None" selected.
- Password:** A text input field.
- Authentication Key:** A text input field.
- Privacy Key (16 Hexa Chars):** A text input field.
- Submit:** A button located below the form fields.

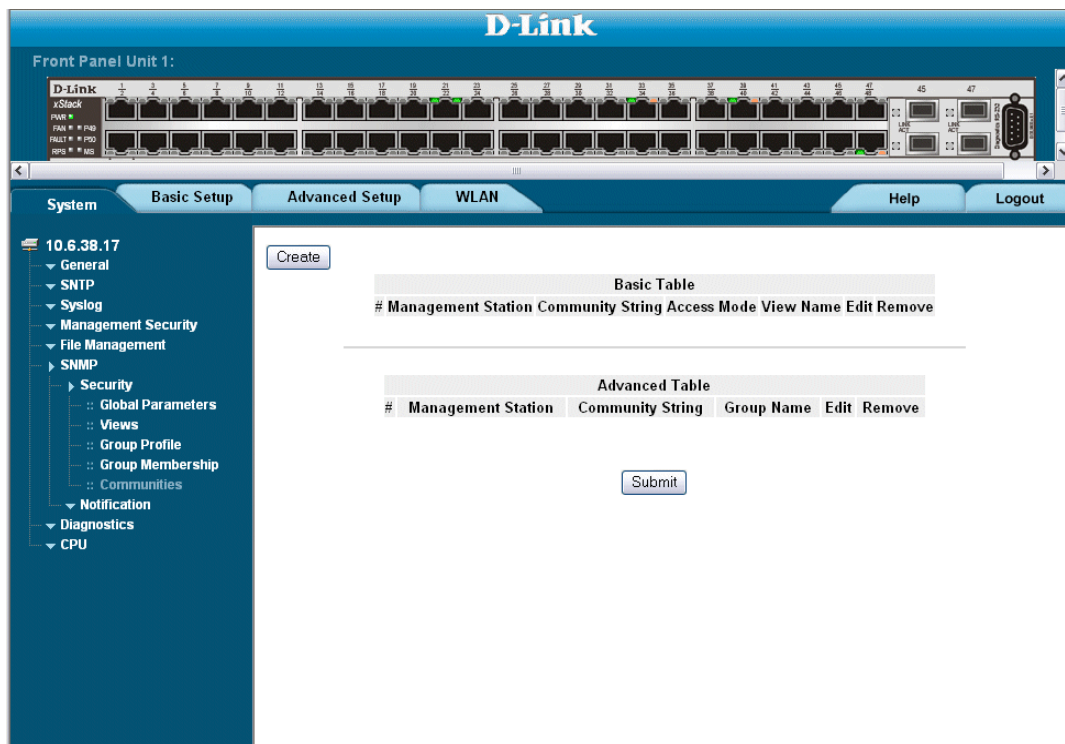
3. Modify the *Group Name*, *Engine ID*, *Authentication Method*, *Password*, *Authentication Key*, and *Privacy Key* fields.
4. Click . The SNMP group membership is modified, and the device is updated.

Defining SNMP Communities

Access rights are managed by defining communities in the *SNMP Communities Page*. When the community names are changed, access rights are also changed. SNMP communities are defined only for SNMP v1 and SNMP v2c. To define SNMP communities:

1. Click **System > SNMP > Security > Communities**. The *SNMP Communities Page* opens:

Figure 148: SNMP Communities Page



The *SNMP Communities Page* is divided into the following tables:

- Basic Table
- Advanced Table

SNMP Communities Basic Table

The *SNMP Communities Basic Table* contains the following fields:

- **Management Station** — Displays the management station IP address for which the basic SNMP community is defined.
- **Community String** — Defines the password used to authenticate the management station to the device.
- **Access Mode** — Defines the access rights of the community. The possible field values are:
 - *Read Only* — Management access is restricted to read-only, and changes cannot be made to the community.

- *Read Write* — Management access is read-write and changes can be made to the device configuration, but not to the community.
- *SNMP Admin* — User has access to all device configuration options, as well as permissions to modify the community.
- **View Name** — Contains a list of user-defined SNMP views
- **Remove** — Removes a community. The possible field values are:
 - *Checked* — Removes the selected SNMP community.
 - *Unchecked* — Maintains the SNMP communities.

SNMP Communities Advanced Tables

The *SNMP Communities Advanced Table* contains the following fields:

- **Management Station** — Displays the management station IP address for which the advanced SNMP community is defined.
 - **Community String** — Defines the password used to authenticate the management station to the device.
 - **Group Name** — Defines advanced SNMP community group names.
 - **Remove** — Removes a community. The possible field values are:
 - *Checked* — Removes the selected SNMP communities.
 - *Unchecked* — Maintains the SNMP communities.
2. Click . The *Add SNMP Community Page* opens:

Figure 149: Add SNMP Community Page

The screenshot shows a web form titled "Add SNMP Community". The form contains the following elements:

- SNMP Management Station:** A radio button selected for a text input field containing "(X.X.X.X)", and another radio button for "All (0.0.0.0)".
- Community String:** A text input field.
- Basic:** A radio button selected. It includes "Access Mode" set to "Read Only" and "View Name" set to "Default".
- Advanced:** A radio button. It includes a "Group Name" dropdown menu.
- Submit:** A button at the bottom of the form.

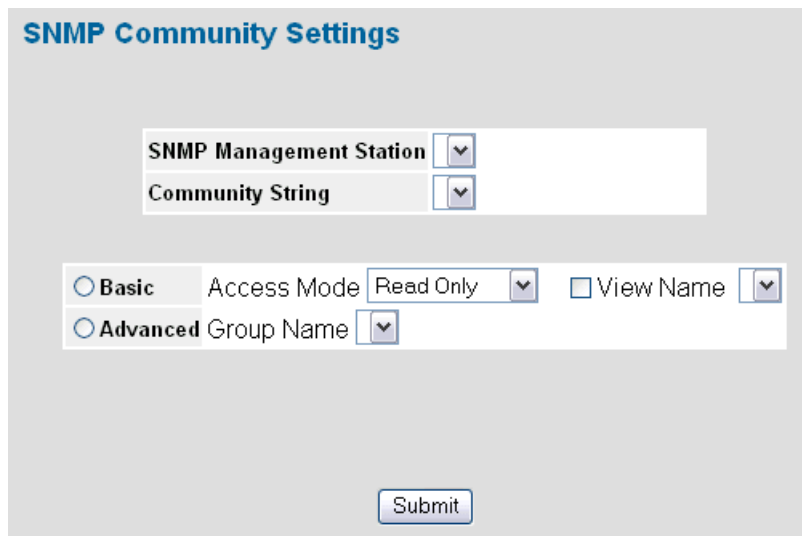
3. Define the *SNMP Management Station*, *Community String*, and *Basic or Advanced* fields.
4. Click . The SNMP community is added, and the device is updated.

To modify SNMP Group Membership Settings:


1. Click **System > SNMP > Security > Communities**. The *SNMP Communities Page* opens.

2. Click  . The *SNMP Community Settings Page* opens:

Figure 150: SNMP Community Settings Page



The screenshot shows the 'SNMP Community Settings' page. It features a title 'SNMP Community Settings' in blue. Below the title, there are two dropdown menus: 'SNMP Management Station' and 'Community String'. Underneath these, there are two radio button options: 'Basic' and 'Advanced'. The 'Basic' option is selected. To the right of the 'Basic' option, there is an 'Access Mode' dropdown menu set to 'Read Only' and a 'View Name' dropdown menu. The 'Advanced' option has a 'Group Name' dropdown menu. At the bottom center of the form is a 'Submit' button.

3. Modify the *SNMP Management Station*, *Community String*, and *Basic or Advanced* fields.
4. Click  . The SNMP community is modified, and the device is updated.

Configuring SNMP Notifications

This section contains information for configuring SNMP Notifications, and contains the following topics:

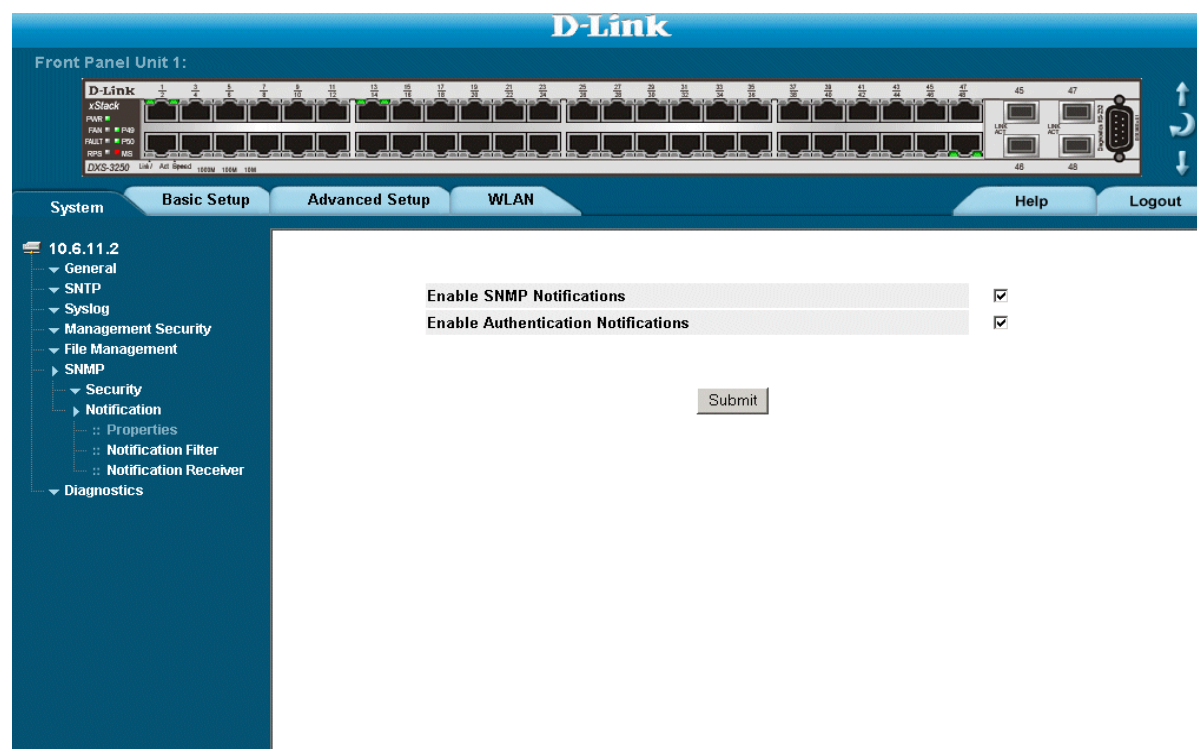
- Defining SNMP Notification Global Parameters
- Defining SNMP Notification Filters
- Defining SNMP Notification Recipients

Defining SNMP Notification Global Parameters

The *SNMP Notification Properties Page* contains parameters for defining SNMP notification parameters. To define SNMP notification global parameters:

1. Click **System > SNMP > Notification > Properties**. The *SNMP Notification Properties Page* opens:

Figure 151: SNMP Notification Properties Page



The *SNMP Notification Properties Page* contains the following fields:

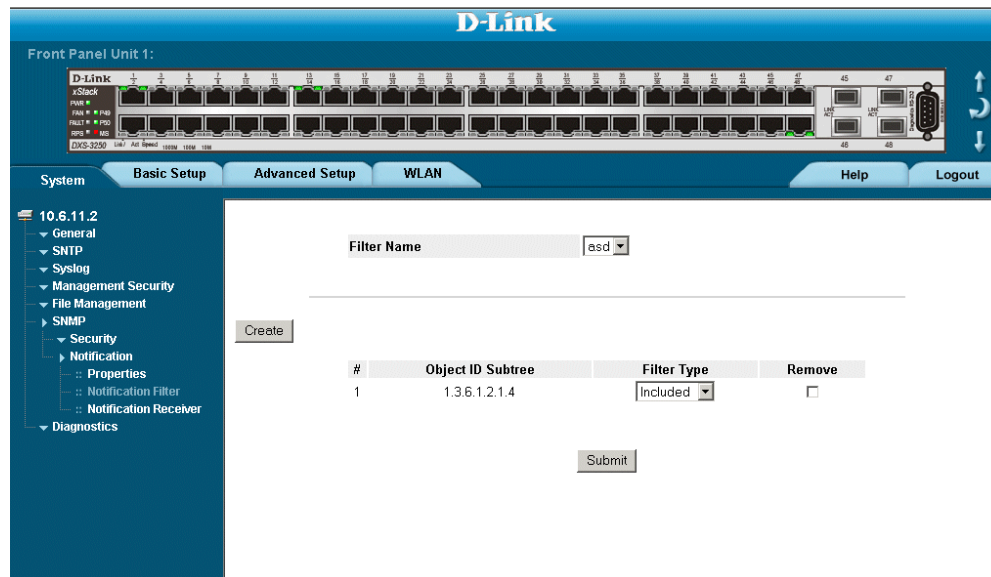
- **Enable SNMP Notifications** — Specifies whether the device can send SNMP notifications. The possible field values are:
 - *Enable* — Enables SNMP notifications.
 - *Disable* — Disables SNMP notifications.
 - **Enable Authentication Notifications** — Specifies whether SNMP authentication failure notification is enabled on the device. The possible field values are:
 - *Enable* — Enables the device to send authentication failure notifications.
 - *Disable* — Disables the device from sending authentication failure notifications.
2. Define the *Enable SNMP Notification* and *Enable Authentication Notifications* fields.
 3. Click **Submit**. The SNMP notification properties are defined, and the device is updated.

Defining SNMP Notification Filters

The *SNMP Notification Filter Page* permits filtering traps based on OIDs. Each OID is linked to a device feature or a portion of a feature. The *SNMP Notification Filter Page* also allows network managers to filter notifications. To define SNMP notification filters:

1. Click **System > SNMP > Notification > Notification Filter**. The *SNMP Notification Filter Page* opens:

Figure 152: SNMP Notification Filter Page



The *SNMP Notification Filter Page* contains the following fields:

- **Filter Name** — Contains a list of user-defined notification filters.
- **Object Identifier Subtree** — Displays the OID for which notifications are sent or blocked. If a filter is attached to an OID, traps or informs are generated and sent to the trap recipients. OIDs are selected from either the *Select from* field or the *Object ID* field.
- **Filter Type** — Indicates whether to send traps or informs relating to the selected OID.
 - *Excluded* — Does not send traps or informs.
 - *Included* — Sends traps or informs.
- **Remove** — Deletes filters.
 - Checked — Deletes the selected filter.
 - Unchecked — Maintains the list of filters.

2. Click **Create**. The *Add SNMP Notification Filter Page* opens:

Figure 153: Add SNMP Notification Filter Page

Add SNMP Notification Filter

Filter Name

New Object Identifier Tree Select from List

- system
- interfaces
- ip
- icmp
- tcp

Up Down

Object ID

Filter Type

Submit

3. Define the *Filter Name*, *New Object Identifier Tree*, and *Filter Type* fields.
4. Click . The SNMP notification filter is defined, and the device is updated.

Defining SNMP Notification Recipients

The *SNMP Notification Receiver Page* contains information for defining filters that determine whether traps are sent to specific users, and the trap type sent. SNMP notification filters provide the following services:

- Identifying Management Trap Targets
- Trap Filtering
- Selecting Trap Generation Parameters
- Providing Access Control Checks

To define SNMP notification filters:

1. Click **System > SNMP > Notification > Notification Receiver**. The *SNMP Notification Receiver Page* opens:

Figure 154: SNMP Notification Receiver Page

The screenshot shows the D-Link web interface for configuring SNMP notification recipients. The page is titled "SNMPv1,2 Notification Recipient" and "SNMPv3 Notification Recipient".

SNMPv1,2 Notification Recipient Table:

#	Recipients IP	Notification Type	Community String	Notification Version	UDP Filter Port Name	Timeout	Retries	Edit	Remove
1	10.6.5.38	Traps	public	SNMPv2	162	15	3		<input type="checkbox"/>
2	10.6.22.8	Traps	public	SNMPv2	162	15	3		<input type="checkbox"/>

SNMPv3 Notification Recipient Table:

#	Recipients IP	Notification Type	User Name	Security Level	UDP Filter Port Name	Timeout	Retries	Edit	Remove
---	---------------	-------------------	-----------	----------------	----------------------	---------	---------	------	--------

The page also includes a "Submit" button at the bottom.

The *SNMP Notification Receiver Page* is divided into the following tables:

- SNMPv1,2c Notification Recipient
- SNMPv3 Notification Recipient

SNMPv1,2c Notification Recipient

The *SNMP v1, v2c Recipient* table contains the following fields:

- **Recipients IP** — Displays the IP address to which the traps are sent.
- **Notification Type** — Displays the notification sent. The possible field values are:
 - *Trap* — Indicates traps are sent.
 - *Inform* — Indicates informs are sent.
- **Community String** — Displays the community string of the trap manager.
- **Notification Version** — Displays the trap type. The possible field values are:
 - *SNMP V1* — Indicates that SNMP Version 1 traps are sent.
 - *SNMP V2c* — Indicates that SNMP Version 2 traps are sent.
- **UDP Port** — Displays the UDP port used to send notifications. The default is 162.
- **Filter Name** — Indicates if the SNMP filter for which the SNMP Notification filter is defined.
- **Timeout** — Indicates the amount of time (in seconds) the device waits before re-sending informs. The default is 15 seconds.
- **Retries** — Indicates the amount of times the device re-sends an inform request. The default is 3 seconds.
- **Remove** — Deletes the currently selected recipient. The possible field values are:
 - *Checked* — Removes the selected recipient from the list of recipients.
 - *Unchecked* — Maintains the list of recipients.

SNMPv3 Notification Recipient

The *SNMPv3 Notification Recipient* table contains the following fields:

- **Recipient IP** — Displays the IP address to which the traps are sent.
- **Notification Type** — Displays the type of notification sent. The possible field values are:
 - *Trap* — Indicates that traps are sent.
 - *Inform* — Indicates that informs are sent.
- **User Name** — Displays the user to which SNMP notifications are sent.
- **Security Level** — Displays the means by which the packet is authenticated. The possible field values are:
 - *No Authentication* — Indicates that the packet is neither authenticated nor encrypted.
 - *Authentication* — Indicates that the packet is authenticated.
- **UDP Port** — The UDP port used to send notifications. The field range is 1-65535. The default is 162.
- **Filter Name** — Includes or excludes SNMP filters.
- **Timeout** — The amount of time (seconds) the device waits before resending informs. The field range is 1-300. The default is 10 seconds.
- **Retries** — The amount of times the device resends an inform request. The field range is 1-255. The default is 3.
- **Remove** — Deletes the currently selected recipient. The possible field values are:
 - *Checked* — Removes the selected recipient from the list of recipients.
 - *Unchecked* — Maintains the list of recipients.

2. Click . The *Add SNMP Notification Receiver Page* opens:

Figure 155: Add SNMP Notification Receiver Page

Add SNMP Notification Receiver

Recipient IP

Notification Type

SNMPv1,2

Community String

Notification Version

SNMPv3

User Name

Security Level

UDP Port

Filter Name

Timeout (sec)

Retries

3. Define the fields.

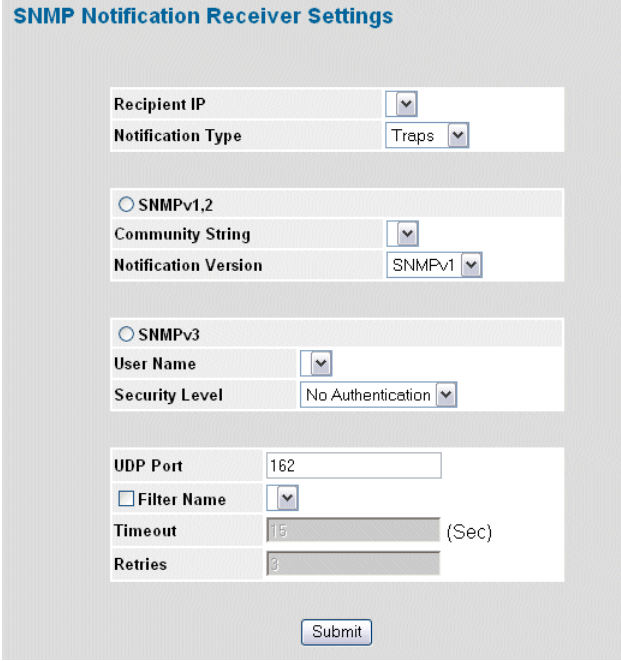
4. Click . The SNMP Notification recipients are defined, and the device is updated.

To modify SNMP notification recipients:

1. Click **System > SNMP > Notification > Notification Receiver**. The *SNMP Notification Receiver Page* opens.

2. Click . The *SNMP Notification Receiver Settings Page* opens:

Figure 156: SNMP Notification Receiver Settings Page



The image shows a web form titled "SNMP Notification Receiver Settings". The form is organized into several sections:

- Recipient IP**: A dropdown menu.
- Notification Type**: A dropdown menu with "Traps" selected.
- SNMPv1.2**: A radio button is selected. Below it are:
 - Community String**: A dropdown menu.
 - Notification Version**: A dropdown menu with "SNMPv1" selected.
- SNMPv3**: A radio button is unselected. Below it are:
 - User Name**: A dropdown menu.
 - Security Level**: A dropdown menu with "No Authentication" selected.
- UDP Port**: A text input field containing "162".
- Filter Name**: A checkbox followed by a dropdown menu.
- Timeout**: A text input field containing "15" followed by "(Sec)".
- Retries**: A text input field containing "3".

At the bottom of the form is a "Submit" button.

3. Modify the fields.
4. Click **Submit**. The SNMP notification recipients are defined, and the device is updated.

This page is left blank intentionally.

Section 18. Configuring Quality of Service

This section contains information for configuring QoS, and includes the following topics:

- Quality of Service Overview
- Defining General QoS Settings
- Configuring QoS Mapping

Click . The policy is bound to the interface, and the device is updated.

Quality of Service Overview

Quality of Service (QoS) provides the ability to implement QoS and priority queuing within a network. For example, certain types of traffic that require minimal delay, such as Voice, Video, and real-time traffic can be assigned a high priority queue, while other traffic can be assigned a lower priority queue. The result is an improved traffic flow for traffic with high demand. QoS is defined by:

- **Classification** — Specifies which packet fields are matched to specific values. All packets matching the user-defined specifications are classified together.
- **Action** — Defines traffic management where packets are forwarded are based on packet information, and packet field values such as *VLAN Priority Tag* (VPT) and *DiffServ Code Point* (DSCP).

VPT Classification Information

VLAN Priority Tags (VPT) are used to classify packets by mapping packets to one of the egress queues. VPT-to-queue assignments are user-definable. Packets arriving untagged are assigned a default VPT value, which is set on a per-port basis. The assigned VPT is used to map the packet to the egress queue.

CoS Services

After packets are assigned to a specific egress queue, CoS services can be assigned to the queue. Egress queues are configured with a scheduling scheme by one of the following methods:

- **Strict Priority** — Ensures that time-sensitive applications are always forwarded. Strict Priority (SP) allows the prioritization of mission-critical, time-sensitive traffic over less time-sensitive applications. For example, under SP, voice over IP (VoIP) traffic can be prioritized so that it is forwarded before FTP or e-mail (SMTP) traffic.
- **Weighted Round Robin** — Ensures that a single application does not dominate the device forwarding capacity. Weighted Round Robin (WRR) forwards entire queues in a round robin order. All queues can participate in WRR, except SP queues. SP queues are serviced before WRR queues. If the traffic flow is minimal, and SP queues do not occupy the whole bandwidth allocated to a port, the WRR queues can share the bandwidth with the SP queues. This ensures that the remaining bandwidth is distributed according to the weight ratio. If WRR is selected, the following weights are assigned to the queues: 1, 2, 4, 8.

Defining General QoS Settings

This section contains information for defining general QoS settings and includes the following topics:

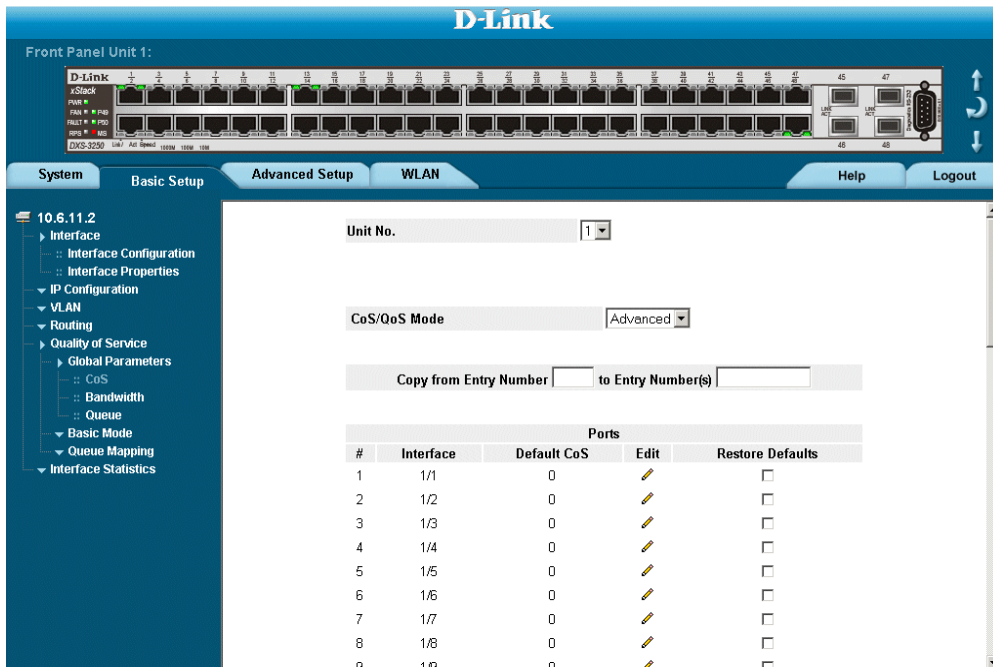
- Configuring QoS General Settings
- Configure Bandwidth Settings
- Defining Queues

Configuring QoS General Settings

The *CoS Page* contains information for enabling QoS globally and on specific interfaces. After QoS has been configured, the original device QoS default settings can be reassigned to the interface in the *CoS Page*. To enable QoS:

1. Click **Basic Setup > Quality of Service > Global Parameters > CoS**. The *CoS Page* opens:

Figure 157: CoS Page



The *CoS* Page contains the following:

- **Quality of Service** — Determines whether QoS is enabled on the interface. The possible values are:
 - *Enable* — Enables QoS on the interface.
 - *Disable* — Disables QoS on the interface.
- **Trust Mode** — Defines which packet fields to use for classifying packets entering the device. When no rules are defined, the traffic containing the predefined packet CoS field is mapped according to the relevant trust modes table. Traffic not containing a predefined packet field is mapped to best effort. The possible Trust Mode field values are:
 - *CoS* — Classifies traffic based on the CoS tag value.
 - *DSCP* — Classifies traffic based on the DSCP tag value.
- **Copy from Entry Number**— Indicates the row number from which CoS parameters are copied.
- **to Entry Number(s)**— Indicates the row number to which CoS parameters are copied.
- **Interface** — Displays the interface for which the global QoS parameters are defined.
 - *Port* — Selects the port for which the global QoS parameters are defined.
 - *LAG* — Selects the LAG for which the global QoS parameters are defined.
- **Default CoS for Incoming Traffic**— Determines the default CoS value for incoming packets for which a VLAN tag is not defined. The possible field values are **0-7**. The default CoS is **0**.

2. Select *Enable* in the *Quality of Service* field.
3. Define the *Trust Mode* field.
4. Click **Submit**. Quality of Service is enabled on the device.

Restoring Factory Default QoS Interface Settings

1. Click **Basic Setup > Quality of Service > General Settings > General Settings**. The *CoS Page* opens.
2. Select an interface by clicking the
3. Check the Restore Defaults checkbox.
4. Click **Submit**. The factory defaults are restored on the interface.

Configure Bandwidth Settings

The *Bandwidth Settings Page* allows network managers to define the bandwidth settings for a specified egress interface. Modifying queue scheduling affects the queue settings globally.

Queue shaping can be based per queue and/or per interface. Shaping is determined by the lower specified value. The queue shaping type is selected in the *Bandwidth Settings Page*.

To define bandwidth settings:

1. Click **Basic Setup > Quality of Service > Global Parameters > Bandwidth**. The *Bandwidth Settings Page* opens:

Figure 158: Bandwidth Settings Page

The screenshot shows the D-Link web interface for configuring bandwidth settings. The top navigation bar includes 'System', 'Basic Setup', 'Advanced Setup', 'WLAN', 'Help', and 'Logout'. The left sidebar shows a tree view with 'Quality of Service' expanded to 'Bandwidth'. The main content area shows a table of bandwidth settings for ports 1/1 through 1/16. The table has columns for '#', 'Port', 'Ingress Rate Limit' (Status and Rate Limit), 'Egress Shaping Rates' (Status, CIR, and CbS), and an 'Edit' column with a pencil icon.

#	Port	Ingress Rate Limit		Egress Shaping Rates			Edit
		Status	Rate Limit	Status	CIR	CbS	
1	1/1	Disable		Disable			
2	1/2	Disable	0	Disable	0	128000	
3	1/3	Disable	0	Disable	0	128000	
4	1/4	Disable		Disable			
5	1/5	Disable		Disable			
6	1/6	Disable		Disable			
7	1/7	Disable		Disable			
8	1/8	Disable		Disable			
9	1/9	Disable		Disable			
10	1/10	Disable		Disable			
11	1/11	Disable		Disable			
12	1/12	Disable		Disable			
13	1/13	Disable		Disable			
14	1/14	Disable		Disable			
15	1/15	Disable		Disable			
16	1/16	Disable		Disable			

The *Bandwidth Settings Page* contains the following fields:


- **Unit no**— Indicates the stacking members for which the bandwidth settings are displayed.
 - **Port**— Indicates the port that is being displayed
 - **Ingress Rate Limit** — Indicates the traffic limit for the port.
 - **Egress Shaping Rates** — Configures the traffic shaping type for selected interfaces. The possible field values are:
 - *CIR* — Defines CIR as the queue shaping type. The possible field value is 4096 - 1,000,000,000 bits per second.
 - *CBS* — Defines CBS as the queue shaping type. The possible field value is 4096-16,000,000 bytes.
 - **Remove** — Deletes the currently selected view. The possible field values are:
 - *Checked* — Removes the settings for the selected port.
 - *Unchecked* — Maintains the settings.
2. Select an interface.
3. Click  . The *Bandwidth Settings Edit Page* opens.

Figure 159: Bandwidth Settings Edit Page

Bandwidth Settings

Interface Port LAG

Egress Shaping Rate on Selected Port

Committed Information Rate (CIR) (64-10000000 Kbps)

Committed Information Rate (CIR) (0.07-9765.63 Mbps)

Committed Burst Size (CbS) (4096-10000000 Kbps)

Committed Burst Size (CbS) (4-9765.63 Mbps)

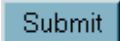
Ingress Rate Limit Status

Rate Limit (1-10000000 Kbps)

Rate Limit (0.01-9765.63 Mbps)

Shaping per Queue on Selected Port

Queue		CIR Bits per Second	CBS Bytes
1	<input type="checkbox"/>	<input type="text" value="64"/>	<input type="text" value="4096"/>
2	<input type="checkbox"/>	<input type="text" value="64"/>	<input type="text" value="4096"/>
3	<input type="checkbox"/>	<input type="text" value="64"/>	<input type="text" value="4096"/>
4	<input type="checkbox"/>	<input type="text" value="64"/>	<input type="text" value="4096"/>
5	<input type="checkbox"/>	<input type="text" value="64"/>	<input type="text" value="4096"/>
6	<input type="checkbox"/>	<input type="text" value="64"/>	<input type="text" value="4096"/>
7	<input type="checkbox"/>	<input type="text" value="64"/>	<input type="text" value="4096"/>
8	<input type="checkbox"/>	<input type="text" value="64"/>	<input type="text" value="4096"/>

4. Define the fields.
5. Click  . The bandwidth settings are saved to interface, and the device is updated.

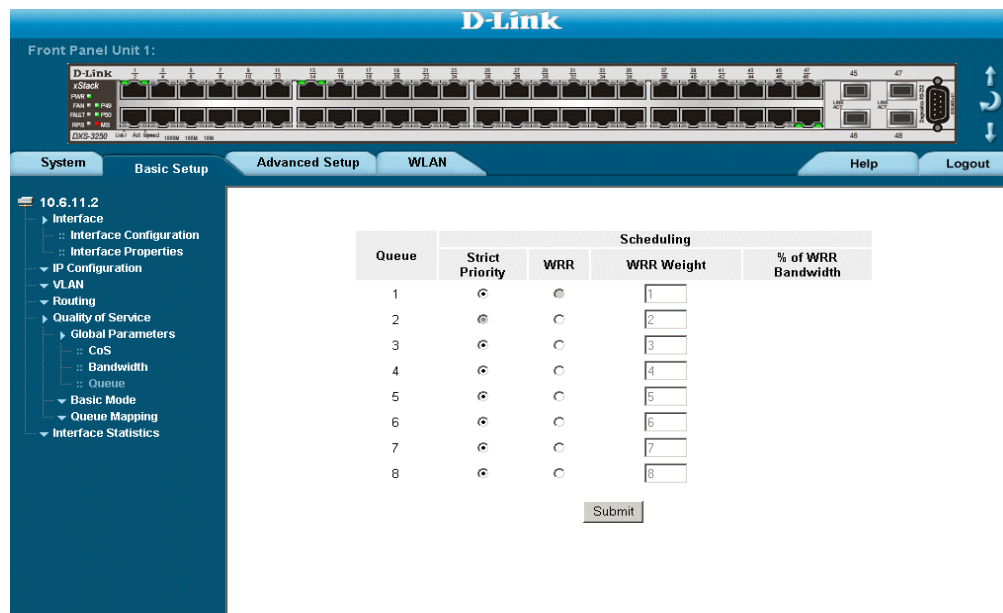
Defining Queues

The *Queue Page* contains fields for defining the QoS queue forwarding types.

To set the queue settings:

1. Click **Basic Setup > Quality of Service > Global Parameters > Queue**. The *Queue Page* opens.

Figure 160: Queue Page



The *Queue Page* contains the following fields:

- **Strict Priority** — Specifies whether traffic scheduling is based strictly on the queue priority.
 - **WRR** — Assigns WRR weights to queues. This field is enabled only for queues in WRR queue mode. If a queue is set to 0 weight, the queue is not operational and is effectively closed. Each queue has a weight range, queues 1-3 have the range 0-255, and queue 4 has the range 1-255.
 - **WRR Weight** — Assigns the specific WRR value to the Queue.
 - **% of WRR Bandwidth** — Displays the amount of bandwidth assigned to the queue. These values are fixed and are not user defined.
2. Select *Strict Priority* or *WRR Fields*.
 3. Click **Submit**. The queue settings are set, and the device is updated.

Configuring QoS Mapping

This section contains information for mapping CoS and DSCP values to queues, and includes the following sections:

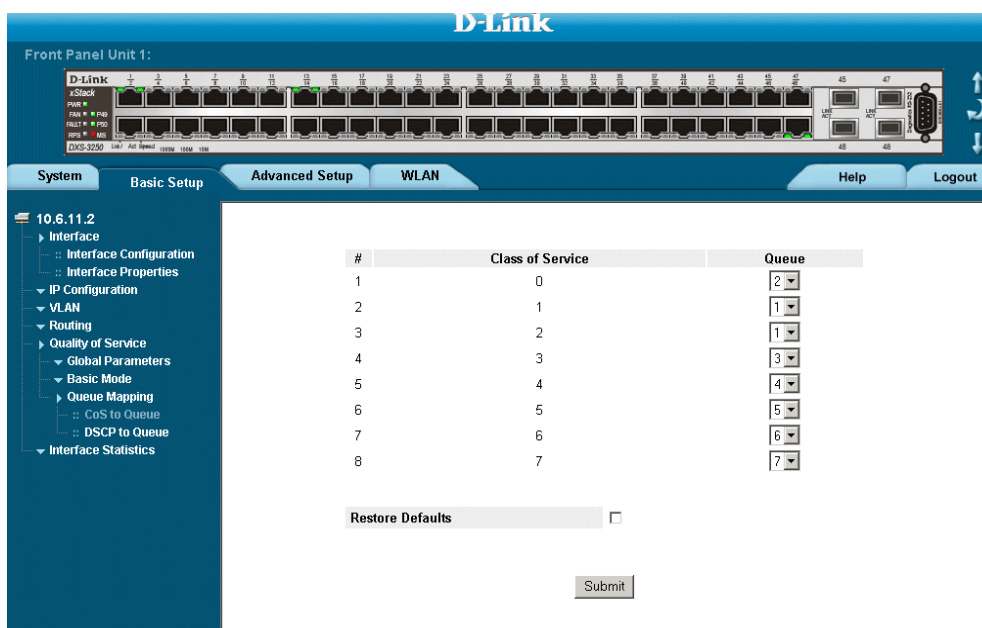
- Mapping CoS Values to Queues
- Mapping DSCP Values to Queues

Mapping CoS Values to Queues

The *CoS to Queue Page* contains fields for mapping CoS values to traffic queues. To map CoS values to queues:

1. Click **Basic Setup > Quality of Service > Queue Mapping > CoS to Queue**. The *CoS to Queue Page* opens.

Figure 161: CoS to Queue Page



The *CoS to Queue Page* contains the following fields:

- **Class of Service** — Specifies the CoS priority tag values, where zero is the lowest and 7 is the highest.
- **Queue** — Defines the traffic forwarding queue to which the CoS priority is mapped. Eight traffic priority queues are supported.
- **Restore Defaults** — Restores the device factory defaults for mapping CoS values to a forwarding queue.

2. Define the queue number in the *Queue* field next to the required CoS value.
3. Click **Submit**. The CoS value is mapped to a queue, and the device is updated.

Mapping DSCP Values to Queues

The *DSCP to Queue Page* contains fields for mapping DSCP settings to traffic queues. For example, a packet with a DSCP tag value of 3 can be assigned to queue 2. To map CoS values to queues:

1. Click **Basic Setup > Quality of Service > Queue Mapping > DSCP to Queue**. The *DSCP to Queue Page* opens.

Figure 162: DSCP to Queue Page

The screenshot shows the D-Link web interface for configuring DSCP to Queue mapping. The interface includes a navigation menu on the left and a main configuration area with a table of DSCP values and their corresponding queue numbers.

DSCP In	Queue	DSCP In	Queue	DSCP In	Queue
0	1	21	3	42	5
1	1	22	3	43	5
2	1	23	3	44	5
3	1	24	3	45	6
4	1	25	3	46	6
5	1	26	3	47	6
6	1	27	4	48	6
7	1	28	4	49	6
8	1	29	4	50	6
9	2	30	4	51	6
10	2	31	4	52	6
11	2	32	4	53	6
12	2	33	4	54	7
13	2	34	4	55	7

The *DSCP to Queue Page* contains the following fields:

- **DSCP In** — Displays the incoming packet's DSCP value.
 - **Queue** — Specifies the traffic forwarding queue to which the DSCP priority is mapped. Eight traffic priority queues are supported.
2. Define the queue number in the *Queue* field next to the required DSCP value.
 3. Click **Submit**. The DSCP value is mapped to a queue, and the device is updated.

Configuring Advanced QoS Settings

This section contains information for configuring advanced QoS features, and includes the following topics:

- Defining Policy Properties
- Defining Policy Profiles

Defining Policy Properties

This section contains information for configuring advanced policy properties, and includes the following topics:

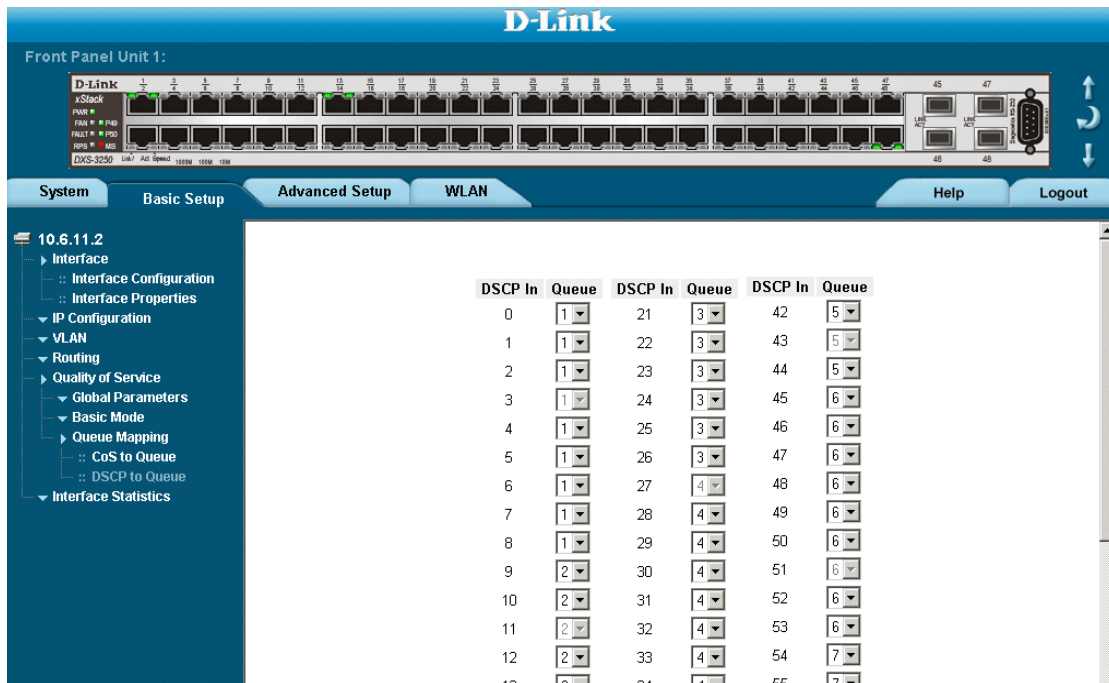
- Mapping DSCP Values
- Defining Tail Dropping
- Creating Class Maps
- Aggregating Policers

Mapping DSCP Values

When traffic exceeds user-defined limits, use the Advanced DSCP to Queue Page to configure the DSCP tag to use in place of the incoming DSCP tags. To define Advance QoS DSCP mapping

1. Click **Basic Setup > Quality of Service > Queue Mapping > DSCP to Queue**. The *Advanced DSCP to Queue Page* opens.

Figure 163: Advanced DSCP to Queue Page



The *Advanced DSCP to Queue Page* contains the following fields:

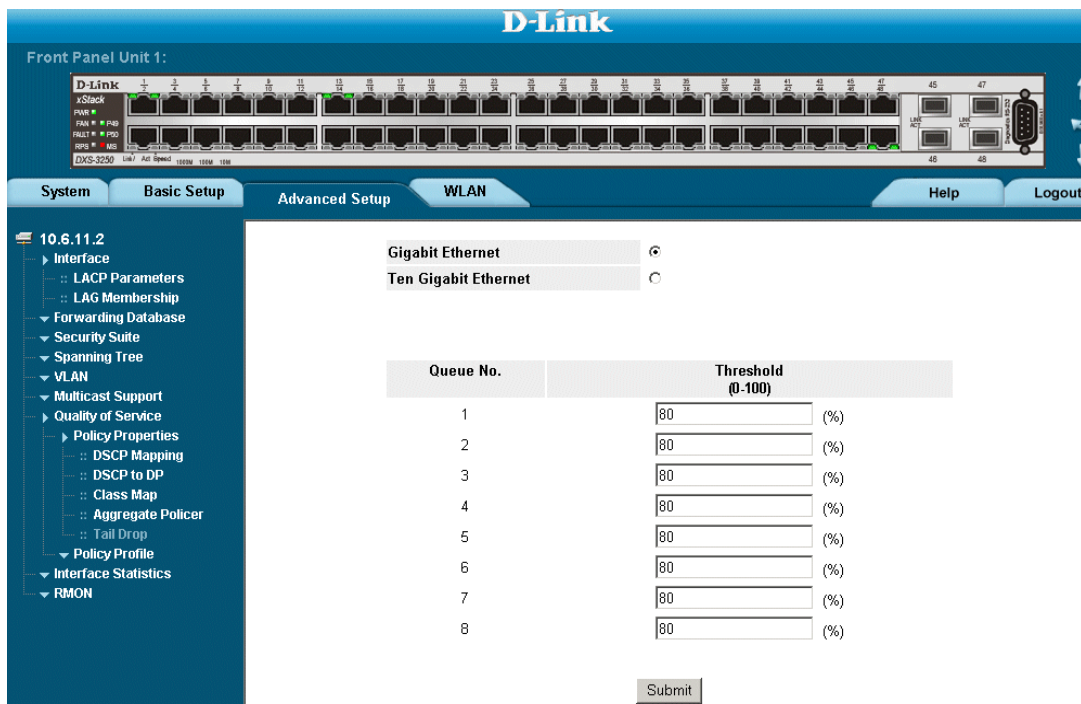
- **DSCP In** — Displays the incoming packet's DSCP value.
 - **Queue** — Specifies the traffic forwarding queue to which the DSCP priority is mapped. Eight traffic priority queues are supported.
2. Define the queue number in the *Queue* field next to the required DSCP value.
 3. Click **Submit**. The Advanced Mode DSCP value is mapped to a queue, and the device is updated.

Defining Tail Dropping

The *Tail Drop Page* permits network managers to set the device to drop packets which exceed the threshold size. Tail Drop is configured per queue.

- Click **Advance Setup > Quality of Service > Policy Properties > Tail Drop**. The *Tail Drop Page* opens.

Figure 164: Tail Drop Page



The *Tail Drop Page* contains the following field:

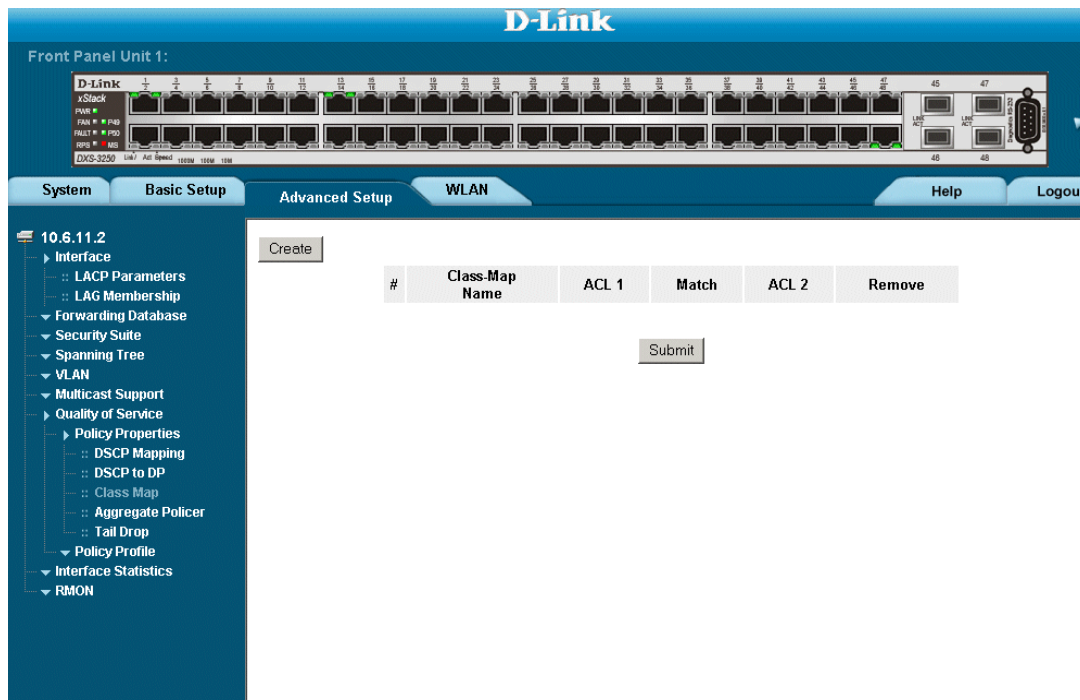
- **Interface** — Defines the Tail Drop policy applied to the interface. The possible field values are:
 - *Tail Drop* — Applies the Tail Drop policy to the interface. All packets exceeding their limit will be dropped.
 - *Default* — Maintains the device defaults.

Creating Class Maps

One IP ACL and/or one MAC ACL comprise a class map. Class maps are configured to match packet criteria, and are matched to packets on a first-fit basis. For example, Class Map A is assigned packets based only on an IP-based ACL or a MAC-based ACL. Class Map B is assigned to packets based on both an IP-based and a MAC-based ACL. To define class maps:

1. Click **Advance Setup > Quality of Service > Policy Properties> Class Map**. The *Class Map Page* opens:

Figure 165: Class Map Page



The *Class Map Page* contains the following fields:


- **Class-Map Name** — Displays the user-defined name of the class map.
- **Preferred ACL** — Indicates if packets are first matched to an IP based ACL or a MAC based ACL.
- **ACL 1**— Contains a list of the user defined ACLs.
- **Match** — Indicates the criteria used to match class maps with an ACL's address. Possible values are:
 - *And* — Matches both ACL 1 and ACL 2 to the packet.
 - *Or* — Matches either ACL 1 or ACL 2 to the packet.
- **ACL 2** — Contains a list of the user defined ACLs.
- **Remove** — Removes Class Maps. The possible field values are:
 - *Checked* — Removes the selected Class Maps.
 - *Unchecked* — Maintains the current Class Maps.

2. Click **Create**. The Add Class Map Page opens.

Figure 166: Add Class Map Page

The screenshot shows a configuration form for adding a class map. It contains the following fields and controls:

- Class Map Name:** A text input field.
- Preferred ACL:** A dropdown menu currently showing "IP Based".
- IP ACL:** A checkbox followed by a dropdown menu.
- Match:** A dropdown menu currently showing "Or".
- MAC ACL:** A checkbox followed by a dropdown menu.
- Submit:** A button located at the bottom center of the form.

3. Define the fields.
4. Click . The Class Map is defined, and the device is updated.

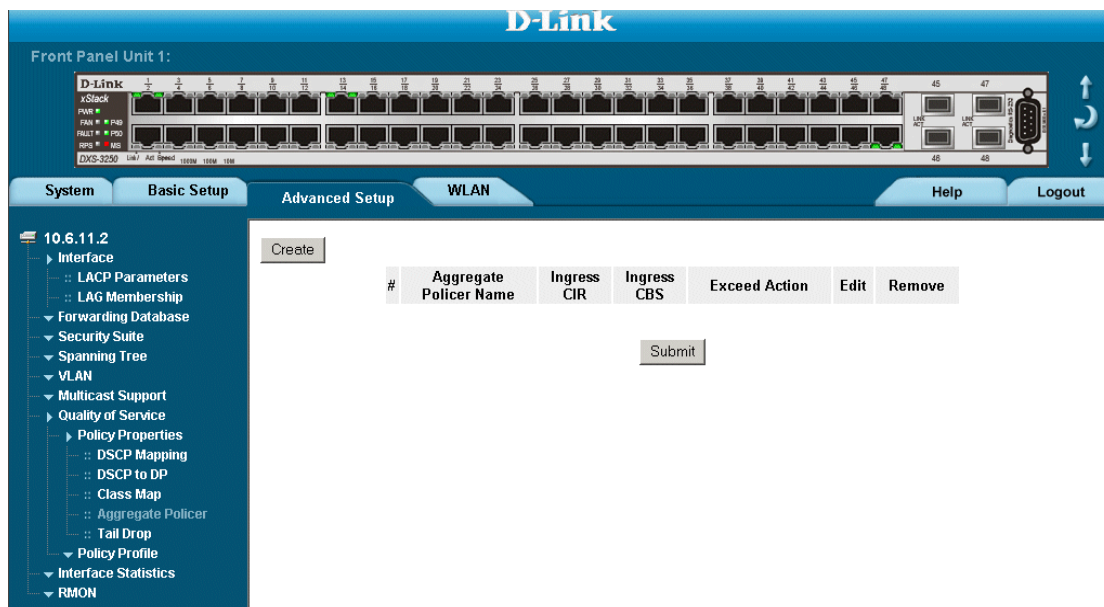
Aggregating Policers

After a packet is classified, the policing process begins. A policier specifies the bandwidth limit for incoming traffic on the classified flow and actions are defined for packets that exceed the limits. These actions include forwarding packets, dropping packets, or remarking packets with a new DSCP value. The device supports per flow and aggregate policiers.

Aggregate policers enforce limits on a group of flows. An aggregate policer cannot be deleted if it is being used in a policy map. The *Aggregated Policier Page* contains information for defining the bandwidth limits and define actions to take on packets that do not meet the requirements. To configure Aggregated Policers:

1. Click **Advance Setup > Quality of Service > Policy Properties > Aggregated Policier**. The *Aggregated Policier Page* opens:

Figure 167: Aggregated Policier Page



The *Aggregated Policier Page* contains the following fields:

- **Aggregate Policier Name** — Specifies the aggregate policier name.
 - **Ingress CIR**— Defines the CIR in bits per second.
 - **Ingress CBS** — Defines the CBS in bytes per second.
 - **Exceed Action** — Indicates the action assigned to incoming information exceeds the traffic limits. Possible values are:
 - *Drop* — Packets exceeding the limits are dropped.
 - *Remark DSCP* — Packets exceeding the limits are forwarded with a flagged/remarked DSCP value.
 - *None* — Packets exceeding the limits are forwarded.
2. Click **Create**. The *Add Aggregated Policier Page* opens.

Figure 168: Add Aggregated Policier Page

Add QoS Aggregate Policier

Aggregate Policier Name	<input type="text"/>	
Ingress Committed Information Rate (CIR)	<input type="text" value="3"/>	(Kbits per Second)
Ingress Committed Burst Size (CBS)	<input type="text" value="3000"/>	(Bytes per second)
Exceed Action	<input type="text" value="None"/>	

3. Define the fields.
4. Click . The Aggregated Policier is defined, and the device is updated.

Defining Policy Profiles

This section contains information for configuring policy profiles, and includes the following topics:

- Defining Policies
- Attaching Policies to Interfaces

Defining Policies

A policy is a collection of classes, each of which is a combination of a class map and a QoS action to apply to matching traffic. Classes are applied in a first-fit manner within a policy.

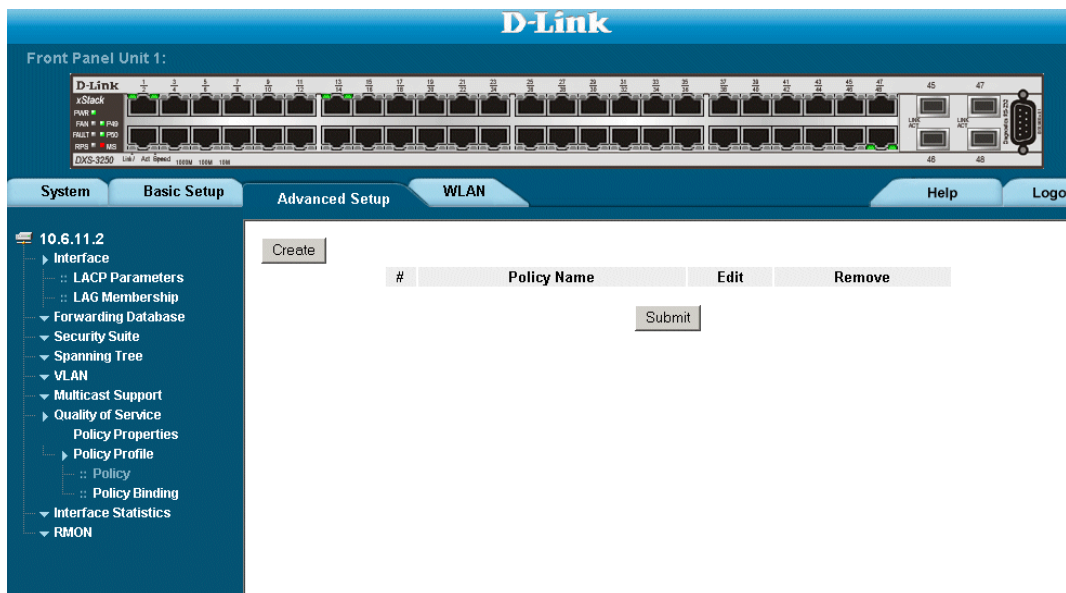
Before configuring policies for classes whose match criteria are defined in a class map, a class map must first be defined, or the name of the policy map to be created, added to, or modified must first be specified. Class policies can be configured in a policy map only if the classes have defined match criteria.

An aggregate policer can be applied to multiple classes in the same policy map, but an aggregate policer cannot be used across different policy maps. Define an aggregate policer if the policer is shared with multiple classes. Policers in one port cannot be shared with other policers in another device. Traffic from two different ports can be aggregated for policing purposes.

To define policies:

1. Click **Advance Setup > Quality of Service > Policy Profiles >Policy**. The *Policy Page* opens:

Figure 169:Policy Page



The *Policy Page* contains the following fields:

- **Policy Name** — Displays the user-defined policy name.

- **Remove** — Removes policies. The possible field values are:
 - *Checked* — Removes the selected policy.
 - *Unchecked* — Maintains policies.
- 2. Click **Create**. The *Add QoS Policy Profile Page* opens:

Figure 170: Add QoS Policy Profile Page

Add QoS Policy Profile

New Policy Name

Class Map

Action Trust Set New Value (0 - 63)

Police

Type

Aggregate Policer

Ingress Committed Information Rate (CIR) (Kbits per Second)

Ingress Committed Burst Size (CBS) (Bytes)

Exceed Action

In addition to the fields in the *Policy Page*, the *Add QoS Policy Profile Page* contains the following fields:

- **Class Map** — Selects a class map for the class.
- **Action** — Optional action for the class. Possible values are:
 - *Trust* — Enables Trust Mode for the class. This command is used to distinguish the QoS trust behavior for given traffic. When a given type is trusted, the QoS mechanism maps a packet to a queue using the received or default value and the relevant map, as defined on the QoS Settings. By designating trust, it is possible to trust only incoming traffic with certain DSCP values.
 - *Set/Mark* — Sets the Trust value to a user-defined value.
 - *New Value* — Defines the Set/Mark value.
- **Police** — Selects the option of configuring a Police entry.
- **Type** — Policer type for the class. Possible values are:
 - *Aggregate* — Configures the class to use a configured aggregate policer selected from the drop-down menu. An aggregate policer is defined if the policer is shared with multiple classes. Traffic from two different ports can be configured for policing purposes. An aggregate policer can be applied to multiple classes in the same policy map, but cannot be used across different policy maps.
 - *Single* — Configures the class to use manually configured information rates and exceed actions.
- **Aggregate Policer** — User-defined aggregate policers.

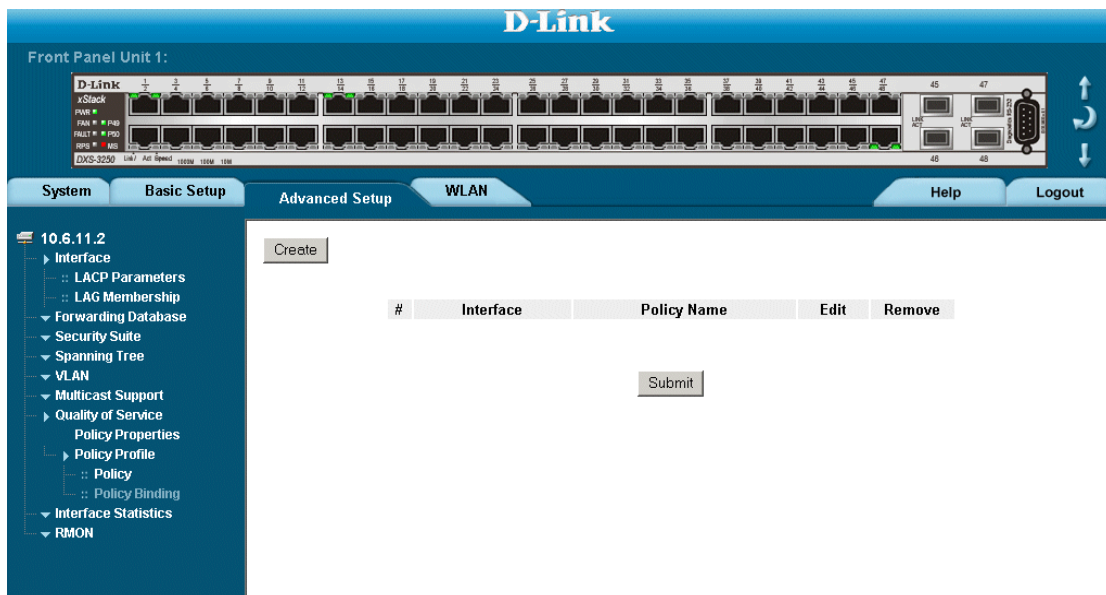
- **Ingress Committed Information Rate (CIR)** — CIR in bits per second. This field is only relevant when the **Police** value is **Single**.
 - **Ingress Committed Burst Size (CBS)** — CBS in bytes per second. This field is only relevant when the **Police** value is **Single**.
 - **Exceed Action** — Action assigned to incoming packets exceeding the CIR. This field is only relevant when the **Police** value is **Single**. Possible values are:
 - *Drop* — Drops packets exceeding the defined CIR value.
 - *Remark DSCP* — Remarks packets' DSCP values exceeding the defined CIR value.
3. Define the fields.
 4. Click . The policy is defined, and the device is updated.

Attaching Policies to Interfaces

The *Policy Binding Page* contains information for attaching policies on interfaces. To attach a policy to an interface:

1. Click **Advance Setup > Quality of Service > Policy Profiles > Policy Binding**. The *Policy Binding Page* opens:

Figure 171: Policy Binding Page



The *Policy Binding Page* contains the following fields:

- **Interface** — Selects an interface.
- **Policy Name** — Contains a list of user-defined policies that can be attached to the interface.
- **Remove** — Removes policies.
 - *Checked* — Removes the selected policies.
 - *Unchecked* — Maintains the policies.

2. Select an interface.
3. Define the *Policy Name* field.
4. Click . The policy is bound to the interface, and the device is updated.

Section 19. Managing System Files

File maintenance includes both configuration file management as well as device access. This section contains the following topics:

- File Management Overview
- Downloading System Files
- Uploading System Files
- Activating Image Files
- Copying Files
- Managing System Files

File Management Overview

The configuration file structure consists of the following configuration files:

- **Startup Configuration File** — Contains the commands required to reconfigure the device to the same settings as when the device is powered down or rebooted. The Startup file is created by copying the configuration commands from the Running Configuration file or the Backup Configuration file.
- **Running Configuration File** — Contains all configuration file commands, as well as all commands entered during the current session. After the device is powered down or rebooted, all commands stored in the Running Configuration file are lost. During the startup process, all commands in the Startup file are copied to the Running Configuration File and applied to the device. During the session, all new commands entered are added to the commands existing in the Running Configuration file. Commands are not overwritten. To update the Startup file, before powering down the device, the Running Configuration file must be copied to the Startup Configuration file. The next time the device is restarted, the commands are copied back into the Running Configuration file from the Startup Configuration file.
- **Image files** — Software upgrades are used when a new version file is downloaded. The file is checked for the right format, and that it is complete. After a successful download, the new version is marked, and is used after the device is reset.

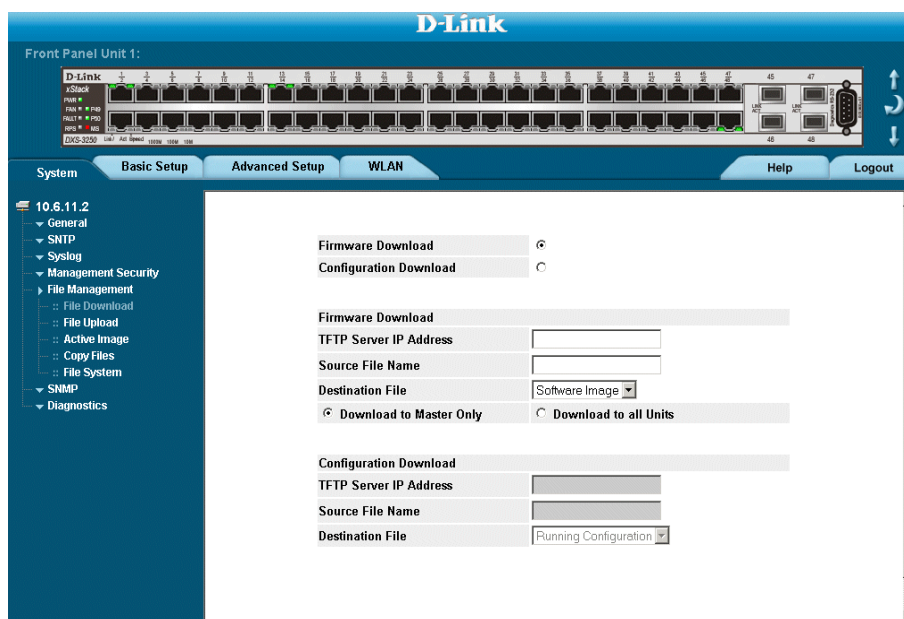
Downloading System Files

There are two types of files, firmware files and configuration files. The firmware files manage the device, and the configuration files configure the device for transmissions. Only one type of download can be performed at any one time. To download a file:

The *File Download* page contains parameters for downloading system files. To download system files:

- Click **System > File Management > File Download**. The *File Download Page* opens.

Figure 172: File Download Page



The *File Download Page* is divided into the following sections:

- Firmware Download
- Configuration Download

Firmware Download

The *Firmware Download* section contains the following fields:

- **Firmware Download** — Indicates that the download is for firmware. If *Firmware Download* is selected, the Configuration Download fields are grayed out.
- **TFTP Server IP Address** — Specifies the TFTP Server IP Address from which files are downloaded.
- **Source File Name** — Specifies the file to be downloaded.
- **Destination File** — Specifies the destination file type to which the file is downloaded. The possible field values are:
 - *Software Image* — Downloads the Image file.
 - *Boot Code* — Downloads the Boot file.

Configuration Download

The *Configuration Download* section contains the following fields:

- **Configuration Download** — Indicates that the download is for configuration files. If *Configuration Download* is selected, the Firmware Download fields are grayed out.
- **TFTP Server IP Address** — Specifies the TFTP Server IP Address from which the configuration files are downloaded.
- **Source File Name** — Specifies the configuration files to be downloaded.
- **Destination File** — Specifies the destination file to which the configuration file is downloaded. The possible field values are:
 - *Running Configuration* — Downloads commands into the Running Configuration file.
 - *Startup Configuration* — Downloads the Startup Configuration file, and overwrites the old Startup Configuration file.

To Download files:

1. Open the *File Download Page*.
2. Select the file type.
3. Define the TFTP server address.
4. Define the *Source File Name* and *Destination File* fields.
5. Click . The files are downloaded.

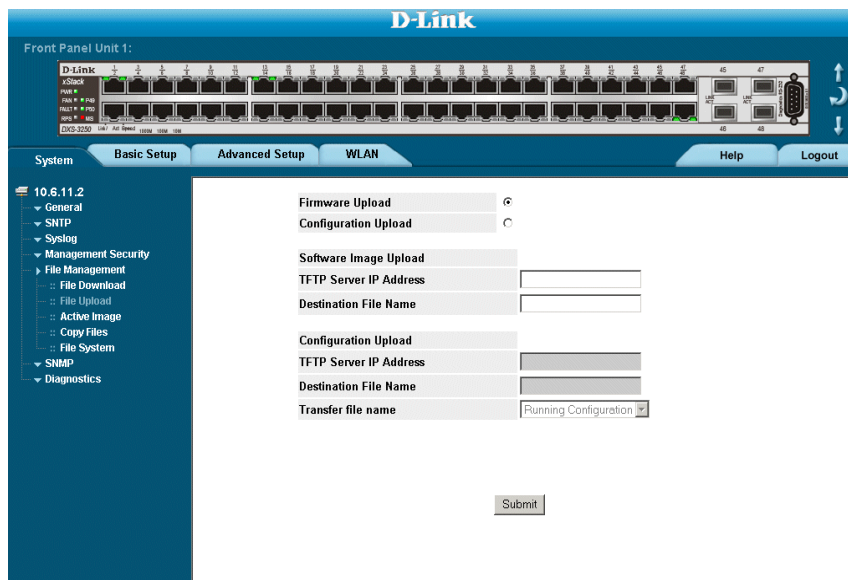
Uploading System Files

The *File Upload Page* contains fields for uploading the software from the device to the TFTP server.

To upload system files:

1. Click **System > File Management > File Upload**. The *File Upload Page* opens:

Figure 173: File Upload Page



The *File Upload Page* is divided into the following sections:

- Software Image Upload
- Configuration Upload

Upload Type

The *Upload Type* section contains the following fields:

- **Firmware Upload** — Specifies that the software image file is uploaded. If *Firmware Upload* is selected, the Configuration Upload fields are grayed out.
- **Configuration Upload** — Specifies that the Configuration file is uploaded. If *Configuration Upload* is selected, the Software Image Upload fields are grayed out.

Software Image Upload

The *Software Image Upload* section contains the following fields:


- **TFTP Server IP Address** — Specifies the TFTP Server IP Address to which the Software Image is uploaded.
- **Destination File Name** — Specifies the software image file path to which the file is uploaded.

Configuration Upload

The *Configuration Upload* section contains the following fields:

- **TFTP Server IP Address** — Specifies the TFTP Server IP Address to which the Configuration file is uploaded.
- **Destination File Name**— Specifies the file name to which the Startup Configuration file is uploaded.
- **Transfer file name** — Specifies the Configuration file name that is uploaded. The possible field values are:
 - *Running Configuration* — Uploads the Running Configuration file.
 - *Startup Configuration* — Uploads the Startup Configuration file.

To upload files:

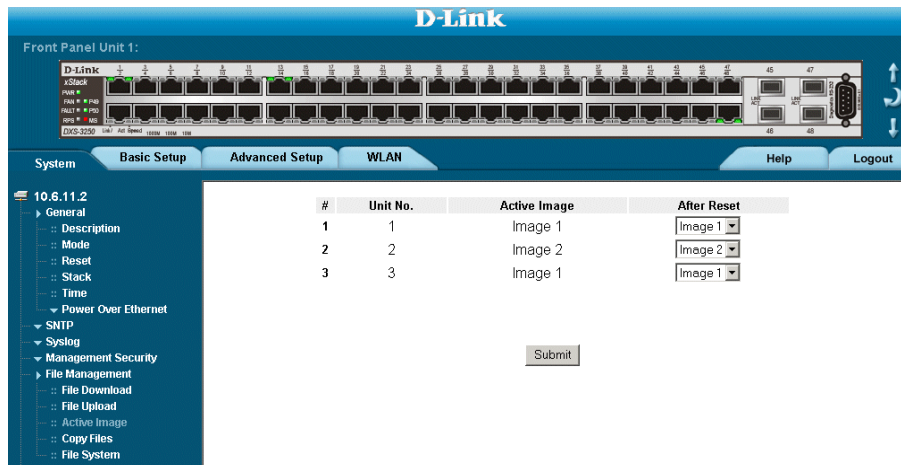
1. Open the *File Upload Page*.
2. Define the file type to upload.
3. Define the fields.
4. Click . The software is uploaded to the device.

Activating Image Files

The *Active Image Page* allows network managers to select and reset the Image files. The Active Image file for each unit in a stacking configuration can be individually selected.

1. Click **System > File Management > Active Image**. The *Active Image Page* opens:

Figure 174: Active Image Page



The *Active Image Page* contains the following fields:

- **Unit No.** — The unit number for which the Image file is selected.
 - **Active Image** — The Image file which is currently active on the unit.
 - **After Reset** — The Image file which is active on the unit after the device is reset. The possible field values are:
 - *Image 1* — Activates Image file 1 after the device is reset.
 - *Image 2* — Activates Image file 2 after the device is reset.
2. Define the *After Reset* field.
 3. Click **Submit**. The select image file is activated after the device is reset.

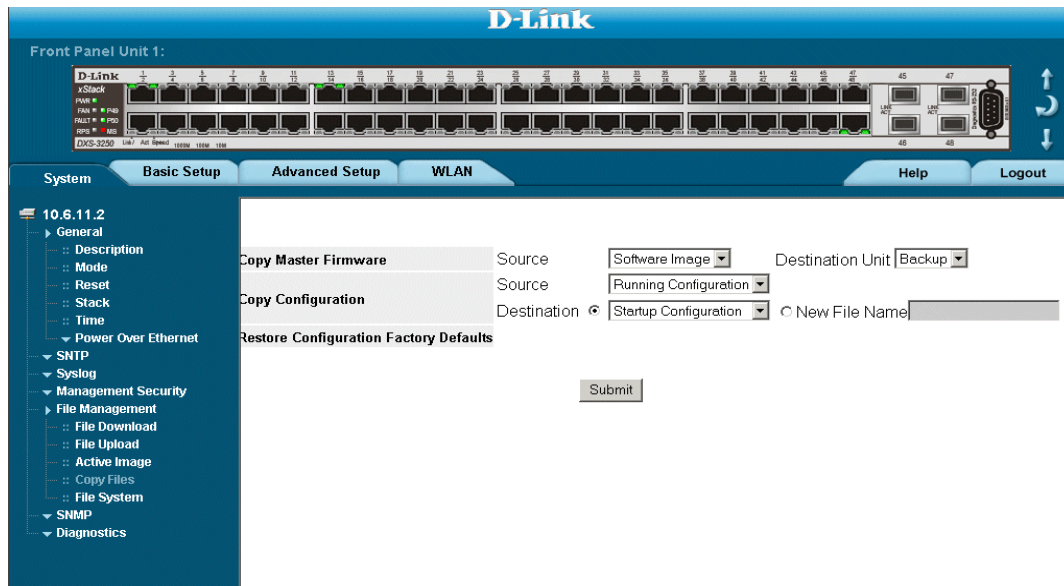
Copying Files

Files can be copied and deleted from the *Copy Files Page*.

To copy files:

1. Click **System > File Management > Copy Files**. The *Copy Files Page* opens.

Figure 175: Copy Files Page



The *Copy Files Page* contains the following fields:

- **Copy Configuration** — Copies the Running Configuration file to the Startup Configuration file.
- **Source** — Indicates the Running Configuration file is selected.
- **Destination** — Indicates the Startup Configuration file is selected.
- **Restore Configuration Factory Defaults** — Resets the Configuration file to the factory defaults. The factory defaults are reset after the device is reset. When unselected, the device maintains the current Configuration file.

2. Select *Copy Configuration*.
3. Click **Submit**. The file is copied.

Restoring the Default Configuration File

1. Click **System > File Management > Copy Files**. The *Copy Files Page* opens.
2. Select *Restore Configuration Factory Defaults*.
3. Click **Submit**. The factory defaults are restored, and the device is updated.

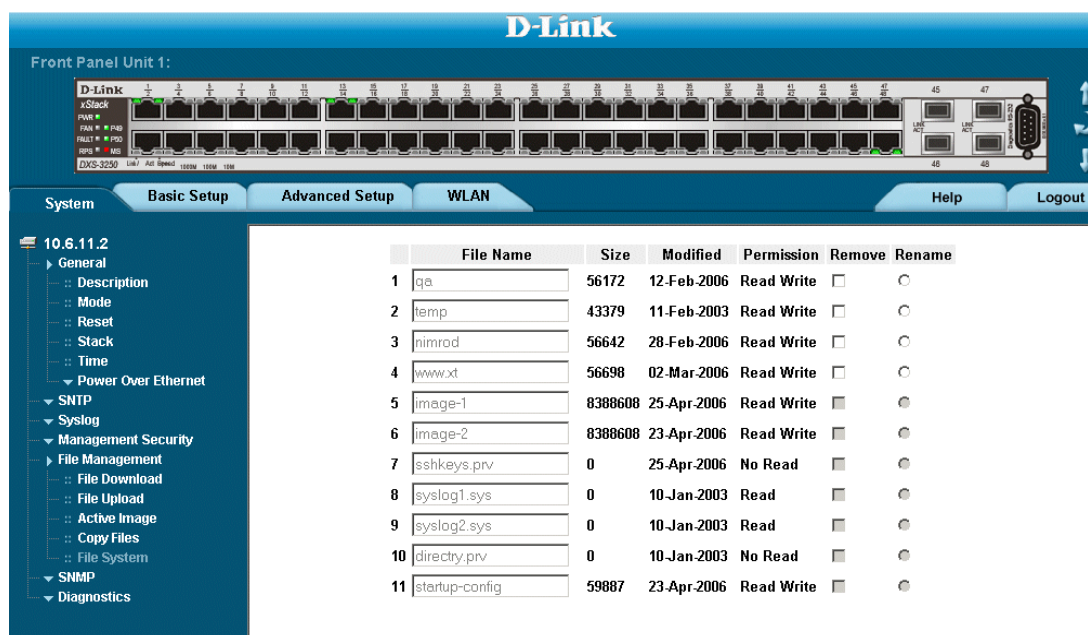
Managing System Files

The *File System Page* provides information about files currently stored on the system, including file names, file sizes, files modifications, and file permissions. The file system permits managing up to five files and a total file size of 3MB.

To manage files:

1. Click **System** > **File Management** > **File System**. The *File System Page* opens:

Figure 176: File System Page



The *File System Page* contains the following fields:

- **File Name** — Indicates the file currently stored in the file management system.
 - **Size** — Indicates the file size.
 - **Modified** — Indicates the date the file was last modified.
 - **Permission** — Indicates the permission type assigned to the file. The possible field values are:
 - *Read Only* — Indicates a read-only file.
 - *Read Write* — Indicates a read-write file.
 - **Remove** — Deletes the file, when checked.
 - **Rename** — Permits renaming the file. The file name is renamed in the File Name field.
 - **Total Bytes** — Indicates the total amount of the space currently used.
 - **Free Bytes** — Indicates the remaining amount of the space currently free.
2. Define the *File Name* field.
 3. Click . The file is updated.

Section 20. Managing System Logs

This section provides information for managing system logs. The system logs enable viewing device events in real time, and recording the events for later usage. System Logs record and manage events and report errors and informational messages.

Event messages have a unique format, as per the Syslog protocols recommended message format for all error reporting. For example, Syslog and local device reporting messages are assigned a severity code, and include a message mnemonic, which identifies the source application generating the message. It allows messages to be filtered based on their urgency or relevancy. Each message severity determines the set of event logging devices that are sent per each event message.

The following table lists the log severity levels:

Table 14: System Log Severity Levels

Severity	Level	Message
Emergency	Highest (0)	The system is not functioning.
Alert	1	The system needs immediate attention.
Critical	2	The system is in a critical state.
Error	3	A system error has occurred.
Warning	4	A system warning has occurred.
Notice	5	The system is functioning properly, but a system notice has occurred.
Informational	6	Provides device information.
Debug	7	Provides detailed information about the log. If a Debug error occurs, contact Customer Tech Support.

This section includes the following topics:

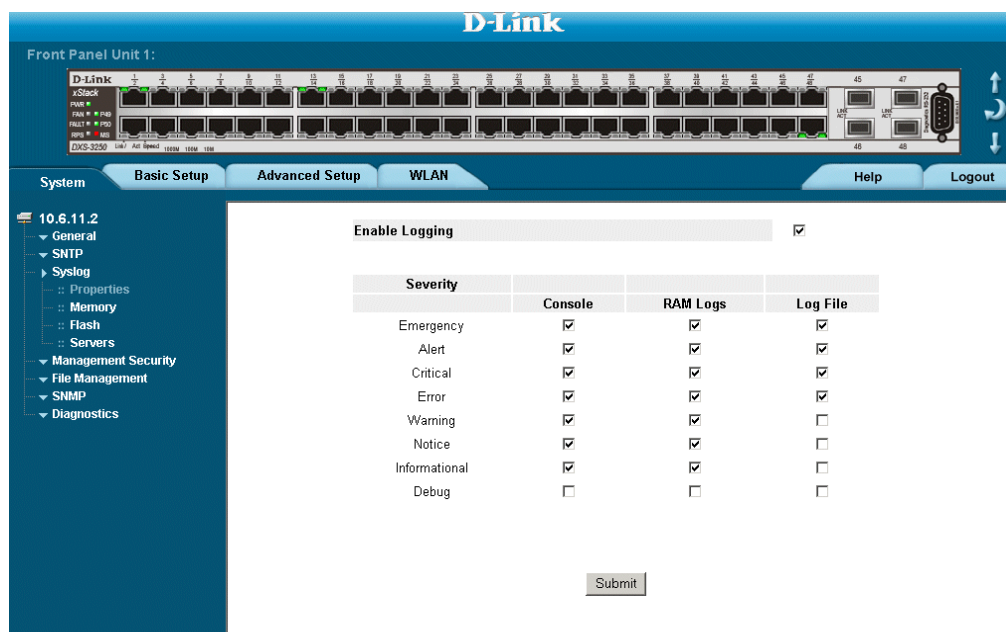
- Enabling System Logs
- Viewing the Device Memory Logs
- Viewing the FLASH Logs
- Defining Servers Log Parameters

Enabling System Logs

The *Syslog Properties Page* contains fields for defining which events are recorded to which logs. It contains fields for enabling logs globally, and parameters for defining logs. Log messages are listed from the highest severity to the lowest severity level. To define system log parameters:

1. Click **System > Syslog > Properties**. The *Syslog Properties Page* opens.

Figure 177: Syslog Properties Page



The *Syslog Properties Page* contains the following fields:

- **Enable Logging** — Indicates if device global logs for Cache, File, and Server Logs are enabled. Console logs are enabled by default. The possible field values are:
 - *Checked* — Enables device logs.
 - *Unchecked* — Disables device logs.
- **Severity** — The following are the available log severity levels:
 - *Emergency* — The highest warning level. If the device is down or not functioning properly, an emergency log message is saved to the specified logging location.
 - *Alert* — The second highest warning level. An alert log is saved, if there is a serious device malfunction; for example, all device features are down.
 - *Critical* — The third highest warning level. A critical log is saved if a critical device malfunction occurs; for example, two device ports are not functioning, while the rest of the device ports remain functional.
 - *Error* — A device error has occurred, for example, if a single port is offline.
 - *Warning* — The lowest level of a device warning. The device is functioning, but an operational problem has occurred.
 - *Notice* — Provides device information.

- *Informational* — Provides device information.
- *Debug* — Provides debugging messages.



Note

When a severity level is selected, all severity level choices above the selection are selected automatically.

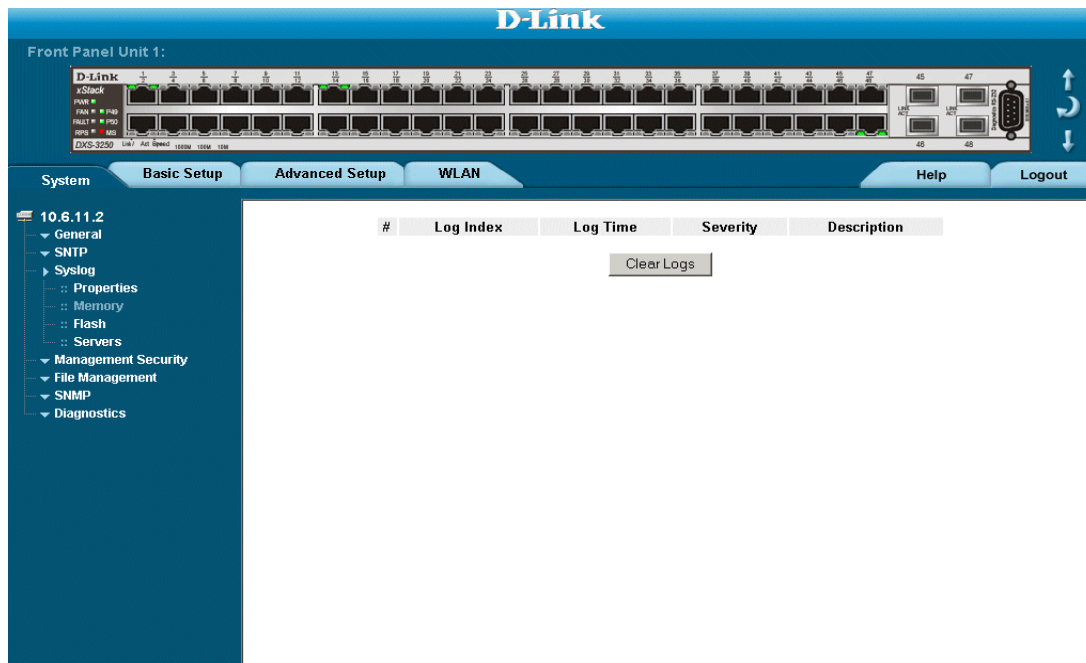
- **Console** — Defines the minimum severity level from which logs are sent to the console.
 - **RAM Logs** — Defines the minimum severity level from which logs are sent to the RAM Log kept in RAM (Cache).
 - **Log File**— Defines the minimum severity level from which logs are sent to the log file kept in FLASH memory.
2. Define the *Enable logging*, and *Severity* fields.
 3. Click The global log parameters are set, and the device is updated.

Viewing the Device Memory Logs

The *Device Memory Log Page* contains all system logs in a chronological order that are saved in RAM (Cache). To open the *Device Memory Log Page*:

- Click **System** > **Syslog** > **Memory**. The *Device Memory Log Page* opens.

Figure 178: Device Memory Log Page



The *Device Memory Log Page* contains the following fields:

- **Log Index** — Displays the log number.
- **Log Time** — Displays the time at which the log was generated.
- **Severity** — Displays the log severity.
- **Description** — Displays the log message text.

Clearing Device Memory Logs

Message logs can be cleared from the *Device Memory Log Page*. To clear message logs:

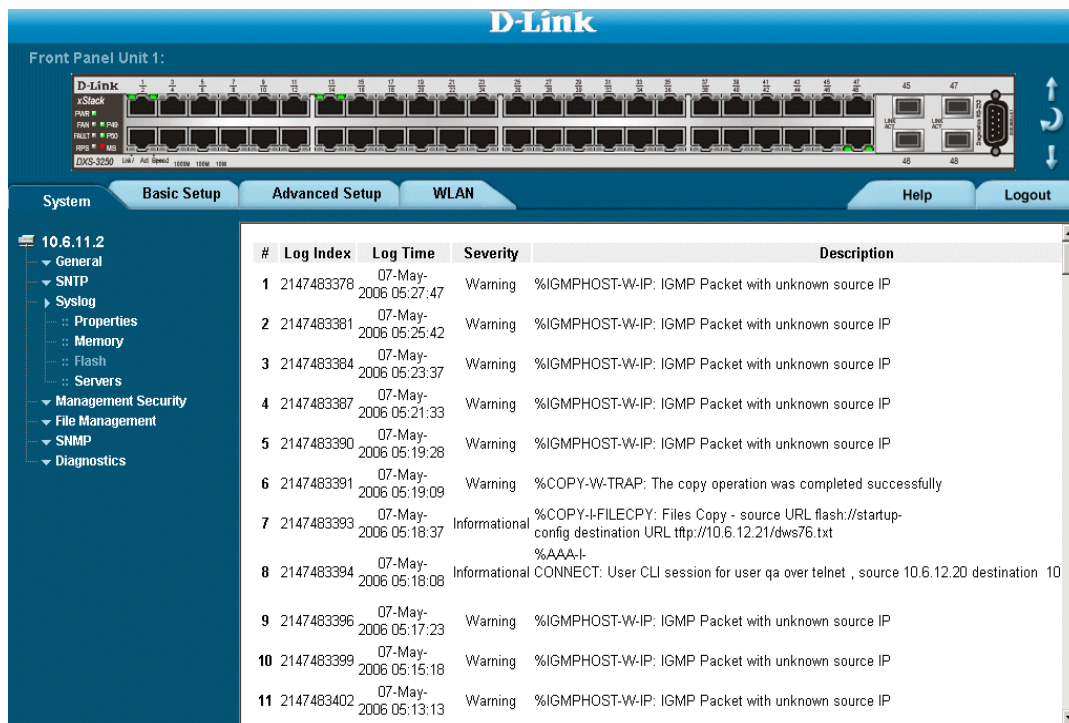
1. Click **System** > **Syslog** > **Memory**. The *Device Memory Log Page* opens.
2. Click . The message logs are cleared.

Viewing the FLASH Logs

The *Syslog Flash Page* contains information about log entries saved to the log file in Flash, including the time the log was generated, the log severity, and a description of the log message. The message log is available after reboot. To view the message logs:

- Click **System > Syslog > Flash**. The *Syslog FLASH Page* opens:

Figure 179: Syslog FLASH Page



The *Syslog Flash Page* contains the following fields:

- **Log Index** — Displays the log number.
- **Log Time** — Displays the time at which the log was generated.
- **Severity** — Displays the log severity.
- **Description** — Displays the log message text.

Clearing FLASH Logs

Message logs can be cleared from the *Syslog Flash Page*. To clear message logs:

1. Click **System > Syslog > Flash**. The *Syslog FLASH Page* opens.
2. Click **Clear Logs**. The message logs are cleared.

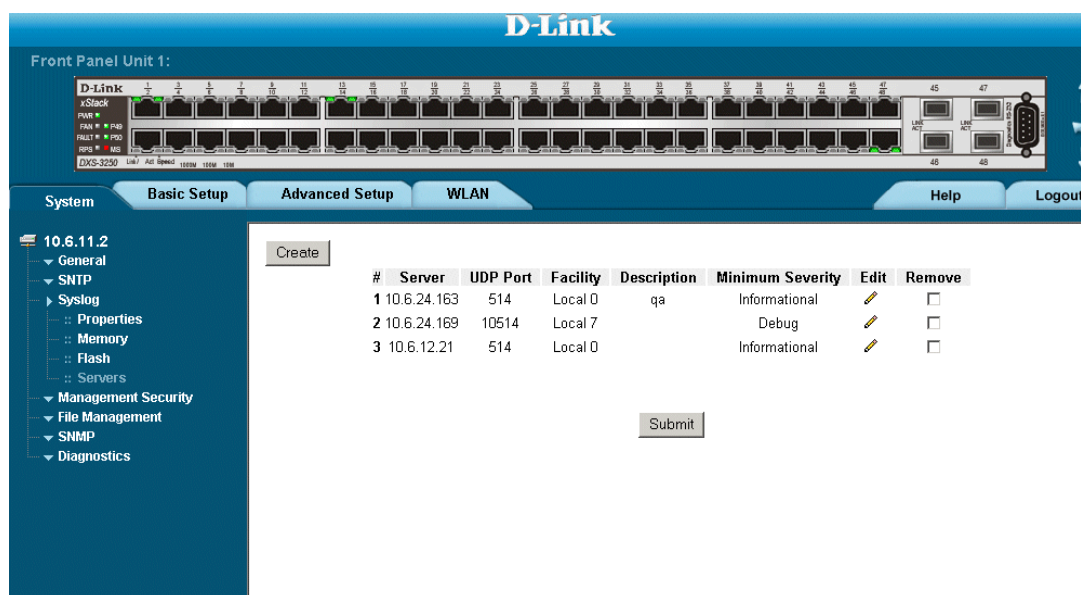
Defining Servers Log Parameters

The *Syslog Server Settings Page* contains information for viewing and configuring the remote log servers. New log servers can be defined, and the log severity sent to each server.

To open the *Syslog Server Settings Page*:

1. Click **System** > **Syslog** > **Servers**. The *Syslog Server Settings Page* opens.

Figure 180: Syslog Server Settings Page



The *Syslog Server Settings Page* contains the following fields:

- **Server** — Specifies the server to which logs can be sent.
- **UDP Port** — Defines the UDP port to which the server logs are sent. The possible range is 1 - 65535. The default value is 514.
- **Facility** — Defines 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 overridden. All applications defined for a device utilize the same facility on a server. The field default is *Local 7*. The possible field values are *Local 0 - Local 7*.
- **Description** — A user-defined server description.
- **Minimum Severity** — Indicates the minimum severity from which logs are sent to the server. For example, if *Notice* is selected, all logs with a severity level of *Notice* and higher are sent to the remote server.
- **Remove** — Deletes the currently selected server from the Servers list. The possible field values are:
 - *Checked* — Removes the selected server from the *Servers Log Parameters Page*. Once removed, logs are no longer sent to the removed server.
 - *Unchecked* — Maintains the remote servers.

2. Click **Create**. The *Add Syslog Server Page* opens:

Figure 181: Add Syslog Server Page

Add Remote Logs

New Log Server IP Address

UDP Port

Facility

Description

Minimum Severity

3. Define the *Log Server IP Address*, *UDP Port*, *Facility*, *Description*, and *Minimum severity* fields.
4. Click . The Syslog Server is defined, and the device is updated.

This page is left blank intentionally.

Section 21. Managing Device Diagnostics

This section contains the following topics:

- Configuring Port Mirroring
- Viewing Integrated Cable Tests
- Viewing Optical Transceivers
- Viewing the CPU Utilization

Configuring Port Mirroring

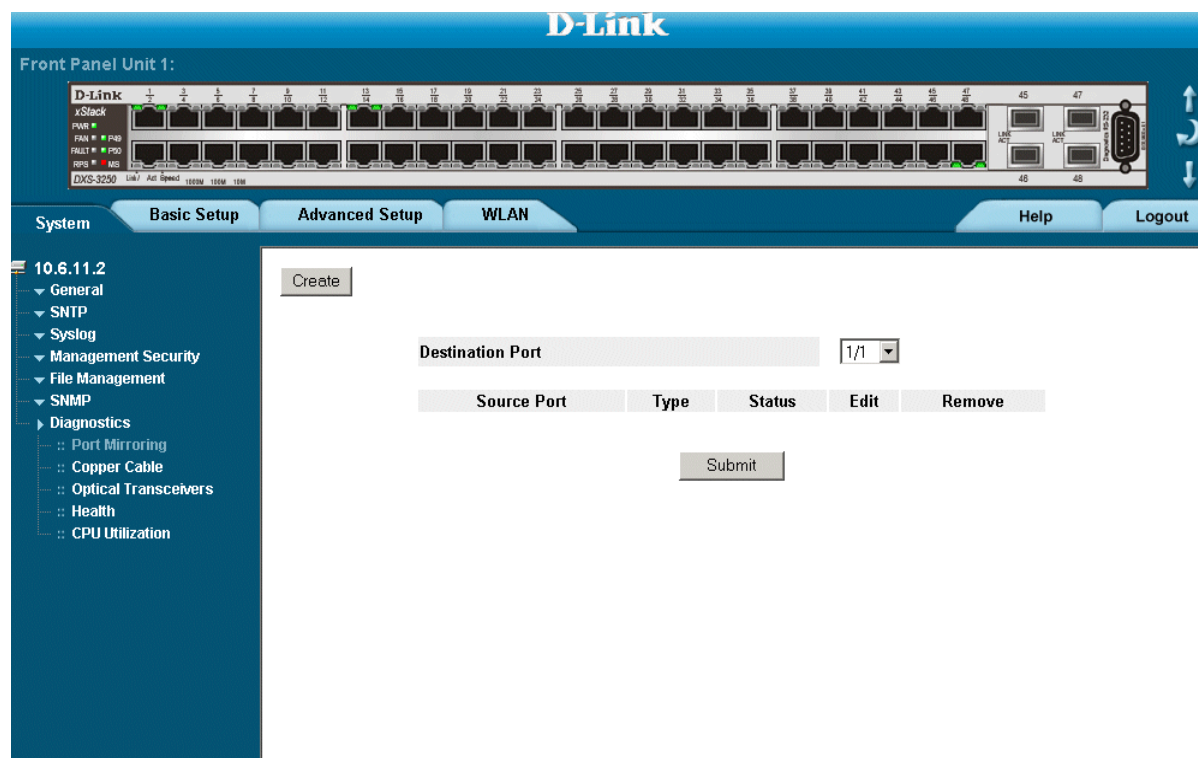
Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port. Port mirroring can be used as a diagnostic tool as well as a debugging feature. Port mirroring also enables switch performance monitoring.

Network administrators can configure port mirroring by selecting a specific port from which to copy all packets, and other ports to which the packets copied.

To enable port mirroring:

1. Click **System > Diagnostics > Port Mirroring**. The *Port Mirroring Page* opens:

Figure 182: Port Mirroring Page

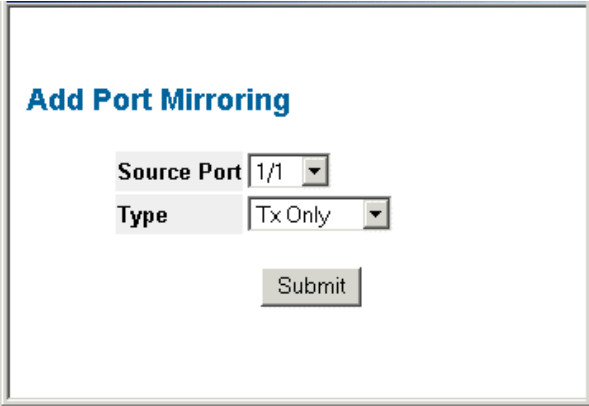


The *Port Mirroring Page* contains the following fields:

- **Destination Port** — Defines the port number to which port traffic is copied.
- **Source Port** — Indicates the port from which the packets are mirrored.
- **Type** — Indicates the port mode configuration for port mirroring. The possible field values are:
 - *RX* — Defines the port mirroring on receiving ports.
 - *TX* — Defines the port mirroring on transmitting ports.
 - *Both* — Defines the port mirroring on both receiving and transmitting ports. This is the default value.
- **Status** — Indicates if the port is currently monitored. The possible field values are:
 - *Active* — Indicates the port is currently monitored.

- *Ready* — Indicates the port is not currently monitored.
 - **Remove** — Removes the port mirroring session. The possible field values are:
 - *Checked* — Removes the selected port mirroring sessions.
 - *Unchecked* — Maintains the port mirroring session.
2. Click **Create**. The *Add Port Mirroring Page* opens:

Figure 183: Add Port Mirroring Page



Add Port Mirroring

Source Port 1/1

Type Tx Only

Submit

3. Select a port in the *Source Port* field.
4. Select a port type in the *Type* field.
5. Click **Submit**. The port mirroring session is defined, and the device is updated.

To edit the port mirroring settings:

1. Click **System > Diagnostics > Port Mirroring**. The *Port Mirroring Page* opens.

2. Click . The *Port Mirroring Settings Page* opens:

Figure 184: Port Mirroring Settings Page



Port Mirroring Settings

Source Port 3

Type

3. Modify the *Type* field.

4. Click . The port mirroring settings are modified, and the device is updated.

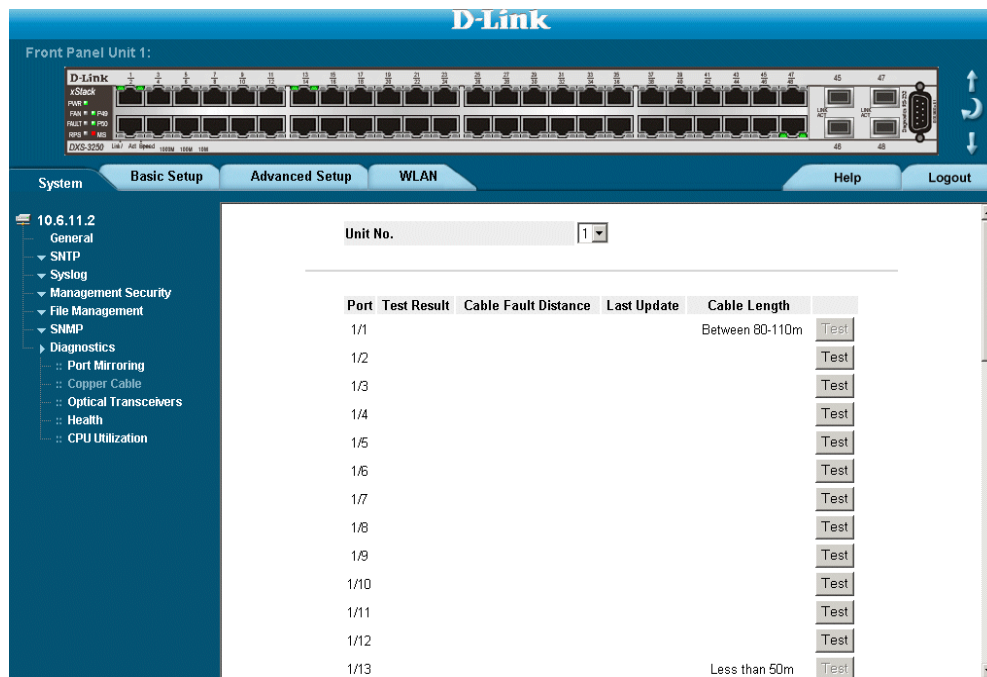
Viewing Integrated Cable Tests

The *Copper Cable Tests Page* contains fields for performing tests on copper cables. Cable testing provides information about where errors occurred in the cable, the last time a cable test was performed, and the type of cable error, which occurred. The tests use Time Domain Reflectometry (TDR) technology to test the quality and characteristics of a copper cable attached to a port. Cables up to 120 meters long can be tested. Cables are tested when the ports are in the down state, with the exception of the Approximated Cable Length test.

To test cables:

1. Click **System > Diagnostics > Copper Cable**. The *Copper Cable Tests Page* opens:

Figure 185: Copper Cable Tests Page



The *Copper Cable Tests Page* contains the following fields:

- **Port** — Specifies the port to which the cable is connected.
- **Test Result** — Displays the cable test results. Possible values are:
 - *No Cable* — Indicates that a cable is not connected to the port.
 - *Open Cable* — Indicates that a cable is connected on only one side.
 - *Short Cable* — Indicates that a short has occurred in the cable.
 - *OK* — Indicates that the cable passed the test.
- **Cable Fault Distance** — Indicates the distance from the port where the cable error occurred.

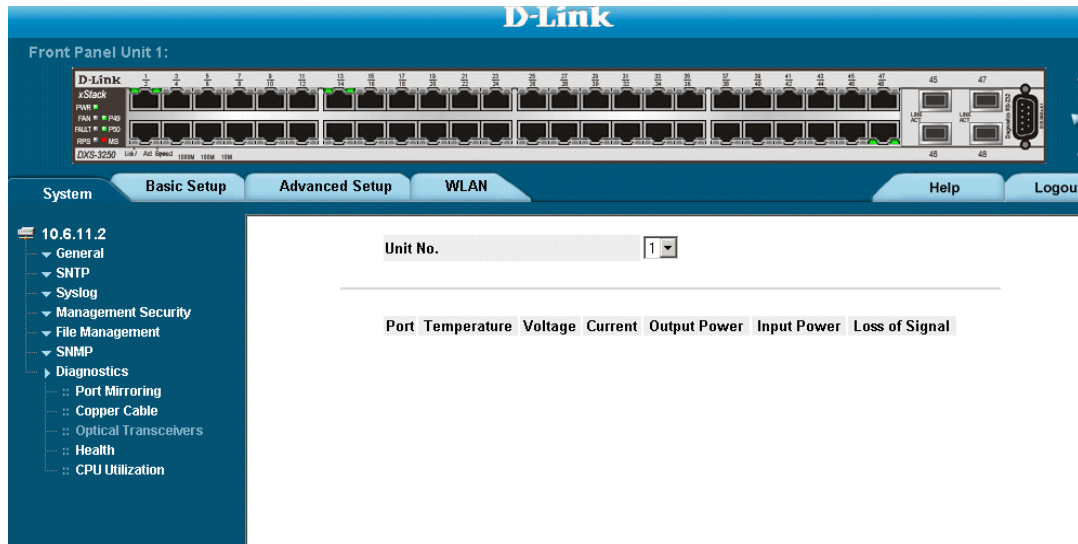
- **Last Update** — Indicates the last time the port was tested.
 - **Cable Length** — Indicates the approximate cable length. This test can only be performed when the port is up and operating at 1 Gbps.
2. Click . The test results are displayed.

Viewing Optical Transceivers

The Optical Transceiver page allows network managers to perform tests on Fiber Optic cables. Optical transceiver diagnostics can be performed only when the link is present. To test cables:

- Click **System > Diagnostics > Optical Transceivers** tab. The *Optical Transceivers Page* opens:

Figure 186: Optical Transceivers Page



The *Optical Transceivers Page* contains the field:

- **Port** — Displays the port IP address on which the cable is tested.
- **Temperature** — Displays the temperature (C) at which the cable is operating.
- **Voltage** — Displays the voltage at which the cable is operating.
- **Current** — Displays the current at which the cable is operating.
- **Output Power** — Indicates the rate at which the output power is transmitted.
- **Input Power** — Indicates the rate at which the input power is transmitted.
- **Loss of Signal** — Indicates if a signal loss occurred in the cable.



Note

This page is dependent on the optical transceiver. If the information is not provided or supported by the transceiver, the switch would not be able to provide such information.

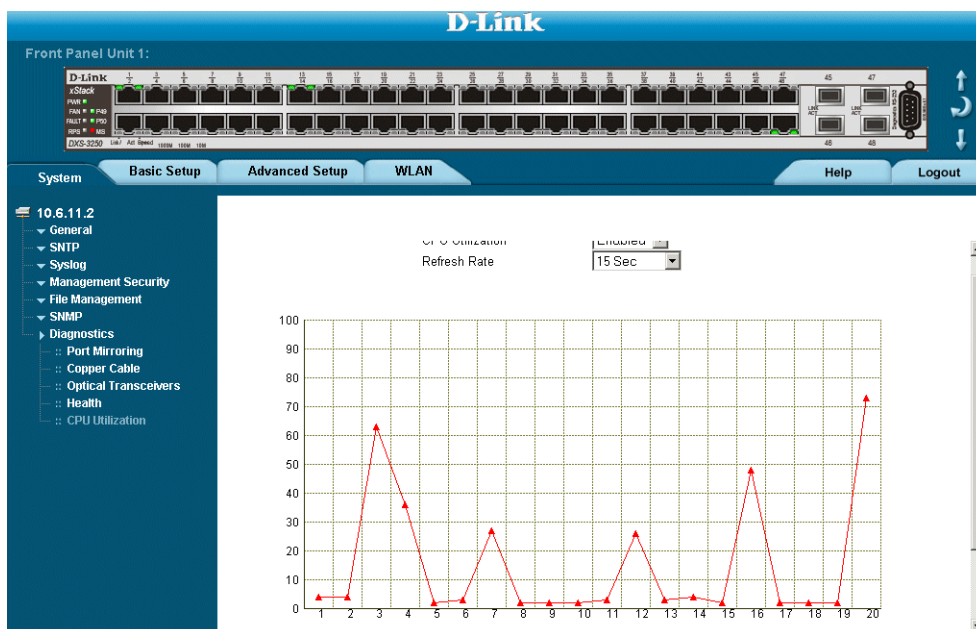
Viewing the CPU Utilization

The *CPU Utilization Page* contains information about the system's CPU utilization.

To view the CPU Utilization:

- Click **System > CPU > CPU Utilization**. The *CPU Utilization Page* opens:

Figure 187: CPU Utilization Page



The *CPU Utilization Page* contains the following fields:

- **CPU Utilization** — Displays CPU resource utilization information. The possible field values are:
 - *Enabled* — Enables viewing CPU utilization information. This is the default value.
 - *Disabled* — Disables viewing the CPU utilization information.
- **Refresh Rate** — Amount of time that passes before the statistics are refreshed.
- **Usage Percentages** — Indicates the percentage of the CPU's resources consumed by the device.
- **Time** — Indicates the time, in 15 second intervals, the usage samples are taken.

Section 22. Configuring System Time

This section provides information for configuring system time parameters, including:

- Configuring Daylight Savings Time
- Configuring SNTP

Configuring Daylight Savings Time

The *Time Page* contains fields for defining system time parameters for both the local hardware clock and the external SNTP clock. If the system time is kept using an external SNTP clock, and the external SNTP clock fails, the system time reverts to the local hardware clock. Daylight Savings Time can be enabled on the device.

The following is a list of Daylight Savings Time start and end times in specific countries:

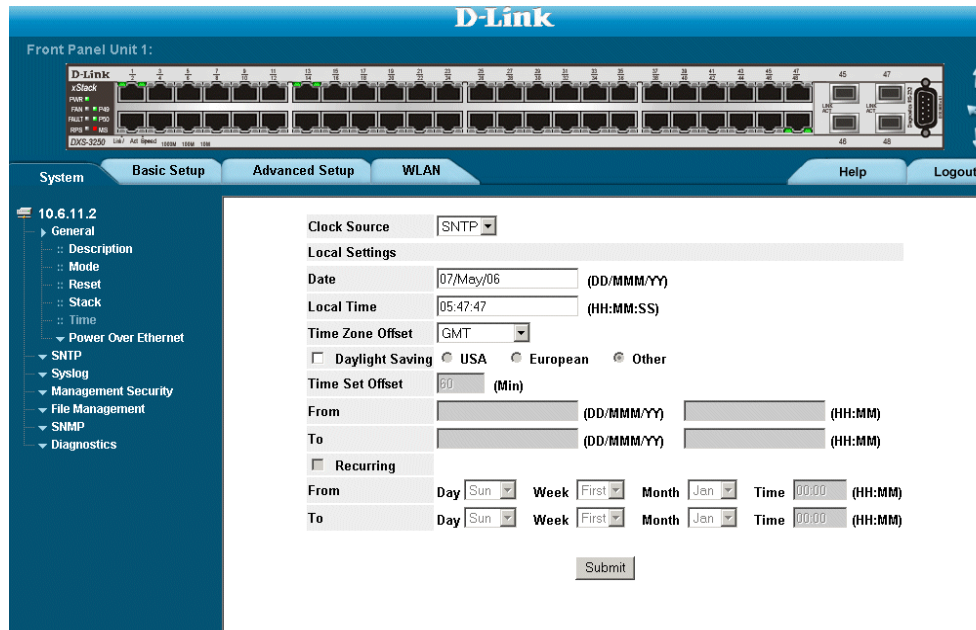
- **Albania** — From the last weekend of March until the last weekend of October.
- **Australia** — From the end of October until the end of March.
- **Australia - Tasmania** — From the beginning of October until the end of March.
- **Armenia** — From the last weekend of March until the last weekend of October.
- **Austria** — From the last weekend of March until the last weekend of October.
- **Bahamas** — From April to October, in conjunction with Daylight Savings Time in the United States.
- **Belarus** — From the last weekend of March until the last weekend of October.
- **Belgium** — From the last weekend of March until the last weekend of October.
- **Brazil** — From the third Sunday in October until the third Saturday in March. During the period of Daylight Saving Time, Brazilian clocks go forward one hour in most of the Brazilian southeast.
- **Chile** — In Easter Island, from March 9 until October 12. In the rest of the country, from the first Sunday in March or after 9th March.
- **China** — China does not use Daylight Saving Time.
- **Canada** — From the first Sunday in April until the last Sunday of October. Daylight Saving Time is usually regulated by provincial and territorial governments. Exceptions may exist in certain municipalities.
- **Cuba** — From the last Sunday of March to the last Sunday of October.
- **Cyprus** — From the last weekend of March until the last weekend of October.
- **Denmark** — From the last weekend of March until the last weekend of October.
- **Egypt** — From the last Friday in April until the last Thursday in September.
- **Estonia** — From the last weekend of March until the last weekend of October.
- **Finland** — From the last weekend of March until the last weekend of October.
- **France** — From the last weekend of March until the last weekend of October.
- **Germany** — From the last weekend of March until the last weekend of October.
- **Greece** — From the last weekend of March until the last weekend of October.
- **Hungary** — From the last weekend of March until the last weekend of October.
- **India** — India does not use Daylight Saving Time.
- **Iran** — From Farvardin 1 until Mehr 1.
- **Iraq** — From April 1 until October 1.
- **Ireland** — From the last weekend of March until the last weekend of October.
- **Israel** — Varies year-to-year.

- **Italy** — From the last weekend of March until the last weekend of October.
- **Japan** — Japan does not use Daylight Saving Time.
- **Jordan** — From the last weekend of March until the last weekend of October.
- **Latvia** — From the last weekend of March until the last weekend of October.
- **Lebanon** — From the last weekend of March until the last weekend of October.
- **Lithuania** — From the last weekend of March until the last weekend of October.
- **Luxembourg** — From the last weekend of March until the last weekend of October.
- **Macedonia** — From the last weekend of March until the last weekend of October.
- **Mexico** — From the first Sunday in April at 02:00 to the last Sunday in October at 02:00.
- **Moldova** — From the last weekend of March until the last weekend of October.
- **Montenegro** — From the last weekend of March until the last weekend of October.
- **Netherlands** — From the last weekend of March until the last weekend of October.
- **New Zealand** — From the first Sunday in October until the first Sunday on or after March 15.
- **Norway** — From the last weekend of March until the last weekend of October.
- **Paraguay** — From April 6 until September 7.
- **Poland** — From the last weekend of March until the last weekend of October.
- **Portugal** — From the last weekend of March until the last weekend of October.
- **Romania** — From the last weekend of March until the last weekend of October.
- **Russia** — From the last weekend of March until the last weekend of October.
- **Serbia** — From the last weekend of March until the last weekend of October.
- **Slovak Republic** - From the last weekend of March until the last weekend of October.
- **South Africa** — South Africa does not use Daylight Saving Time.
- **Spain** — From the last weekend of March until the last weekend of October.
- **Sweden** — From the last weekend of March until the last weekend of October.
- **Switzerland** — From the last weekend of March until the last weekend of October.
- **Syria** — From March 31 until October 30.
- **Taiwan** — Taiwan does not use Daylight Saving Time.
- **Turkey** — From the last weekend of March until the last weekend of October.
- **United Kingdom** — From the last weekend of March until the last weekend of October.
- **United States of America** — From the first Sunday in April at 02:00 to the last Sunday in October at 02:00.

To configure the system time:

1. Click **System > General > Time**. The *Time Page* opens.

Figure 188: Time Page



The *Time Page* contains the following sections:

- **Clock Source** — The source used to set the system clock. The possible field values are:
 - *None* — Indicates that a clock source is not used. The clock is set locally.
 - *SNTP* — Indicates that the system time is set via an SNTP server.
- **Date** — The system date. The field format is Day/Month/Year. For example: 04/May/50 (May 4, 2050).
- **Local Time** — The system time. The field format is HH:MM:SS. For example: 21:15:03.
- **Time Zone Offset** — The difference between Greenwich Mean Time (GMT) and local time. For example, the Time Zone Offset for Paris is GMT +1, while the Time Zone Offset for New York is GMT –5.
- **Daylight Savings** — Enables automatic Daylight Savings Time (DST) on the device based on the device's location. There are two types of daylight settings, either by a specific date in a particular year or a recurring setting irrespective of the year. For a specific setting in a particular year complete the *Daylight Savings* area, and for a recurring setting, complete the *Recurring* area. The possible field values are:
 - *USA* — The device switches to DST at 2:00 a.m. on the first Sunday of April, and reverts to standard time at 2:00 a.m. on the last Sunday of October.
 - *European* — The device switches to DST at 1:00 am on the last Sunday in March and reverts to standard time at 1:00 am on the last Sunday in October. The *European* option applies to EU members, and other European countries using the EU standard.
 - *Other* — The DST definitions are user-defined based on the device locality. If *Other* is selected, the *From* and *To* fields must be defined.
- **Time Set Offset (1-1440)** — Used for non-USA and European countries to set the amount of time for DST (in minutes). The default time is 60 minutes.
- **From** — Indicates the time that DST begins in countries other than the USA and Europe, in the format Day/Month/Year in one field and HH:MM in another. For example, if DST begins on October 25, 2007 at 5:00 am, the two fields should be set to 25/Oct/07 and 05:00. The possible field values are:

- *Date* — The date on which DST begins. The possible field range is 1-31.
 - *Month* — The month of the year in which DST begins. The possible field range is Jan-Dec.
 - *Year* — The year in which the configured DST begins.
 - *Time* — The time at which DST begins. The field format is HH:MM. For example: 05:30.
 - **To** — Indicates the time that DST ends in countries other than the USA and Europe, in the format Day/Month/Year in one field and HH:MM in another. For example, if DST ends on March 23, 2008 at midnight, the two fields should be 23/Mar/08 and 00:00. The possible field values are:
 - *Date* — The date on which DST ends. The possible field range is 1-31.
 - *Month* — The month of the year in which DST ends. The possible field range is Jan-Dec.
 - *Year* — The year in which the configured DST ends.
 - *Time* — The time at which DST starts. The field format is HH:MM. For example: 05:30.
 - **Recurring** — Enables user-defined DST for countries in which DST is constant from year to year, other than the USA and Europe.
 - **From** — The time that DST begins each year. In the example, DST begins locally every first Sunday in April at midnight. The possible field values are:
 - *Day* — The day of the week from which DST begins every year. The possible field range is Sunday-Saturday.
 - *Week* — The week within the month from which DST begins every year. The possible field range is 1-5.
 - *Month* — The month of the year in which DST begins every year. The possible field range is Jan-Dec.
 - *Time* — The time at which DST begins every year. The field format is Hour:Minute. For example: 02:10.
 - **To** — The time that DST ends each year. In the example, DST ends locally every first Sunday in October at midnight. The possible field values are:
 - *Day* — The day of the week at which DST ends every year. The possible field range is Sunday-Saturday.
 - *Week* — The week within the month at which DST ends every year. The possible field range is 1-5.
 - *Month* — The month of the year in which DST ends every year. The possible field range is Jan-Dec.
 - *Time* — The time at which DST ends every year. The field format is HH:MM. For example: 05:30.
2. Define the *Date*, *Local Time* and *Time Zone Offset* fields.
 3. To configure the device to automatically switch to DST, select *Daylight Savings* and select either *USA*, *European*, or *Other*. If you select *Other*, you must define its *From* and *To* fields. To configure DST parameters that will recur every year, select *Recurring* and define its *From* and *To* fields.
 4. Click . The DST settings are saved, and the device is updated.

Configuring SNTP

The device supports the Simple Network Time Protocol (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. The device operates only as an SNTP client, and cannot provide time services to other systems. The device can poll the following server types for the server time:

- Unicast
- Anycast
- Broadcast

Time sources are established by stratum. Stratum defines the accuracy of the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock. The device receives time from stratum 1 and above.

The following is an example of stratum:

- **Stratum 0** — A real time clock (such as a GPS system) is used as the time source.
- **Stratum 1** — A server that is directly linked to a Stratum 0 time source is used. Stratum 1 time servers provide primary network time standards.
- **Stratum 2** — The time source is distanced from the Stratum 1 server over a network path. For example, a Stratum 2 server receives the time over a network link, via NTP, from a Stratum 1 server.

Information received from SNTP servers is evaluated based on the Time level and server type. SNTP time definitions are assessed and determined by the following time levels:

- **T1** — The time at which the original request was sent by the client.
- **T2** — The time at which the original request was received by the server.
- **T3** — The time at which the server sent the client a reply.
- **T4** — The time at which the client received the server's reply.

Polling for Unicast Time Information

Polling for Unicast information is used for polling a server for which the IP address is known. T1 - T4 are used to determine the server time. This is the preferred method for synchronizing device time.

Polling for Anycast Time Information

Polling for Anycast information is used when the SNTP server IP address is unknown. The first Anycast server to return a response is used to set the time value. Time levels T3 and T4 are used to determine the server time. Using Anycast time information for synchronizing device time is preferred to using Broadcast time information.

Broadcast Time Information

Broadcast information is used when the server IP address is unknown. When a broadcast message is sent from an SNTP server, the SNTP client listens for the response. The SNTP client neither sends time information requests nor receives responses from the Broadcast server.

Message Digest 5 (MD5) Authentication safeguards device synchronization paths to SNTP servers. MD5 is an algorithm that produces a 128-bit hash. MD5 is a variation of MD4, and increases MD4 security. MD5 verifies the integrity of the communication, authenticates the origin of the communication.

This section contains the following topics:

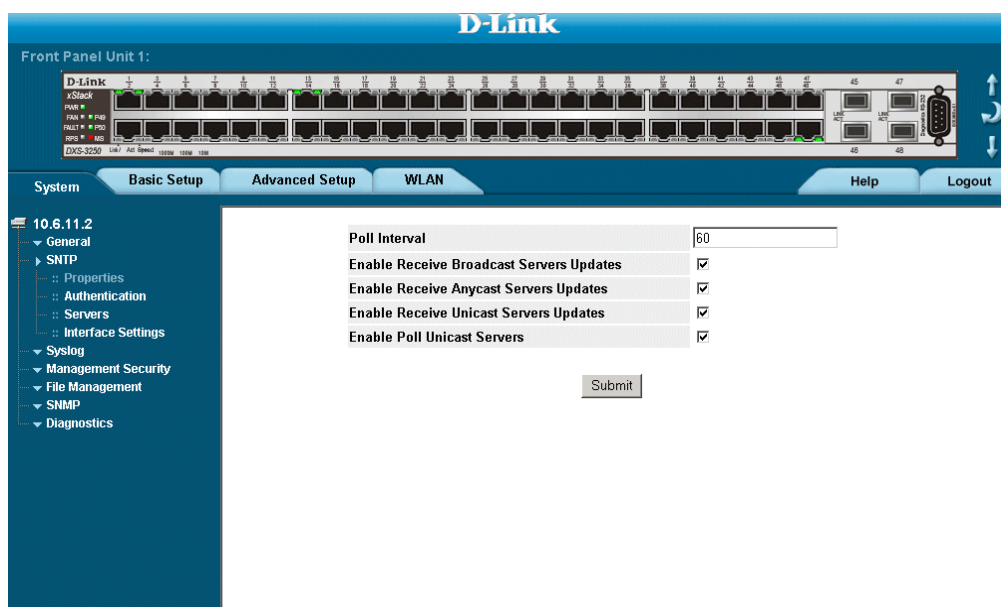
- 2 Defining SNTP Global Settings
- Defining SNTP Authentication
- Defining SNTP Servers
- Defining SNTP Interface Settings

Defining SNTP Global Settings

The *SNTP Properties Page* provides information for defining SNTP parameters globally. To define SNTP global parameters:

1. Click **System > SNTP > Properties**. The *SNTP Properties Page* opens:

Figure 189: SNTP Properties Page



The *SNTP Properties Page* contains the following fields:

- **Poll Interval** — Defines the interval (in seconds) at which the SNTP server is polled for Unicast information. The Poll Interval default is 1024 seconds.
- **Enable Receive Broadcast Servers Updates** — Defines whether or not the device monitors the SNTP servers for Broadcast server time information on the selected interfaces. The possible values are:
 - *Enable* — Enables the device to receive Broadcast server updates.
 - *Disable* — Disables the device from receiving Broadcast server updates.
- **Enable Receive Anycast Servers Updates** — Defines whether or not the device polls the SNTP server for Anycast server time information. If both the *Enable Receive Anycast Servers Update* and the *Enable Receive Broadcast Servers Update* fields are enabled, the system time is set according to the Anycast server time information. The possible values are:
 - *Enable* — Enables the device to receive Anycast server updates.
 - *Disable* — Disables the device from receiving Anycast server updates.

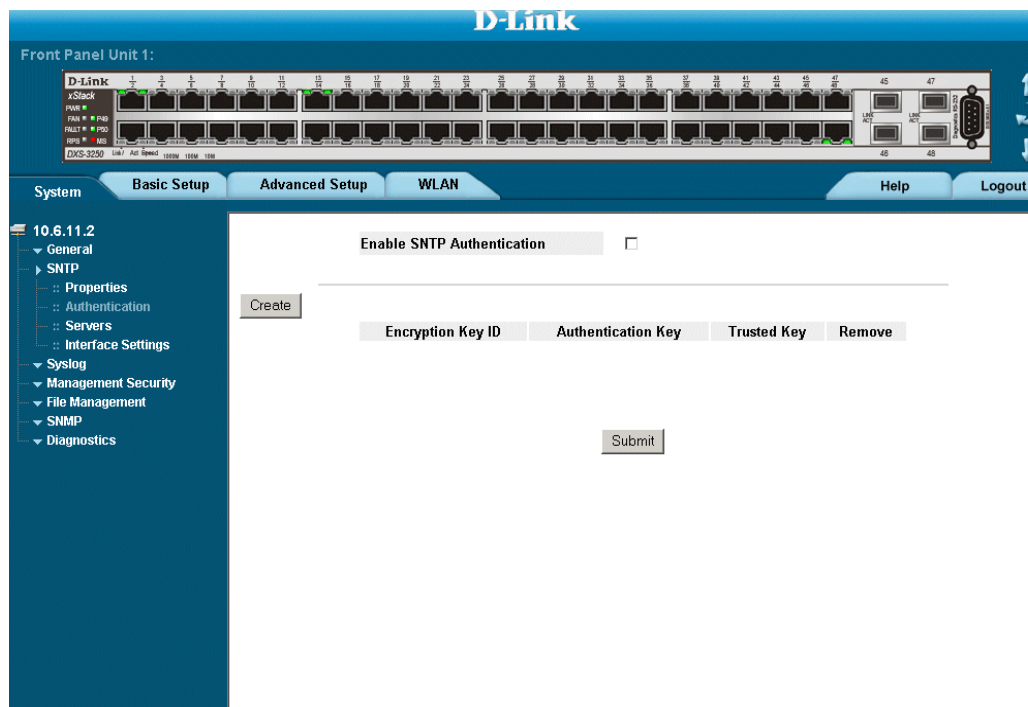
- **Enable Receive Unicast Servers Updates** — Defines whether or not the device polls the SNTP server for Unicast server time information. If the *Enable Receive Broadcast Servers Updates*, *Enable Receive Anycast Servers Updates*, and *Enable Receive Unicast Servers Updates* fields are all enabled, the system time is set according to the Unicast server time information. The possible values are:
 - *Enable* — Enables the device to receive Unicast server updates.
 - *Disable* — Disables the device from receiving Unicast server updates.
 - **Enable Poll Unicast Servers** — Defines whether or not the device sends SNTP Unicast forwarding information to the SNTP server. The possible values are:
 - *Enable* — Enables the device to receive Poll Unicast server updates.
 - *Disable* — Disables the device from receiving Poll Unicast server updates.
2. Define the *Poll Interval*, *Enable Receive Broadcast Servers Update*, *Enable Receive Anycast Servers Update*, *Enable Receive Unicast Servers Update*, and *Enable Poll Unicast Servers* fields and select at least one of the *Enable* fields.
 3. Click . The SNTP global settings are defined, and the device is updated.

Defining SNMP Authentication

The *SNMP Authentication Page* provides parameters for defining the means by which the SNMP server is authenticated. To define SNMP authentication:

1. Click **System > SNMP > Authentication**. The *SNMP Authentication Page* opens:

Figure 190: SNMP Authentication Page



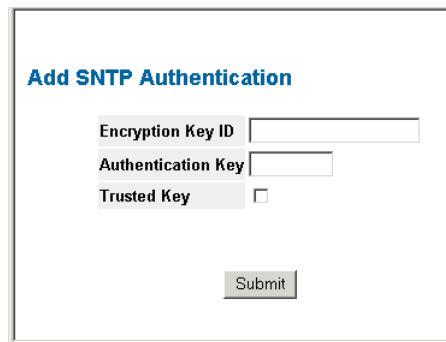
The *SNMP Authentication Page* contains the following fields:

- **Enable SNMP Authentication** — Indicates if authenticating an SNMP session between the device and an SNMP server is enabled on the device. The possible field values are:
 - *Checked* — Authenticates SNMP sessions between the device and SNMP server.
 - *Unchecked* — Disables authenticating SNMP sessions between the device and SNMP server.
 - **Encryption Key ID** — Indicates if the encryption key identification is used to authenticate the SNMP server and device. The field value is up to 4294967295.
 - **Authentication Key** — Indicates the key used for authentication.
 - **Trusted Key** — Indicates the encryption key used (Unicast/Anycast) or elected (Broadcast) to authenticate the SNMP server.
 - **Remove** — Removes Encryption Key IDs. The possible field values are:
 - *Checked* — Removes the selected Encryption Key ID.
 - *Unchecked* — Maintains the Encryption Key IDs. This is the default value.
2. To enable SNMP Authentication, select *Enable SNMP Authentication* and click **Submit**. SNMP Authentication is defined, and the device is updated.

To define SNTP authentication parameters:

1. Click **Create**. The *Section Figure 191: "Add SNTP Authentication"* page opens:

Figure 191: Add SNTP Authentication



Add SNTP Authentication

Encryption Key ID

Authentication Key

Trusted Key

Submit

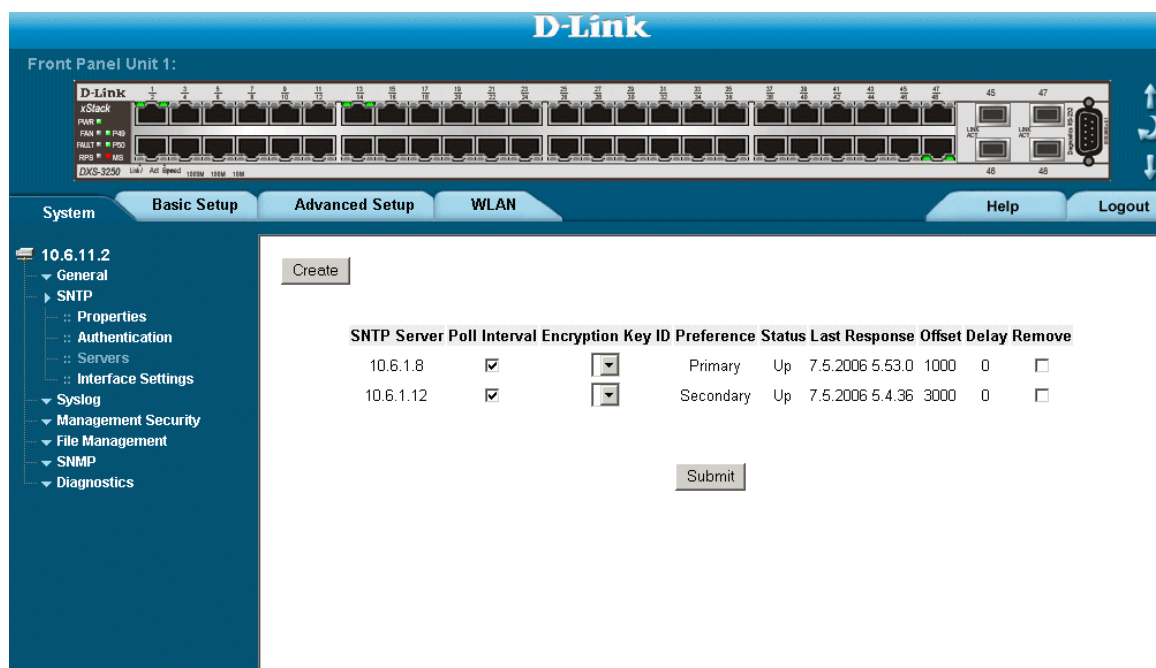
2. Define the *Encryption Key ID*, *Authentication Key*, and *Trusted Key* fields.
3. Click **Yes**. The SNTP Authentication Key is added, and the device is updated.

Defining SNMP Servers

The *SNTP Servers Page* contains information for enabling SNMP servers, as well as adding new SNMP servers. In addition, the *SNTP Servers Page* enables the device to request and accept SNMP traffic from a server. To define an SNMP server:

1. Click **System > SNMP > Servers**. The *SNTP Servers Page* opens:

Figure 192: SNMP Servers Page



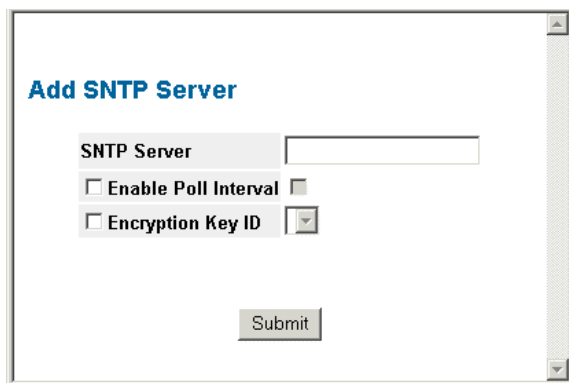
The *SNTP Servers Page* contains the following fields:

- **SNTP Server** — Displays user-defined SNMP server IP addresses. Up to eight SNMP servers can be defined.
- **Poll Interval** — Indicates whether or not the device polls the selected SNMP server for system time information.
- **Encryption Key ID** — Displays the encryption key identification used to communicate between the SNMP server and device. The field range is 1-4294967295.
- **Preference** — Indicates which SNMP server provides the SNMP system time. The possible field values are:
 - *Primary* — Indicates the primary server provides SNMP information.
 - *Secondary* — Indicates the backup server provides SNMP information.
- **Status** — **The operating SNMP server status. The possible field values are:**
 - *Up* — Indicates the SNMP server is currently operating normally.
 - *Down* — Indicates that a SNMP server is currently not available. For example, the SNMP server is currently not connected or is currently down.
 - *In progress* — Indicates the SNMP server is currently sending or receiving SNMP information.
 - *Unknown* — Indicates the progress of the SNMP information currently being sent is unknown. For example, the device is currently looking for an interface.

- **Last Response** — Displays the last time a response was received from the SNTP server.
- **Offset** — Indicates the time difference between the device local clock and the acquired time from the SNTP server.
- **Delay** — Indicates the amount of time it takes for a device request to reach the SNTP server.
- **Remove** — Removes SNTP servers from the SNTP server list. The possible field values are:
 - *Checked* — Removes the SNTP server.
 - *Unchecked* — Maintains the SNTP server. This is the default value.

2. Click **Create** . The *Add SNTP Server Page* opens:

Figure 193: Add SNTP Server Page



The screenshot shows a web form titled "Add SNTP Server". The form includes the following elements:

- A text input field labeled "SNTP Server".
- A checkbox labeled "Enable Poll Interval".
- A dropdown menu labeled "Encryption Key ID".
- A "Submit" button at the bottom center.

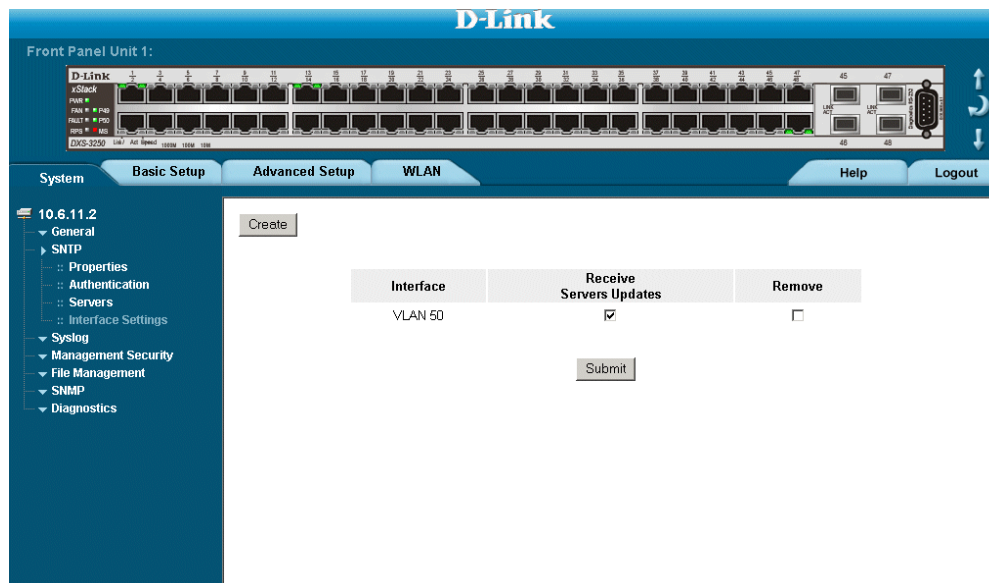
3. Define the *SNTP Server*, *Enable Poll Interval*, and *Encryption Key ID* fields.
4. Click **Submit** . The SNTP Server is added, and the device is updated.

Defining SNTP Interface Settings

The *SNTP Interface Settings Page* contains fields for setting SNTP on different interfaces. To define SNTP interface settings:

1. Click **System > SNTP > Interface Settings**. The *SNTP Interface Settings Page* opens:

Figure 194: SNTP Interface Settings Page



The *SNTP Interface Settings Page* contains the following fields:

- **Interface** — Indicates the interface on which SNTP can be enabled. The possible field values are:
 - *Port* — Indicates the specific port number on which SNTP is enabled.
 - *LAG* — Indicates the specific LAG number on which SNTP is enabled.
 - *VLAN* — Indicates the specific VLAN number on which SNTP is enabled.
 - **Receive Servers Updates** — Enables the server to receive or not receive updates.
 - **Remove** — Removes SNTP interfaces.
 - *Checked* — Removes the selected SNTP interface.
 - *Unchecked* — Maintains the selected SNTP interfaces.
2. Click **Create**. The *Add SNTP Interface Page* opens.

Figure 195: Add SNTP Interface Page

Add SNTP Interface

Interface Port 1/1 LAG VLAN 1

Receive Server Updates

Submit

3. Define the *Interface* and *Receive Server Updates* fields.
4. Click **Submit**. The SNTP interface is added, and the device is updated.

This page is left blank intentionally.

Section 23. Viewing Statistics

This section provides device statistics for RMON, interfaces, GVRP, EAP, and Etherlike statistics. This section contains the following topics:

- Viewing Interface Statistics
- Managing RMON Statistics

Viewing Interface Statistics

This section contains the following topics:

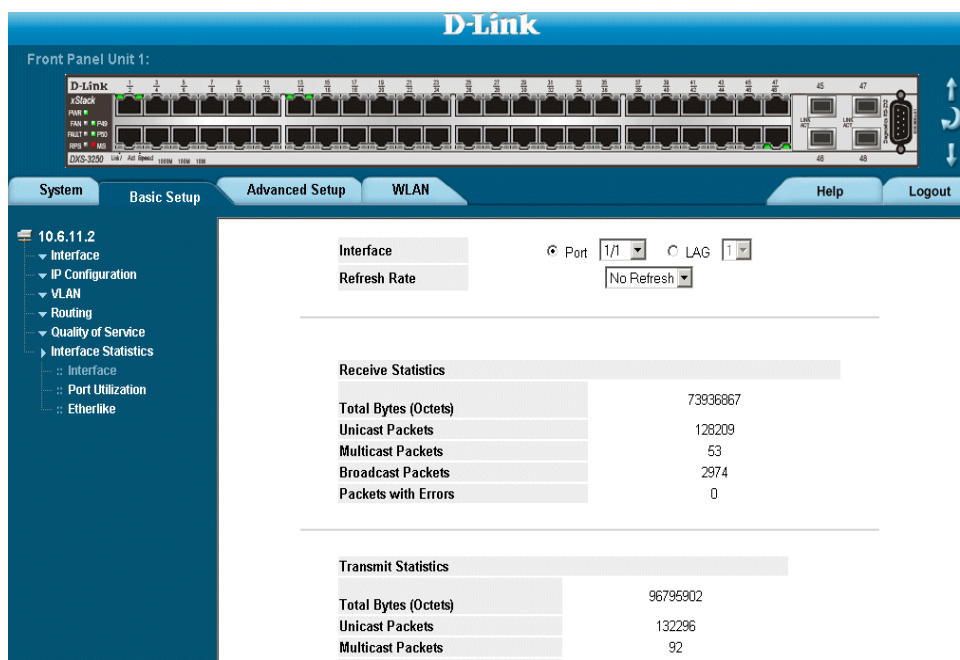
- Viewing Device Interface Statistics
- Viewing Etherlike Statistics
- Viewing GVRP Statistics
- Viewing EAP Statistics

Viewing Device Interface Statistics

The *Interface Statistics Page* contains statistics for both received and transmitted packets.

1. Click **Basic Setup > Interface Statistics > Interface**. The *Interface Statistics Page* opens.

Figure 196: Interface Statistics Page



The *Interface Statistics Page* contains the following fields:

- **Interface** — Indicates the device for which statistics are displayed. The possible field values are:
 - *Port* — Defines the specific port for which interface statistics are displayed.
 - *LAG* — Defines the specific LAG for which interface statistics are displayed.
- **Refresh Rate** — Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:
 - *15 Sec*—Indicates that the Interface statistics are refreshed every 15 seconds.
 - *30 Sec*—Indicates that the Interface statistics are refreshed every 30 seconds.
 - *60 Sec*—Indicates that the Interface statistics are refreshed every 60 seconds.
 - *No Refresh*—Indicates that the Interface statistics are not refreshed.


Receive Statistics

- **Total Bytes (Octets)** — Displays the number of octets received on the selected interface.
- **Unicast Packets** — Displays the number of Unicast packets received on the selected interface.
- **Multicast Packets** — Displays the number of Multicast packets received on the selected interface.
- **Broadcast Packets** — Displays the number of Broadcast packets received on the selected interface.
- **Packets with Errors** — Displays the number of error packets received from the selected interface.

Transmit Statistics

- **Total Bytes (Octets)** — Displays the number of octets transmitted from the selected interface.
 - **Unicast Packets** — Displays the number of Unicast packets transmitted from the selected interface.
 - **Multicast Packets** — Displays the number of Multicast packets transmitted from the selected interface.
 - **Broadcast Packets** — Displays the number of Broadcast packets transmitted from the selected interface.
2. Select an interface in the *Interface* field. The interface statistics are displayed.

Resetting Interface Statistics Counters

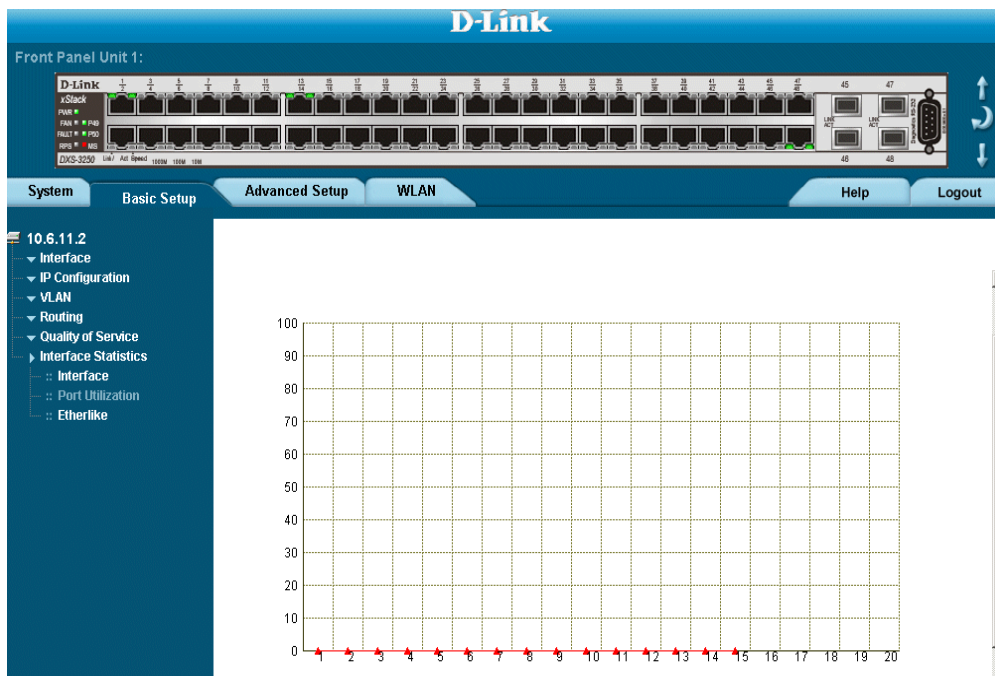
1. Open the *Interface Statistics Page*.
2. Click . The interface statistics counters are cleared.

Viewing Port Utilization Statistics

The *Port Utilization Page* contains port utilization information for specific ports. To view the port utilization statistics:

1. Click **Basic Setup > Interface Statistics > Port Utilization**. The *Port Utilization Page* opens.

Figure 197: Port Utilization Page



The *Port Utilization Page* contains the following fields:

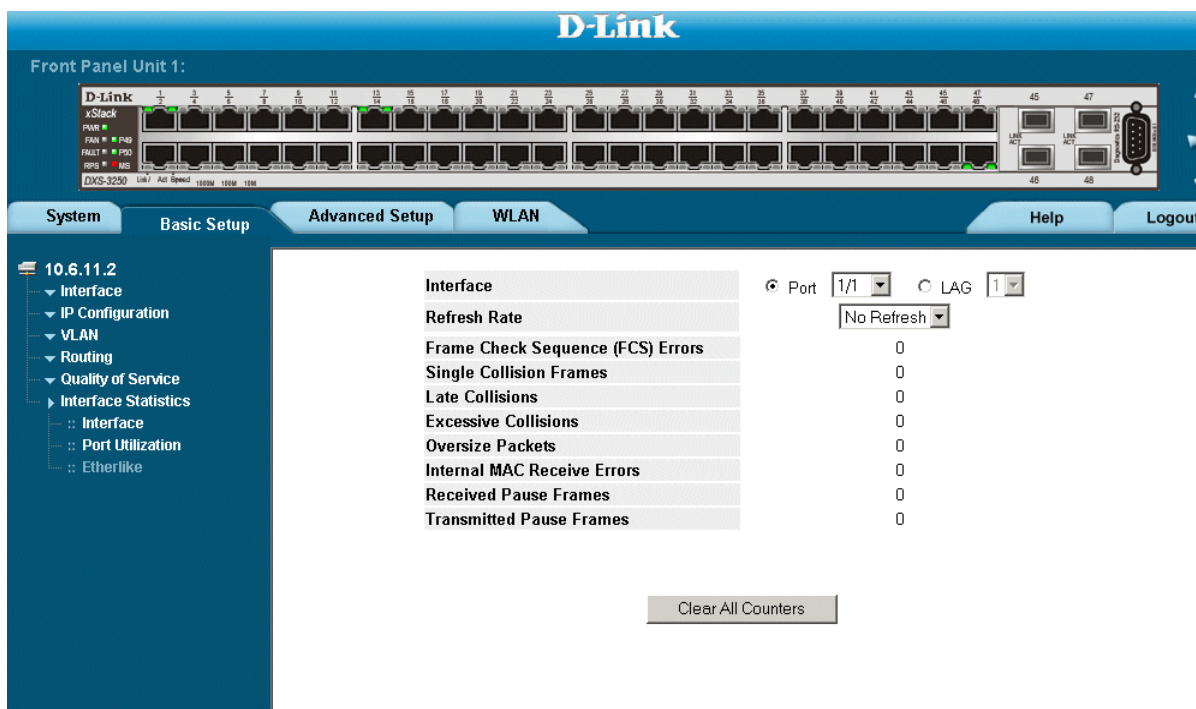
- **Port** — Indicates the port for which the utilization statistics are displayed.
- **Refresh Rate** — Amount of time that passes before the statistics are refreshed.
- **Usage Percentages** — Indicates the percentage of the port resources consumed by the device.
- **Time** — Indicates the time, in 15 second intervals, the usage samples are taken.

Viewing Etherlike Statistics

The *Etherlike Statistics Page* contains interface statistics. To view Etherlike Statistics:

1. Click **Basic Setup > Interfaces Statistics > Etherlike**. The *Etherlike Statistics Page* opens

Figure 198: Etherlike Statistics Page

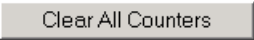


The *Etherlike Statistics Page* contains the following fields:

- **Interface** — Indicates the device for which statistics are displayed. The possible field values are:
 - *Port* — Defines the specific port for which Etherlike statistics are displayed.
 - *LAG* — Defines the specific LAG for which Etherlike statistics are displayed.
- **Refresh Rate** — Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:
 - *No Refresh*—Indicates that the Etherlike statistics are not refreshed.
 - *15 Sec*—Indicates that the Etherlike statistics are refreshed every 15 seconds.
 - *30 Sec*—Indicates that the Etherlike statistics are refreshed every 30 seconds.
 - *60 Sec*—Indicates that the Etherlike statistics are refreshed every 60 seconds.
- **Frame Check Sequence (FCS) Errors** — Displays the number of FCS errors received on the selected interface.
- **Single Collision Frames** — Displays the number of single collision frames received on the selected interface.
- **Late Collisions** — Displays the number of late collision frames received on the selected interface.
- **Excessive Collisions** — Displays the number of excessive collisions received on the selected interface.

- **Internal MAC Transmit Errors** — Displays the number of internal MAC transmit errors on the selected interface.
 - **Oversize Packets** — Displays the number of oversized packet errors on the selected interface.
 - **Internal MAC Receive Errors** — Number of internal MAC received errors on the selected interface.
 - **Received Pause Frames** — Displays the number of received paused frames on the selected interface.
 - **Transmitted Paused Frames** — Displays the number of paused frames transmitted from the selected interface.
2. Select an interface in the *Interface* field. The Etherlike statistics are displayed.

Resetting Etherlike Statistics Counters

1. Open the *Etherlike Statistics Page*.
2. Click . The Etherlike statistics counters are cleared.

Viewing GVRP Statistics

The *GVRP Statistics Page* contains device statistics for GVRP. To view GVRP statistics:

- Click **Advanced Setup > Interface Statistics > GVRP**. The *GVRP Statistics Page* opens.

Figure 199: GVRP Statistics Page

The screenshot shows the D-Link web interface for viewing GVRP statistics. The top navigation bar includes tabs for System, Basic Setup, Advanced Setup, WLAN, Help, and Logout. The left navigation menu is expanded to show the path: 10.6.11.2 > Interface > Interface Statistics > GVRP. The main content area displays the following fields:

- Interface:** Port 1/1, LAG 1
- Refresh Rate:**
- GVRP Statistics Table:**

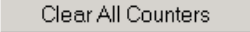
Attribute (Counter)	Received	Transmitted
Join Empty		
Empty		
Leave Empty		
Join In		
Leave In		
Leave All		
- GVRP Error Statistics:**
 - Invalid Protocol ID
 - Invalid Attribute Type
 - Invalid Attribute Value
 - Invalid Attribute Length
 - Invalid Event

The *GVRP Statistics Page* contains the following fields:

- **Interface**—Specifies the interface type for which the statistics are displayed.
 - *Port*—Indicates port statistics are displayed.
 - *LAG*—Indicates LAG statistics are displayed.
- **Refresh Rate**—Indicates the amount of time that passes before the GVRP statistics are refreshed. The possible field values are:
 - *No Refresh*—Indicates that the GVRP statistics are not refreshed.
 - *15 Sec*—Indicates that the GVRP statistics are refreshed every 15 seconds.
 - *30 Sec*—Indicates that the GVRP statistics are refreshed every 30 seconds.
 - *60 Sec*—Indicates that the GVRP statistics are refreshed every 60 seconds.
- **Join Empty**—Displays the device GVRP Join Empty statistics.
- **Empty**—Displays the device GVRP Empty statistics.
- **Leave Empty**—Displays the device GVRP Leave Empty statistics.
- **Join In**—Displays the device GVRP Join In statistics.

- **Leave In**—Displays the device GVRP Leave in statistics.
 - **Leave All**—Displays the device GVRP Leave all statistics.
 - **Invalid Protocol ID**—Displays the device GVRP Invalid Protocol ID statistics.
 - **Invalid Attribute Type**—Displays the device GVRP Invalid Attribute ID statistics.
 - **Invalid Attribute Value**—Displays the device GVRP Invalid Attribute Value statistics.
 - **Invalid Attribute Length**—Displays the device GVRP Invalid Attribute Length statistics.
 - **Invalid Event**—Displays the device GVRP Invalid Event statistics.
3. Select an interface in the *Interface* field. The GVRP statistics are displayed.

Resetting GVRP Statistics Counters

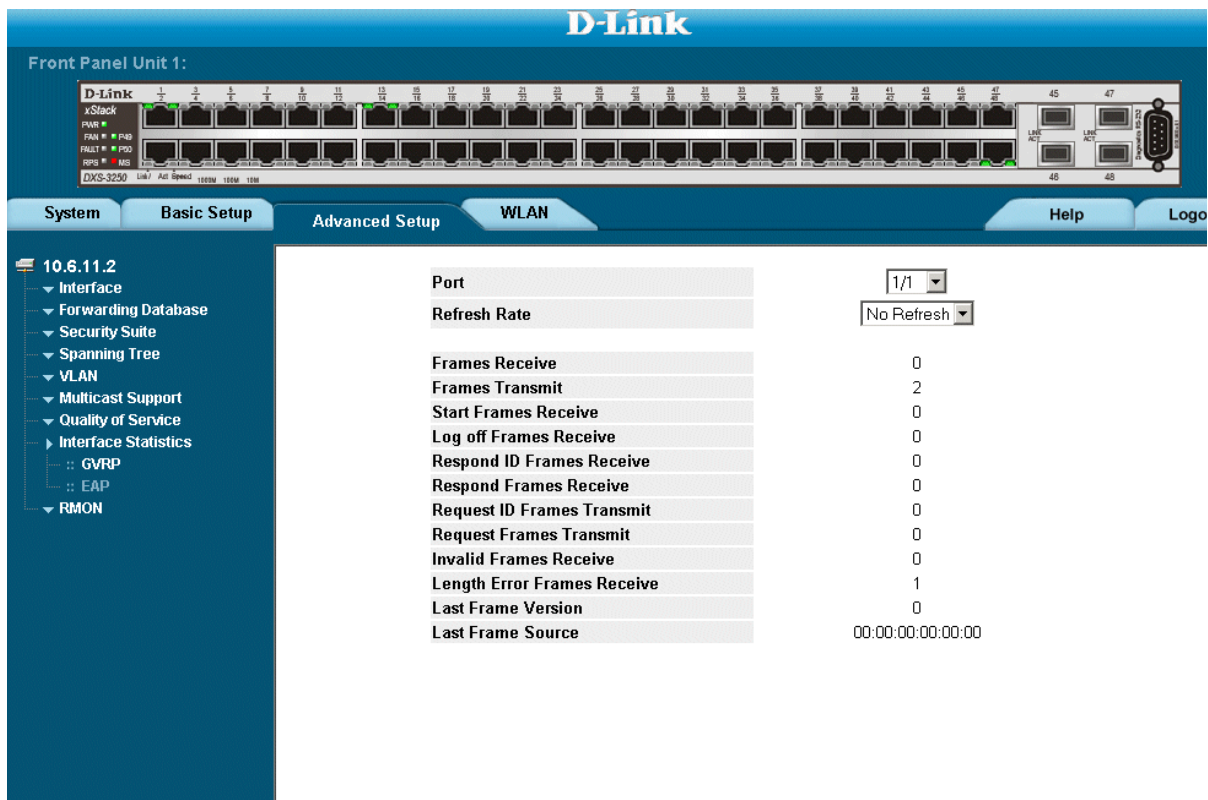
1. Open the *GVRP Statistics Page*.
2. Click . The GVRP statistics counters are cleared.

Viewing EAP Statistics

The *EAP Statistics Page* contains information about EAP packets received on a specific port. To view the EAP Statistics:

- Click **Advanced Setup > Interface Statistics > EAP**. The *EAP Statistics Page* opens.

Figure 200: EAP Statistics Page



The *EAP Statistics Page* contains the following fields:

- **Port**—Indicates the port, which is polled for statistics.
- **Refresh Rate**—Indicates the amount of time that passes before the EAP statistics are refreshed. The possible field values are:
 - *No Refresh* — Indicates that the EAP statistics are not refreshed.
 - *15 Sec*—Indicates that the EAP statistics are refreshed every 15 seconds.
 - *30 Sec* — Indicates that the EAP statistics are refreshed every 30 seconds.
 - *60 Sec* — Indicates that the EAP statistics are refreshed every 60 seconds.
- **Frames Receive** — Indicates the number of valid EAPOL frames received on the port.
- **Frames Transmit** — Indicates the number of EAPOL frames transmitted via the port.
- **Start Frames Receive** — Indicates the number of EAPOL Start frames received on the port.
- **Log off Frames Receive** — Indicates the number of EAPOL Logoff frames that have been received on the port.

- **Respond ID Frames Receive** — Indicates the number of EAP Resp/Id frames that have been received on the port.
- **Respond Frames Receive** — Indicates the number of valid EAP Response frames received on the port.
- **Request ID Frames Transmit** — Indicates the number of EAP Req/Id frames transmitted via the port.
- **Request Frames Transmit** — Indicates the number of EAP Request frames transmitted via the port.
- **Invalid Frames Receive** — Indicates the number of unrecognized EAPOL frames that have been received by on this port.
- **Length Error Frames Receive** — Indicates the number of EAPOL frames with an invalid Packet Body Length received on this port.
- **Last Frame Version** — Indicates the protocol version number attached to the most recently received EAPOL frame.
- **Last Frame Source** — Indicates the source MAC address attached to the most recently received EAPOL frame.

Managing RMON Statistics

This section contains the following topics:

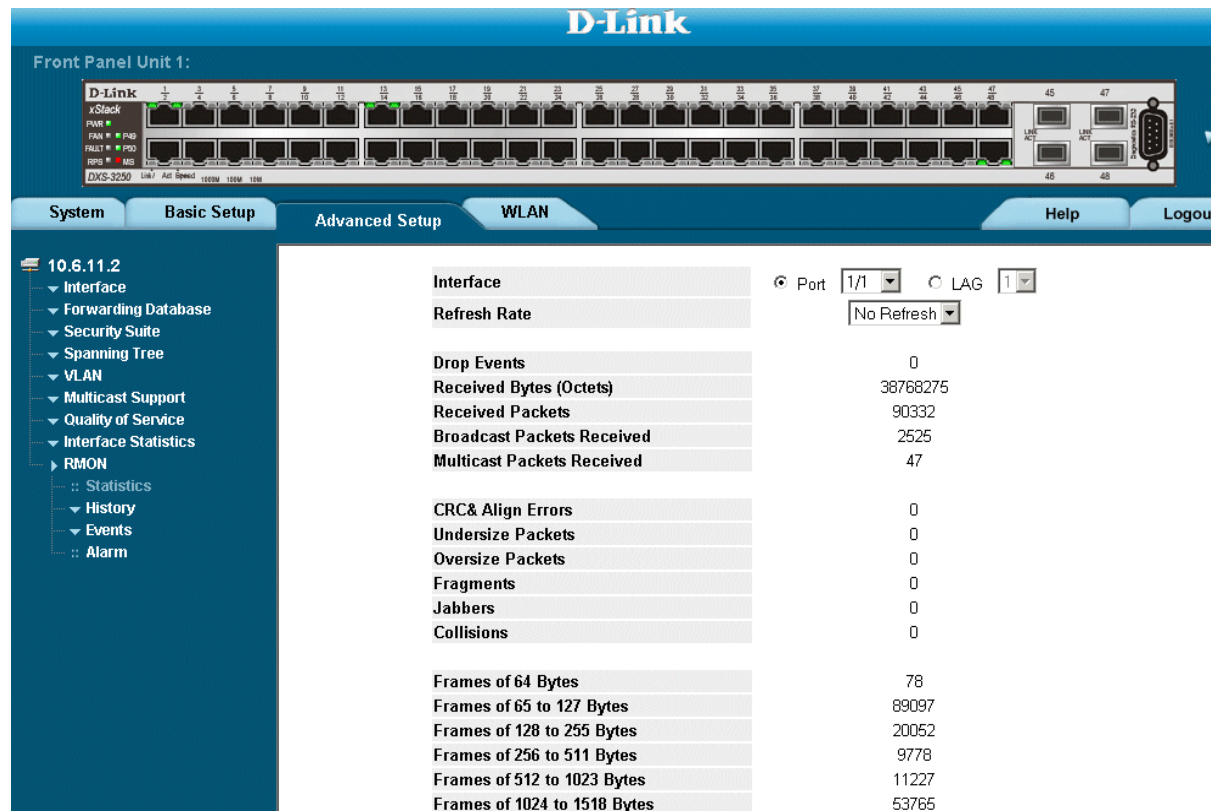
- Viewing RMON Statistics
- Configuring RMON History
- Configuring RMON Events
- Defining RMON Alarms

Viewing RMON Statistics

The *Viewing RMON Statistics* contains fields for viewing information about device utilization and errors that occurred on the device. To view RMON statistics:

1. Click **Advanced Setup > RMON > Statistics**. The *RMON Statistics Page* opens.

Figure 201:RMON Statistics Page




The *RMON Statistics Page* contains the following fields:

- **Interface** — Indicates the device for which statistics are displayed. The possible field values are:
 - *Port* — Defines the specific port for which RMON statistics are displayed.
 - *LAG* — Defines the specific LAG for which RMON statistics are displayed.
- **Refresh Rate** — Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:
 - *15 Sec* — Indicates that the RMON statistics are refreshed every 15 seconds.
 - *30 Sec* — Indicates that the RMON statistics are refreshed every 30 seconds.
 - *60 Sec* — Indicates that the RMON statistics are refreshed every 60 seconds.
- **Drop Events** — Displays the number of dropped events that have occurred on the interface since the device was last refreshed.

- **Received Bytes (Octets)** — Displays the number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
 - **Received Packets** — Displays the number of packets received on the interface, including bad packets, Multicast and broadcast packets, since the device was last refreshed.
 - **Broadcast Packets Received** — Displays the number of good broadcast packets received on the interface since the device was last refreshed. This number does not include Multicast packets.
 - **Multicast Packets Received** — Displays the number of good Multicast packets received on the interface since the device was last refreshed.
 - **CRC & Align Errors** — Displays the number of CRC and Align errors that have occurred on the interface since the device was last refreshed.
 - **Undersize Packets** — Displays the number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.
 - **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.
 - **Fragments** — Displays the number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the device was last refreshed.
 - **Jabbers** — Displays the total number of received packets that were longer than 1518 octets. This number excludes frame bits, but includes FCS octets that had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. The field range to detect jabbers is between 20 ms and 150 ms.
 - **Collisions** — Displays the number of collisions received on the interface since the device was last refreshed.
 - **Frames of xx Bytes** — Number of xx-byte frames received on the interface since the device was last refreshed.
2. Select an interface in the *Interface* field. The RMON statistics are displayed.

Resetting RMON Statistics Counters

1. Open the *RMON Statistics Page*.
2. Click . The RMON statistics counters are cleared.

Configuring RMON History

This section contains the following topics:

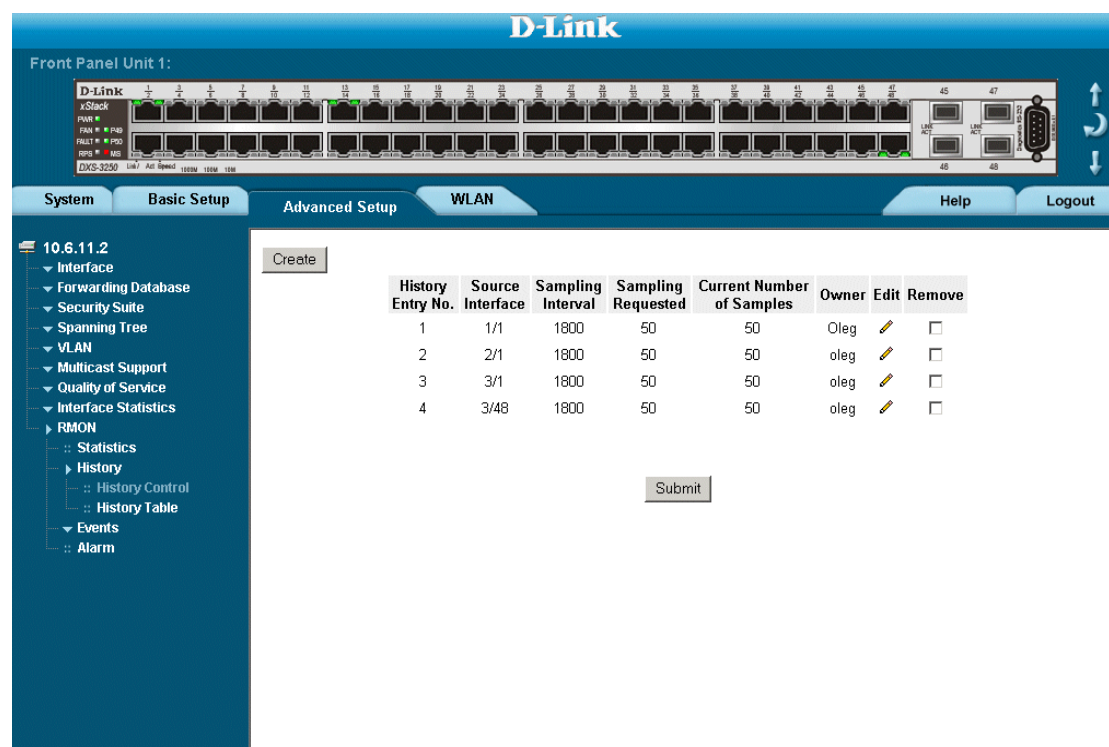
- Defining RMON History Control
- Viewing the RMON History Table

Defining RMON History Control

The *RMON History Control Page* contains information about samples of data taken from ports. For example, the samples may include interface definitions or polling periods. To view RMON history information:

1. Click **Advanced Setup > RMON > History > History Control**. The *RMON History Control Page* opens.

Figure 202: RMON History Control Page



The *RMON History Control Page* contains the following fields:

- **History Entry No.** — Displays the entry number for the History Control Table page.
- **Source Interface** — Displays the interface from which the history samples were taken. The possible field values are:
 - *Port* — Specifies the port from which the RMON information was taken.
 - *LAG* — Specifies the port from which the RMON information was taken.
- **Sampling Interval** — Indicates in seconds the time that samplings are taken from the ports. The field range is 1-3600. The default is 1800 seconds (equal to 30 minutes).

- **Sampling Requested**— Displays the number of samples to be saved. The field range is 1-65535. The default value is 50.
 - **Current Number of Samples**— Displays the current number of samples taken.
 - **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.
 - **Remove** — Removes History Control entries. The possible field values are:
 - *Checked* — Removes the selected History Control entry.
 - *Unchecked* — Maintains the current History Control entries.
2. Click **Create**. The *RMON History Control Settings Page* opens:

Figure 203: RMON History Control Settings Page

Add History Entry

New History Entry	1
Source Interface	<input checked="" type="radio"/> Port 1/1 <input type="radio"/> LAG
Owner	<input type="text"/>
Max No. of Samples to Keep	50
Sampling Interval	1800

Submit

3. Define *the* fields.
4. Click **Submit**. The entry is added to the *RMON History Control Page*, and the device is updated.

Viewing the RMON History Table

The *RMON History Table Page* contains interface specific statistical network samplings. Each table entry represents all counter values compiled during a single sample. To view the RMON History Table:

1. Click **Advanced Setup > RMON > History > History Table**. The *RMON History Table Page* opens.

Figure 204: RMON History Table Page

The screenshot shows the D-Link web interface for 'Front Panel Unit 1'. The navigation menu on the left is expanded to 'RMON' > 'History' > 'History Table'. The main content area displays the following table:

Sample No.	Drop Events	Received Bytes (Octets)	Received Packets	Broadcast Packets	Multicast Packets	CRC Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Util
1	0	12735716	37115	925	20	0	0	0	0	0	0	
2	0	7541601	28528	1040	19	0	0	0	0	0	0	

The *RMON History Table Page* contains the following fields:

- **History Entry No.** — Displays the entry number for the History Control Table page.
- **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.
- **Sample No.** — Indicates the sample number from which the statistics were taken.
- **Drop Events** — Displays the number of dropped events that have occurred on the interface since the device was last refreshed.
- **Received Bytes (Octets)** — Displays the number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Received Packets** — Displays the number of packets received on the interface since the device was last refreshed, including bad packets, Multicast and Broadcast packets.
- **Broadcast Packets** — Displays the number of good Broadcast packets received on the interface since the device was last refreshed. This number does not include Multicast packets.
- **Multicast Packets** — Displays the number of good Multicast packets received on the interface since the device was last refreshed.

- **CRC Align Errors** — Displays the number of CRC and Align errors that have occurred on the interface since the device was last refreshed.
 - **Undersize Packets** — Displays the number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.
 - **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.
 - **Fragments** — Displays the number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the device was last refreshed.
 - **Jabbers** — Displays the total number of received packets that were longer than 1518 octets. This number excludes frame bits, but includes FCS octets that had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. The field range to detect jabbers is between 20 ms and 150 ms.
 - **Collisions** — Displays the number of collisions received on the interface since the device was last refreshed.
 - **Utilization** — Displays the percentage of the interface utilized.
2. Select an entry in the *History Entry No.* field. The Statistics are displayed.

Configuring RMON Events

This section includes the following topics:

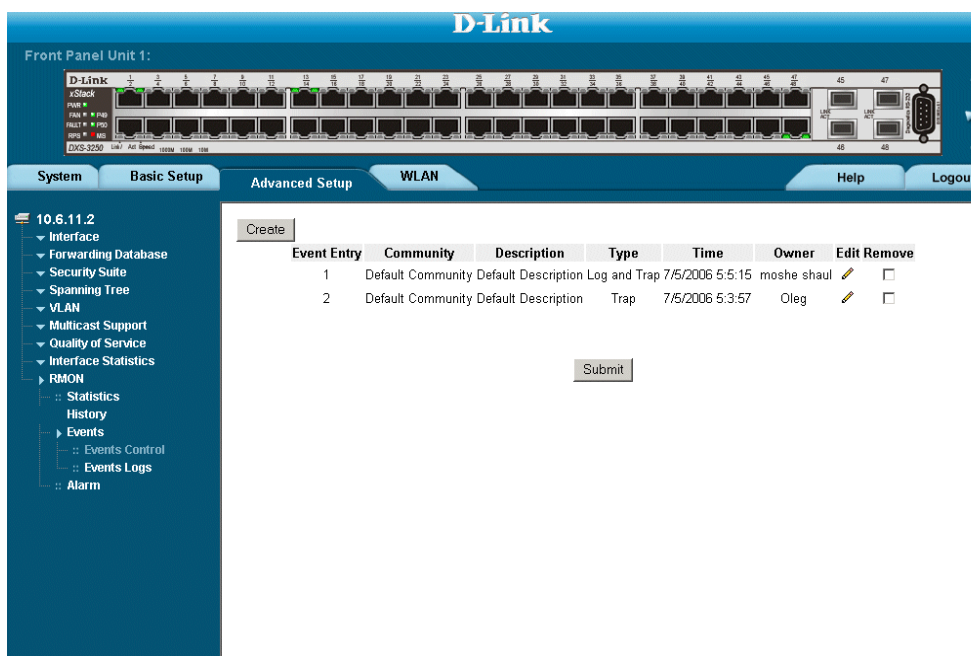
- Defining RMON Events Control
- Viewing the RMON Events Logs

Defining RMON Events Control

The *RMON Events Control Page* contains fields for defining RMON events. To view RMON events:

- Click **Advanced Setup > RMON > Events > Events Control**. The *RMON Events Control Page* opens.

Figure 205: RMON Events Control Page



The *RMON Events Control Page* contains the following fields:

- **Event Entry** — Displays the event.
- **Community** — Displays the community to which the event belongs.
- **Description** — Displays the user-defined event description.
- **Type** — Describes the event type. Possible values are:
 - *Log* — Indicates that the event is a log entry.
 - *Trap* — Indicates that the event is a trap.
 - *Log and Trap* — Indicates that the event is both a log entry and a trap.
 - *None* — Indicates that no event occurred.
- **Time** — Displays the time that the event occurred.

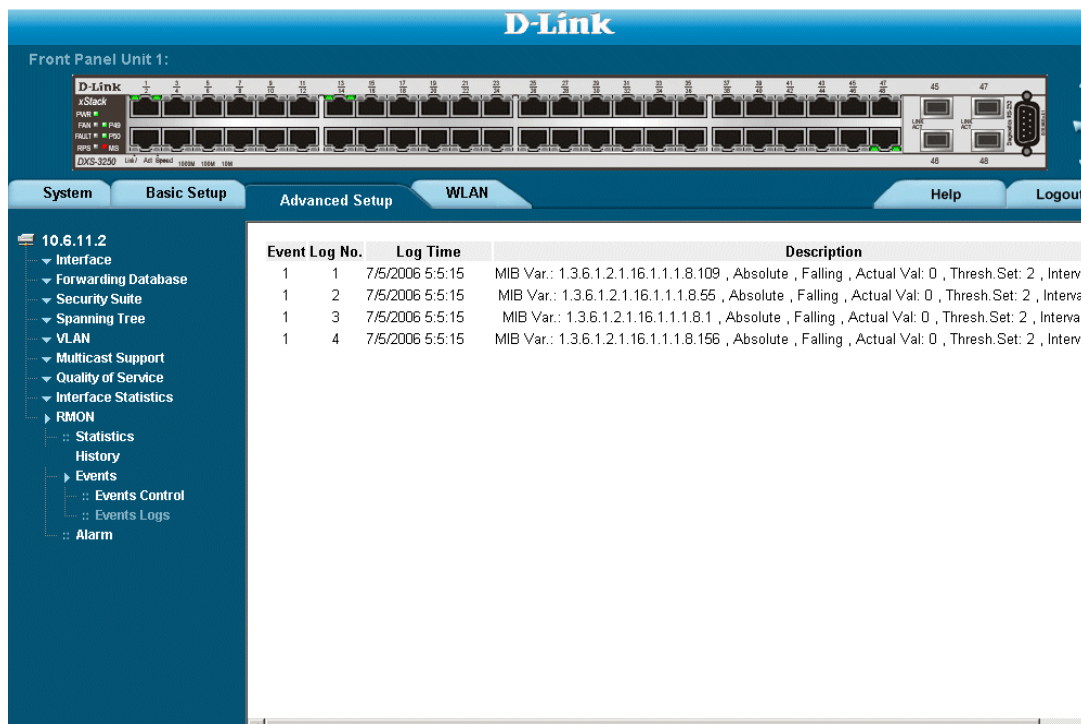
- **Owner** — Displays the device or user that defined the event.
- **Remove** — Removes a RMON event. The possible field values are:
 - *Checked* — Removes a selected RMON event.
 - *Unchecked* — Maintains RMON events.

Viewing the RMON Events Logs

The *RMON Events Logs Page* contains a list of RMON events. To view RMON event logs:

- Click **Advanced Setup > RMON > Events > Events Logs**. The *RMON Events Logs Page* opens.

Figure 206: RMON Events Logs Page



The *RMON Events Logs Page* contains the following fields:

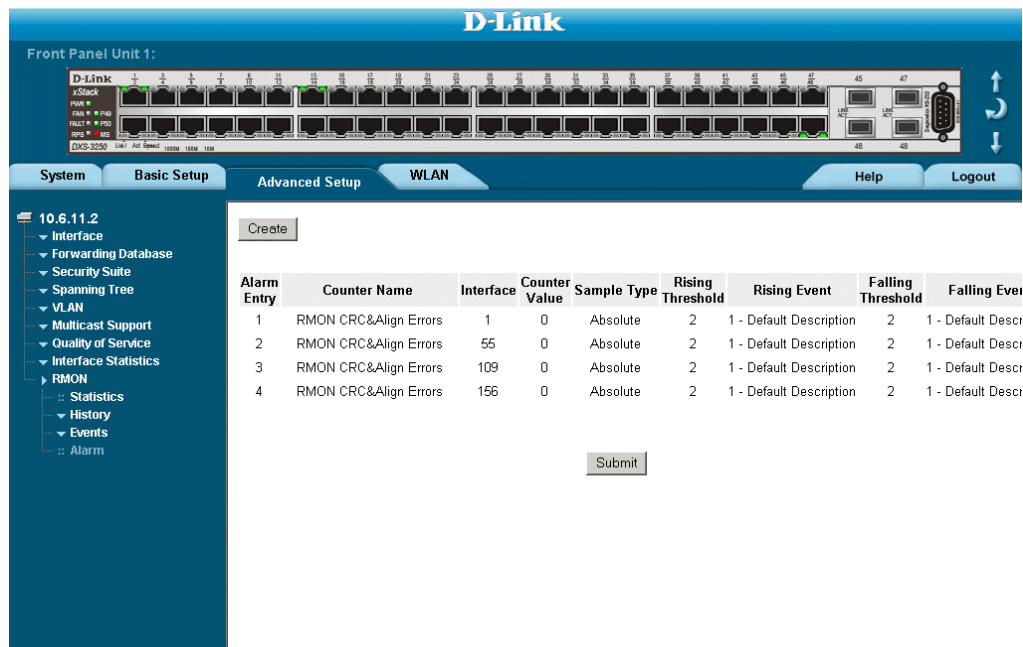
- **Event** — Displays the RMON Events Log entry number.
- **Log No.**— Displays the log number.
- **Log Time** — Displays the time when the log entry was entered.
- **Description** — Displays the log entry description.

Defining RMON Alarms

The *RMON Alarm Page* contains fields for setting network alarms. Network alarms occur when a network problem, or event, is detected. Rising and falling thresholds generate events. To set RMON alarms:

1. Click **Advanced Setup > RMON > Alarm**. The *RMON Alarm Page* opens.

Figure 207: RMON Alarm Page



The *RMON Alarm Page* contains the following fields:

- **Alarm Entry** — Indicates a specific alarm.
- **Counter Name** — Displays the selected MIB variable.
- **Interface** — Displays interface for which RMON statistics are displayed. The possible field values are:
 - *Port* — Displays the RMON statistics for the selected port.
 - *LAG* — Displays the RMON statistics for the selected LAG.
- **Counter Value** — Displays the selected MIB variable value.
- **Sample Type** — Defines the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:
 - *Delta* — Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.
 - *Absolute* — Compares the values directly with the thresholds at the end of the sampling interval.
- **Rising Threshold** — Displays the rising counter value that triggers the rising threshold alarm. The rising threshold is presented on top of the graph bars. Each monitored variable is designated a color.
- **Rising Event** — Displays the mechanism in which the alarms are reported. The possible field values are:
 - *LOG* — Indicates there is not a saving mechanism for either the device or in the management system. If the device is not reset, the entry remains in the Log Table.

- *TRAP* — Indicates that an SNMP trap is generated, and sent via the Trap mechanism. The Trap can also be saved using the Trap mechanism.
 - *Both* — Indicates that both the Log and Trap mechanism are used to report alarms.
 - **Falling Threshold** — Displays the falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on top of the graph bars. Each monitored variable is designated a color.
 - **Falling Event** — Displays the mechanism in which the alarms are reported.
 - **Startup Alarm** — Displays the trigger that activates the alarm generation. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.
 - **Interval** — Defines the alarm interval time in seconds.
 - **Owner** — Displays the device or user that defined the alarm.
 - **Remove** — Removes the RMON Alarms Table entry.
2. Click **Create**. The Add Alarms Entry Page opens:

Figure 208: Add Alarms Entry Page

Add Alarm Entry

Alarm Entry	1
Interface	<input checked="" type="radio"/> Port 1 <input type="radio"/> LAG
Counter Name	Total Bytes (Octets)- Receive
Sample Type	Absolute
Rising Threshold	100
Rising Event	
Falling Threshold	20
Falling Event	
Startup Alarm	Rising and Falling
Interval	100
Owner	

Submit

3. Define the Interface, Counter Name, Sample Type, Rising Threshold, Rising Event, Falling Threshold, Falling Event, Startup Alarm, Interval, and Owner fields.
4. Click **Submit**. The RMON alarm is added, and the device is updated.

Appendix A, WLAN Country Settings

This appendix contains vital information for configuring WLAN, including the country codes, power regulations, and frequency ranges.

Country	Country Code	Access Point Domain	Channels Allowed	Maximum Transmit Power (Radio Tx + Antenna Gain = EIRP)	Frequency Range (GHz)
Austria	AT	-E	36, 40, 44, 48	60 mW EIRP	5.15-5.25
			1 - 11	100 mW EIRP	2.4-2.4835
Australia	AU	-N	36, 40, 44, 48,52, 56, 60, 64,149, 153, 157, 161	200 mW EIRP 200 mW EIRP 1 W EIRP	5.15-5.25 5.25-5.35 5.725-5.825
			1 - 11	200 mW EIRP	2.4-2.4835
Belgium	BE	-E	36, 40, 44, 48,52, 56, 60, 64	120 mW EIRP 120 mW EIRP	5.15-5.25
			1 - 12,13	100 mW EIRP 100 mW EIRP	2.4-2.4835
Brazil	BR	-C	36, 40, 44, 48,52, 56, 60, 64,149, 153, 157, 161	200 mW EIRP 1 W EIRP	5.725-5.85
			1 - 11	1 W EIRP	2.4-2.4835
Canada	CA	-A	36, 40, 44, 48,52, 56, 60, 64,149, 153, 157, 161	50 mW+6 dBi=200 mW, 250 mW+6 dBi=1 W, 1 W+6 dBi=4 W	5.15-5.25 5.25-5.35 5.725-5.85
			1-11	1 W+Restricted Antennas	2.4-2.4835
Switzerland and Liechtenstein	CH	-E	36, 40, 44, 48,52, 56, 60, 64	200 mW EIRP 200 mW EIRP	5.15-5.255.25-5.35
			1-11	100 mW EIRP	2.4-2.4835

Country	Country Code	Access Point Domain	Channels Allowed	Maximum Transmit Power (Radio Tx + Antenna Gain = EIRP)	Frequency Range (GHz)
China	CN	-C	149, 153, 157, 161	150 mW+6 dBi~600 mW	5.725-5.825
			1-13	150 mW+6 dBi~600 mW	2.4-2.4835
Cyprus	CY	-E	36, 40, 44, 48,52, 56, 60, 64,149, 153, 157, 161	50 mW+6 dBi=200 mW 250 mW+6 dBi=1 W 1 W+6 dBi=4 W	5.15-5.25 5.25-5.35 5.725-5.85
			1-11	1 W+Restricted Antennas	2.4-2.4835
Czech Republic	CZ	-E	36, 40, 44, 48,52, 56, 60, 64,149, 153, 157, 161	200 mW EIRP 200 mW EIRP1 W EIRP	5.15-5.25 5.25-5.35 5.725-5.825
			1-11	200 mW EIRP	2.4-2.4835
Germany	DE	-E	36, 40, 44, 48,52, 56, 60, 64,104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP1 W EIRP	5.15-5.25 5.25-5.35 5.47-5.725
			1-11		2.4-2.4835
Denmark	DK	-E	36, 40, 44, 48,52, 56, 60, 64,104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP1 W EIRP	5.15-5.25 5.25-5.35 5.47-5.725
			1-11	100 mW EIRP	2.4-2.4835
Estonia	EE	-E	36, 40, 44, 48,52, 56, 60, 64,149, 153, 157, 161	50 mW+6 dBi=200 mW 250 mW+6 dBi=1 W 1 W+6 dBi=4 W	5.15-5.25 5.25-5.35 5.725-5.85
			1-11	1 W+Restricted Antennas	2.4-2.4835
Spain	ES	-E			
			1-11	100 mW EIRP	

Country	Country Code	Access Point Domain	Channels Allowed	Maximum Transmit Power (Radio Tx + Antenna Gain = EIRP)	Frequency Range (GHz)
Finland	FI	-E	36, 40, 44, 48,52, 56, 60,	200 mW EIRP200 mW EIRP1 W EIRP	5.15-5.255.25-5.355.47-5.725
			64,104, 108,		
			112, 116, 120,		
			124, 128, 132,		
			140		
			1-11	100 mW EIRP	2.4-2.4835
France	FR	-E	36, 40, 44, 48,52, 56, 60, 64	200 mW EIRP200 mW EIRP	5.15-5.255.25-5.35
			1 - 7,8 - 11	100 mW EIRP100 mW EIRP	2.4-2.48352.4-2.454
United Kingdom	GB	-E	36, 40, 44, 48,52, 56, 60, 64,104, 108,	200 mW EIRP200 mW EIRP1 W EIRP	5.15-5.25 5.25-5.35 5.47-5.725
			112, 116, 120,		
			124, 128, 132,		
			140		
			1-11	100 mW EIRP	2.4-2.4835
Greece	GR	-E	1-11	100 mW EIRP	2.4-2.4835
Hong Kong	HK	-N	36, 40, 44, 48,52, 56, 60, 64,149, 153, 157, 161	200 mW EIRP200 mW EIRP1 W+6 dBi=4 W	5.15-5.25 5.25-5.35 5.725-5.85
			1-11	100 mW EIRP	2.4-2.4835
Hungary	HU	-E	36, 40, 44, 48,52, 56, 60, 64	200 mW EIRP	5.15-5.255.25-5.35
			1-11	1 W EIRP	2.4-2.4835
Indonesia	ID	-R	N/A	N/A	5.725-5.875
			1-13	100 mW EIRP	2.4-2.5

Country	Country Code	Access Point Domain	Channels Allowed	Maximum Transmit Power (Radio Tx + Antenna Gain = EIRP)	Frequency Range (GHz)
Ireland	IE	-E	36, 40, 44, 48,52, 56, 60, 64	200 mW EIRP200 mW EIRP1 W EIRP	5.15-5.25 5.25-5.35 5.47-5.725
			1-11	100 mW EIRP	2.4-2.4835
Israel	IL	-I	36, 40, 44, 48,52, 56, 60, 64	200 mW EIRP200 mW EIRP	5.15-5.25 5.25-5.35
			1-13	100 mW EIRP	2.4-2.4835
Israel OUTDOOR	ILO		36, 40, 44, 48,52, 56, 60, 64	200 mW EIRP200 mW EIRP	5.15-5.255.25-5.35
			5-13	100 mW EIRP	2.4-2.4835
India	IN	TBA	N/A	N/A	N/A
				4 W EIRP	2.4-2.4835
Iceland	IS	-E	36, 40, 44, 48,52, 56, 60,	200 mW EIRP200 mW EIRP1 W EIRP	5.15-5.25 5.25-5.35 5.47-5.725
			64,104, 108,		
			112, 116, 120,		
			124, 128, 132,		
			140		
			1-11	100 mW EIRP	2.4-2.4835
Italy	IT	-E	36, 40, 44, 48,52, 56, 60,	200 mW EIRP200 mW EIRP1 W EIRP	5.15-5.25 5.25-5.35 5.47-5.725
			64,104, 108, 112, 116, 120,		
			124, 128, 132,		
			140		
			1-11	100 mW EIRP	2.4-2.4835
Japan	JP	-J	1-3,1-4	100 mW EIRP100 mW EIRP	5.03-5.09 5.15-5.25

Country	Country Code	Access Point Domain	Channels Allowed	Maximum Transmit Power (Radio Tx + Antenna Gain = EIRP)	Frequency Range (GHz)
			1-14	10 mW/ MHz~200mW EIRP	2.4-2.497
			1-13	10 mW/ MHz~200mW EIRP	2.4-2.497
Republic of Korea	KR	-C	149, 153, 157, 161	150 mW+6 dBi~600 mW	5.725-5.825
			1-13	150 mW+6 dBi~600 mW	2.4-2.4835
Lithuania	LT	-E	36, 40, 44, 48,52, 56, 60,	50 mW+6 dBi=200 mW 250 mW+6	5.15-5.25 5.25-5.35 5.725-5.85
			64,149, 153,	dBi=1 W1 W+6	
			157, 161	dBi=4 W	
			1-11	1 W+Restricted Antennas	2.4-2.4835
Luxembourg	LU	-E	36, 40, 44, 48,52, 56, 60,	200 mW EIRP 200 mW EIRP1 W EIRP	5.15-5.25 5.25-5.35 5.47-5.725
			64,104, 108,		
			112, 116, 120, 124, 128, 132,		
			140		
			1-11	100 mW EIRP	2.4-2.4835
Latvia	LV	-E	36, 40, 44, 48,52, 56, 60,	50 mW+6 dBi=200 mW 250 mW+6	5.15-5.25 5.25-5.35 5.725-5.85
			64,149, 153,	dBi=1 W1 W+6	
			157, 161	dBi=4 W	
			1-11	1 W+Restricted Antennas	2.4-2.4835
Malaysia	MY	-E	1-13	100 mW EIRP	2.4-2.5
Netherlands	NL	-E	36, 40, 44, 48,52, 56, 60,	200 mW EIRP 200 mW EIRP1 W EIRP	5.15-5.25 5.25-5.35 5.47-5.725
			64,104, 108,		
			112, 116, 120,		

Country	Country Code	Access Point Domain	Channels Allowed	Maximum Transmit Power (Radio Tx + Antenna Gain = EIRP)	Frequency Range (GHz)
			124, 128, 132,		
			140		
			1-11	100 mW EIRP	2.4-2.4835
Norway	NO	-E	36, 40, 44, 48,52, 56, 60, 64,104, 108,	200 mW EIRP200 mW EIRP1 W EIRP	5.15-5.25 5.25- 5.35 5.47-5.725
			112, 116, 120,		
			124, 128, 132, 140		
			1-11	100 mW EIRP	2.4-2.4835
New Zealand	NZ	-N	36, 40, 44, 48,52, 56, 60,	50 mW+6 dBi=200 mW250 mW+6	5.15-5.25 5.25- 5.35 5.725-5.85
			64,149, 153,	dBi=1 W1 W+6	
			157, 161	dBi=4 W	
			1-11	1 W+Restricted Antennas	2.4-2.4835
Philippines	PH	-C	TBA	TBA	5.725-5.875
				100 mW EIRP	2.4-2.4835
Poland	PL	-E	36, 40, 44, 48,52, 56, 60,	200 mW EIRP 1 W EIRP	2.4-2.4835
			64,149, 153,		
			157, 161		
			1-11	100 mW EIRP	2.4-2.4835
Portugal	PT	-E	36, 40, 44, 48,52, 56, 60,	200 mW EIRP200 mW EIRP1 W EIRP	5.15-5.25 5.25- 5.35 5.47-5.725
			64,104, 108,		
			112, 116, 120, 124, 128, 132,		
			140		
			1-11	100 mW EIRP	2.4-2.4835

Country	Country Code	Access Point Domain	Channels Allowed	Maximum Transmit Power (Radio Tx + Antenna Gain = EIRP)	Frequency Range (GHz)
Sweden	SE	-E	36, 40, 44, 48,52, 56, 60,	200 mW EIRP200 mW EIRP1 W EIRP	5.15-5.25 5.25-5.35 5.47-5.725
			64,104, 108,		
			112, 116, 120,		
			124, 128, 132,		
			140		
			1-11	100 mW EIRP	2.4-2.4835
Singapore	SG	-S	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	200 mW EIRP200 mW EIRP1 W EIRP	5.15-5.25 5.25-5.35 5.725-5.85
			1-13	200 mW EIRP	2.4-2.4835
Slovenia	SI	-E	36, 40, 44, 48,52, 56, 60,	50 mW+6 dBi=200 mW250 mW+6	5.15-5.255.25-5.355.725-5.85
			64,149, 153,	dBi=1 W1 W+6	
			157, 161	dBi=4 W	
			1-11	1 W+Restricted Antennas	2.4-2.4835
Slovak Republic	SK	-E	36, 40, 44, 48,52, 56, 60, 64,149, 153, 157, 161	50 mW+6 dBi=200 mW250 mW+6 dBi=1 W1 W+6 dBi=4 W	5.15-5.25 5.25-5.35 5.725-5.85
			1-11	1 W+Restricted Antennas	2.4-2.4835
Thailand	TL	-R	N/A	N/A	5.725-5.875
			1-13	100 mW EIRP	2.4-2.5
Taiwan	TW	-T	56, 60, 64, 100 - 140,149, 153,	50 mW+6 dBi=200 mW250 mW+6	5.25-5.35 5.47-5.725 5.725-5.825
			157, 161	dBi=1 W1 W+6	
				dBi=4 W	
			1-13	1 W EIRP	2.4-2.4835

Country	Country Code	Access Point Domain	Channels Allowed	Maximum Transmit Power (Radio Tx + Antenna Gain = EIRP)	Frequency Range (GHz)
United States	US	-A	36, 40, 44,	50 mW+6 dBi=200	5.15-5.25 5.25-5.35
of America			48,52, 56, 60,	mW250 mW+6	5.725-5.85
			64,149, 153,	dBi=1 W1 W+6	
			157, 161	dBi=4 W	
			1-11	1 W Conducted Output	2.4-2.4835
United States of America	USE	-A	36, 40, 44, 48,52, 56, 60, 64	50 mW+6 dBi=200 mW250 mW+6 dBi=1 W	5.15-5.25 5.25-5.35
			1-11	1 W Conducted Output	2.4-2.4835
United States of America LOW	USL	-A	36, 40, 44, 48,52, 56, 60, 64	50 mW+6 dBi=200 mW250 mW+6 dBi=1 W	5.15-5.25 5.25-5.35
			1-11	1 W Conducted Output	2.4-2.4835
United States of America EXTENDED	USX	TBA	36, 40, 44, 48,52, 56, 60, 64	50 mW+6 dBi=200 mW250 mW+6 dBi=1 W	5.15-5.25 5.25-5.35
			1-11	1 W Conducted Output	2.4-2.4835
South Africa	ZA	TBA	N/A	N/A	5.25-5.355.725-5.825
			1-13	1 W EIRP	2.4-2.4835

Appendix B, Device Specifications & Features

This appendix contains the device specifications and features pertaining to the DXS/DWS-3200 series. This section contains the following topics:

- Hardware Specifications
- DXS-3227, DXS-3227P, and DXS-3250 Features (any reference to PoE is only specific to the DXS-3227P and DWS-3227P model).

Hardware Specifications

Ports	<ul style="list-style-type: none"> • DXS/DWS-3250 - 48Gigabit Ethernet ports, RS-232 Console port, 4 SFP Ports • DXS/DWS-3227/3227P - 24 Gigabit Ethernet ports, RS-232 Console port, XFP Port, 4 SFP Ports
CPU Flash	32MB SDRAM
PoE Per port power	15.4 W (MAX)
PoE Total available power	375 W (MAX)
AC Input	110 ~ 240V AC Internal universal power supply
Operating Temperature	0 ~ 50°C
Storage Temperature	-10 ~ 70°C
Operating Humidity	10%-90% RH
Storage Humidity	5% ~ 90% RH
Dimensions (W x H x D)	
DXS/DWS-3250	440mm X 44mm X 430mm, 17.3 inch X 1.73 inch X 16.9 inch
DXS/DWS-3227	440mm X 44mm X 310mm, 17.3 inch X 1.73 inch X 12.2 inch
DXS/DWS-3227P	440mm X 44mm X 430mm, 17.3 inch X 1.73 inch X 16.9 inch

DXS-3227, DXS-3227P, and DXS-3250 Features

This appendix describes the device features. The system supports the following features:

Feature	Description
Auto Negotiation	<p>Auto negotiation allows an device to advertise modes of operation. The auto negotiation function provides the means to exchange information between two devices that share a point-to-point link segment, and to automatically configure both devices to take maximum advantage of their transmission capabilities.</p> <p>Auto negotiation provides port advertisement. Port advertisement allows the system administrator to configure the port speeds advertised.</p>
Automatic MAC Addresses Aging	<p>MAC addresses from which no traffic is received for a given period are aged out. This prevents the Bridging Table from overflowing.</p>
Back Pressure	<p>On half-duplex links, the receiving port prevents buffer overflows by occupying the link so that it is unavailable for additional traffic.</p>
Class Of Service	<p>The IEEE 802.1p signaling technique is an OSI Layer 2 standard for marking and prioritizing network traffic at the data link/MAC sub-layer. 802.1p traffic is classified and sent to the destination. No bandwidth reservations or limits are established or enforced. 802.1p is a spin-off of the 802.1Q (VLANs) standard. 802.1p establishes eight levels of priority, similar to the IP Precedence IP Header bit-field.</p>
Command Line Interface	<p><i>Command Line Interface</i> (CLI) syntax and semantics conform as much as possible to common industry practice. Syslog</p> <p>Syslog is a protocol that enables event notifications to be sent to a set of remote servers, where they can be stored, examined and acted upon. The system sends notifications of significant events in real time, and keeps a record of these events for after-the-fact usage.</p>
Configuration File Management	<p>The device configuration is stored in a configuration file. The Configuration file includes both system wide and port specific device configuration. The system can display configuration files in the form of a collection of CLI commands, which are stored and manipulated as text files.</p>
DHCP Clients	<p><i>Dynamic Host Client Protocol</i>. DHCP enables additional setup parameters to be received from a network server upon system startup. DHCP service is an on-going process.</p>

Feature	Description
Domain Name System	<i>Domain Name System</i> (DNS) converts user-defined domain names into IP addresses. Each time a domain name is assigned the DNS service translates the name into a numeric IP address. For example, www.ipexample.com is translated to 192.87.56.2. DNS servers maintain domain name databases and their corresponding IP addresses.
Fast Link	STP can take up to 30-60 seconds to converge. During this time, STP detects possible loops, allowing time for status changes to propagate and for relevant devices to respond. 30-60 seconds is considered too long of a response time for many applications. The Fast Link option bypasses this delay, and can be used in network topologies where forwarding loops do not occur.
Full 802.1Q VLAN Tagging Compliance	IEEE 802.1Q defines an architecture for virtual bridged LANs, the services provided in VLANs and the protocols and algorithms involved in the provision of these services. An important requirement included in this standard is the ability to mark frames with a desired Class of Service (CoS) tag value.
GVRP Support	GARP VLAN Registration Protocol (GVRP) provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. When GVRP is enabled, the device registers and propagates VLAN membership on all ports that are part of the active underlying <i>Spanning Tree Protocol Features</i> topology.
IGMP Snooping	IGMP Snooping examines IGMP frame contents, when they are forwarded by the device from work stations to an upstream Multicast router. From the frame, the device identifies work stations configured for Multicast sessions, and which Multicast routers are sending Multicast frames.
LACP	LACP uses peer exchanges across links to determine, on an ongoing basis, the aggregation capability of various links, and continuously provides the maximum level of aggregation capability achievable between a given pair of systems. LACP automatically determines, configures, binds and monitors the port binding within the system.
Link Aggregated Groups	<i>Link Aggregated Group</i> (LAG). The system provides up-to eight Aggregated Links may be defined, each with up to eight member ports, to form a single. LAGs provide: <ul style="list-style-type: none"> • Fault tolerance protection from physical link disruption • Higher bandwidth connections • Improved bandwidth granularity • High bandwidth server connectivity LAG is composed of ports with the same speed, set to full-duplex operation.
MAC Address Capacity Support	The device supports up to 8K MAC addresses. The device reserves specific MAC addresses for system use.

Feature	Description
MAC Multicast Support	Multicast service is a limited broadcast service, which allows one-to-many and many-to-many connections for information distribution. Layer 2 Multicast service is where a single frame is addressed to a specific Multicast address, from where copies of the frame are transmitted to the relevant ports.
MDI/MDIX Support	The device automatically detects whether the cable connected to an RJ-45 port is crossed or straight through, when auto-negotiation is enabled. Standard wiring for end stations is <i>Media-Dependent Interface (MDI)</i> and the standard wiring for hubs and switches is known as <i>Media-Dependent Interface with Crossover (MDIX)</i> .
Multiple Spanning Tree	Multiple Spanning Tree (MSTP) operation maps VLANs into STP instances. MSTP provides differing load balancing scenario. Packets assigned to various VLANs are transmitted along different paths within MSTP Regions (MST Regions). Regions are one or more MSTP bridges by which frames can be transmitted. The standard lets administrators assign VLAN traffic to unique paths.
Password Management	Password management provides increased network security and improved password control. Passwords for SSH, Telnet, HTTP, HTTPS, and SNMP access are assigned security features. For more information on Password Management, see "Configuring Passwords".
Port Based Authentication	Port based authentication enables authenticating system users on a per-port basis via an external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the Remote Authentication Dial In User Service (RADIUS) server using the Extensible Authentication Protocol (EAP).
Port Based Virtual LANs	Port-based VLANs classify incoming packets to VLANs based on their ingress port.
Port Mirroring	Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from a monitored port to a monitoring port. Users specify which target port receives copies of all traffic passing through a specified source port.

Feature	Description
Power over Ethernet	<p><i>Power over Ethernet (PoE)</i> provide power to devices over existing LAN cabling, without updating or modifying the network infrastructure. Power over Ethernet removes the necessity of placing network devices next to power sources. Power over Ethernet can be used in the following applications:</p> <ul style="list-style-type: none"> • IP Phones • Wireless Access Points • IP Gateways • PDAs • Audio and video remote monitoring
Private VLANs	Private VLAN ports are a Layer 2 security feature which provide isolation between ports within the same Broadcast domain.
RADIUS Clients	RADIUS is a client/server-based protocol. A RADIUS server maintains a user database, which contains per-user authentication information, such as user name, password and accounting information.
Rapid Spanning Tree	Spanning Tree can take 30-60 seconds for each host to decide whether its ports are actively forwarding traffic. Rapid Spanning Tree (RSTP) detects uses of network topologies to enable faster convergence, without creating forwarding loops.
Remote Monitoring	<i>Remote Monitoring (RMON)</i> is an extension to SNMP, which provides comprehensive network traffic monitoring capabilities (as opposed to SNMP which allows network device management and monitoring). RMON is a standard MIB that defines current and historical MAC-layer statistics and control objects, allowing real-time information to be captured across the entire network.
Self-Learning MAC Addresses	The device enables automatic MAC address learning from incoming packets. The MAC addresses are stored in the Bridging Table
SNMP Alarms and Trap Logs	<p>The system logs events with severity codes and timestamps. Events are sent as SNMP traps to a Trap Recipient List.</p> <p>For more information on SNMP Alarms and Traps, see “<i>SNMP Security Global Parameters Page.</i>”</p>
SNMP Versions 1, 2 and 3	<i>Simple Network Management Protocol (SNMP)</i> over the UDP/IP protocol controls access to the system, a list of community entries is defined, each of which consists of a community string and its access privileges. There are 3 levels of SNMP security read-only, read-write and super. Only a super user can access the community table.

Feature	Description
SNTP	The <i>Simple Network Time Protocol</i> (SNTP) assures accurate network Ethernet Switch clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. Time sources are established by Stratum. Stratum define the distance from the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock.
Spanning Tree Protocol	802.1d Spanning tree is a standard Layer 2 switch requirement that allows bridges to automatically prevent and resolve L2 forwarding loops. Switches exchange configuration messages using specifically formatted frames and selectively enable and disable forwarding on ports.
SSH 2.0	Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH version 2 is currently supported. The SSH server feature enables an SSH client to establish a secure, encrypted connection with a device. This connection provides functionality that is similar to an inbound telnet connection. SSH uses RSA and DSA Public Key cryptography for device connections and authentication.
SSL 3.0	Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. It relies upon certificates and public and private keys.
Static MAC Entries	MAC entries can be manually entered in the Bridging Table, as an alternative to learning them from incoming frames. These user-defined entries are not subject to aging, and are preserved across resets and reboots.
TACACS+	TACACS+ provides centralized security for validation of users accessing the device. TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes.
TCP	<i>Transport Control Protocol</i> (TCP). TCP connections are defined between 2 ports by an initial synchronization exchange. TCP ports are identified by an IP address and a 16-bit port number. Octets streams are divided into TCP packets, each carrying a sequence number.
TFTP Trivial File Transfer Protocol	The device supports boot image, software and configuration upload/download via TFTP.
Traceroute	Traceroute discovers IP routes that packets were forwarded along during the forwarding process. The CLI Traceroute utility can be executed from either the user-exec or privileged modes.
Virtual Cable Testing	VCT detects and reports copper link cabling occurrences, such as open cables and cable shorts.

Feature	Description
VLAN Support	VLANs are collections of switching ports that comprise a single broadcast domain. Packets are classified as belonging to a VLAN based on either the VLAN tag or based on a combination of the ingress port and packet contents. Packets sharing common attributes can be grouped in the same VLAN.
VLAN-aware MAC-based Switching	The device always performs VLAN-aware bridging. Classic bridging(IEEE802.1D) is not performed, where frames are forwarded based only on their destination MAC address. However, a similar functionality may be configured for untagged frames. Frames addressed to a destination MAC address that is not associated with any port are flooded to all ports of the relevant VLAN.
Web Based Management	With web based management, the system can be managed from any web browser. The system contains an Embedded Web Server (EWS), which serves HTML pages, through which the system can be monitored and configured. The system internally converts web-based input into configuration commands, MIB variable settings and other management-related settings.

This page is left blank intentionally.

Appendix B, Troubleshooting

This section describes problems that may arise when installing the and how to resolve these issue. This section includes the following topics:

- **Problem Management** — Provides information about problem management with DXS-3250/DXS-3227P/DXS-3227.
- **Troubleshooting Solutions** — Provides a list of troubleshooting issues and solutions for using DXS-3250/DXS-3227P/DXS-3227.

Problem Management

Problem management includes isolating problems, quantifying the problems, and then applying the solution. When a problem is detected, the exact nature of the problem must be determined. This includes how the problem is detected, and what are the possible causes of the problem. With the problem known, the effect of the problem is recorded with all known results from the problem. Once the problem is quantified, the solution is applied. Solutions are found either in this chapter, or through customer support. If no solution is found in this chapter, contact Customer Support.

Troubleshooting Solutions

Listed below are some possible troubleshooting problems and solutions. These error messages include:

- Cannot connect to management using RS-232 serial connection
- Cannot connect to switch management using Telnet, HTTP, SNMP, etc.
- Self-test exceeds 15 seconds
- No connection is established and the port LED is on
- Device is in a reboot loop
- No connection and the port LED is off
- Add and Edit pages do not open.
- Lost password.

Problems	Possible Cause	Solution
Cannot connect to management using RS-232 serial connection		Be sure the terminal emulator program is set to VT-100 compatible, 9600 baud rate, no parity, 8 data bits and one stop bit Use the included cable, or be sure that the pin-out complies with a standard null-modem cable
Cannot connect to switch management using Telnet, HTTP, SNMP, etc.		Be sure the switch has a valid IP address, subnet mask and default gateway configured Check that your cable is properly connected with a valid link light, and that the port has not been disabled Ensure that your management station is plugged into the appropriate VLAN to manage the device If you cannot connect using Telnet or the web, the maximum number of connections may already be open. Please try again at a later time.
No response from the terminal emulation software	Faulty serial cable Incorrect serial cable Software settings	Replace the serial cable Replace serial cable for a pin-to-pin straight/flat cable Reconfigure the emulation software connection settings.
Response from the terminal emulations software is not readable	Faulty serial cable Software settings	Replace the serial cable Reconfigure the emulation software connection settings.

Problems	Possible Cause	Solution
Self-test exceeds 15 seconds	The device may not be correctly installed.	Remove and reinstall the device. If that does not help, consult your technical support representative.
No connection is established and the port LED is on	Wrong network address in the workstation No network address set Wrong or missing protocol Faulty ethernet cable Faulty port Faulty module Incorrect initial configuration	Configure the network address in the workstation Configure the network address in the workstation Configure the workstation with IP protocol Replace the cable Replace the module Replace the module Erase the connection and reconfigure the port
Device is in a reboot loop	Software fault	Download and install a working or previous software version from the console
No connection and the port LED is off	Incorrect ethernet cable, e.g., crossed rather than straight cable, or vice versa, split pair (incorrect twisting of pairs) Fiber optical cable connection is reversed Bad cable Wrong cable type	Check pinout and replace if necessary Change if necessary. Check Rx and Tx on fiber optic cable Replace with a tested cable Verify that all 10 Mbps connections use a Cat 5 cable Check the port LED or zoom screen in the NMS application, and change setting if necessary

Problems	Possible Cause	Solution
Add and Edit pages do not open.	A pop-up blocker is enabled.	Disable pop-up blockers.
Lost password		<p>The Password Recovery Procedure enables the user to override the current password configuration, and disables the need for a password to access the console.</p> <p>The password recovery is effective until the device is reset. If the password/user name has been forgotten or lost. The password must be reconfigured using either the CLI commands or via the Embedded Web Interface.</p> <p>The Password Recovery Procedure is invoked from the Startup menu:</p> <ol style="list-style-type: none"> 1. Reboot the system either by disconnecting the power supply, or enter the command: the following message is displayed: <pre>Console #reload Are you sure you want to reboot the system (y/n) [n]?</pre> 2. Enter Y. The device reboots. After the POST, when the text "Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom." is displayed, press <Enter>. The Startup Menu is displayed. <pre>[1] Download software [2] Erase flash file [3] Erase flash sectors [4] Password Recovery Procedure [5] Enter Diagnostic Mode [6] Back</pre> 3. Enter 4 within 15 seconds after the bootup process from the StartUp menu. If the startup menu option is not selected within 15 seconds, the accessibility requirements are erased, and the system continues to load. The password is defined using the CLI mode. 4. Enter the CLI configuration mode. 5. Enter the password commands: <code>username, enable password, or password [line]</code>. For example: <code>enable password level 1 password *****</code> 6. Enter the command <code>exit</code>. The CLI mode is exited.

Contacting D-Link Technical Support

Software updates and user documentation can be found on the D-Link website. D-Link provides free technical support for customers within the United States and within Canada for the warranty duration.

For more information on locating the D-Link office in your region, see International Offices.

Technical Support

You can find software updates and user documentation on the D-Link website.

D-Link provides free technical support for customers within the United States and within Canada for the duration of the warranty period on this product.

U.S. and Canadian customers can contact D-Link technical support through our website, or by phone.

Tech Support for customers within the United States:

D-Link Technical Support over the Telephone:

(888) 843-6100

Hours of Operation: 8:00AM to 6:00PM PST

D-Link Technical Support over the Internet:

<http://support.dlink.com>

[email:support@dlink.com](mailto:support@dlink.com)

Tech Support for customers within Canada:

D-Link Technical Support over the Telephone:

(800) 361-5265

Monday to Friday 7:30am to 12:00am EST

D-Link Technical Support over the Internet:

<http://support.dlink.ca>

[email:support@dlink.ca](mailto:support@dlink.ca)



Technical Support

You can find software updates and user documentation on the D-Link websites.

D-Link provides free technical support for customers within Canada, the United Kingdom, and Ireland.

Customers can contact D-Link technical support through our websites, or by phone.

For Customers within The United Kingdom & Ireland:

D-Link UK & Ireland Technical Support over the Telephone:

(08456 12 0003 (United Kingdom)

+44 8456 12 0003 (Ireland)

Monday to Friday 8:00 am to 10:00 pm GMT

Sat & Sun 10.00 am to 7.00 pm GMT

D-Link UK & Ireland Technical Support over the Internet:

<http://www.dlink.co.uk>

<ftp://ftp.dlink.co.uk>

For Customers within Canada:

D-Link Canada Technical Support over the Telephone:

1-800-361-5265 (Canada)

Monday to Friday 7:30 am to 12:00 am EST

D-Link Canada Technical Support over the Internet:

<http://support.dlink.ca>

email: support@dlink.ca

D-Link[®]
Building Networks for People

Technische Unterstützung

Aktualisierte Versionen von Software und Benutzerhandbuch finden Sie auf der Website von D-Link.

D-Link bietet kostenfreie technische Unterstützung für Kunden innerhalb Deutschlands, Österreichs, der Schweiz und Osteuropas.

Unsere Kunden können technische Unterstützung über unsere Website, per E-Mail oder telefonisch anfordern.

Web: <http://www.dlink.de>

E-Mail: support@dlink.de

Telefon: +49 (1805)2787

0,12€/Min aus dem Festnetz der Deutschen Telekom.

Telefonische technische Unterstützung erhalten Sie Montags bis Freitags von 09.00 bis 17.30 Uhr.

Wenn Sie Kunde von D-Link außerhalb Deutschlands, Österreichs, der Schweiz und Osteuropas sind, wenden Sie sich bitte an die zuständige Niederlassung aus der Liste im Benutzerhandbuch.



Assistance technique

Vous trouverez la documentation et les logiciels les plus récents sur le site web **D-Link**.

Le service technique de **D-Link** est gratuit pour les clients aux Etats-Unis durant la période de garantie.

Ceux-ci peuvent contacter le service technique de **D-Link** par notre site internet ou par téléphone.

Support technique destiné aux clients établis en France:

Assistance technique D-Link par téléphone :

0 820 0803 03

Assistance technique D-Link sur internet :

<http://www.dlink.fr>

e-mail : support@dlink.fr

Support technique destiné aux clients établis au Canada :

Assistance technique D-Link par téléphone :

(800) 361-5265

Lun.-Ven. 7h30 à 21h00 HNE.

Assistance technique D-Link sur internet :

<http://support.dlink.ca>

e-mail : support@dlink.ca

D-Link[®]
Building Networks for People

Asistencia Técnica

Puede encontrar el software más reciente y documentación para el usuario en el sitio web de **D-Link**. **D-Link** ofrece asistencia técnica gratuita para clientes dentro de España durante el periodo de garantía del producto. Los clientes españoles pueden ponerse en contacto con la asistencia técnica de **D-Link** a través de nuestro sitio web o por teléfono.

Asistencia Técnica de D-Link por teléfono:
902 304545

de lunes a viernes desde las 9:00 hasta las 14:00 y de las 15:00 hasta las 18:00

Asistencia Técnica de D-Link a través de Internet:
<http://www.dlink.es>
email: soporte@dlink.es

D-Link[®]
Building Networks for People

Supporto tecnico

Gli ultimi aggiornamenti e la documentazione sono disponibili sul sito D-Link.

Supporto tecnico per i clienti residenti in Italia

D-Link Mediterraneo S.r.L.

Via N. Bonnet 6/B 20154 Milano

Supporto Tecnico dal lunedì al venerdì dalle ore
9.00 alle ore 19.00 con orario continuato
Telefono: 02-39607160

URL : <http://www.dlink.it/supporto.html>
Email: tech@dlink.it



Technical Support

You can find software updates and user documentation on the D-Link website.

D-Link provides free technical support for customers within Benelux for the duration of the warranty period on this product.

Benelux customers can contact D-Link technical support through our website, or by phone.

Tech Support for customers within the Netherlands:

D-Link Technical Support over the Telephone:

0900 501 2007

Monday to Friday 8:00 am to 10:00 pm

D-Link Technical Support over the Internet:

www.dlink.nl

Tech Support for customers within Belgium:

D-Link Technical Support over the Telephone:

+32(0)2 717 3248

Monday to Friday 8:00 am to 10:00 pm

D-Link Technical Support over the Internet:

www.dlink.be

Tech Support for customers within Luxemburg:

D-Link Technical Support over the Telephone:

+352 342 080 82 13

Monday to Friday 8:00 am to 10:00 pm

D-Link Technical Support over the Internet:

www.dlink.be

D-Link®
Building Networks for People

Pomoc techniczna

Najnowsze wersje oprogramowania i dokumentacji użytkownika można znaleźć w serwisie internetowym firmy D-Link.

D-Link zapewnia bezpłatną pomoc techniczną klientom w Polsce w okresie gwarancyjnym produktu.

Klienci z Polski mogą się kontaktować z działem pomocy technicznej firmy D-Link za pośrednictwem Internetu lub telefonicznie.

Telefoniczna pomoc techniczna firmy D-Link:
+49 (1805)-2787

Pomoc techniczna firmy D-Link świadczona przez Internet:

URL: <http://www.dlink.pl>
e-mail: pomoc_techiczna@dlink.de



Technická podpora

Aktualizované verze software a uživatelských příruček najdete na webových stránkách firmy D-Link.

D-Link poskytuje svým zákazníkům bezplatnou technickou podporu

Zákazníci mohou kontaktovat oddělení technické podpory přes webové stránky, mailem nebo telefonicky

Web: <http://www.dlink.de>

E-Mail: support@dlink.de

Telefon: +49 (1805)-2787

Telefonická podpora je v provozu:

PO-ČT od 08.00 do 19.00

PÁ od 08.00 do 17.00

D-Link[®]
Building Networks for People

Technikai Támogatás

Meghajtó programokat és frissítéseket a **D-Link** Magyarország weblapjáról tölthet le.

Telefonon technikai segítséget munkanapokon hétfőtől-csütörtökig 9.00 – 16.00 óráig és pénteken 9.00 – 14.00 óráig kérhet a **(1) 461-3001** telefonszámon vagy a **support@dlink.hu** emailcímen.

Magyarországi technikai támogatás :

D-Link Magyarország

1074 Budapest, Alsóerdősor u. 6. – R70 Irodaház 1 em.

Tel. : 06 1 461-3001

Fax : 06 1 461-3004

email : support@dlink.hu

URL : <http://www.dlink.hu>

D-Link®
Building Networks for People

Teknisk Support

Du kan finne programvare oppdateringer og bruker dokumentasjon på D-Links web sider.

D-Link tilbyr sine kunder gratis teknisk support under produktets garantitid.

Kunder kan kontakte D-Links teknisk support via våre hjemmesider, eller på tlf.

Teknisk Support:

D-Link Teknisk telefon Support:

800 10 610
(Hverdager 08:00-20:00)

D-Link Teknisk Support over Internett:

<http://www.dlink.no>

D-Link®
Building Networks for People

Teknisk Support

Du finder software opdateringer og bruger-dokumentation på D-Link's hjemmeside.

D-Link tilbyder gratis teknisk support til kunder i Danmark i hele produktets garantiperiode.

Danske kunder kan kontakte D-Link's tekniske support via vores hjemmeside eller telefonisk.

D-Link teknisk support over telefonen:

Tlf. 7026 9040

Åbningstider: kl. 08:00 – 20:00

D-Link teknisk support på Internettet:

<http://www.dlink.dk>

[email:support@dlink.dk](mailto:support@dlink.dk)

D-Link[®]
Building Networks for People

Teknistä tukea asiakkaille Suomessa:

D-Link tarjoaa teknistä tukea asiakkailleen.
Tuotteen takuun voimassaoloajan.
Tekninen tuki palvelee seuraavasti:

Arkisin klo. 9 - 21
numerosta
0800-114 677

Internetin kautta
Ajurit ja lisätietoja tuotteista.
<http://www.dlink.fi>

Sähköpostin kautta
voit myös tehdä kyselyitä.
support@dlink.fi

D-Link[®]
Building Networks for People

Teknisk Support

På vår hemsida kan du hitta mer information om mjukvaru uppdateringar och annan användarinformation.

D-Link tillhandahåller teknisk support till kunder i Sverige under hela garantitiden för denna produkt.

Teknisk Support för kunder i Sverige:

D-Link Teknisk Support via telefon:

0770-33 00 35

Vardagar 08.00-20.00

D-Link Teknisk Support via Internet:

<http://www.dlink.se>

email: support@dlink.se

D-Link®
Building Networks for People

Technical Support

You can find software updates and user documentation on the D-Link website.

Tech Support for customers within Australia:

D-Link Technical Support over the Telephone:

1300-766-868

Monday to Friday 8:00am to 8:00pm EST

Saturday 9:00am to 1:00pm EST

D-Link Technical Support over the Internet:

<http://www.dlink.com.au>

email: support@dlink.com.au

Tech Support for customers within New Zealand:

D-Link Technical Support over the Telephone:

0800-900-900

Monday to Friday 8:30am to 8:30pm

Saturday 9:00am to 5:00pm

D-Link Technical Support over the Internet:

<http://www.dlink.co.nz>

email: support@dlink.co.nz

D-Link[®]
Building Networks for People

Technical Support

You can find software updates and user documentation on the D-Link website.

Tech Support for customers within South Eastern Asia and Korea:

D-Link South Eastern Asia and Korea Technical Support over the Telephone:

+65-6895-5355

Monday to Friday 9:00am to 12:30pm, 2:00pm-6:00pm
Singapore Time

D-Link Technical Support over the Internet:

email: support@dlink.com.sg

D-Link[®]
Building Networks for People

Technical Support

You can find software updates and user documentation on the D-Link website.

Tech Support for customers within India

D-Link Technical Support over the Telephone:

+91-22-26526741

+91-22-26526696 –ext 161 to 167

Monday to Friday 9:30AM to 7:00PM

D-Link Technical Support over the Internet:

<http://www.dlink.co.in>

<http://www.dlink.co.in/dlink/drivers/support.asp>

<ftp://support.dlink.co.in>

email: techsupport@dlink.co.in



Technical Support

You can find software updates and user documentation on the D-Link website.

D-Link provides free technical support for customers for the duration of the warranty period on this product.

Customers can contact D-Link technical support through our web site or by phone.

Tech Support for customers within the Russia

D-Link Technical Support over the Telephone:

(095) 744-00-99

Monday to Friday 10:00am to 6:30pm

D-Link Technical Support over the Internet

<http://www.dlink.ru>

email: support@dlink.ru



Technical Support

You can find software updates and user documentation on the D-Link website.

Tech Support for customers within the U.A.E & North Africa:

D-Link Technical Support over the Telephone:

(971) 4-391-6480 (U.A.E)

Sunday to Wednesday 9:00am to 6:00pm GMT+4

Thursday 9:00am to 1:00pm GMT+4

D-Link Middle East & North Africa

D-Link Technical Support over the Internet:

<http://support.dlink-me.com>

[email:support@dlink-me.com](mailto:support@dlink-me.com)

Tech Support for customers within Israel:

D-Link Technical Support over the Telephone:

(972) 971-5701

Sunday to Thursday 9:00am to 5:00pm

D-Link Technical Support over the Internet:

<http://www.dlink.co.il/forum>

e-mail: support@dlink.co.il

Tech Support for customers within Turkey:

D-Link Technical Support over the Telephone:

(+90) 212-289 56 59

Monday to Friday 9:00am to 6:00pm

D-Link Technical Support over the Internet:

<http://www.dlink.com.tr>

e-mail: turkiye@dlink-me.com

Tech Support for customers within Egypt:

D-Link Technical Support over the Telephone:

(202) 414-4295

Sunday to Thursday 9:00am to 5:00pm

D-Link Technical Support over the Internet:

<http://support.dlink-me.com>

e-mail: amostafa@dlink-me.com

D-Link[®]
Building Networks for People

Technical Support

You can find software updates and user documentation on the D-Link website.

Tech Support for customers within South Africa and Sub Sahara Region:

D-Link South Africa and Sub Sahara Technical Support over the Telephone:

+27-12-665-2165

08600 DLINK (For South Africa only)

Monday to Friday 8:30am to 9:00pm South Africa Time

D-Link Technical Support over the Internet:

<http://www.d-link.co.za>

[email:support@d-link.co.za](mailto:support@d-link.co.za)

D-Link[®]
Building Networks for People

Technical Support

You can find updates and user documentation on the D-Link website

Tech Support for Latin America customers:

D-Link Technical Support over the followings Telephones:

Argentina: 0800-666 1442	Monday to Friday 09:00am to 22:00pm
Chile: 800-214 422	Monday to Friday 08:00am to 21:00pm
Colombia: 01800-700 1588	Monday to Friday 07:00am to 20:00pm
Ecuador: 1800-777 711	Monday to Friday 07:00am to 20:00pm
El Salvador: 800-6137	Monday to Friday 06:00am to 19:00pm
Guatemala: 1800-300 0017	Monday to Friday 06:00am to 19:00pm
Panama: 0800-560 0193	Monday to Friday 07:00am to 20:00pm
Peru: 0800-52049	Monday to Friday 07:00am to 20:00pm
Venezuela: 0800-100 3470	Monday to Friday 08:00am to 21:00pm

D-Link Technical Support over the Internet:

www.dlinkla.com
www.dlinklatinamerica.com
email: support@dlink.cl

Tech Support for customers within Brazil:

D-Link Technical Support over the Telephone:

0800-7014104
Monday to Friday 8:30am to 18:30pm

D-Link Technical Support over the Internet:

www.dlinkbrasil.com.br
email: suporte@dlinkbrasil.com.br

D-Link®
Building Networks for People

Техническая поддержка

Обновления программного обеспечения и документация доступны на Интернет-сайте D-Link.

D-Link предоставляет бесплатную поддержку для клиентов в течение гарантийного срока.

Клиенты могут обратиться в группу технической поддержки D-Link по телефону или через Интернет.

Техническая поддержка D-Link:
(095) 744-00-99

Техническая поддержка через Интернет
<http://www.dlink.ru>
email: support@dlink.ru

D-Link®
Building Networks for People

Asistencia Técnica

D-Link Latin América pone a disposición de sus clientes, especificaciones, documentación y software mas reciente a través de nuestro Sitio Web **www.dlinklatinamerica.com**

El servicio de soporte técnico tiene presencia en numerosos países de la Región Latino América, y presta asistencia gratuita a todos los clientes de D-Link, en forma telefónica e internet, a través de la casilla **soporte@dlinkla.com**

Soporte Técnico Help Desk Argentina:

Teléfono: 0800-6661442 Lunes a Viernes 09:00 am a 22:00 pm

Soporte Técnico Help Desk Chile:

Teléfono: 800-214422 Lunes a Viernes 08:00 am a 21:00 pm

Soporte Técnico Help Desk Colombia:

Teléfono: 01800-7001588 Lunes a Viernes 07:00 am a 20:00 pm

Soporte Técnico Help Desk Ecuador:

Teléfono: 1800-777 711 Lunes a Viernes 07:00 am a 20:00 pm

Soporte Técnico Help Desk El Salvador:

Teléfono: 800-6137 Lunes a Viernes 06:00 am a 19:00 pm

Soporte Técnico Help Desk Guatemala:

Teléfono: 1800-300 0017 Lunes a Viernes 06:00 am a 19:00 pm

Soporte Técnico Help Desk Panamá:

Teléfono: 0800-560 0193 Lunes a Viernes 07:00 am a 20:00 pm

Soporte Técnico Help Desk Perú:

Teléfono: 0800-52049 Lunes a Viernes 07:00 am a 20:00 pm

Soporte Técnico Help Desk Venezuela:

Teléfono: 0800-1003470 Lunes a Viernes 08:00 am a 21:00 pm



Suporte Técnico

Você pode encontrar atualizações de software e documentação de usuário no site da D-Link Brasil www.dlinkbrasil.com.br.

A D-Link fornece suporte técnico gratuito para clientes no Brasil durante o período de vigência da garantia deste produto.

Suporte Técnico para clientes no Brasil:

Telefone

São Paulo (11) 2185-9301

Segunda à sexta

Das 8h30 às 18h30

Demais Regiões do Brasil 0800 70 14 104

E-mail:

email: suporte@dlinkbrasil.com.br



友冠技術支援

台灣地區用戶可以透過我們的網站，電子郵件或電話與友冠資訊技術支援人員聯絡。

支援服務時間從
週一到週五，上午8:30 a.m. 到 7:00 p.m

Web: <http://www.dlinktw.com.tw/>
FAQ: <http://www.dlinktw.com.tw/support.asp>
Email: dssqa_service@dlinktw.com.tw

Phone: 0800-002-615

如果您是台灣地區以外的用戶，請參考使用手冊中記載的D-Link 全球各地分公司的聯絡資訊取得支援服務。

產品維修與保固相關資訊，請參考友冠資訊網頁說明：
<http://www.dlinktw.com.tw/suppQuick.asp>

D-Link®
Building Networks for People

技术支持

办公地址：北京市朝阳区建国路 71 号惠通时代广场 C1 座
202 室 邮编: 100025

技术支持中心电话：8008868192/(028)85176977

技术支持中心传真：(028)85176948

维修中心地址：北京市海淀区中关村南大街 9 号理工大厦
1107 室 邮编:100081

维修中心电话：(010)68477035/68477036/68477037

维修中心传真：(010)68477036

网址：<http://www.dlink.com.cn>

办公时间：周一到周五，早09:00到晚18:00

D-Link[®]
Building Networks for People

Warranty

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. (“D-Link”) provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

Limited Warranty: D-Link warrants that the hardware portion of the D-Link product described below (“Hardware”) will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below (“Warranty Period”), except as otherwise stated herein. Limited Lifetime Warranty for the product is defined as follows: Hardware: For as long as the original customer/end user owns the product, or five (5) years after product discontinuance, whichever occurs first (excluding power supplies and fans)

Power supplies and fans: Three (3) Year

Spare parts and spare kits: Ninety (90) days

The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware or part thereof that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product (“Software”) will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days (“Software Warranty Period”), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates. Non-Applicability of Warranty: The Limited Warranty provided hereunder for Hardware and Software portions of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the

product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim: The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at <https://rma.dlink.com/>.
- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.

The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer.

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming. **What Is Not Covered:** The Limited Warranty provided herein by D-Link does not cover: Products that, in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by any-one other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90)

DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT. Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOP-PAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

Governing Law: This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

Trademarks: D-Link is a registered trademark of D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective owners.

Copyright Statement: No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976 and any amendments thereto. Contents are subject to change without prior notice. Copyright 2006 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

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

FCC Statement: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. Operation of this equipment in a residential environment is likely to cause harmful interference to radio or television reception. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Reorient or relocate the receiving antenna. Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

Product Registration

D-Link products can be registered online at <http://support.dlink.com/register/>. Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

International Offices**U.S.A**

17595 Mt. Herrmann Street
Fountain Valley, CA. 92708
TEL: 714-885-6000
Fax 866-743-4905
URL: www.dlink.com

Canada

2180 Winston Park Drive
Oakville, Ontario, L6H 5W1
Canada

TEL: 1-905-8295033
FAX: 1-905-8295223
URL: www.dlink.ca

Europe (U. K.)

4th Floor, Merit House
Edgware Road, Colindale
London NW9 5AB

U.K.

TEL: 44-20-8731-5555
FAX: 44-20-8731-5511
URL: www.dlink.co.uk

Germany

Schwalbacher Strasse 74
D-65760 Eschborn
Germany

TEL: 49-6196-77990
FAX: 49-6196-7799300
URL: www.dlink.de

France

Le Florilege #.2, Allee de la Fresnerie
78330 Fontenay le Fleury
France

TEL: 33-1-30238688
FAX: 33-1-30238689
URL: www.dlink-france.fr

Netherlands

Weena 290
3012 NJ Rotterdam
Netherlands

Tel: +31-10-282-1445
Fax: +31-10-282-1331
URL: www.dlink-benelux.com

Belgium

Rue des Colonies 11
B-1000 Brussels
Belgium

Tel: +32(0)2 517 7111
Fax: +32(0)2 517 6500
URL: www.dlink-benelux.com

Italy

Via Nino Bonnet n. 6/b
20154 ñ Milano,
Italy

TEL: 39-02-2900-0676
FAX: 39-02-2900-1723
URL: www.dlink.it

Sweden

P.O. Box 15036, S-167 15 Bromma
Sweden

TEL: 46-(0)8564-61900
FAX: 46-(0)8564-61901
URL: www.dlink.se

Denmark

Naverland 2, DK-2600
Glostrup, Copenhagen,
TEL: 45-43-969040
FAX: 45-43-424347
URL: www.dlink.dk

Norway

Karihaugveien 89
1086 Oslo
Norway

TEL: 47-23-897189
FAX: 47-22-309085
URL: www.dlink.no

Finland

Pakkalankuja 7A
01510 Vantaa,
Finland

TEL : +358-9-2707 5080
FAX: + 358-9-2707 5081
URL: www.dlink.fi

Iberia

C/Sabino De Arana,
56 Bajos
08028 Barcelona

TEL: 34 93 4090770
FAX: 34 93 4910795
URL: www.dlinkiberia.es

Singapore

1 International Business Park
#03-12 The Synergy
Singapore 609917

TEL: 65-6774-6233
FAX: 65-6774-6322
URL: www.dlink-intl.com

Australia

1 Giffnock Avenue,
North Ryde, NSW 2113
Australia

TEL: 61-2-8899-1800
FAX: 61-2-8899-1868
URL: www.dlink.com.au

India

D-Link House, Kurla Bandra Complex
Road,
Off CST Road, Santacruz (East), Mumbai -
400098.

India

TEL: 91-022-26526696/56902210
FAX: 91-022-26528914
URL: www.dlink.co.in

Middle East (Dubai)

P.O.Box: 500376
Office No.:103, Building:3
Dubai Internet City
Dubai, United Arab Emirates
Tel:+971-4-3916480
Fax:+971-4-3908881
URL: www.dlink-me.com

Turkey

Regus Offices
Beybi Giz Plaza, Ayazaga Mah. Meydan
Sok.

No:28
Maslak 34396, Istanbul-Turkiye
TEL: +90 212 335 2553
FAX: +90 212 335 2500
URL: www.dlink.com.tr

Egypt

19 El-Shahed Helmy, El Masri
Al-Maza, Heliopolis
Cairo, Egypt.
TEL:+202 414 4295
FAX:+202 415 6704
URL: www.dlink-me.com

Israel

11 Hamanofim Street
Ackerstein Towers, Regus Business
Center

P.O.B 2148, Hertzelia-Pituach 46120.
Israel
TEL: +972-9-9715700
FAX: +972-9-9715601
URL: www.dlink.co.il

Latin America

Isidora Goyechea 2934 of 702,
Las Condes

Santiago ñ Chile S.A.
TEL: 56-2-232-3185
FAX: 56-2-232-0923
URL: www.dlink.cl

Brasil

Av das Nacoes Unidas,
11857 - 14 - andar - cj 141/142
Brooklin Novo

Sao Paulo - SP - Brazil
CEP 04578-000
TEL: +55 11 55039320
FAX: +55 11 55039322
URL: www.dlinkbrasil.com.br

South Africa

Einstein Park II
Block B
102-106 Witch-Hazel Avenue

Highveld Technopark
Centurion
Gauteng

Republic of South Africa
TEL: 27-12-665-2165
FAX: 27-12-665-2186
URL: www.d-link.co.za

Russia
Grafsky per., 14, floor 6

-Moscow
129626 Russia
TEL: 7-095-744-0099
FAX: 7-095-744-0099 #350
URL: www.dlink.ru

China

No.202,C1 Building, Huitong Office Park,
No.71, Jianguo Road, Chaoyang District,
Beijing,
100025, China.

TEL +86-10-58635800
FAX: +86-10-58635799
URL: www.dlink.com.cn

Taiwan

2F, No. 119, Pao-Chung Rd.
Hsin-Tien, Taipei
Taiwan

TEL: 886-2-2910-2626
FAX: 886-2-2910-1515
URL: www.dlinktw.com.tw

Headquarters

2F, No. 233-2, Pao-Chiao Rd.
Hsin-Tien, Taipei
Taiwan

TEL: 886-2-2916-1600
FAX: 886-2-2914-6299
URL: www.dlink.com