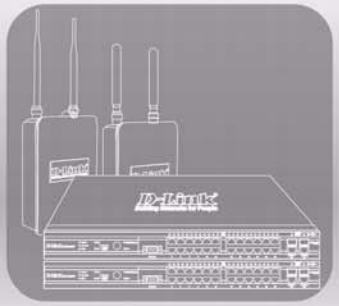
D-Link
Building Networks for People



Wired Configuration Guide

Product Model : **DWS-3000 Series**

Unified Wired & Wireless Access System

Release 2.1

April 2008

Table of Contents

List of Figures

List of Tables

About This Book

This document provides an understanding of the CLI and Web configuration options for D-Link DWS-3000 features.

Document Organization

This document shows examples of the use of the Unified Switch in a typical network. It describes the use and advantages of specific functions provided by the Unified Switch and includes information about configuring those functions using the command-line interface (CLI) and Web interface.

The Unified Switch can operate as a Layer 2 switch, a Layer 3 router, or a combination switch/router. The switch also includes support for network management and Quality of Service functions such as Access Control Lists and Differentiated Services. The functions you choose to activate will depend on the size and complexity of your network.

This document illustrates configuration for the following functions:

- L2 Features
  - Virtual LANs (VLANs)
  - 802.1x Network Access Control
  - Storm Control
  - Trunking (Link Aggregation/Port Channels)
  - Internet Group Management Protocol (IGMP) Snooping
  - Port Mirroring
  - Port Security
  - Link Layer Discovery Protocol (LLDP)
  - Denial of Service Attack Protection
- L3 Features
  - Port Routing
  - VLAN Routing
  - Virtual Router Redundancy Protocol (VRRP)
  - Proxy ARP
- Quality of Service (QoS)
  - Access Control Lists (ACLs)
  - Class of Service (CoS)
  - Differentiated Services

- Management
  - RADIUS
  - TACACS+
  - DHCP Filtering
  - Traceroute
  - Configuration Scripting
  - Outbound Telnet
  - Pre-Login Banner
  - Simple Network Time Protocol (SNTP)
  - Syslog
  - Port Description

CLI/Web Examples - Slot/Port Designations

To help you understand configuration tasks, this document contains examples from the CLI and Web Interfaces. The examples are based on the D-Link DWS-3000 switch and use the slot/port naming convention for interfaces, *e.g.* 0/2

Audience

Use this guide if you are a(n):

- Experienced system administrator who is responsible for configuring and operating a network using the D-Link DWS-3000 switch
- Level 1 and/or Level 2 Support provider

To obtain the greatest benefit from this guide, you should have an understanding of the Unified Switch. You should also have basic knowledge of Ethernet and networking concepts.

CLI Documentation

The *DWS-3000 CLI Command Reference* gives information about the CLI commands used to configure the switch. The document provides CLI descriptions, syntax, and default values.

Refer to the *DWS-3000 CLI Command Reference* for information on:

- D-Link DWS-3000 switch command overview
- Command structure

1

Getting Started

Connect a terminal to the switch to begin configuration.

In-Band and Out-of-Band Connectivity

Ask the system administrator to determine whether you will configure the switch for in-band or out-of-band connectivity. To use the Web Interface, you must set up your system for in-band connectivity.

Configuring for In-Band Connectivity

In-band connectivity allows you to access the switch from a remote workstation using the Ethernet network. To use in-band connectivity, you must configure the switch with IP information (IP address, subnet mask, and default gateway).

Configure for In-band connectivity using one of the following methods:

- BootP or DHCP
- EIA-232 port

Using BootP or DHCP

You can assign IP information initially over the network or over the Ethernet service port through BootP or DHCP. Check with your system administrator to determine whether BootP or DHCP is enabled.

You need to configure the BootP or DHCP server with information about the switch —obtain this information through the serial port connection using the **`show network`** command. Set up the server with the following values:

IP Address

Unique IP address for the switch. Each IP parameter is made up of four decimal numbers, ranging from 0 to 255. The default for all IP parameters is 10.90.90.90.

Subnet

Subnet mask for the LAN

Gateway

IP address of the default router, if the switch is a node outside the IP range of the LAN

MAC Address

MAC address of the switch

When you connect the switch to the network for the first time after setting up the BootP or DHCP server, it is configured with the information supplied above. The switch is ready for in-band connectivity over the network.

If you do not use BootP or DHCP, access the switch through the EIA-232 port, and configure the network information as described below.

Using the EIA-232 Port

You can use a locally or remotely attached terminal to configure in-band management through the EIA-232 port.

1. To use a locally attached terminal, attach one end of a null-modem serial cable to the EIA-232 port of the switch and the other end to the COM port of the terminal or workstation.
   For remote attachment, attach one end of the serial cable to the EIA-232 port of the switch and the other end to the modem.
2. Set up the terminal for VT100 terminal emulation.
   A. Set the terminal ON.
   B. Launch the VT100 application.
   C. Configure the COM port as follows:
      I. Set the data rate to 115,200 baud.
      II. Set the data format to 8 data bits, 1 stop bit, and no parity.
      III. Set the flow control to none.
      IV. Select the proper mode under **Properties**.
      V. Select Terminal keys.
3. The Log-in User prompt displays when the terminal interface initializes.

   Enter an approved user name and password. The default is **`admin`** for the user name and the password is blank.

   The switch is installed and loaded with the default configuration.
4. Reduce network traffic by turning off the Network Configuration Protocol. Enter the following command:
   `configure network protocol none`
5. Set the IP address, subnet mask, and gateway address by issue the following command:
   `config network parms <ipaddress> <netmask> [<gateway>]`

IP Address

Unique IP address for the switch. Each IP parameter is made up of four decimal numbers, ranging from 0 to 255. The default for all IP parameters is 10.90.90.90.

Subnet

Subnet mask for the LAN.

Gateway

IP address of the default router, if the switch is a node outside the IP range of the LAN.

6. To enable these changes to be retained during a reset of the switch, type **CTRL+Z** to return to the main prompt, type `save config` at the main menu prompt, and type `y` to confirm the changes.
7. To view the changes and verify in-band information, issue the command: `show network`.
8. The switch is configured for in-band connectivity and ready for Web-based management.

Configuring for Out-of-Band Connectivity

To monitor and configure the switch using out-of-band connectivity, use the console port to connect the switch to a terminal desktop system running terminal emulation software. The console port connector is a female DB-9 connector, implemented as a data terminal equipment (DTE) connector.

The following hardware is required to use the console port:

- VT100-compatible terminal, or a desktop, or a portable system with a serial port running VT100 terminal emulation software.
- An RS-232 cable with a male DB-9 connector for the console port and the appropriate connector for the terminal.

Perform the following tasks to connect a terminal to the switch console port using out-of-band connectivity:

1. Connect the RS-232 cable to the terminal running VT100 terminal emulation software.
2. Configure the terminal emulation software as follows:
   A. Select the appropriate serial port (serial port 1 or serial port 2) to connect to the console.
   B. Set the data rate to 115,200 baud.
   C. Set the data format to 8 data bits, 1 stop bit, and no parity.
   D. Set the flow control to none.
   E. Select the proper mode under **Properties**.
   F. Select Terminal keys.

NOTE: When using HyperTerminal with Microsoft Windows 2000, make sure 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 more information on Windows 2000 service packs.

3. Connect the RS-232 cable directly to the switch console port, and tighten the captive retaining screws.

Starting the Switch

1. Make sure that the switch console port is connected to a VT100 terminal or a VT100 terminal emulator via the RS-232 crossover cable.
2. Locate an AC power receptacle.
3. Deactivate the AC power receptacle.
4. Connect the switch to the AC receptacle.
5. Activate the AC power receptacle.

When the power is turned on with the local terminal already connected, the switch goes through a power-on self-test (POST). POST runs every time the switch is initialized and checks hardware components to determine if the switch is fully operational before completely booting. If POST detects a critical problem, the startup procedure 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. The boot process runs for approximately 60 seconds.

Initial Configuration

NOTE: The initial simple configuration procedure is based on the following assumptions:

- The switch was not configured before and is in the same state as when you received it.
- The switch booted successfully.
- The console connection was established and the console prompt appears on the screen of a VT100 terminal or terminal equivalent.

The initial switch configuration is performed through the console port. After the initial configuration, you can manage the switch either from the already-connected console port or remotely through an interface defined during the initial configuration.

NOTE: The switch is not configured with a default user name and password.

NOTE: All of the settings below are necessary to allow the remote management of the switch through Telnet (Telnet client) or HTTP (Web browser).

Before setting up the initial configuration of the switch, obtain the following information from your network administrator:

- The IP address to be assigned to the management interface through which the switch is managed.
- The IP subnet mask for the network.
- The IP address of the default gateway.

Unified Switch Installation

This section contains procedures to help you become acquainted quickly with the switch software.

Before installing the Unified Switch, you should verify that the switch operates with the most recent firmware.

Quick Starting the Networking Device

1. Configure the switch for In-band or Out-of-Band connectivity. In-band connectivity allows access to the Unified Switch locally or from a remote workstation. You must configure the device with IP information (IP address, subnet mask, and default gateway).
2. Turn the Power ON.
3. Allow the device to load the software until the login prompt appears. The device initial state is called the default mode.
4. When the prompt asks for operator login, do the following steps:
   - Type **`admin`** at the login prompt. Since a number of the Quick Setup commands require administrator account rights, D-Link suggests logging into an administrator account.
     Do not enter a password because the default mode does not use a password - after typing **`admin,`** press Enter two times.
   - The CLI User EXEC prompt is displayed.
   - Type **`enable`** to switch to the Privileged EXEC mode from User EXEC.
   - Type **`configure`** to switch to the Global Config mode from Privileged EXEC.
   - Type **`exit`** to return to the previous mode.
   - Enter **`?`** to show a list of commands that are available in the current mode.

NOTE: For more information about the configuration modes, see the *CLI Command Reference*.

System Information and System Setup

This section describes the commands you use to view system information and to setup the network device. The tables below contain the Quick Start commands that allow you to view or configure the following information:

- Software versions
- Physical port data
- User account management
- IP address configuration
- Uploading from Networking Device to Out-of-Band PC (Only XMODEM)
- Downloading from Out-of-Band PC to Networking Device (Only XMODEM)
- Downloading from TFTP Server
- Restoring factory defaults

For each of these tasks, a table shows the command syntax, the mode you must be in to execute the command, and the purpose and output of the command. If you configure any network parameters, you should execute the **`write`** command.

This command saves the changes to the configuration file. You must be in the correct mode to execute the command. If you do not save the configuration, all changes are lost when you power down or reset the networking device.

Quick Start up Software Version Information

Table 1. Quick Start up Software Version Information

Command	Details
show hardware (Privileged EXEC Mode)	**Switch: 1** **System Description..... D-Link DWS-3026** **Machine Model..... DWS-3026** **Serial Number..... 123456abcdef** **FRU Number.....** **Maintenance Level..... A** **Manufacturer..... 0xbc00** **Burned In MAC Address..... 00:01:17:86:34:55** **Software Version..... D.4.18.8** **Additional Packages..... QOS** **Wireless**

Quick Start up Physical Port Data

Table 2. Quick Start up Physical Port Data

Command	Details
show port all (Privileged EXEC Mode)	Displays the ports Interface - slot/port, See the *CLI Command Reference* for more information about naming conventions. Type - Indicates if the port is a special type of port. Admin Mode - Selects the Port Control Administration State. Physical Mode - Selects the desired port speed and duplex mode. Physical Status - Indicates the port speed and duplex mode. Link Status - Indicates whether the link is up or down. Link Trap - Determines whether or not to send a trap when link status changes. LACP Mode - Displays whether LACP is enabled or disabled on this port.

Quick Start up User Account Management

Table 3. Quick Start up User Account Management

Command	Details
show users (Privileged EXEC Mode)	Displays all of the users who are allowed to access the networking device Access Mode - Shows whether the user is able to change parameters on the networking device(Read/Write) or is only able to view them (Read Only). As a factory default, the *admin* user has Read/Write access and the *guest* user has Read Only access. There can only be one Read/Write user and up to five Read Only users.
show loginsession (User EXEC Mode)	Displays all of the login session information.
users passwd *<username>* (Global Config Mode)	Allows the user to set passwords or change passwords needed to login A prompt appears after the command is entered requesting the user's old password. In the absence of an old password, leave the area blank. The user must press **Enter** to execute the command. The system then prompts the user for a new password; then a prompt to confirm the new password. If the new password and the confirmed password match, a confirmation message is displayed. A user password should not be more than eight characters in length.
write (Privileged EXEC Mode)	This command saves passwords and all other changes to the device. If you do not save the configuration by entering this command, all configurations are lost when a power cycle is performed on the networking device or when the networking device is reset.
logout (User EXEC and Privileged EXEC Modes)	Logs the user out of the networking device.

Quick Start up IP Address

To view the network parameters the operator can access the device by the following three methods.

- Simple Network Management Protocol - SNMP
- Telnet
- Web Browser

NOTE: Helpful Hint: The user should do a 'copy system:running-config nvram:startup-config' after configuring the network parameters so that the configurations are not lost

Table 4. Quick Start up IP Address

Command	Details
show network (User EXEC Mode)	Displays the Network Configurations
	IP Address - IP Address of the interface
	Default IP is 10.90.90.90
	Subnet Mask - IP Subnet Mask for the interface
	Default is 255.0.0.0
	Default Gateway - The default Gateway for this interface
	Default value is 0.0.0.0
	Burned in MAC Address - The Burned in MAC Address used for in-band connectivity
	Locally Administered MAC Address - Can be configured to allow a locally administered MAC address
	MAC Address Type - Specifies which MAC address should be used for in-band connectivity
	Network Configurations Protocol Current - Indicates which network protocol is being used
	Default is none
	Management VLAN ID - Specifies VLAN ID
network parms *<ipaddr> <netmask> [gateway]* **(Privileged EXEC Mode)**	Sets the IP Address, subnet mask, and gateway of the router. The IP Address and the gateway must be on the same subnet.
	IP Address range from 0.0.0.0 to 255.255.255.255
	Subnet Mask range from 0.0.0.0 to 255.255.255.255
	Gateway Address range from 0.0.0.0 to 255.255.255.255

Quick Start up Uploading from Networking Device to Out-of-Band PC (XMODEM)

Table 5. Uploading from Networking Device to Out-of-Band PC (XMODEM)

Command	Details
copy nvram:startup-config *<url>* (Privileged EXEC Mode) **copy nvram:errorlog** *<url>* (Privileged EXEC Mode) **copy nvram:log** *<url>* (Privileged EXEC Mode) **copy nvram:traplog** *<url>* (Privileged EXEC Mode)	Starts the upload, displays the mode and type of upload, and confirms the upload is progressing. The types are: • config - configuration file • errorlog - error log • log- message log • traplog - trap log The *<url>* must be specified as: **xmodem:<filepath>/<filename>** If you are using HyperTerminal, you must specify where the file is to be received by the PC.

Quick Start up Downloading from Out-of-Band PC to Networking Device (XMODEM)

Table 6. Downloading from Out-of-Band PC to Networking Device (XMODEM)

Command	Details
copy *<url>* **nvram:startup-config** (Privileged EXEC Mode) **copy** *<url>* **system:image** (Privileged EXEC Mode)	Sets the destination (download) datatype to be an image (system:image) or a configuration file (nvram:startup-config). The *<url>* must be specified as: **xmodem:<filepath>/<filename>** If you are using Hyper Terminal, you must specify which file is to be sent to the networking device.

Quick Start up Downloading from TFTP Server

Before starting a TFTP server download, the operator must complete the Quick Start up for the IP Address.

Table 7. Downloading from TFTP Server

Command	Details
copy *<tftp://<ipaddress>/<filepath>/<filename>>* **nvram:startup-config** (Privileged EXEC Mode) **copy** *<tftp://<ipaddress>/<filepath>/<filename>>* **system:image** (Privileged EXEC Mode)	Sets the destination (download) datatype to be an image (system:image) or a configuration file (nvram:startup-config). The URL must be specified as: tftp://<ipaddress>/<filepath>/<filename>. The nvram:startup-config option downloads the configuration file using tftp and system:image option downloads the code file.

Quick Start up Factory Defaults

Table 8. Setting to Factory Defaults

Command	Details
clear config (Privileged EXEC Mode)	Enter **yes** when the prompt pops up to clear all the configurations made to the networking device.
write	Enter **yes** when the prompt pops up that asks if you want to save the configurations made to the networking device.
reload (or cold boot the networking device) (Privileged EXEC Mode)	Enter **yes** when the prompt pops up that asks if you want to reset the system. You can reset the networking device or cold start the networking device.

2

Using the Web Interface

This chapter is a brief introduction to the Web interface — it explains how to access the Web-based management panels to configure and manage the system.

Tip: Use the Web interface for configuration instead of the CLI interface. Web configuration is quicker and easier than entering multiple required CLI commands.

You can manage your switch through a Web browser and Internet connection. This is referred to as Web-based management. To use Web-based management, the system must be set up for in-band connectivity.

To access the switch, the Web browser must support:

- HTML version 4.0, or later
- HTTP version 1.1, or later
- JavaScript™ version 1.2, or later
- Java™ Runtime Plug-in 1.50-06 or later

There are equivalent functions in the Web interface and the terminal interface — both applications usually employ the same menus to accomplish a task. For example, when you log in, there is a Main Menu with the same functions available, etc.

There are several differences between the Web and terminal interfaces. For example, on the Web interface the entire forwarding database can be displayed, while the terminal interface only displays 10 entries starting at specified addresses.

To terminate the Web interface session, click the **Logout** button.

Configuring for Web Access

To enable Web access to the switch:

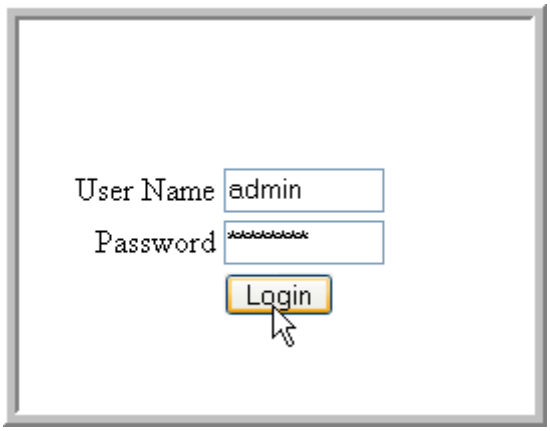
1. Configure the switch for in-band connectivity. The *Getting Started* section of this document gives instructions for doing this.
2. Enable Web mode:
   A. At the CLI prompt, enter the **`show network`** command.
   B. Set **Web Mode** to Enabled.

Starting the Web Interface

Follow these steps to start the switch Web interface:

1. Enter the IP address of the switch in the Web browser address field.
2. Enter the appropriate User Name and Password. The User Name and associated Password are the same as those used for the terminal interface. Click on the Login button.

Figure 1. Web Interface Panel-Example



3. The System Description Menu displays as shown in Figure 2, with the navigation tree appearing to the left of the screen.
4. Make a selection by clicking on the appropriate item in the navigation tree.

Web Page Layout

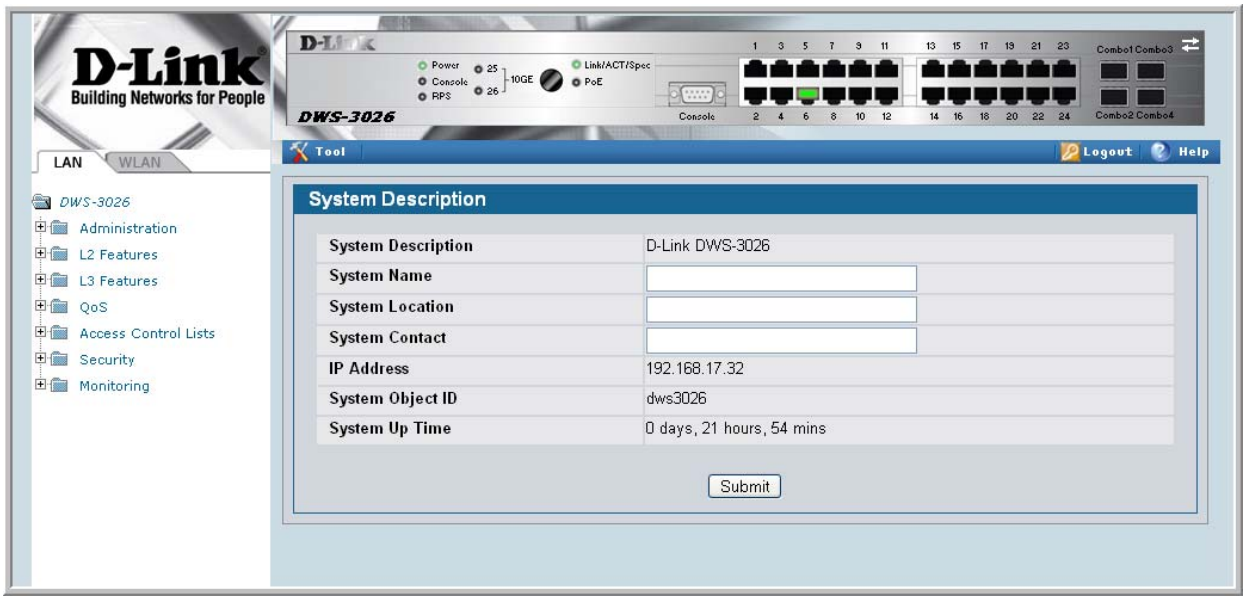
A Web interface panel for the switch Web page consists of three areas (Figure 2).

A banner graphic of the switch appears across the top of the panel.

The second area, a hierarchical-tree view appears to the left of the panel. The tree consists of a combination of folders, subfolders, and configuration and status HTML pages. You can think of the folders and subfolders as branches and the configuration and status HTML pages as leaves. Only the selection of a leaf (not a folder or subfolder) will cause the display of a new HTML page. A folder or subfolder has no corresponding HTML page.

The third area, at the bottom-right of the panel, displays the currently selected device configuration status and/or the user configurable information that you have selected from the tree view.

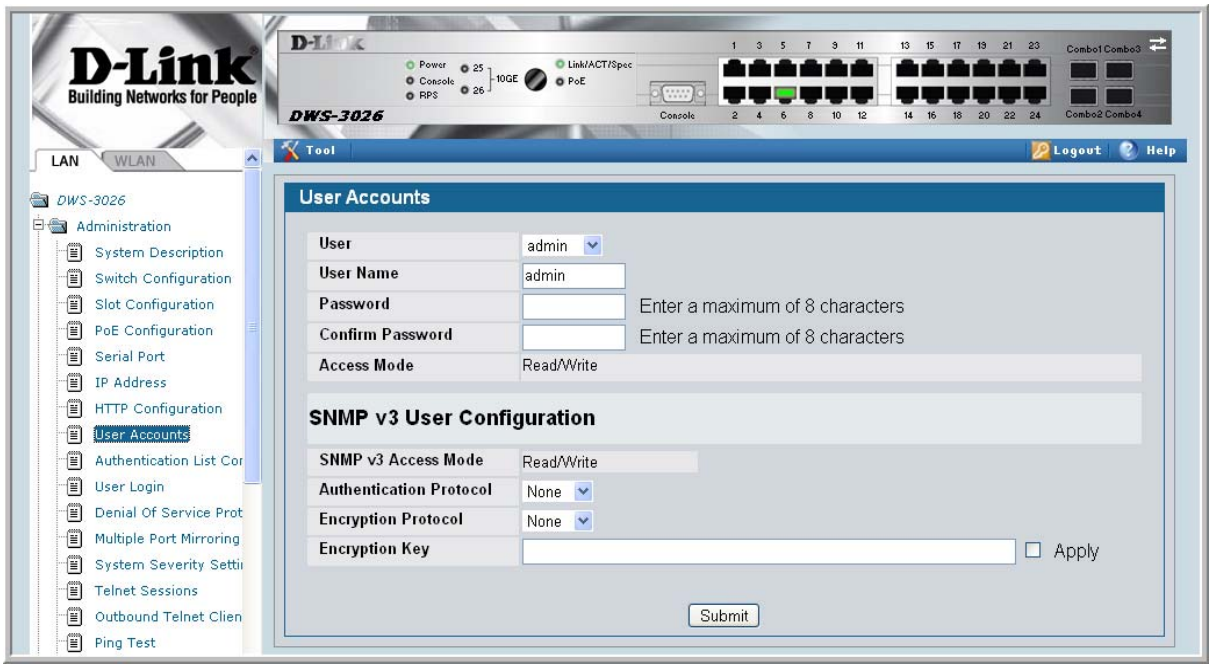
Figure 2. Web Interface Panel-Example



Configuring an SNMP V3 User Profile

Configuring an SNMP V3 user profile is a part of user configuration. Any user can connect to the switch using the SNMPv3 protocol, but for authentication and encryption, additional steps are needed. Use the following steps to configure an SNMP V3 new user profile.

Figure 3. Configuring an SNMP V3 User Profile



1. From the LAN navigation menu, select **LAN> Administration>User Accounts** (see Figure 3).

2. Using the **User** pull-down menu, select **Create** to create a new user.
3. Enter a new user name in the User Name field.
4. Enter a new user password in the Password field and then retype it in the Confirm Password field.

NOTE: If SNMPv3 Authentication is to be implemented for this user, set a password of eight or more alphanumeric characters.

5. If you do not need authentication, go to Step 9.
6. To enable authentication, use the **Authentication Protocol** pull-down menu to select either MD5 or SHA for the authentication protocol.
7. If you do not need encryption, go to Step 9.
8. To enable encryption, use the **Encryption Protocol** pull-down menu to select **DES** for the encryption scheme. Then, enter an encryption code of eight or more alphanumeric characters in the Encryption Key field.
9. Click **Submit**.

Command Buttons

The following command buttons are used throughout the Web interface panels for the switch:

Save	Pressing the **Save** button implements and saves the changes you just made. Some settings may require you to reset the system in order for them to take effect.
Refresh	Pressing the **Refresh** button that appears next to the Apply button in Web interface panels refreshes the data on the panel.
Submit	Pressing the **Submit** button sends the updated configuration to the switch. Configuration changes take effect immediately, but these changes are not retained across a power cycle unless a save is performed.

3

Virtual LANs

Adding Virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast. Like a router, it partitions the network into logical segments, which provides better administration, security and management of multicast traffic.

A VLAN is a set of end stations and the switch ports that connect them. You can have many reasons for the logical division, for example, department or project membership. The only physical requirement is that the end station, and the port to which it is connected, both belong to the same VLAN.

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station may omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet may either reject it or insert a tag using its default VLAN ID. A given port may handle traffic for more than one VLAN, but it can only support one default VLAN ID.

Two features let you define packet filters that the switch uses as the matching criteria to determine if a particular packet belongs to a particular VLAN.

- The IP-subnet Based VLAN feature lets you map IP addresses to VLANs by specifying a source IP address, network mask, and the desired VLAN ID.
- The MAC-based VLAN feature let packets originating from end stations become part of a VLAN according to source MAC address. To configure the feature, you specify a source MAC address and a VLAN ID.

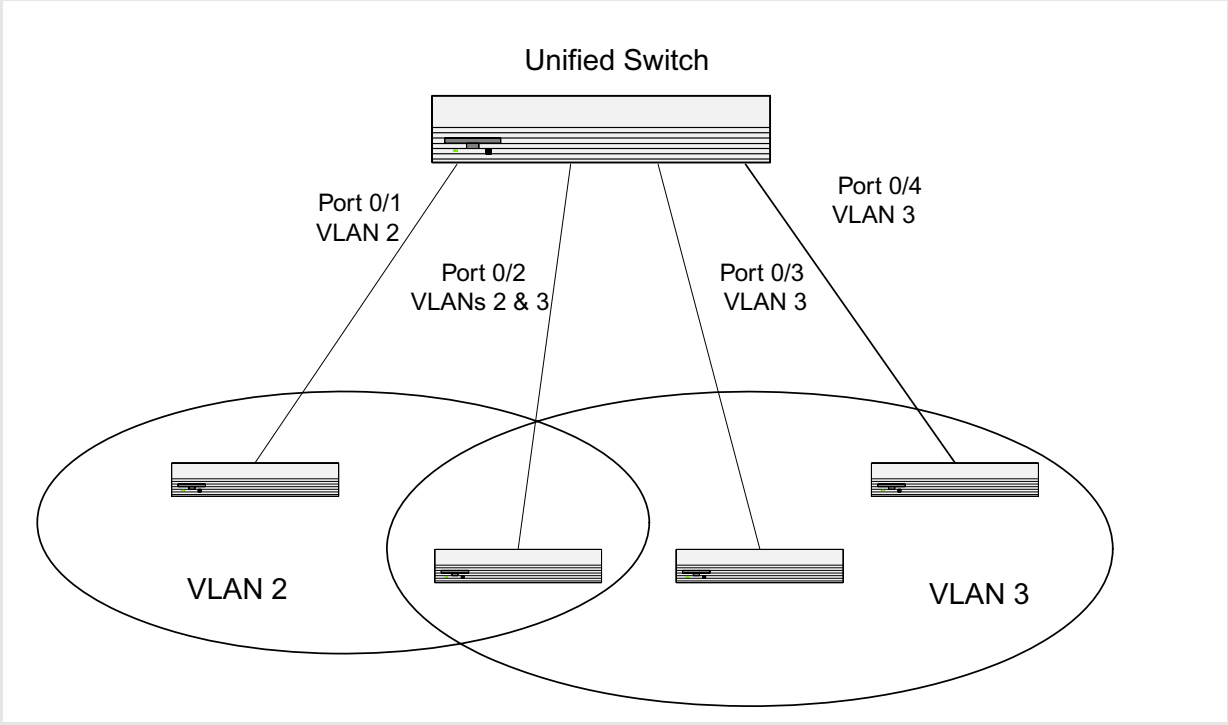
The Private Edge VLAN feature lets you set protection between ports located on the switch. This means that a protected port cannot forward traffic to another protected port on the same switch.

The feature does not provide protection between ports located on different switches.

VLAN Configuration Example

The diagram in this section shows a switch with four ports configured to handle the traffic for two VLANs. Port 0/2 handles traffic for both VLANs, while port 0/1 is a member of VLAN 2 only, and ports 0/3 and 0/4 are members of VLAN 3 only. The script following the diagram shows the commands you would use to configure the switch as shown in the diagram.

Figure 4. VLAN Example Network Diagram



Configuring a Guest VLAN

You can configure a Guest VLAN for clients to limit network access. If a client station fails to authenticate using 802.1X or RADIUS, or if the client does not support 802.1X, then after the authentication times out, the station is put on the guest VLAN configured for that switch port.

For more information about how to configure a Guest VLAN for wired clients, see “Guest VLAN” on page 39.

Configuring Dynamic VLAN Assignments

The software supports VLAN assignment for clients based on the RADIUS server authentication. You need an external RADIUS server to use the dynamic VLAN assignment feature. For information about how to configure the switch to allow dynamic VLAN assignments, see “Configuring Dynamic VLAN Assignment” on page 41.

CLI Examples

The following examples show how to create VLANs, assign ports to the VLANs, and assign a VLAN as the default VLAN to a port.

Example #1: Create Two VLANs

Use the following commands to create two VLANs and to assign the VLAN IDs while leaving the names blank.

```
(DWS-3024) #vlan database
(DWS-3024) (Vlan)#vlan 2
(DWS-3024) (Vlan)#vlan 3
(DWS-3024) (Vlan)#exit
```

Example #2: Assign Ports to VLAN2

This sequence shows how to assign ports to VLAN2, specify that frames will always be transmitted tagged from all member ports, and that untagged frames will be rejected on receipt.

```
(DWS-3024) #config
(DWS-3024) (Config)#interface 0/1
(DWS-3024) (Interface 0/1)#vlan participation include 2
(DWS-3024) (Interface 0/1)#vlan acceptframe vlanonly
(DWS-3024) (Interface 0/1)#exit
(DWS-3024) (Config)#interface 0/2
(DWS-3024) (Interface 0/2)#vlan participation include 2
(DWS-3024) (Interface 0/2)#vlan acceptframe vlanonly
(DWS-3024) (Interface 0/2)#exit
(DWS-3024) (Config)#exit

(DWS-3024) #config
(DWS-3024) (Config)#vlan port tagging all 2
(DWS-3024) (Config)#exit
```

Example #3: Assign Ports to VLAN3

This example shows how to assign the ports that will belong to VLAN 3, and to specify that untagged frames will be accepted on port 0/4.

Note that port 0/2 belongs to both VLANs and that port 0/1 can never belong to VLAN 3.

```
(DWS-3024) #config
(DWS-3024) (Config)#interface 0/2
(DWS-3024) (Interface 0/2)#vlan participation include 3
(DWS-3024) (Interface 0/2)#exit
(DWS-3024) (Config)#interface 0/3
(DWS-3024) (Interface 0/3)#vlan participation include 3
(DWS-3024) (Interface 0/3)#exit
(DWS-3024) (Config)#interface 0/4
(DWS-3024) (Interface 0/4)#vlan participation include 3
(DWS-3024) (Interface 0/4)#exit
(DWS-3024) (Config)#
(DWS-3024) (Config)#exit
(DWS-3024) #config
(DWS-3024) (Config)#interface 0/4
(DWS-3024) (Interface 0/4)#vlan acceptframe all
```

```
(DWS-3024) (Interface 0/4)#exit
(DWS-3024) (Config)#exit
```

Example #4: Assign VLAN3 as the Default VLAN

This example shows how to assign VLAN 3 as the default VLAN for port 0/2.

```
(DWS-3024) #config
(DWS-3024) (Config)#interface 0/2
(DWS-3024) (Interface 0/2)#vlan pvid 3
(DWS-3024) (Interface 0/2)#exit
(DWS-3024) (Config)#exit
```

Example #5: Assign IP Addresses to VLAN 2

```
(DWS-3024) #vlan database

(DWS-3024) (Vlan)#vlan association subnet 192.168.10.10 255.255.255.0 2
(DWS-3024) (Vlan)#exit
(DWS-3024) #show vlan association subnet

IP Address          IP Mask             VLAN ID
-----------------   -----------------   -------

192.168.10.10       255.255.255.0       2

(DWS-3024) #
```

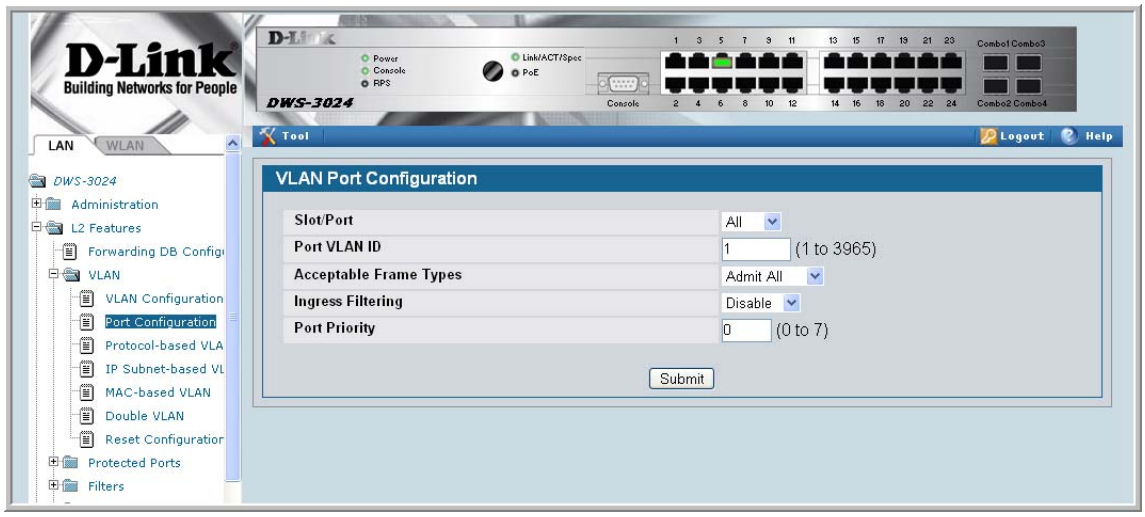
Web Interface

You can perform the same configuration in the CLI Examples section by using the Web interface. To create VLANs and specify port participation, use the **LAN> L2 Features > VLAN> VLAN Configuration** page.

Figure 5. VLAN Configuration

To specify the handling of untagged frames on receipt use the **LAN> L2 Features > VLAN > Port Configuration** page.

Figure 6. VLAN Port Configuration



Private Edge VLANs

Use the Private Edge VLAN feature to prevent ports on the switch from forwarding traffic to each other even if they are on the same VLAN.

- Protected ports cannot forward traffic to other protected ports in the same group, even if they have the same VLAN membership. Protected ports can forward traffic to unprotected ports.
- Unprotected ports can forward traffic to both protected and unprotected ports.

You can also configure groups of protected ports. Each group's configuration consists of a name and a mask of ports. A port can belong to only one set of protected ports. An unprotected port can be added to a group as a protected port.

The group name is configurable by the network administrator.

Use the **switchport protected** command to designate a port as protected. Use the **show switchport protected** command to display a listing of the protected ports.

CLI Example

Example #1: switchport protected

```
(DWS-3024) #config
(DWS-3024) (Config)#interface 0/1
(DWS-3024) (Interface 0/1)#switchport protected ?
<cr> Press Enter to execute the command.
(DWS-3024) (Interface 0/1)#switchport protected
```

Example #2: show switchport protected

```
(DWS-3024) #show switchport protected
0/1
```


4

802.1X Network Access Control

Port-based network access control allows the operation of a system's port(s) to be controlled to ensure that access to its services is permitted only by systems that are authorized to do so.

Port Access Control provides a means of preventing unauthorized access by supplicants or users to the services offered by a System. Control over the access to a switch and the LAN to which it is connected can be desirable in order to restrict access to publicly accessible bridge ports or departmental LANs.

The Unified Switch achieves access control by enforcing authentication of supplicants that are attached to an authenticator's controlled ports. The result of the authentication process determines whether the supplicant is authorized to access services on that controlled port.

A PAE (Port Access Entity) can adopt one of two roles within an access control interaction:

- Authenticator – Port that enforces authentication before allowing access to services available via that Port.
- Supplicant – Port that attempts to access services offered by the Authenticator.

Additionally, there exists a third role:

- Authentication server – Server that performs the authentication function necessary to check the credentials of the supplicant on behalf of the Authenticator.

Completion of an authentication exchange requires all three roles. The Unified Switch supports the authenticator role only, in which the PAE is responsible for communicating with the supplicant. The authenticator PAE is also responsible for submitting information received from the supplicant to the authentication server in order for the credentials to be checked, which determines the authorization state of the port. Depending on the outcome of the authentication process, the authenticator PAE then controls the authorized/unauthorized state of the controlled Port.

Authentication can be handled locally or via an external authentication server. Two are: Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+). The Unified Switch currently supports RADIUS for 802.1X.

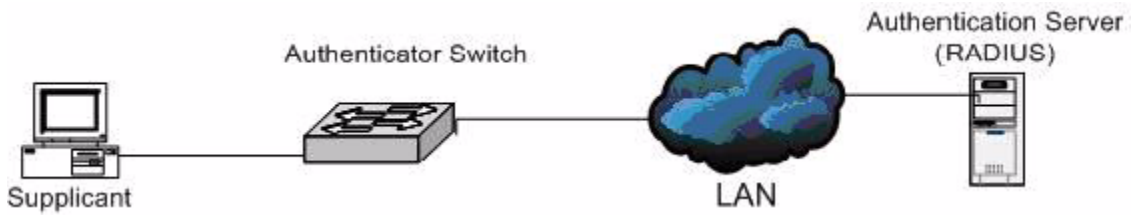
RADIUS supports an accounting function to maintain data on service usages. Under RFC 2866, an extension was added to the RADIUS protocol giving the client the ability to deliver accounting information about a user to an accounting server. Exchanges to the accounting server follow similar guidelines as that of an authentication server but the flows are much

simpler. At the start of service for a user, the RADIUS client that is configured to use accounting sends an accounting start packet specifying the type of service that it will deliver. Once the server responds with an acknowledgement, the client periodically transmits accounting data. At the end of service delivery, the client sends an accounting stop packet allowing the server to update specified statistics. The server again responds with an acknowledgement.

802.1x Network Access Control Example

This example configures a single RADIUS server used for authentication and accounting at 10.10.10.10. The shared secret is configured to be *secret*. The process creates a new authentication list, called radiusList, which uses RADIUS as the authentication method. This authentication list is associated with the 802.1x default login. 802.1x port based access control is enabled for the system, and interface 0/1 is configured to be in force-authorized mode because this is where the RADIUS server and protected network resources are located.

Figure 7. DWS-3000 with 802.1x Network Access Control



If a user, or supplicant, attempts to communicate via the switch on any interface except interface 0/1, the system challenges the supplicant for login credentials. The system encrypts the provided information and transmits it to the RADIUS server. If the RADIUS server grants access, the system sets the 802.1x port state of the interface to authorized and the supplicant is able to access network resources.

```
config
        radius server host auth 10.10.10.10
        radius server key auth 10.10.10.10
                secret
                secret
        radius server host acct 10.10.10.10
        radius server key acct 10.10.10.10
                secret
                secret
        radius accounting mode
        authentication login radiusList radius
        dot1x defaultlogin radiusList
        dot1x system-auth-control
        interface 0/1
                dot1x port-control force-authorized
        exit
exit
```


Guest VLAN

The Guest VLAN feature allows a switch to provide a distinguished service to unauthenticated users. This feature provides a mechanism to allow visitors and contractors to have network access to reach external network with no ability to surf internal LAN.

When a client that does not support 802.1X is connected to an unauthorized port that is 802.1X-enabled, the client does not respond to the 802.1X requests from the switch. Therefore, the port remains in the unauthorized state, and the client is not granted access to the network. If a guest VLAN is configured for that port, then the port is placed in the configured guest VLAN and the port is moved to the authorized state, allowing access to the client.

Client devices that are 802.1X-supplicant-enabled authenticate with the switch when they are plugged into the 802.1X-enabled switch port. The switch verifies the credentials of the client by communicating with an authentication server. If the credentials are verified, the authentication server informs the switch to 'unblock' the switch port and allows the client unrestricted access to the network; i.e., the client is a member of an internal VLAN.

Guest VLAN Supplicant mode is a global configuration for all the ports on the switch. When a port is configured for Guest VLAN in this mode, if a client fails authentication on the port, the client is assigned to the guest VLAN configured on that port. The port is assigned a Guest VLAN ID and is moved to the authorized status. Disabling the supplicant mode does not clear the ports that are already authorized and assigned Guest VLAN IDs.

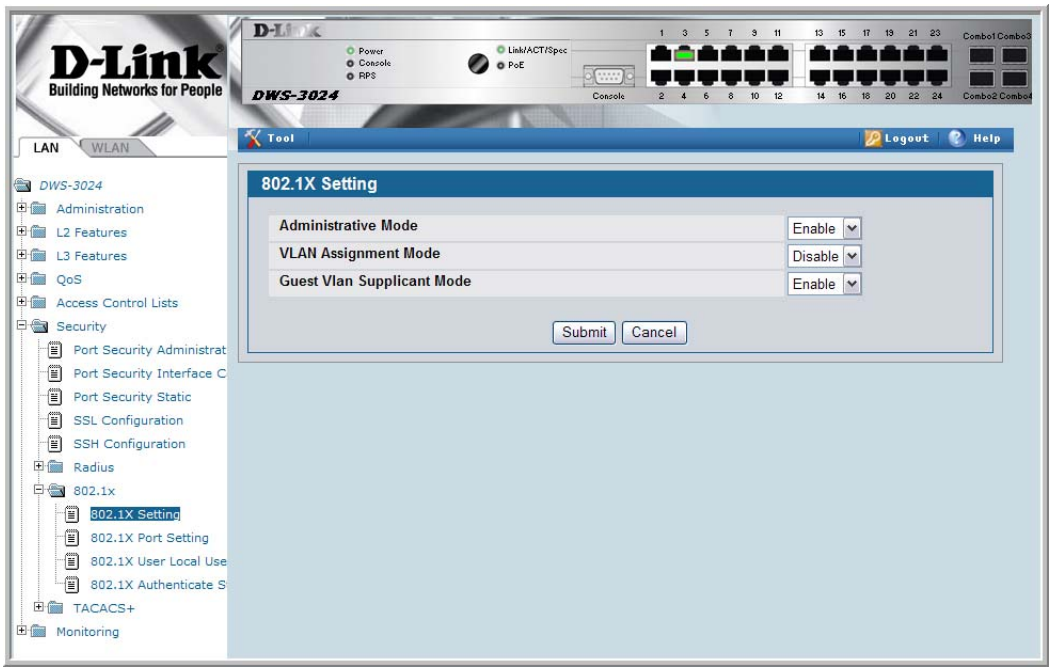
Configuring the Guest VLAN by Using the CLI

To enable the Guest VLAN Supplicant Mode, use the **`dot1x guest-vlan supplicant`** command in Global Config mode.

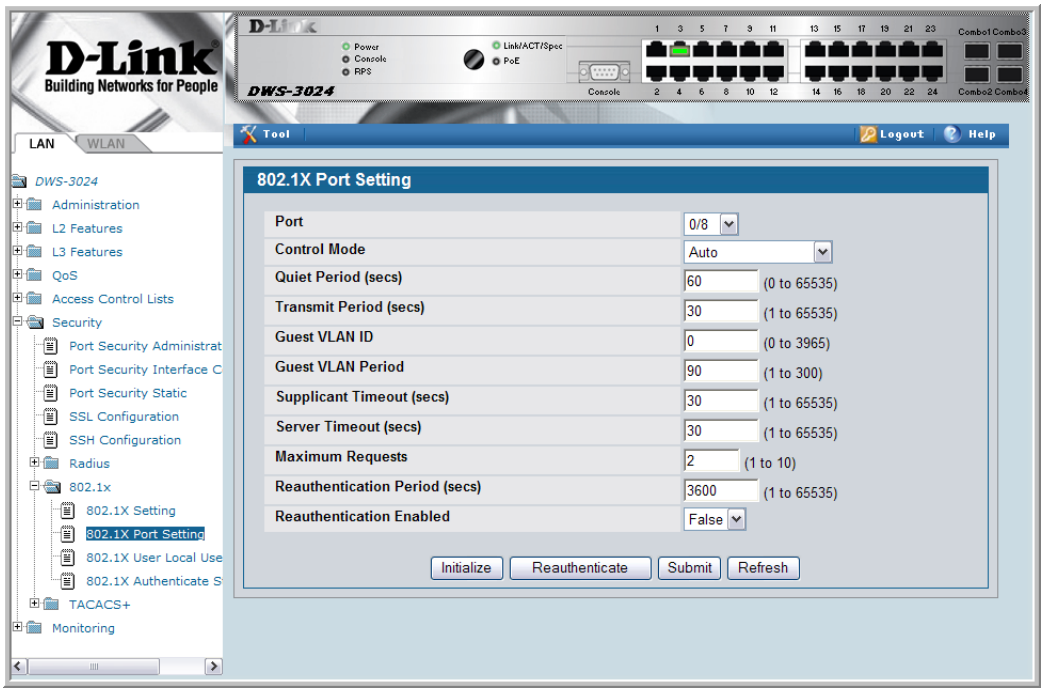
To configure a VLAN as guest VLAN on a per port basis, enter the Interface Config mode for the port and use the **`dot1x guest-vlan`** *`<vlan-id>`* command.

Configuring the Guest VLAN by Using the Web Interface

To enable the Guest VLAN features by using the Web interface, use the **LAN> Security > 802.1x > 802.1X Setting** page.



To configure the Guest VLAN settings on a port, use the **LAN> Security > 802.1x > 802.1X Port Setting** page.

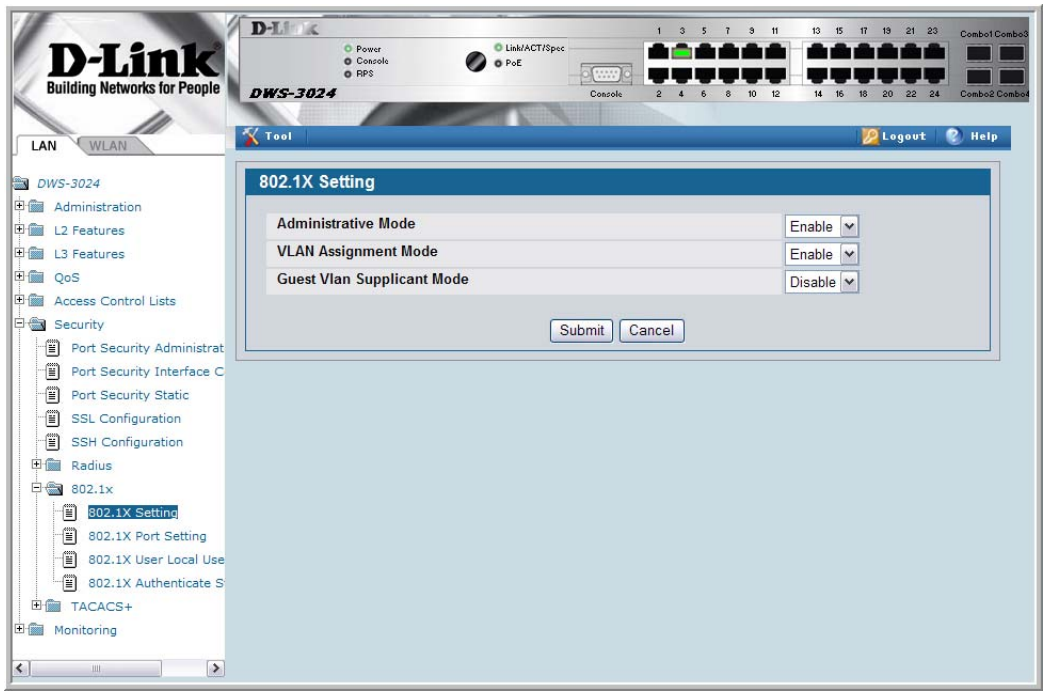


Configuring Dynamic VLAN Assignment

The software also supports VLAN assignment for clients based on the RADIUS server authentication.

To enable the switch to accept VLAN assignment by the RADIUS server, use the **`authorization network radius`** command in Global Config mode.

To enable the VLAN Assignment Mode by using the Web interface, use the **LAN> Security > 802.1x > 802.1X Setting** page and select **Enable** from the **VLAN Assignment Mode** menu.



5

Storm Control

A traffic storm is a condition that occurs when incoming packets flood the LAN, which creates performance degradation in the network. The Unified Switch's Storm Control feature protects against this condition.

The Unified Switch provides broadcast, multicast, and unicast storm recovery for individual interfaces or for all interfaces.

Unicast Storm Control protects against traffic whose MAC addresses are not known by the system.

For broadcast, multicast, and unicast storm control, if the rate of traffic ingressing on an interface increases beyond the configured threshold for that type, the traffic is dropped.

To configure storm control, you'll enable the feature for all interfaces or for individual interfaces, and you'll set the threshold (storm control level) beyond which the broadcast, multicast, or unicast traffic will be dropped.

Configuring a storm-control level also enables that form of storm-control. Disabling a storm-control level (using the "no" version of the command) sets the storm-control level back to default value and disables that form of storm-control. Using the "no" version of the "storm-control" command (not stating a "level") disables that form of storm-control but maintains the configured "level" (to be active next time that form of storm-control is enabled).

CLI Example

Example #1: Set Broadcast Storm Control for All Interfaces

```
(DWS-3024) #config

(DWS-3024) (Config)#storm-control broadcast ?

all                     Configure storm-control features for all ports.

(DWS-3024) (Config)#storm-control broadcast all ?

<cr>                    Press Enter to execute the command.
level                   Configure storm-control thresholds.

(DWS-3024) (Config)#storm-control broadcast all level ?
```

```
<rate>                    Enter the storm-control threshold as percent of port
                          speed.

(DWS-3024) (Config)#storm-control broadcast all level 7

(DWS-3024) (Config)#exit

(DWS-3024)
```

Example #2: Set Multicast Storm Control for All Interfaces

```
(DWS-3024) #config

(DWS-3024) (Config)#storm-control multicast all ?

<cr>                      Press Enter to execute the command.
level                     Configure storm-control thresholds.

(DWS-3024) (Config)#storm-control multicast all level 8

(DWS-3024) (Config)#exit

(DWS-3024) #
```

Example #3: Set Unicast Storm Control for All Interfaces

```
(DWS-3024) #config

(DWS-3024) (Config)#storm-control unicast all level 5

(DWS-3024) (Config)#exit

(DWS-3024) #
```


Web Interface

The Storm Control configuration options are available on the Port Configuration Web page under the Administration folder.

Figure 8. Port Configuration (Storm Control)

6

Trunking (Link Aggregation)

This section shows how to use the Trunking feature (also known as Link Aggregation) to configure port-channels by using the CLI and the Web interface.

The Link Aggregation (LAG) feature allows the switch to treat multiple physical links between two end-points as a single logical link called a port-channel. All of the physical links in a given port-channel must operate in full-duplex mode at the same speed.

You can use the feature to directly connect two switches when the traffic between them requires high bandwidth and reliability, or to provide a higher bandwidth connection to a public network.

You can configure the port-channels as either dynamic or static. Dynamic configuration uses the IEEE 802.3ad standard, which provides for the periodic exchanges of LACPDUs. Static configuration is used when connecting the switch to an external switch that does not support the exchange of LACPDUs.

The feature offers the following benefits:

- Increased reliability and availability -- if one of the physical links in the port-channel goes down, traffic is dynamically and transparently reassigned to one of the other physical links.
- Increased bandwidth -- the aggregated physical links deliver higher bandwidth than each individual link.
- Incremental increase in bandwidth -- A physical upgrade could produce a 10-times increase in bandwidth; LAG produces a two- or five-times increase, useful if only a small increase is needed.

Management functions treat a port-channel as if it were a single physical port.

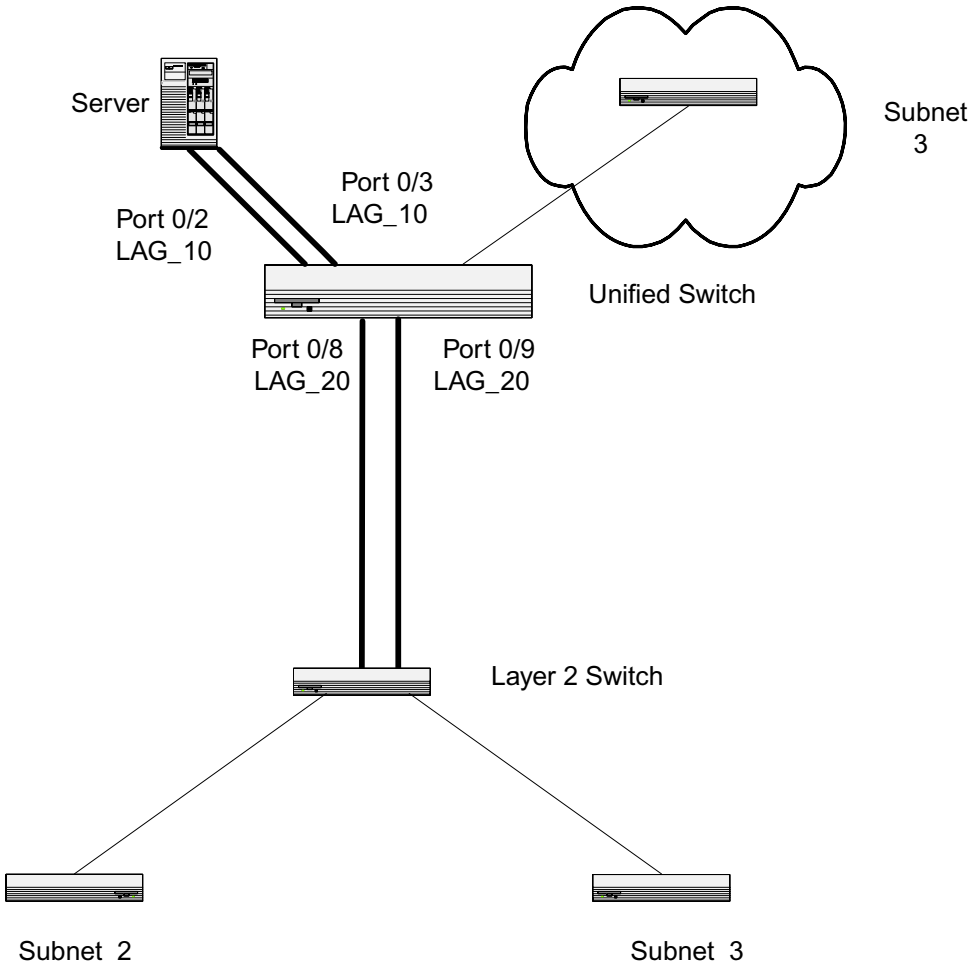
You can include a port-channel in a VLAN. You can configure more than one port-channel for a given switch.

CLI Example

The following shows an example of configuring the Unified Switch to support Link Aggregation (LAG) to a server and to a Layer 2 switch.

Figure 9 shows the example network.

Figure 9. LAG/Port-channel Example Network Diagram



Example 1: Create two port-channels:

```
(DWS-3024) #config
(DWS-3024) (Config)#port-channel lag_10
(DWS-3024) (Config)#port-channel lag_20
(DWS-3024) (Config)#exit
```

Use the **show port-channel all** command to show the logical interface ids you will use to identify the port-channels in subsequent commands. Assume that lag_10 is assigned id 3/1 and lag_20 is assigned id 3/2.


```
(DWS-3024) #show port-channel all

            Port-               Link
Log.       Channel         Adm. Trap  STP           Mbr      Port    Port
Intf        Name     Link  Mode Mode  Mode   Type   Ports    Speed   Active
------ ------------- ----- ---- ---- ------ ------- ------ --------- ------
3/1      lag_10      Down   En.  En.  Dis.  Dynamic
3/2      lag_20      Down   En.  En.  Dis.  Dynamic
```

Example 2: Add the physical ports to the port-channels:

```
(DWS-3024) #config
(DWS-3024) (Config)#interface 0/2
(DWS-3024) (Interface 0/2)#addport 3/1
(DWS-3024) (Interface 0/2)#exit
(DWS-3024) (Config)#interface 0/3
(DWS-3024) (Interface 0/3)#addport 3/1
(DWS-3024) (Interface 0/3)#exit
(DWS-3024) (Config)#exit

(DWS-3024) #config
(DWS-3024) (Config)#interface 0/8
(DWS-3024) (Interface 0/8)#addport 3/2
(DWS-3024) (Interface 0/8)#exit
(DWS-3024) (Config)#interface 0/9
(DWS-3024) (Interface 0/9)#addport 3/2
(DWS-3024) (Interface 0/9)#exit
(DWS-3024) (Config)#exit
```

Example 3: Enable both port-channels.

By default, the system enables link trap notification

```
(DWS-3024) #config
(DWS-3024) (Config)#port-channel adminmode all
(DWS-3024) (Config)#exit
```

At this point, the LAGs could be added to the default management VLAN.

Web Interface Configuration - LAGs/Port-channels

To perform the same configuration using the Web interface, use the **LAN> L2 Features > Trunking > Configuration** page.

Figure 10. Trunking Configuration

To create the port-channels, specify port participation and enable Link Aggregation (LAG) support on the switch.

7

IGMP Snooping

This section describes the Internet Group Management Protocol (IGMP) feature: IGMPv3 and IGMP Snooping. The IGMP Snooping feature enables the switch to monitor IGMP transactions between hosts and routers. It can help conserve bandwidth by allowing the switch to forward IP multicast traffic only to connected hosts that request multicast traffic.

Overview

IGMP:

- Uses Version 3 of IGMP
- Includes snooping
- Snooping can be enabled per VLAN

CLI Examples

The following are examples of the commands used in the IGMP Snooping feature.

Example #1: show igmpsnooping

```
(DWS-3024)              #show igmpsnooping ?

<cr>              Press Enter to execute the command.
<slot/port>       Enter interface in slot/port format.
mrouter           Display IGMP Snooping Multicast Router information.
<1-3965>          Display IGMP Snooping valid VLAN ID information.

(DWS-3024)              #show igmpsnooping

Admin Mode.............................Enable
Multicast Control Frame Count.............0
Interfaces Enabled for IGMP Snooping.....0/10
Vlans enabled for IGMP snooping..........20
```

Example #2: show mac-address-table igmpsnooping

```
(DWS-3024) #show mac-address-table igmpsnooping ?

<cr>                      Press Enter to execute the command.

(DWS-3024) #show mac-address-table igmpsnooping

MAC Address                Type     Description    Interfaces
-----------------------   -------  ------------    -----------
00:01:01:00:5E:00:01:16   Dynamic  Network Assist   Fwd: 0/47
00:01:01:00:5E:00:01:18   Dynamic  Network Assist   Fwd: 0/47
00:01:01:00:5E:37:96:D0   Dynamic  Network Assist   Fwd: 0/47
00:01:01:00:5E:7F:FF:FA   Dynamic  Network Assist   Fwd: 0/47
00:01:01:00:5E:7F:FF:FE   Dynamic  Network Assist   Fwd: 0/47
```

Example #3: set igmp (Global Config Mode)

```
(DWS-3026) (Config)#set igmp ?

<cr>                      Press enter to execute the command.
groupmembership-interval  Configure IGMP Group Membership Interval
                          (secs).
interfacemode             Enable/Disable IGMP Snooping.
maxresponse               Configure IGMP Max Response time (secs).
mcrtrexpiretime           Sets the Multicast Router Present Expiration
                          time on the system.

(DWS-3026) (Config)#set igmp
```

Example #4: set igmp (Interface Config Mode)

```
(DWS-3026) (Config)#interface 0/2

(DWS-3026) (Interface 0/2)#set igmp ?

<cr>                      Press enter to execute the command.
fast-leave                Enable/Disable Fast-Leave on a selected
interface
groupmembership-interval Configure IGMP Group Membership Interval
(secs).
maxresponse               Configure IGMP Max Response time (secs).
mcrtrexpiretime          Sets the Multicast Router Present Expiration
time on
                          the system.
mrouter                   Configure Multicast Router port.

(DWS-3026) (Interface 0/2)#set igmp
```


Web Examples

The following web pages are used in the IGMP Snooping feature. Click **Help** for more information on the web interface.

Figure 11. IGMP Snooping - Global Configuration and Status Page

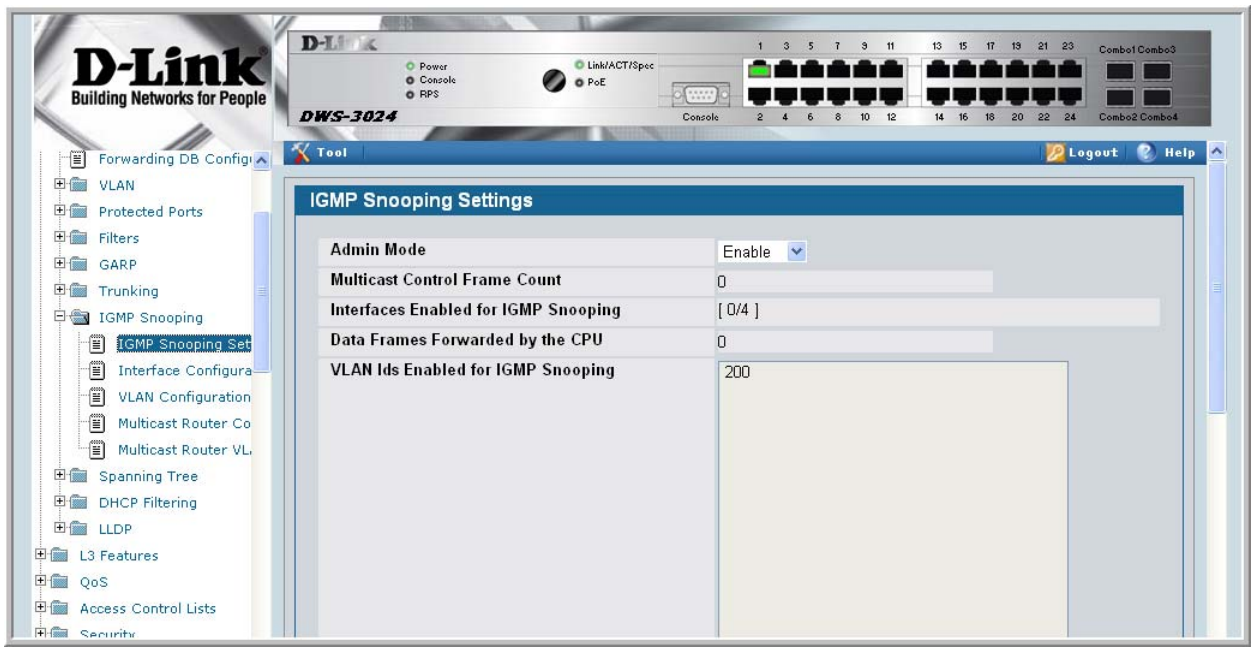


Figure 12. IGMP Snooping - Interface Configuration Page

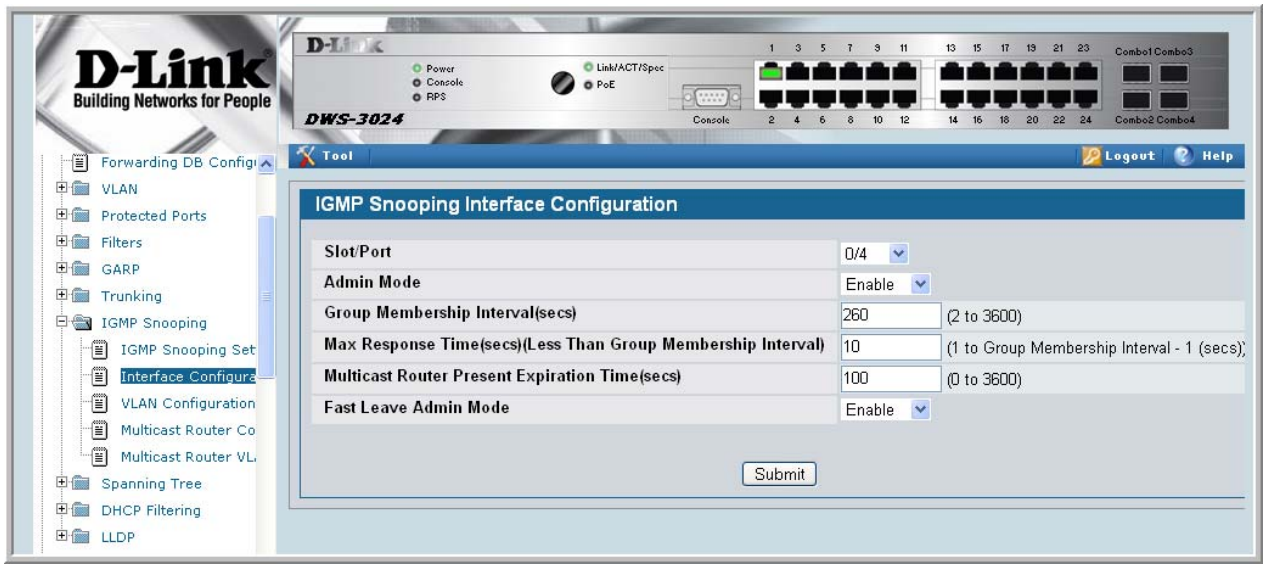


Figure 13. IGMP Snooping VLAN Configuration

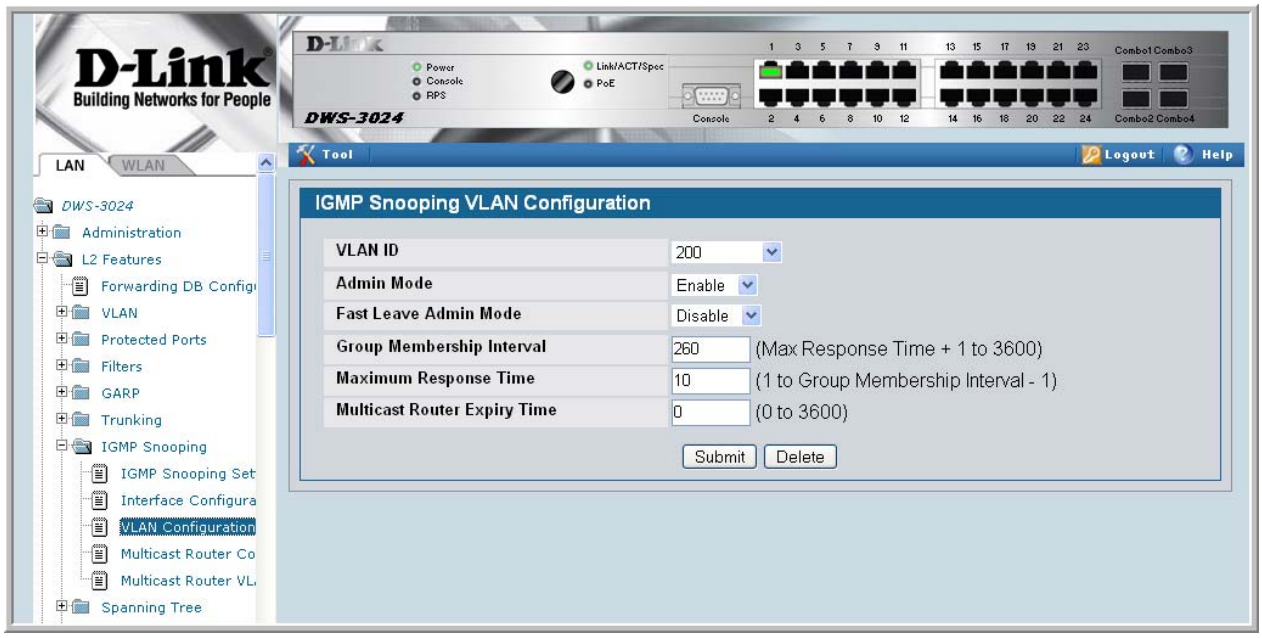


Figure 14. IGMP Snooping - VLAN Status Page

Figure 15. IGMP Snooping - Multicast Router Statistics Page

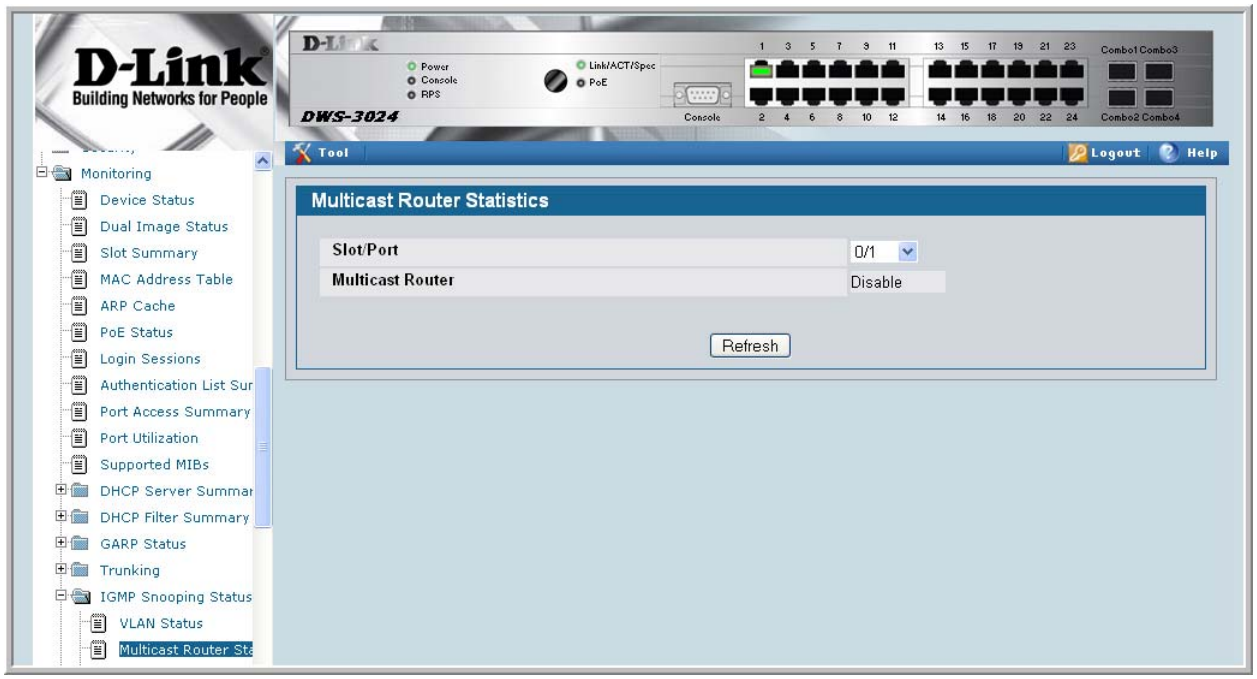


Figure 16. IGMP Snooping - Multicast Router Configuration Page

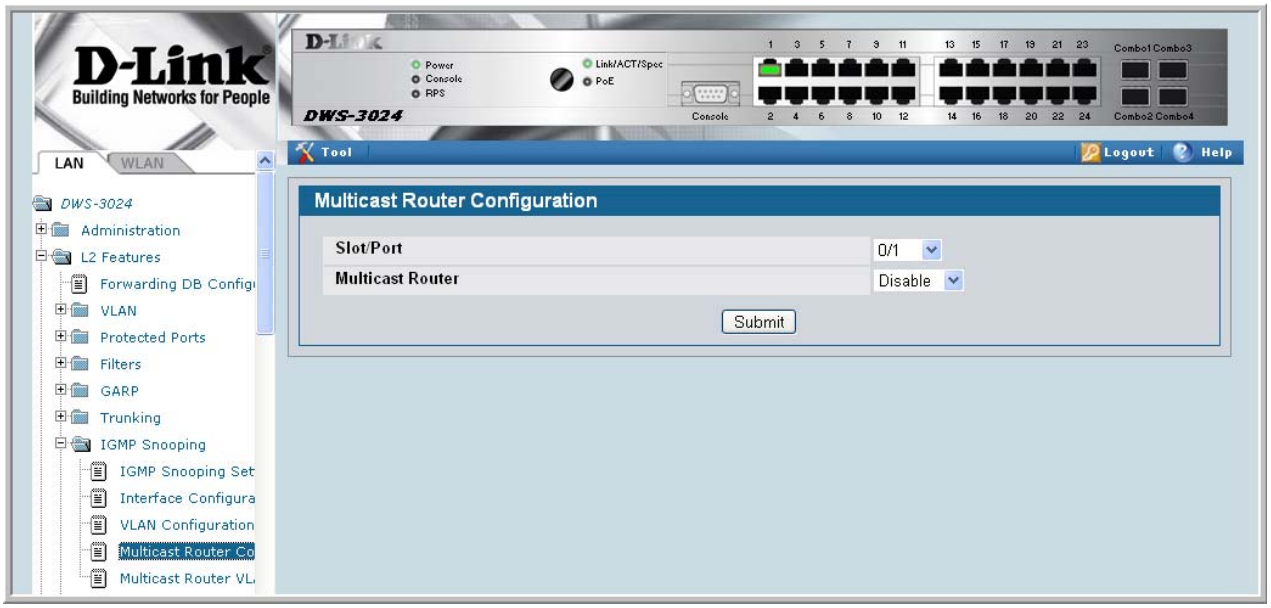


Figure 17. IGMP Snooping - Multicast Router VLAN Statistics Page

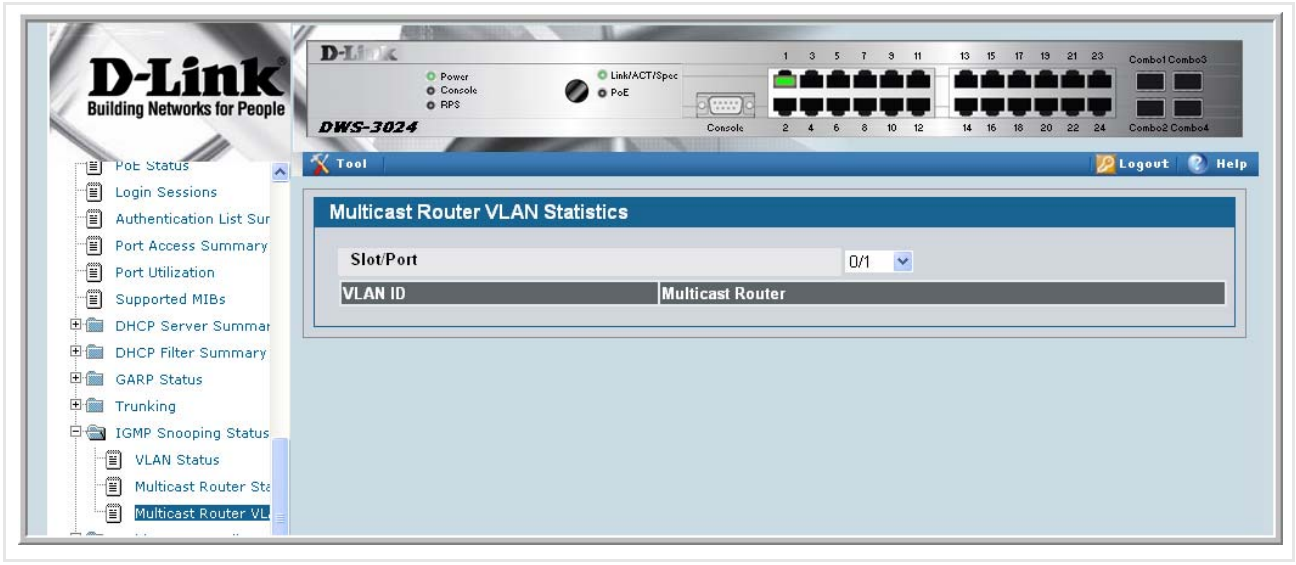
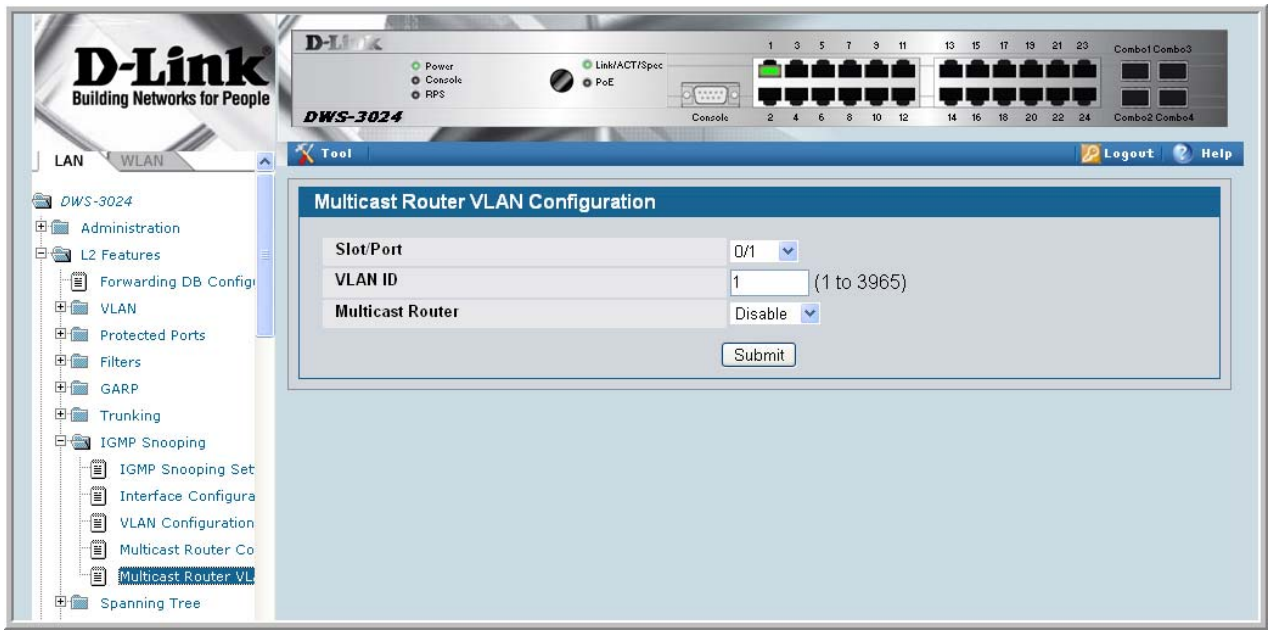


Figure 18. IGMP Snooping - Multicast Router VLAN Configuration Page



8

Port Mirroring

This section describes the Port Mirroring feature, which can serve as a diagnostic tool, debugging tool, or means of fending off attacks.

Overview

Port mirroring selects network traffic from specific ports for analysis by a network analyzer, while allowing the same traffic to be switched to its destination. You can configure many switch ports as source ports and one switch port as a destination port. You can also configure how traffic is mirrored on a source port. Packets received on the source port, transmitted on a port, or both received and transmitted, can be mirrored to the destination port.

CLI Examples

The following are examples of the commands used in the Port Mirroring feature.

Example #1: Set up a Port Mirroring Session

The following command sequence enables port mirroring and specifies a source and destination ports.

```
(DWS-3024) #config

(DWS-3024) (Config)#monitor session 1 mode

(DWS-3024) (Config)#monitor session 1 source interface 0/7 ?

<cr>                    Press Enter to execute the command.
rx                      Monitor ingress packets only.
tx                      Monitor egress packets only.

(DWS-3024) (Config)#monitor session 1 source interface 0/7

(DWS-3024) (Config)#monitor session 1 destination interface 0/8

(DWS-3024) (Config)#exit
```

Example #2: Show the Port Mirroring Session

```
(DWS-3024) #show monitor session 1

Session ID   Admin Mode   Probe Port   Mirrored Port   Type
----------   ----------   ----------   -------------   -----
1            Enable       0/8          0/7             Rx,Tx
```

(DWS-3024) #Monitor session ID “1” - “1” is a hardware limitation.

Example #3: Show the Status of All Ports

```
(DWS-3024) #show port all

                  Admin    Physical  Physical  Link     Link     LACP
Intf    Type      Mode     Mode      Status    Status   Trap     Mode
----    ----      ------   --------  --------  ------   ----     ----
0/1             Enable   Auto               Up       Enable   Enable
0/2             Enable   Auto               Down     Enable   Enable
0/3             Enable   Auto               Down     Enable   Enable
0/4             Enable   Auto               Down     Enable   Enable
0/5             Enable   Auto               Down     Enable   Enable
0/6             Enable   Auto               Down     Enable   Enable
0/7    Mirror   Enable   Auto               Down     Enable   Enable
0/8    Probe    Enable   Auto               Down     Enable   Enable
0/9             Enable   Auto               Down     Enable   Enable
0/10            Enable   Auto               Down     Enable   Enable
```

Example #4: Show the Status of the Source and Destination Ports

Use this command for a specific port. The output shows whether the port is the mirror or the probe port, what is enabled or disabled on the port, etc.

```
(DWS-3024) #show port 0/7

                 Admin    Physical  Physical  Link     Link     LACP
Intf    Type     Mode     Mode      Status    Status   Trap     Mode
----    ----     ------   --------  --------  ------   ----     ----
0/7    Mirror   Enable   Auto               Down     Enable   Enable


(DWS-3024) #show port 0/8

                  Admin    Physical  Physical  Link     Link     LACP
Intf     Type     Mode     Mode      Status    Status   Trap     Mode
----     ----     ------   --------  --------  ------   ----     ----
0/8      Probe    Enable   Auto               Down     Enable   Enable
```


Web Examples

The following web pages are used with the Port Mirroring feature.

Figure 19. Multiple Port Mirroring

Figure 20. Multiple Port Mirroring - Add Source Ports

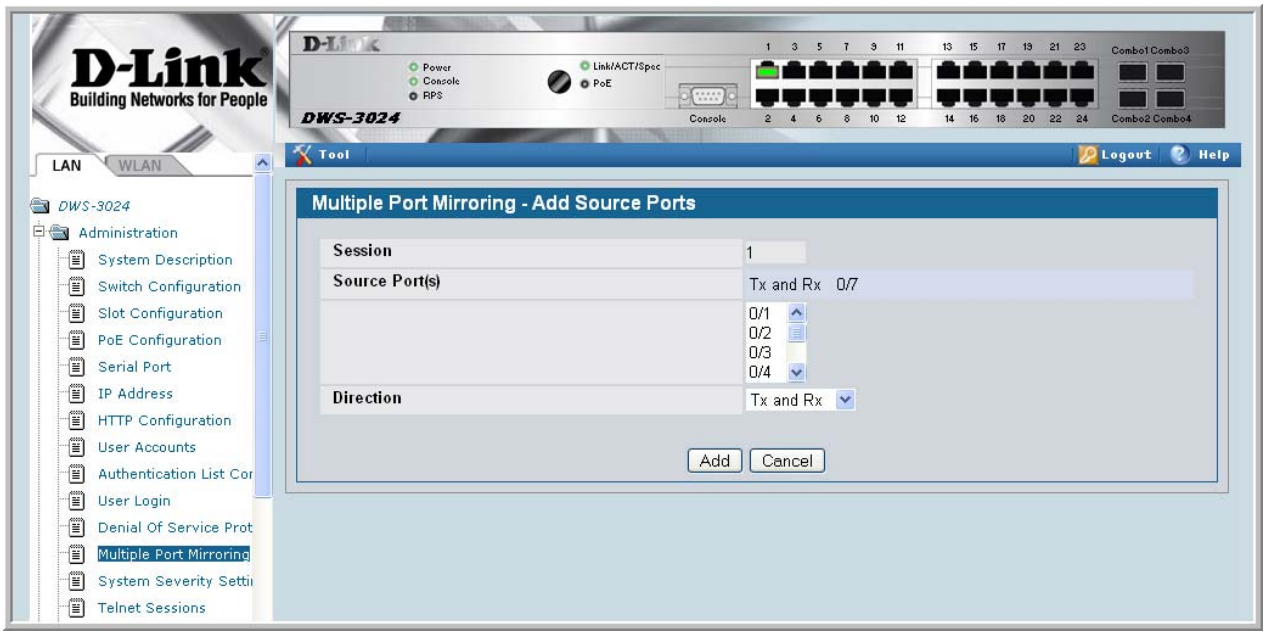
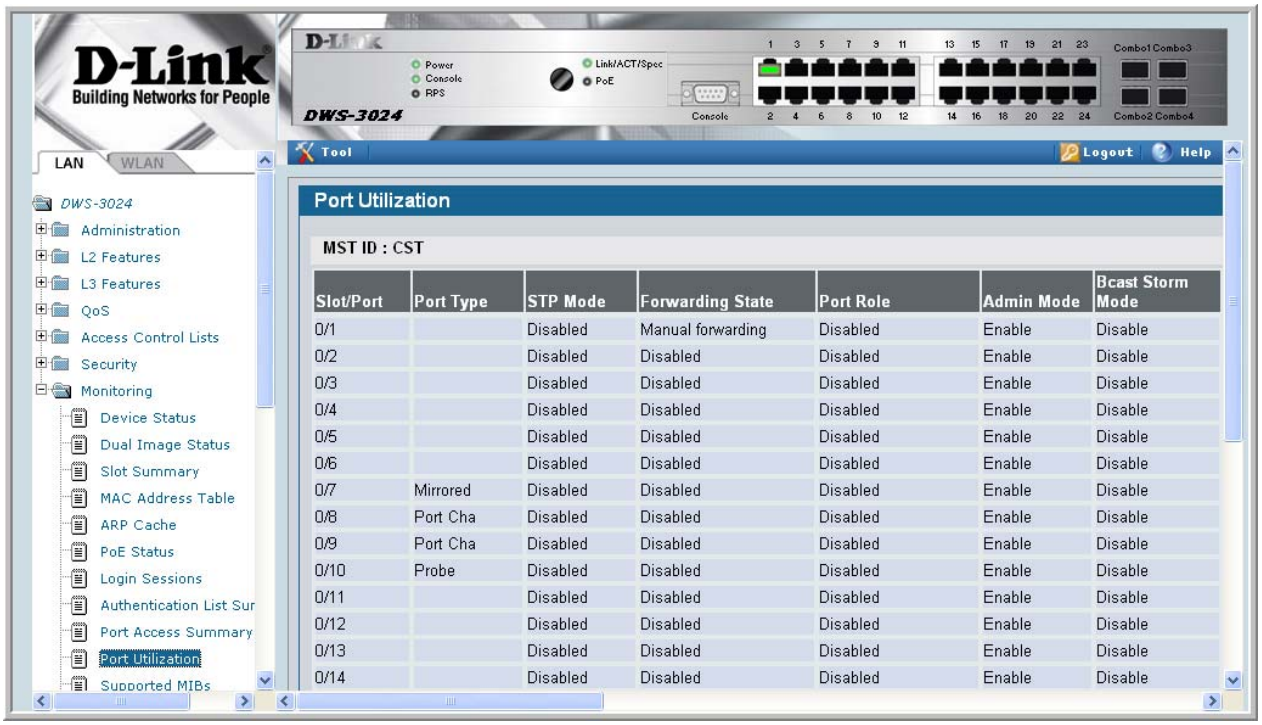


Figure 21. System - Port Utilization Summary



9

Port Security

This section describes the Port Security feature.

Overview

Port Security:

- Allows for limiting the number of MAC addresses on a given port.
- Packets that have a matching MAC address (secure packets) are forwarded; all other packets (unsecure packets) are restricted.
- Enabled on a per port basis.
- When locked, only packets with allowable MAC address will be forwarded.
- Supports both dynamic and static.
- Implement two traffic filtering methods. These methods can be used concurrently.
  - Dynamic Locking - User specifies the maximum number of MAC addresses that can be learned on a port. After the limit is reached, additional MAC addresses are not learned. Only frames with an allowable source MAC address are forwarded.
  - Static Locking - User manually specifies a list of static MAC addresses for a port. Dynamically locked addresses can be converted to statically locked addresses.

Operation

Port Security:

- Helps secure network by preventing unknown devices from forwarding packets.
- When link goes down, all dynamically locked addresses are ‘freed.’
- If a specific MAC address is to be set for a port, set the dynamic entries to 0, then only allow packets with a MAC address matching the MAC address in the static list.
- Dynamically locked MAC addresses are aged out if another packet with that address is not seen within the age-out time. The user can set the time-out value.
- Dynamically locked MAC addresses are eligible to be learned by another port.
- Static MAC addresses are not eligible for aging.
- Dynamically locked addresses can be converted to statically locked addresses.

CLI Examples

The following are examples of the commands used in the Port Security feature.

Example #1: show port security

```
(DWS-3024) #show port-security ?

<cr>                    Press Enter to execute the command.
all                     Display port-security information for all
                        interfaces
<slot/port>             Display port security information for a
                        specific interface.
dynamic                 Display dynamically learned MAC addresses.
static                  Display statically locked MAC addresses.
violation               Display the source MAC address of the last
                        packet that was discarded on a locked port.
```

Example #2: show port security on a specific interface

```
(DWS-3024) #show port-security 0/10

         Admin    Dynamic     Static    Violation
 Intf    Mode      Limit      Limit     Trap Mode
------  -------  ----------  ---------  ----------
0/10  Disabled 600         20         Disabled
```

Example #3: (Config) port security

```
(DWS-3024) (Config)           #port-security ?

<cr>                          Press Enter to execute the command.

(DWS-3024) (Config)           #port-security
```


Web Examples

The following Web pages are used in the Port Security feature.

Figure 22. Port Security Administration

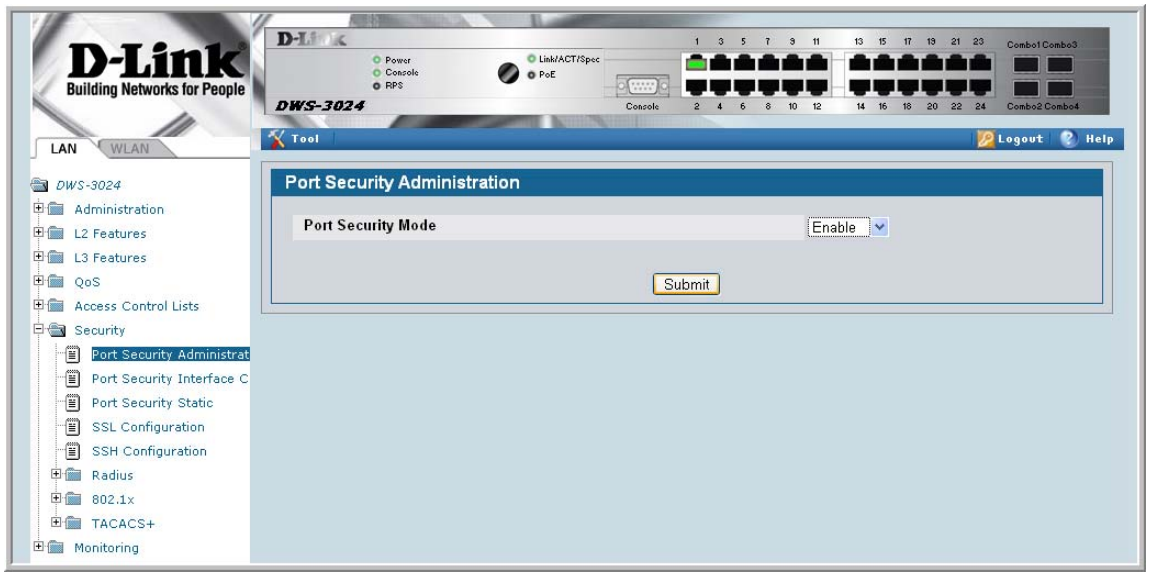
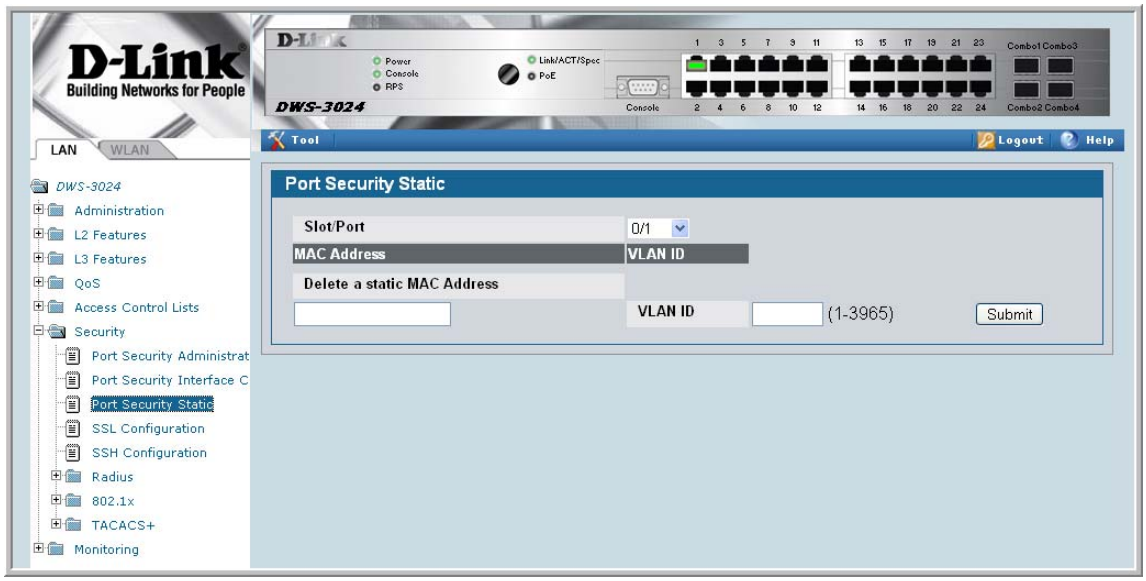


Figure 23. Port Security Interface Configuration

Figure 24. Port Security Statically Configured MAC Addresses



To view Port Security status information, navigate to **LAN> Monitoring > Port Security** from the navigation panel.

Figure 25. Port Security Dynamically Learned MAC Addresses

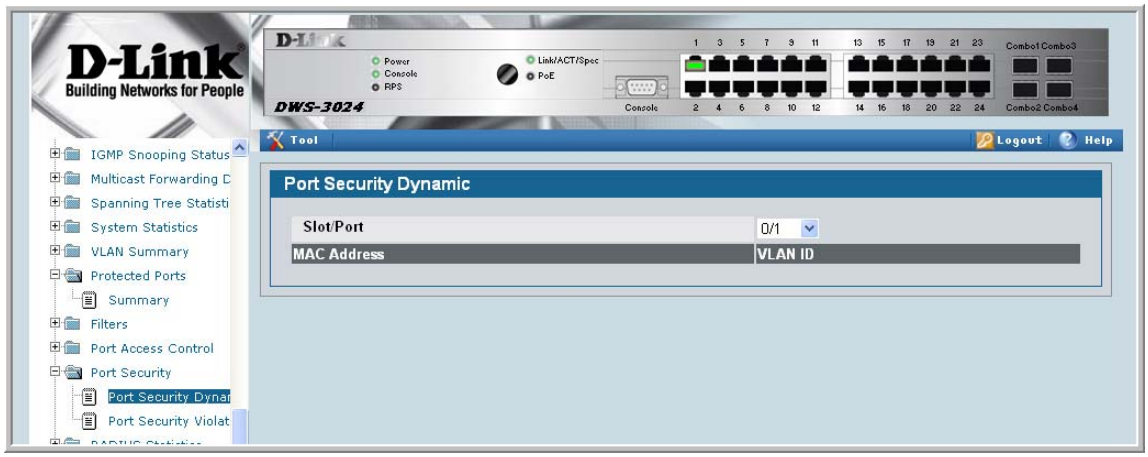
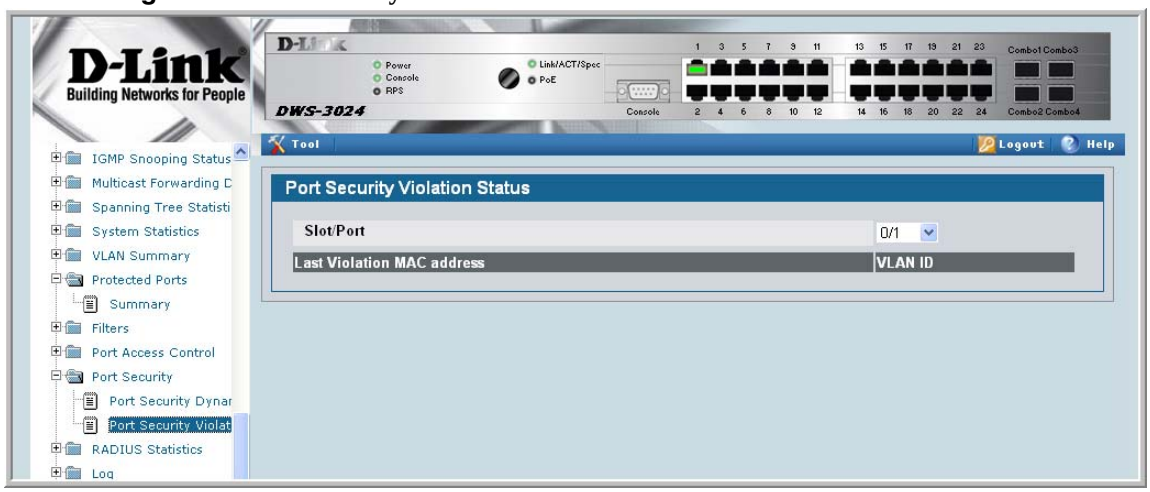


Figure 26. Port Security Violation Status



10

Link Layer Discovery Protocol

The Link Layer Discovery Protocol (LLDP) feature allows individual interfaces on the switch to advertise major capabilities and physical descriptions. Network managers can view this information and identify system topology and detect bad configurations on the LAN.

LLDP has separately configurable transmit and receive functions. Interfaces can transmit and receive LLDP information.

CLI Examples

Example #1: Set Global LLDP Parameters

Use the following sequence to specify switch-wide notification interval and timers for all LLDP interfaces.

```
(DWS-3024) #config

(DWS-3024) (Config)#lldp ?

notification-interval    Configure minimum interval to send remote data
                         change notifications

timers                   Configure the LLDP global timer values.

(DWS-3024) (Config)#lldp notification-interval ?

<interval-seconds>       Range <5 - 3600> seconds.

(DWS-3024) (Config)#lldp notification-interval 1000

(DWS-3024) (Config)#lldp timers ?

<cr>                     Press Enter to execute the command.
hold                     The interval multiplier to set local LLDP data TTL.
interval                 The interval in seconds to transmit local LLDP data.
reinit                   The delay before re-initialization.

(DWS-3024) (Config)#lldp timers hold 8 reinit 5

(DWS-3024) (Config)#exit
```

```
(DWS-3024) #
```

Example #2: Set Interface LLDP Parameters

The following commands configure interface 0/10 to transmit and receive LLDP information.

```
(DWS-3024) #config

(DWS-3024) (Config)#interface 0/10

(DWS-3024) (Interface 0/10)#lldp ?

notification             Enable/Disable LLDP remote data change notifications.
receive                  Enable/Disable LLDP receive capability.
transmit                 Enable/Disable LLDP transmit capability.
transmit-mgmt            Include/Exclude LLDP management address TLV.
transmit-tlv             Include/Exclude LLDP optional TLV(s).

(DWS-3024) (Interface 0/10)#lldp receive

(DWS-3024) (Interface 0/10)#lldp transmit

(DWS-3024) (Interface 0/10)#lldp transmit-mgmt

(DWS-3024) (Interface 0/10)#exit

(DWS-3024) (Config)#exit

(DWS-3024) #
```

Example #3: Show Global LLDP Parameters

```
(DWS-3024) #show lldp

LLDP Global Configuration

Transmit Interval.......................... 30 seconds

Transmit Hold Multiplier................... 8

Reinit Delay............................... 5 seconds

Notification Interval...................... 1000 seconds

(DWS-3024) #
```

Example #4 Show Interface LLDP Parameters

```
(DWS-3024) #show lldp interface 0/10

LLDP Interface Configuration

Interface  Link    Transmit  Receive   Notify    TLVs     Mgmt
---------  ------  --------  --------  --------  -------  ----
0/10     Down    Enabled   Enabled   Disabled           Y

TLV Codes: 0- Port Description,   1- System Name
           2- System Description, 3- System Capabilities

(DWS-3024) #
```

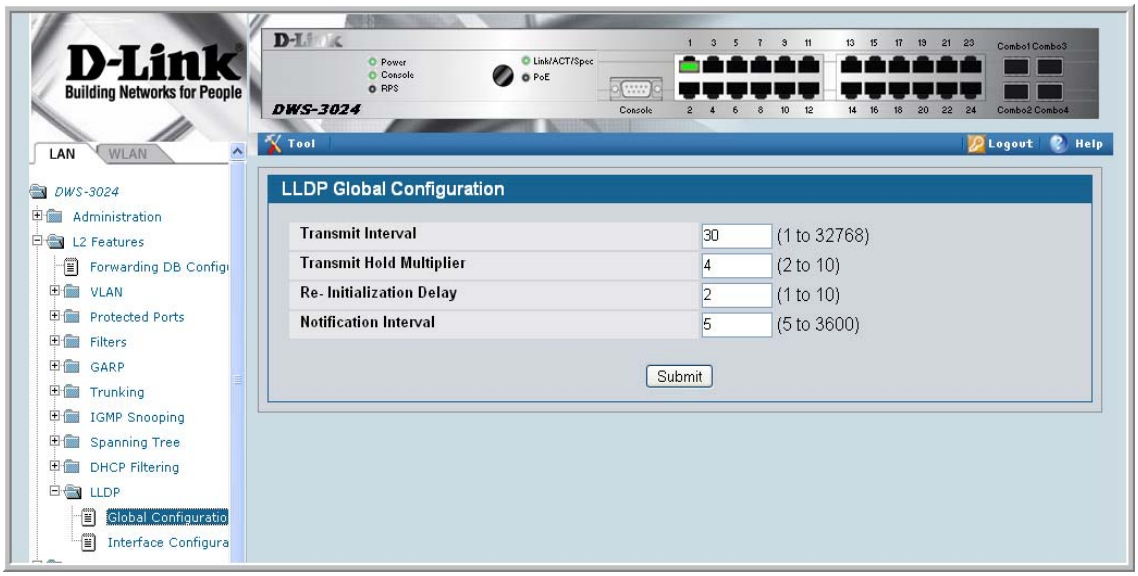

Using the Web Interface to Configure LLDP

The **LLDP** menu page contains links to the following features:

- LLDP Configuration
- LLDP Statistics
- LLDP Connections
- LLDP Configuration

Use the LLDP Global Configuration page to specify LLDP parameters.

Figure 27. LLDP Global Configuration

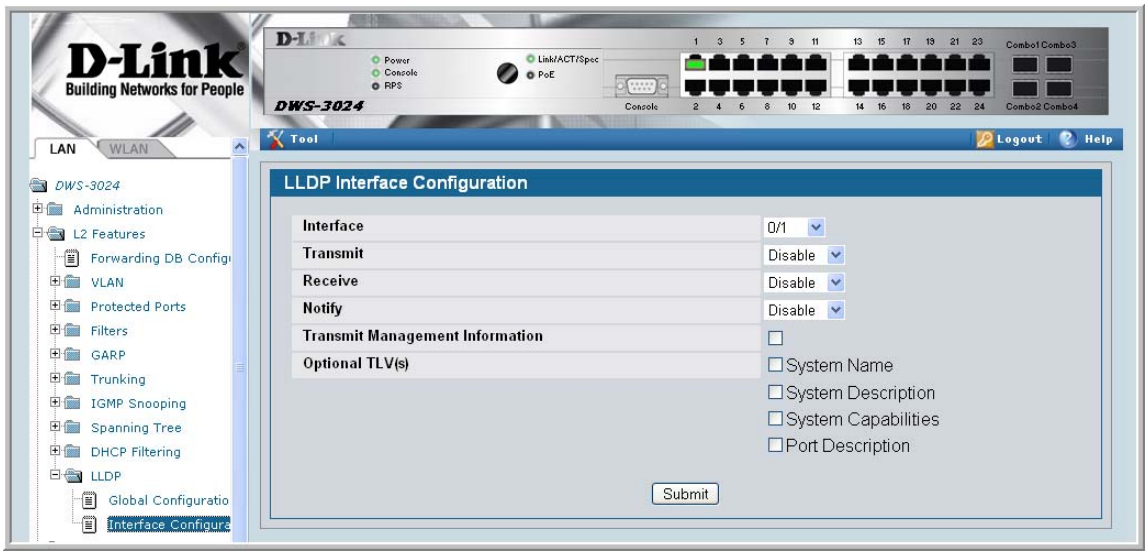


The **LLDP Global Configuration** page contains the following fields:

- **Transmit Interval (1-32768)** — Specifies the interval at which frames are transmitted. The default is 30 seconds.
- **Hold Multiplier (2-10)** — Specifies multiplier on the transmit interval to assign to TTL. Default is 4.
- **Re-Initialization Delay (1-10)** — Specifies delay before a re-initialization. Default is 2 seconds.
- **Notification Interval (5-3600)** — Limits the transmission of notifications. The default is 5 seconds.

Use the LLDP Interface Configuration screen to specify transmit and receive functions for individual interfaces.

Figure 28. LLDP Interface Configuration



Interface Parameters

- **Interface** — Specifies the port to be affected by these parameters.
- **Transmit Mode** — Enables or disables the transmit function. The default is disabled.
- **Receive Mode** — Enables or disables the receive function. The default is disabled.
- **Transmit Management Information** — Enables or disables transmission of management address instance. Default is disabled.
- **Notification Mode** — Enables or disables remote change notifications. The default is disabled.
- **Included TLVs** — Selects TLV information to transmit. Choices include System Name, System Capabilities, System Description, and Port Description.

Figure 29. LLDP Interface Summary

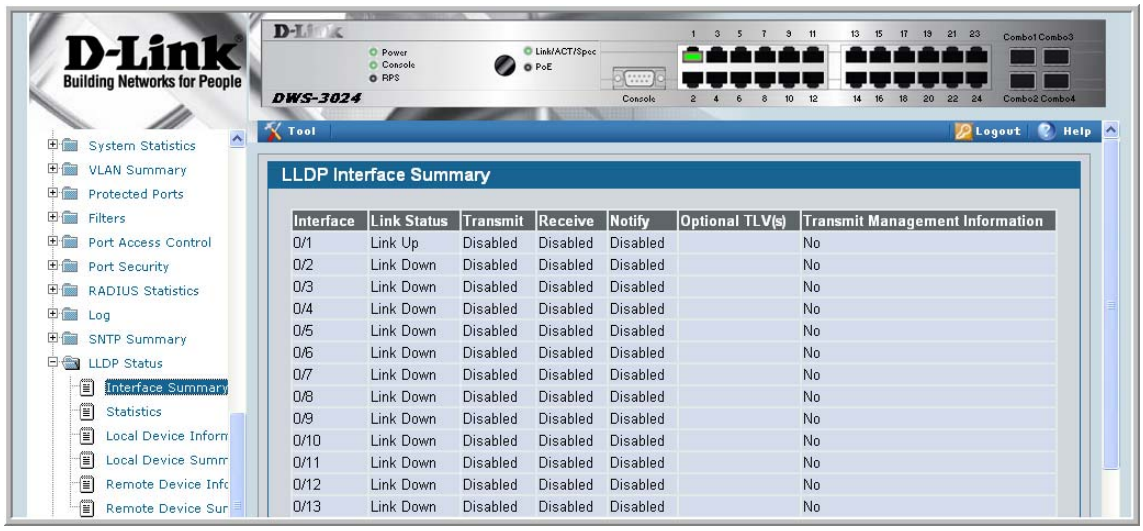
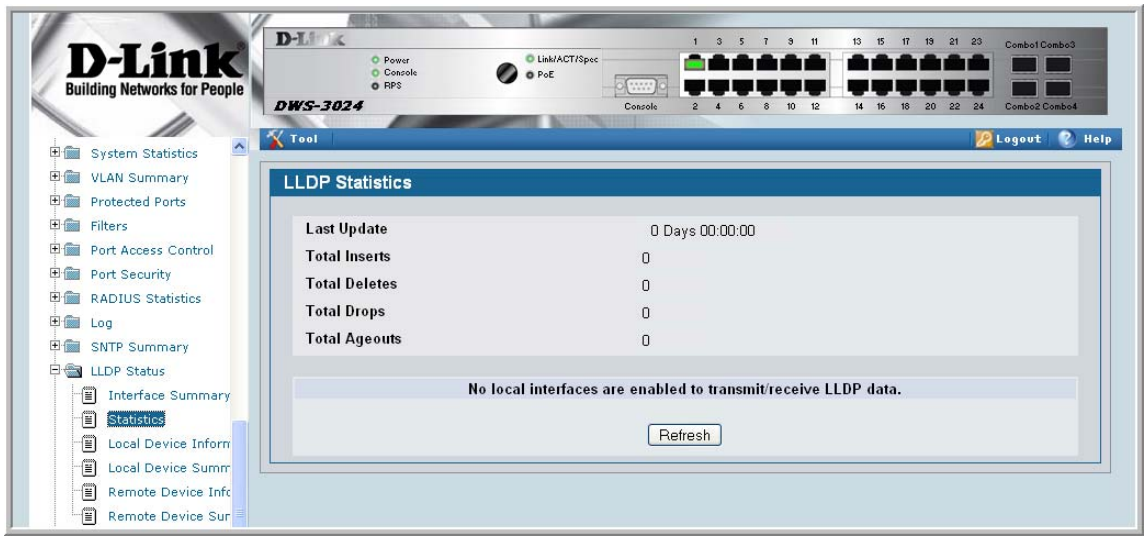


Figure 30. LLDP Statistics



You can also use the pages in the **LAN> Monitoring > LLDP Status** folder to view information about local and remote devices.

11

Denial of Service Attack Protection

This section describes the D-Link DWS-3000 switch's Denial of Service Protection feature.

Overview

Denial of Service:

- Spans two categories:
  - Protection of the Unified Switch
  - Protection of the network
- Protects against the exploitation of a number of vulnerabilities which would make the host or network unstable
- Compliant with Nessus. Nessus is a widely-used vulnerability assessment tool.
- The Unified Switch provides a number of features that help a network administrator protect networks against DoS attacks.

CLI Examples

Enter from Global Config mode:

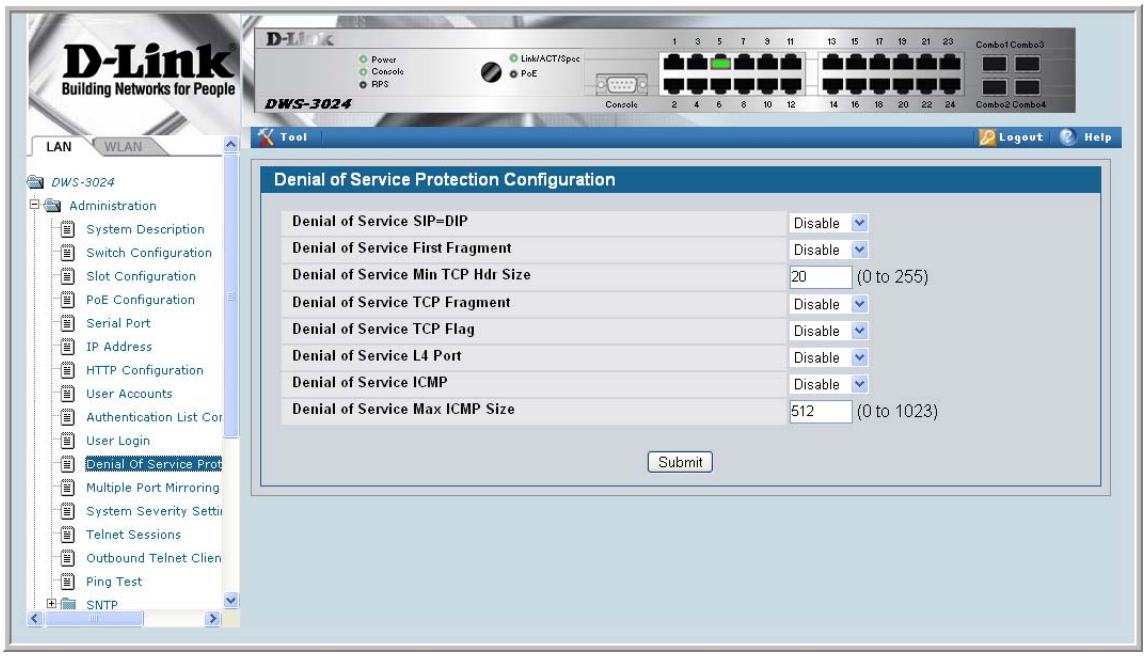
```
(DWS-3024) #configure

(DWS-3024) (Config)#dos-control sipdip

(DWS-3024) (Config)#dos-control firstfrag

(DWS-3024) (Config)#dos-control tcpfrag

(DWS-3024) (Config)#dos-control l4port

(DWS-3024) (Config)#dos-control icmp

(DWS-3024) (Config)#exit

(DWS-3024) #show dos-control

SIPDIP Mode..................................... Enable
```

```
First Fragment Mode.......................... Enable
Min TCP Hdr Size............................. 20
TCP Fragment Mode............................ Enable
TCP Flag Mode................................ Disable
L4 Port Mode................................. Enable
ICMP Mode.................................... Enable
Max ICMP Pkt Size............................ 512
```

Web Interface

You can configure the Denial of Service feature from the **Denial of Service Protection Configuration** page.

Figure 31. Denial of Service Protection Configuration



12

Port Routing

The first networks were small enough for the end stations to communicate directly. As networks grew, Layer 2 bridging was used to segregate traffic, a technology that worked well for unicast traffic, but had problems coping with large quantities of multicast packets. The next major development was routing, where packets were examined and redirected at Layer 3. End stations needed to know how to reach their nearest router, and the routers had to understand the network topology so that they could forward traffic. Although bridges tended to be faster than routers, using routers allowed the network to be partitioned into logical subnetworks, which restricted multicast traffic and also facilitated the development of security mechanisms.

An end station specifies the destination station's Layer 3 address in the packet's IP header but sends the packet to the MAC address of a router. When the Layer 3 router receives the packet, at a minimum it does the following:

- Looks up the Layer 3 address in its address table to determine the outbound port
- Updates the Layer 3 header
- Recreates the Layer 2 header

The router's IP address is often statically configured in the end station, although the Unified Switch supports DHCP that allow the address to be assigned dynamically. You may assign static entries in the routing tables used by the router.

Port Routing Configuration

The Unified Switch always supports Layer 2 bridging, but Layer 3 routing must be explicitly enabled, first for the Unified Switch as a whole, and then for each port which is to participate in the routed network.

The configuration commands used in this section's example enable IP routing on ports 0/2, 0/3, and 0/5. The router ID is set to the Unified Switch's management IP address, or to that of any active router interface if the management address is not configured.

After you've issued the routing configuration commands, the following functions are active:

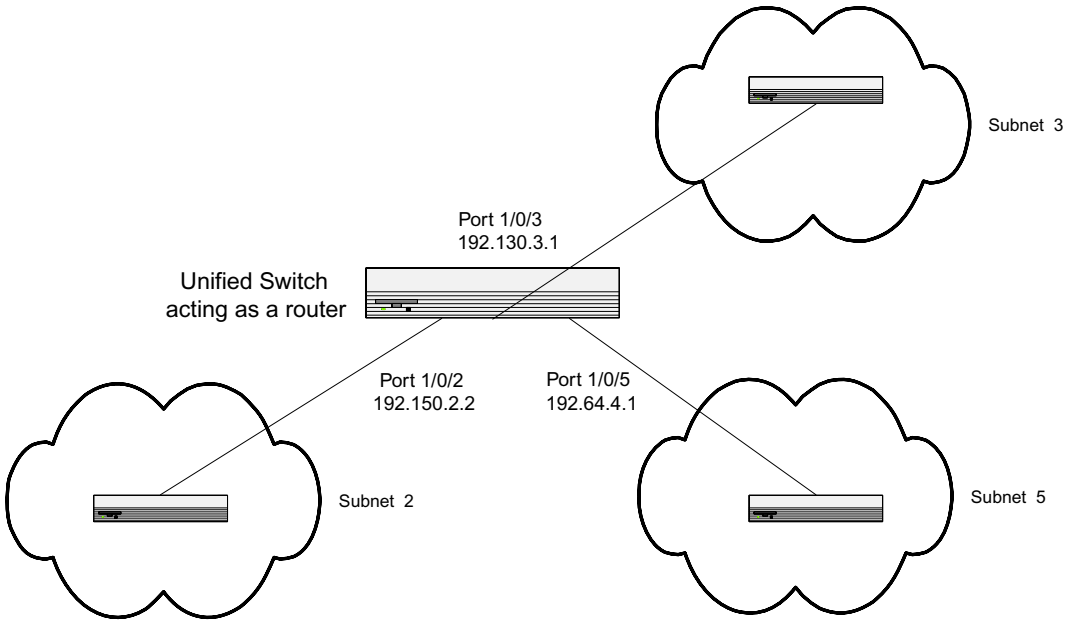
- IP Forwarding - responsible for forwarding received IP packets.

- ARP Mapping - responsible for maintaining the ARP Table used to correlate IP and MAC addresses. The table contains both static entries and entries dynamically updated based on information in received ARP frames.
- Routing Table Object - responsible for maintaining the routing table populated by local and static routes.

CLI Examples

The diagram in this section shows a Unified Switch configured for port routing. It connects three different subnets, each connected to a different port. The script shows the commands you would use to configure a Unified Switch to provide the port routing support shown in the diagram.

Figure 32. Port Routing Example Network Diagram



Example 1. Enabling routing for the Switch

Use the following command to enable routing for the switch. Execution of the command enables IP forwarding by default.

```
config
  ip routing
exit
```


Example 2. Enabling Routing for Ports on the Switch

Use the following commands to enable routing for ports on the switch. The default link-level encapsulation format is Ethernet. Configure the IP addresses and subnet masks for the ports. Network directed broadcast frames are dropped and the maximum transmission unit (MTU) size is 1500 bytes.

```
config
  interface 0/2
    routing
    ip address 192.150.2.2 255.255.255.0
  exit
exit

config
  interface 0/3
    routing
    ip address 192.130.3.1 255.255.255.0
  exit
exit

config
  interface 0/5
    routing
    ip address 192.64.4.1 255.255.255.0
  exit
exit
```

Using the Web Interface to Configure Routing

Use the following screens to perform the same configuration using the Graphical User Interface:

To enable routing for the switch, as shown in Example 1. Enabling routing for the Switch, use the **LAN> L3 Features> IP > Configuration** page.

Figure 33. IP Configuration

To configure routing on each interface, as shown in Example 2. Enabling Routing for Ports on the Switch, use the **LAN> L3 Features > IP > Interface Configuration** page.

Figure 34. IP Interface Configuration

13

VLAN Routing

You can configure the Unified Switch with some ports supporting VLANs and some supporting routing. You can also configure the Unified Switch to allow traffic on a VLAN to be treated as if the VLAN were a router port.

When a port is enabled for bridging (default) rather than routing, all normal bridge processing is performed for an inbound packet, which is then associated with a VLAN. Its MAC Destination Address (MAC DA) and VLAN ID are used to search the MAC address table. If routing is enabled for the VLAN and the MAC DA of an inbound unicast packet is that of the internal bridge-router interface, the packet will be routed. An inbound multicast packet will be forwarded to all ports in the VLAN, plus the internal bridge-router interface if it was received on a routed VLAN.

Since a port can be configured to belong to more than one VLAN, VLAN routing might be enabled for all of the VLANs on the port, or for a subset. VLAN Routing can be used to allow more than one physical port to reside on the same subnet. It could also be used when a VLAN spans multiple physical networks, or when additional segmentation or security is required.

This section shows how to configure the Unified Switch to support VLAN routing. A port can be either a VLAN port or a router port, but not both. However, a VLAN port may be part of a VLAN that is itself a router port.

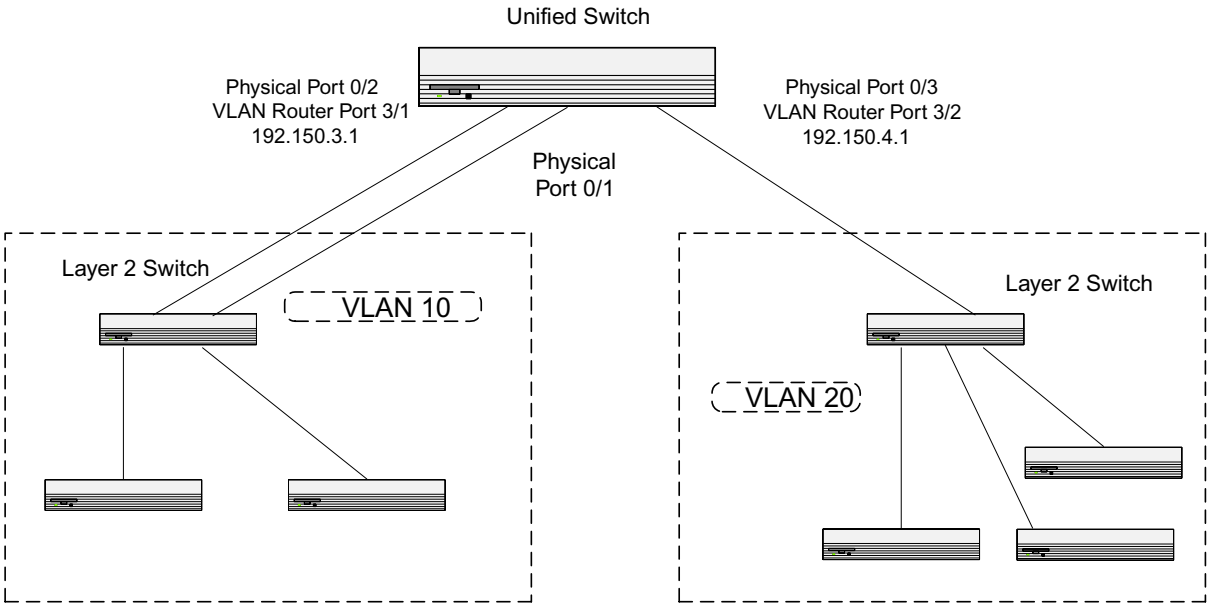
VLAN Routing Configuration

This section provides an example of how to configure the Unified Switch to support VLAN routing. The configuration of the VLAN router port is similar to that of a physical port. The main difference is that, after the VLAN has been created, you must use the **show ip vlan** command to determine the VLAN's interface ID so that you can use it in the router configuration commands.

CLI Examples

The diagram in this section shows a Unified Switch configured for VLAN routing. It connects two VLANs, with two ports participating in one VLAN, and one port in the other. The script shows the commands you would use to configure the Unified Switch to provide the VLAN routing support shown in the diagram.

Figure 35. VLAN Routing Example Network Diagram



Example 1: Create Two VLANs

The following commands show an example of how to create two VLANs with egress frame tagging enabled.

```
vlan database
  vlan 10
  vlan 20
exit

config
  interface 0/1
    vlan participation include 10
  exit
  interface 0/2
    vlan participation include 10
  exit
  interface 0/3
    vlan participation include 20
  exit
exit

config
  vlan port tagging all 10
  vlan port tagging all 20
exit
```


Next specify the VLAN ID assigned to untagged frames received on the ports.

```
config
  interface 0/1
    vlan pvid 10
  exit
  interface 0/2
    vlan pvid 10
  exit
  interface 0/3
    vlan pvid 20
  exit
exit
```

Example 2: Set Up VLAN Routing for the VLANs and the Switch.

The following commands show how to enable routing for the VLANs:

```
vlan database
  vlan routing 10
  vlan routing 20
exit

show ip vlan
```

This returns the logical interface IDs that will be used in subsequent routing commands. Assume that VLAN 10 is assigned ID 4/1 and VLAN 20 is assigned ID 4/2.

Enable routing for the switch:

```
config
  ip routing
exit
```

The next sequence shows an example of configuring the IP addresses and subnet masks for the VLAN router ports.

```
config
  interface 4/1
    ip address 192.150.3.1 255.255.255.0
  exit
  interface 4/2
    ip address 192.150.4.1 255.255.255.0
  exit
exit
```

Using the Web Interface to Configure VLAN Routing

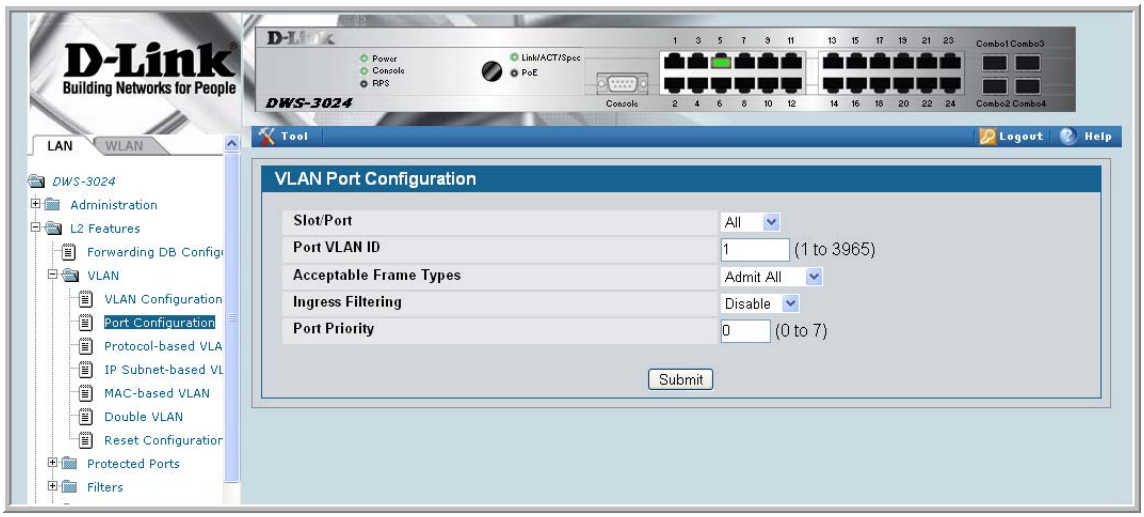
You can perform the same configuration by using the Web Interface.

Use the **LAN> L2 Features > VLAN> VLAN Configuration** page to create the VLANs, specify port participation, and configure whether frames will be transmitted tagged or untagged.

Figure 36. VLAN Configuration

Use the **LAN> L2 Features > VLAN > Port Configuration** page to specify the handling of untagged frames on receipt.

Figure 37. VLAN Port Configuration



Use the **LAN> L3 Features > VLAN Routing > Configuration** page to enable VLAN routing and configure the ports.

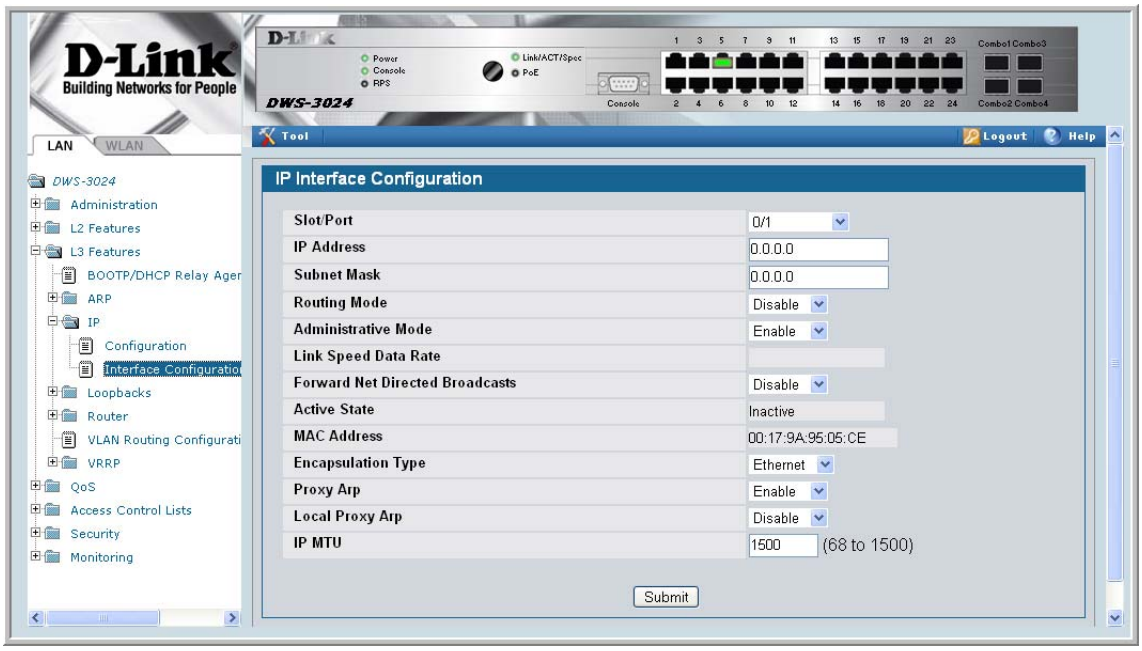
Figure 38. VLAN Routing Configuration

To enable routing for the switch, use the **LAN> L3 Features > IP > Configuration** page.

Figure 39. Enabling Routing

Use the **LAN> L3 Features > IP > Interface Configuration** page to enable routing for the ports and configure their IP addresses and subnet masks.

Figure 40. IP Interface Configuration



14

Virtual Router Redundancy Protocol

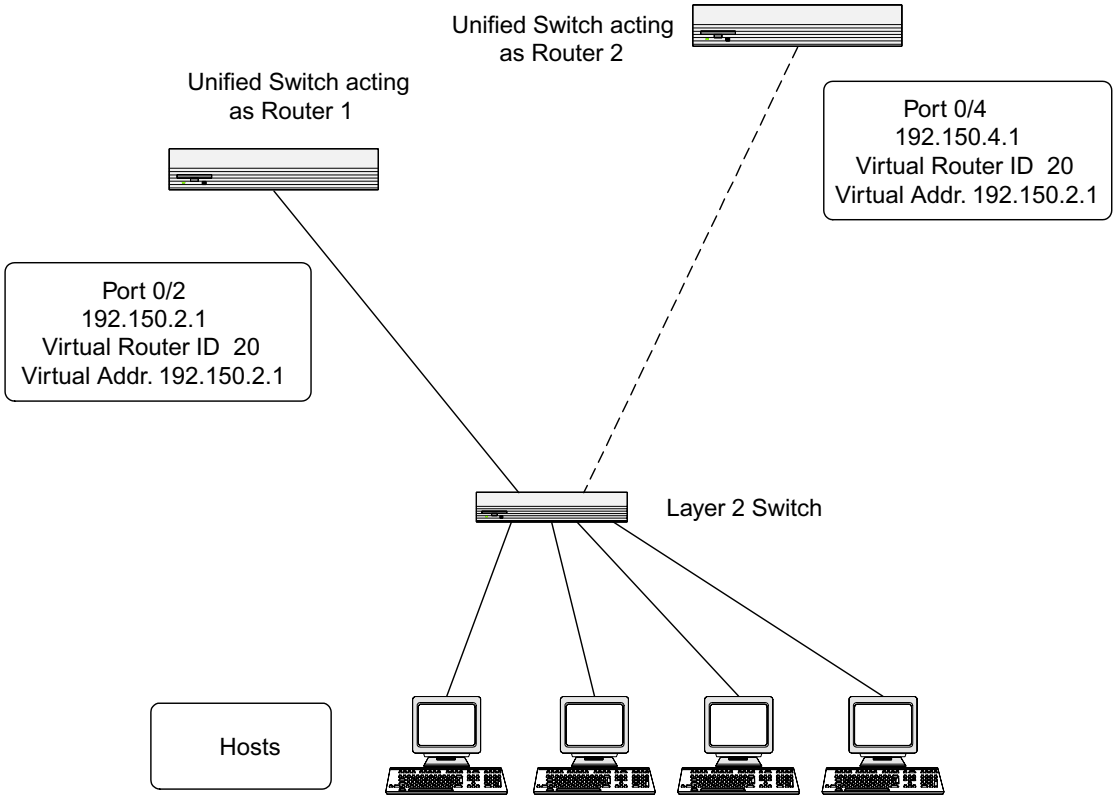
When an end station is statically configured with the address of the router that will handle its routed traffic, a single point of failure is introduced into the network. If the router goes down, the end station is unable to communicate. Since static configuration is a convenient way to assign router addresses, Virtual Router Redundancy Protocol (VRRP) was developed to provide a backup mechanism.

VRRP eliminates the single point of failure associated with static default routes by enabling a backup router to take over from a “master” router without affecting the end stations using the route. The end stations will use a “virtual” IP address that will be recognized by the backup router if the master router fails. Participating routers use an election protocol to determine which router is the master router at any given time. A given port may appear as more than one virtual router to the network, also, more than one port on a Unified Switch may be configured as a virtual router. Either a physical port or a routed VLAN may participate.

CLI Examples

This example shows how to configure the Unified Switch to support VRRP. Router 1 will be the default master router for the virtual route, and Router 2 will be the backup router.

Figure 41. VRRP Example Network Configuration



Example 1: Configuring VRRP on the Switch as a Master Router

Enable routing for the switch. IP forwarding is then enabled by default.

```
config
  ip routing
exit
```

Configure the IP addresses and subnet masks for the port that will participate in the protocol.

```
config
  interface 0/2
  routing
  ip address 192.150.2.1 255.255.255.0
exit
```

Enable VRRP for the switch.

```
config
  ip vrrp
exit
```


Assign virtual router IDs to the port that will participate in the protocol.

```
config
  interface 0/2
  ip vrrp 20
```

Specify the IP address that the virtual router function will recognize. Note that the virtual IP address on port 0/2 is the same as the port's actual IP address, therefore this router will always be the VRRP master when it is active. And the priority default is 255.

```
  ip vrrp 20 ip 192.150.2.1
```

Enable VRRP on the port.

```
  ip vrrp 20 mode
exit
```

Example 2: Configuring VRRP on the Switch as a Backup Router

Enable routing for the switch. IP forwarding is then enabled by default.

```
config
  ip routing
exit
```

Configure the IP addresses and subnet masks for the port that will participate in the protocol.

```
config
  interface 0/4
  routing
  ip address 192.150.4.1 255.255.255.0
exit
```

Enable VRRP for the switch.

```
config
  ip vrrp 20
exit
```

Assign virtual router IDs to the port that will participate in the protocol.

```
config
  interface 0/4
  ip vrrp 20
```

Specify the IP address that the virtual router function will recognize. Since the virtual IP address on port 0/4 is the same as Router 1's port 0/2 actual IP address, this router will always be the VRRP backup when Router 1 is active.

```
  ip vrrp 20 ip 192.150.2.1
```

Set the priority for the port. The default priority is 100.

```
  ip vrrp 20 priority 254
```

Enable VRRP on the port.

```
ip vrrp 20 mode
exit
```

Using the Web Interface to Configure VRRP

Use the following screens to perform the same configuration using the Graphical User Interface:

To enable routing for the switch, use the **LAN > L3 Features > IP > Configuration** page.

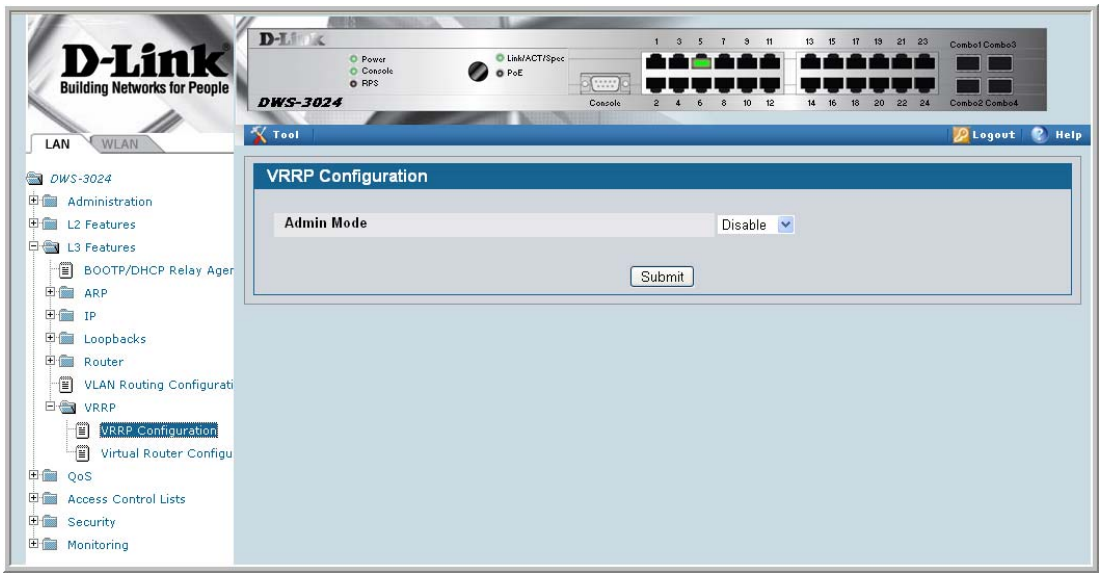
Figure 42. IP Configuration

To enable routing for the ports and configure their IP addresses and subnet masks, use the **LAN> L3 Features > IP > Interface Configuration** page.

Figure 43. IP Interface Configuration

To enable VRRP for the switch, use the **LAN> L3 Features > VRRP > VRRP Configuration** page.

Figure 44. VRRP Configuration



To configure virtual router settings, use the **LAN> L3 Features > VRRP > Virtual Router Configuration** page.

Figure 45. Virtual Router Configuration

15

Proxy Address Resolution Protocol (ARP)

This section describes the Proxy Address Resolution Protocol (ARP) feature.

Overview

- Proxy ARP allows a router to answer ARP requests where the target IP address is not the router itself but a destination that the router can reach.
- If a host does not know the default gateway, proxy ARP can learn the first hop.
- Machines in one physical network appear to be part of another logical network.
- Without proxy ARP, a router responds to an ARP request only if the target IP address is an address configured on the interface where the ARP request arrived.

CLI Examples

The following are examples of the commands used in the proxy ARP feature.

Example #1 show ip interface

```
(DWS-3024) #show ip interface ?

<slot/port>             Enter an interface in slot/port format.
brief                   Display summary information about IP configuration
                        settings for all ports.
loopback                Display the configured Loopback interface information.

(DWS-3024) #show ip interface 0/24

Routing Mode................................... Disable
Administrative Mode............................ Enable
Forward Net Directed Broadcasts................ Disable
Proxy ARP...................................... Enable
Active State................................... Inactive
Link Speed Data Rate........................... Inactive
MAC Address.................................... 00:10:18:82:06:5F
Encapsulation Type............................. Ethernet
IP MTU......................................... 1500
```

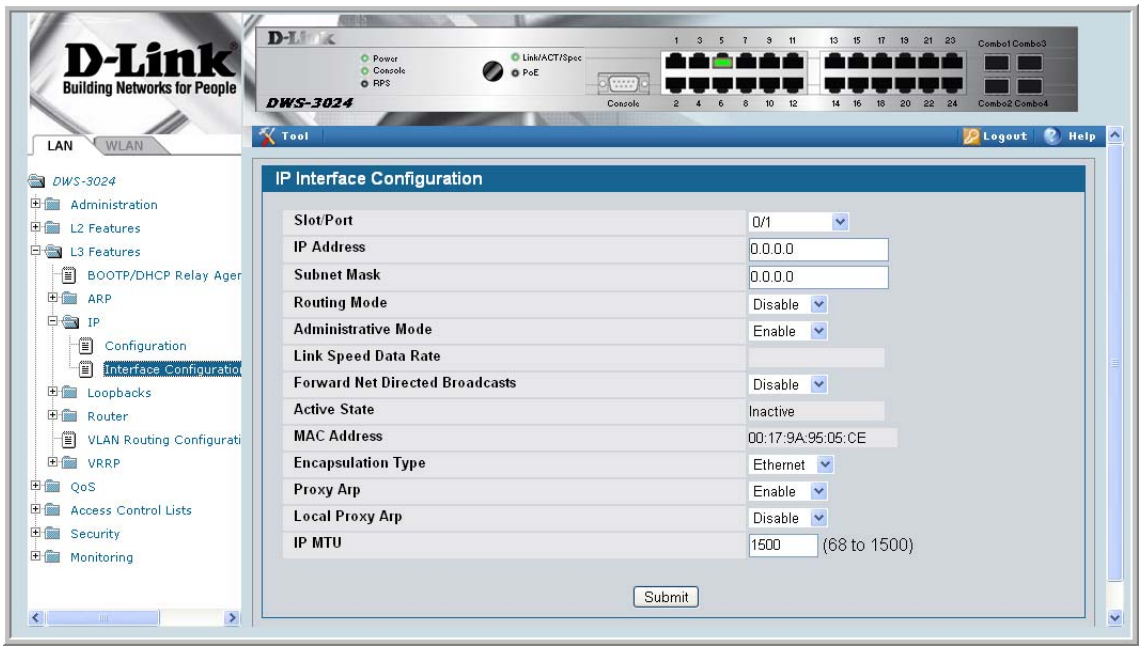
Example #2: ip proxy-arp

```
DWS-3024) (Interface 0/24)#ip proxy-arp ?

<cr>                        Press Enter to execute the command.

(DWS-3024) (Interface 0/24)#ip proxy-arp
```

Web Example

The following web pages are used in the proxy ARP feature.

Figure 46. Proxy ARP Configuration



16

Access Control Lists (ACLs)

This section describes the Access Control Lists (ACLs) feature.

Overview

Access Control Lists (ACLs) are a collection of permit and deny conditions, called rules, that provide security by blocking unauthorized users and allowing authorized users to access specific resources. Normally ACLs reside in a firewall router or in a router connecting two internal networks.

ACL Logging provides a means for counting the number of “hits” against an ACL rule. When you configure ACL Logging, you augment the ACL deny rule specification with a ‘log’ parameter that enables hardware hit count collection and reporting. The D-Link DWS-3000 switch uses a fixed five minute logging interval, at which time trap log entries are written for each ACL logging rule that accumulated a non-zero hit count during that interval. You cannot configure the logging interval.

You can set up ACLs to control traffic at Layer 2, Layer 3, or Layer 4. MAC ACLs operate on Layer 2. IP ACLs operate on Layers 3 and 4.

Limitations

The following limitations apply to ACLs.

- Maximum of 100 ACLs.
- Maximum rules per ACL is 10.
- The system supports ACLs set up for inbound traffic only.
- The system does not support MAC ACLs and IP ACLs on the same interface.
- It may not be possible to log every ACL rule due to limited hardware counter resources. You can define an ACL with any number of logging rules, but the number of rules that are actually logged cannot be determined until the ACL is applied to an interface. Furthermore, hardware counters that become available after an ACL is applied are not retroactively assigned to rules that were unable to be logged (the ACL must be un-applied then re-applied). Rules that are unable to be logged are still active in the ACL for purposes of permitting or denying a matching packet.

- The order of the rules is important: when a packet matches multiple rules, the first rule takes precedence. Also, once you define an ACL for a given port, all traffic not specifically permitted by the ACL is denied access.

MAC ACLs

MAC ACLs are Layer 2 ACLs. You can configure the rules to inspect the following fields of a packet:

- Source MAC address
- Source MAC mask
- Destination MAC address
- Destination MAC mask
- VLAN ID
- Class of Service (CoS) (802.1p)
- Ethertype

L2 ACLs can apply to one or more interfaces.

Multiple access lists can be applied to a single interface - sequence number determines the order of execution.

You can assign packets to queues using the assign queue option.

IP ACLs

IP ACLs classify for Layers 3 and 4.

Each ACL is a set of up to ten rules applied to inbound traffic. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network, and may apply to one or more of the following fields within a packet:

- Destination IP with wildcard mask
- Destination L4 Port
- Every Packet
- IP DSCP
- IP Precedence
- IP TOS
- Protocol
- Source IP with wildcard mask
- Source L4 port
- Destination Layer 4 port

ACL Configuration Process

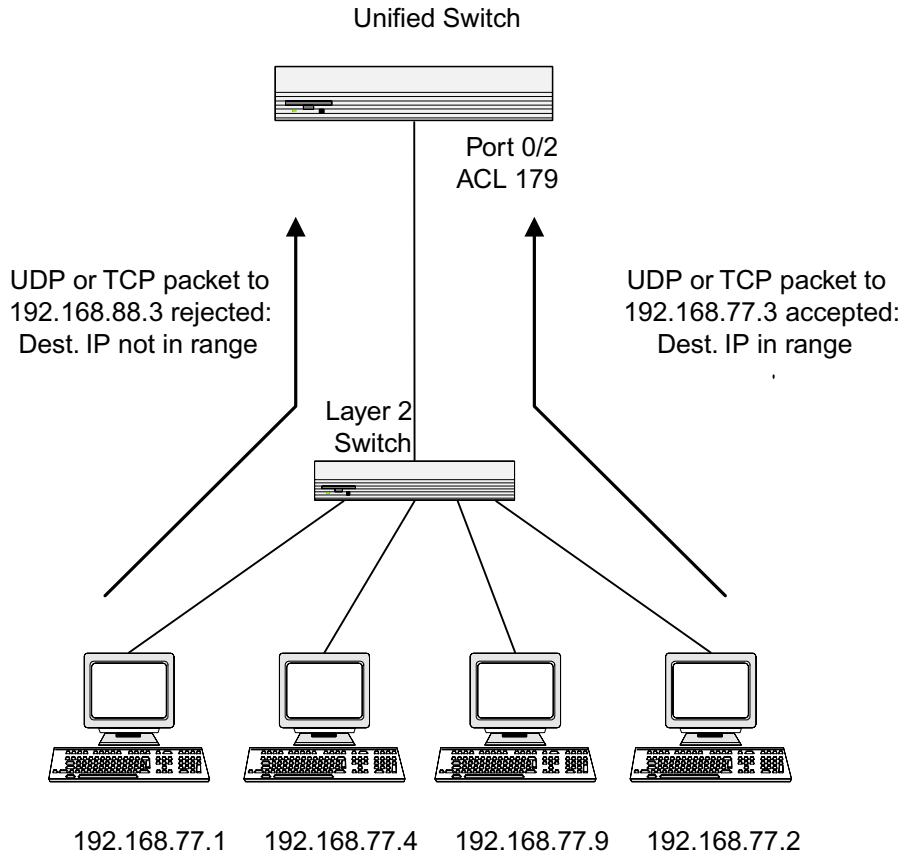
To configure ACLs, follow these steps:

- Create a MAC ACL by specifying a name.
- Create an IP ACL by specifying a number.
- Add new rules to the ACL.
- Configure the match criteria for the rules.
- Apply the ACL to one or more interfaces.

IP ACL CLI Example

The script in this section shows you how to set up an IP ACL with two rules, one applicable to TCP traffic and one to UDP traffic. The content of the two rules is the same. TCP and UDP packets will only be accepted by the Unified Switch if the source and destination stations have IP addresses that fall within the defined sets.

Figure 47. IP ACL Example Network Diagram



Example #1: Create ACL 179 and Define an ACL Rule

After the mask has been applied, it permits packets carrying TCP traffic that matches the specified Source IP address, and sends these packets to the specified Destination IP address.

```
config
access-list 179 permit tcp 192.168.77.0 0.0.0.255 192.168.77.3 0.0.0.0
```

Example #2: Define the Second Rule for ACL 179

Define the rule to set similar conditions for UDP traffic as for TCP traffic.

```
access-list 179 permit udp 192.168.77.0 0.0.0.255 192.168.77.3 0.0.0.255
exit
```

Example #3: Apply the rule to Inbound Traffic on Port 0/2

Only traffic matching the criteria will be accepted.

```
interface 0/2
  ip access-group 179 in
exit
```

MAC ACL CLI Examples

The following are examples of the commands used for the MAC ACLs feature.

Example #4: Set up a MAC Access List

```
(DWS-3024)(Config)#mac access-list ?

extended                              Configure extended MAC Access List parameters.

DWS-3024)(Config)#mac access-list extended ?

<name>                                Enter access-list name up to 31 characters
                                      in length.

rename                                Rename MAC Access Control List.

(DWS-3024)(Config)#mac access-list extended mac1 ?

<cr>                                  Press Enter to execute the command.

(DWS-3024) (Config)#mac access-list extended mac1
```


Example #5: Specify MAC ACL Attributes

```
(DWS-3024) (Config)#mac access-list extended mac1

(DWS-3024) (Config-mac-access-list)#deny ?

<srcmac>                Enter a MAC Address.
any                     Configure a match condition for all the source MAC
                        addresses in the Source MAC Address field.

(DWS-3024) (Config-mac-access-list)#deny any ?

<dstmac>                Enter a MAC Address.
any                     Configure a match condition for all the destination
                        MAC addresses in the Destination MAC Address field.
bpdu                    Match on any BPDU destination MAC Address.

(DWS-3024) (Config-mac-access-list)#deny any 00:11:22:33:44:55 ?

<dstmacmask>            Enter a MAC Address bit mask.

(DWS-3024) (Config-mac-access-list)#deny any 00:11:22:33:44:55 00
:00:00:00:FF:FF ?

<ethertypekey>          Enter one of the following keywords to specify an
                        Ethertype (appletalk, arp, ibmsna, ipv4, ipv6, ipx,
                        mplsmcast, mplsucast, netbios, novell, pppoe, rarp).
<0x0600-0xffff>         Enter a four-digit hexadecimal number in the range of
                        0x0600 to 0xffff to specify a custom Ethertype value.
vlan                    Configure a match condition based on a VLAN ID.
cos                     Configure a match condition based on a COS value.
log                     Configure logging for this access list rule.
assign-queue            Configure the Queue Id assignment attribute.
<cr>                    Press Enter to execute the command.

(DWS-3024) (Config-mac-access-list)#deny any 00:11:22:33:44:55 00:00:00:00:FF:FF log ?
assign-queue            Configure the Queue Id assignment attribute.
<cr>                    Press Enter to execute the command.

(DWS-3024) (Config-mac-access-list)#deny any 00:11:22:33:44:55 00:00:00:00:FF:FF log

(DWS-3024) (Config-mac-access-list)#exit

(DWS-3024) (Config)#exit

(DWS-3024) #
```

Example #6 Configure MAC Access Group

```
(DWS-3024)                (Config)#interface 0/5

(DWS-3024)                (Interface 0/5)#mac ?

access-group              Attach MAC Access List to Interface.

(DWS-3024)                (Interface 0/5)#mac access-group ?

<name>                    Enter name of MAC Access Control List.

(DWS-3024)                (Interface 0/5)#mac access-group mac1 ?

in                        Enter the direction <in>.

(DWS-3024)                (Interface 0/5)#mac access-group mac1 in ?

<cr>                      Press Enter to execute the command.
<1-4294967295>            Enter the sequence number (greater than 0) to
                          rank direction.  A lower sequence number
                          has higher precedence.

(DWS-3024) (Interface 0/5)#mac access-group mac1 in 6 ?

<cr>                      Press Enter to execute the command.

(DWS-3024) (Interface 0/5)#mac access-group mac1 in 6


(DWS-3024) (Interface 0/5)#exit

(DWS-3024) (Config)#exit

(DWS-3024) #
```


Example #7 Set up an ACL with Permit Action

```
(DWS-3024) (Config)#mac access-list extended mac2

(DWS-3024) (Config-mac-access-list)#permit ?

<srcmac>                Enter a MAC Address.
any                     Configure a match condition for all the source MAC
                        addresses in the Source MAC Address field.

(DWS-3024) (Config-mac-access-list)#permit any ?

<dstmac>                Enter a MAC Address.
any                     Configure a match condition for all the destination
                        MAC addresses in the Destination MAC Address field.
bpdu                    Match on any BPDU destination MAC Address.

(DWS-3024) (Config-mac-access-list)#permit any any ?

<ethertypekey>          Enter one of the following keywords to specify an
                        Ethertype (appletalk, arp, ibmsna, ipv4, ipv6, ipx,
                        mplsmcast, mplsucast, netbios, novell, pppoe, rarp).
<0x0600-0xffff>         Enter a four-digit hexadecimal number in the range of
                        0x0600 to 0xffff to specify a custom Ethertype value.
vlan                    Configure a match condition based on a VLAN ID.
cos                     Configure a match condition based on a COS value.
log                     Configure logging for this access list rule.
assign-queue            Configure the Queue Id assignment attribute.
<cr>                    Press Enter to execute the command.

(DWS-3024) (Config-mac-access-list)#permit any any

(DWS-3024) (Config-mac-access-list)#
```

Example #8: Show MAC Access Lists

```
(DWS-3024)                          #show mac access-lists
Current number of all ACLs: 2       Maximum number of all ACLs: 100

MAC ACL Name Rules Direction Interface(s)
------------ ----- --------- ------------
mac1         1     inbound   0/5
mac2         1

(DWS-3024) #show mac access-lists mac1

MAC ACL Name: mac1


Rule Number: 1
Action..................................... deny
Destination MAC Address.................... 00:11:22:33:44:55
Destination MAC Mask....................... 00:00:00:00:FF:FF
Log........................................ TRUE

(DWS-3024) #
```

Web Examples

Use the Web pages in this section to configure and view MAC access control list and IP access control lists.

MAC ACL Web Pages

The following figures show the pages available to view and configure MAC ACL settings.

Figure 48. MAC ACL Configuration Page - Create New MAC ACL

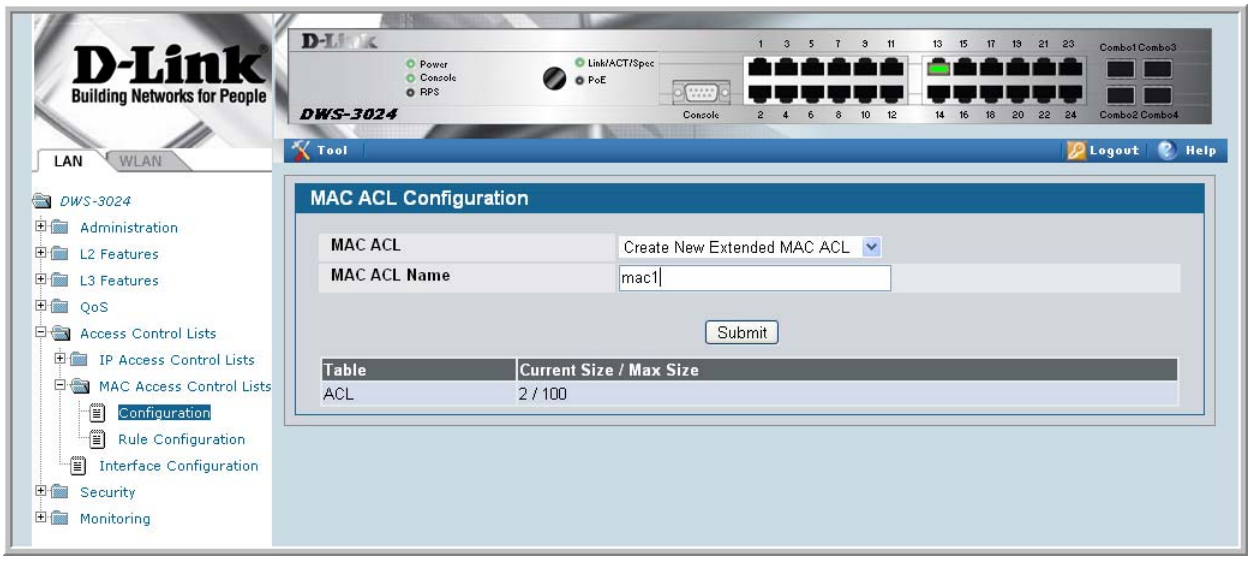


Figure 49. MAC ACL Rule Configuration - Create New Rule

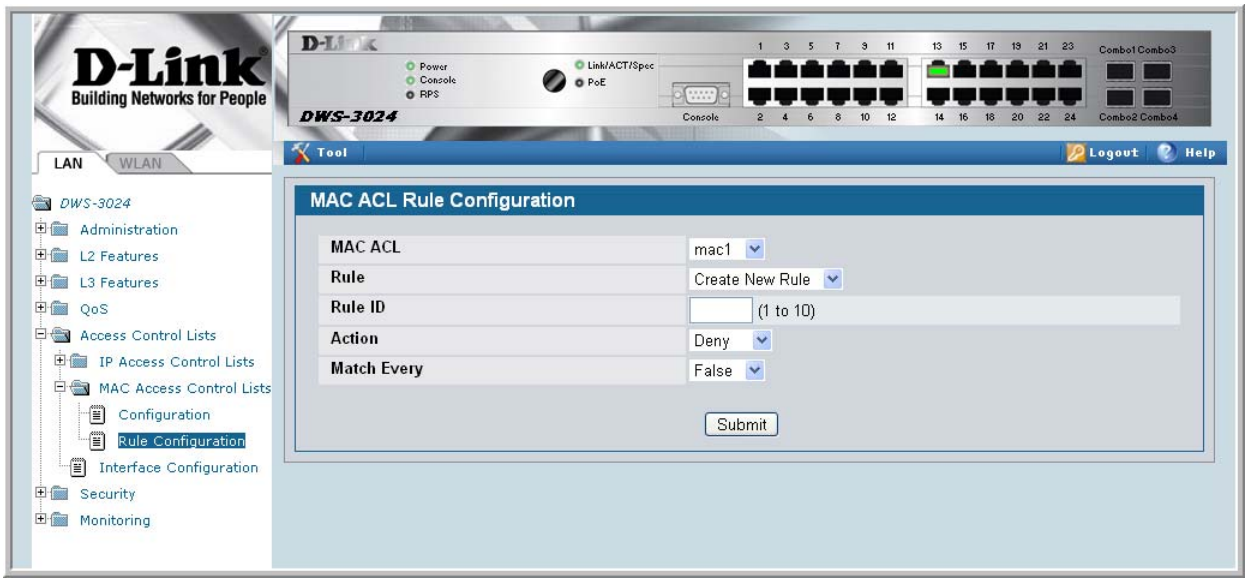


Figure 50. MAC ACL Rule Configuration Page - Add Destination MAC and MAC Mask

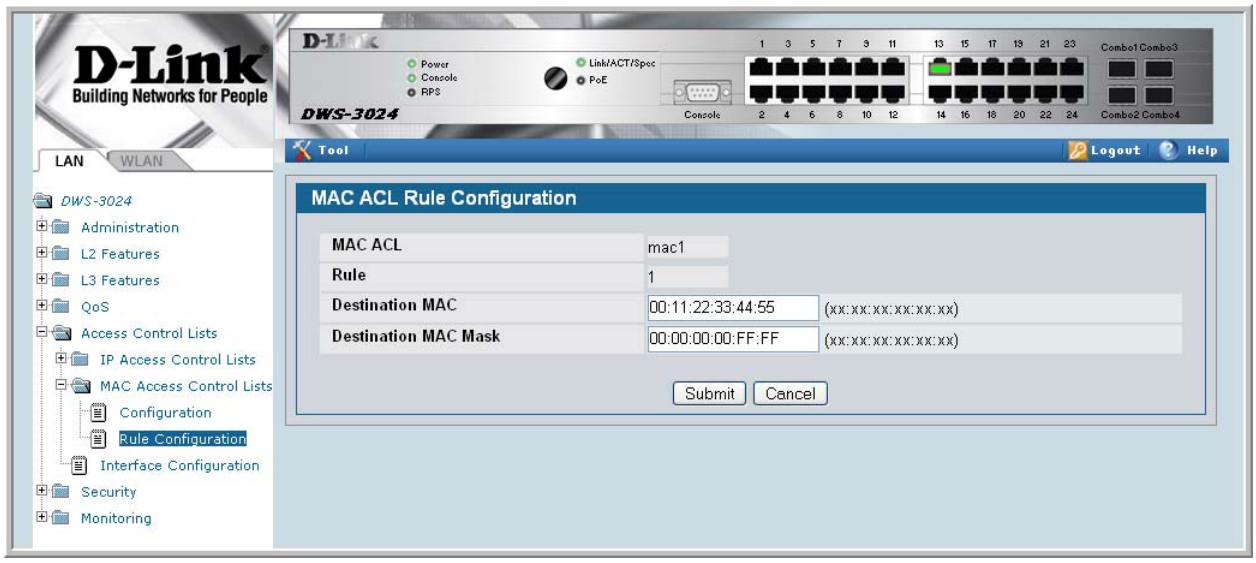


Figure 51. MAC ACL Rule Configuration Page - View the Current Settings

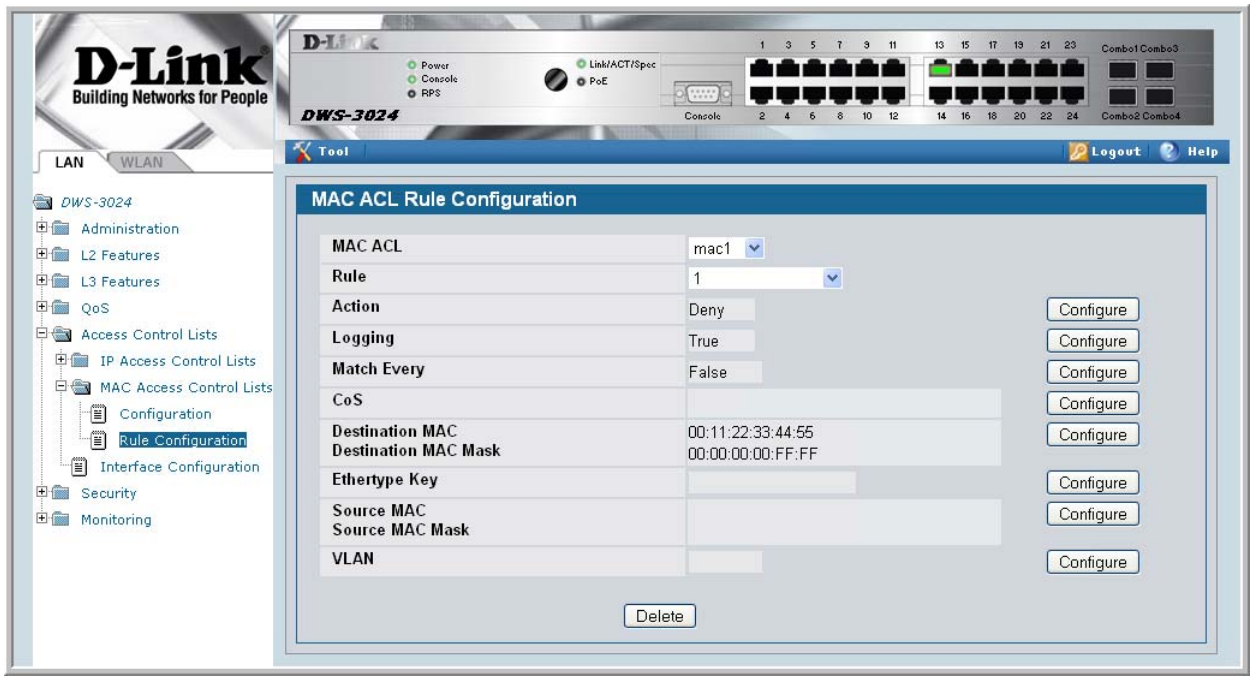


Figure 52. ACL Interface Configuration

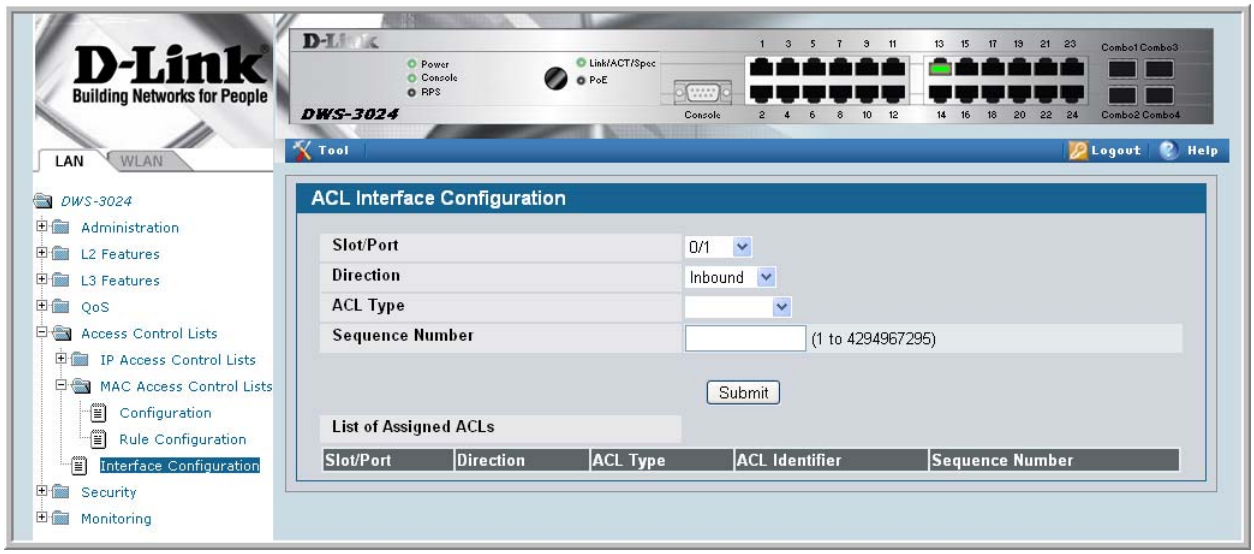
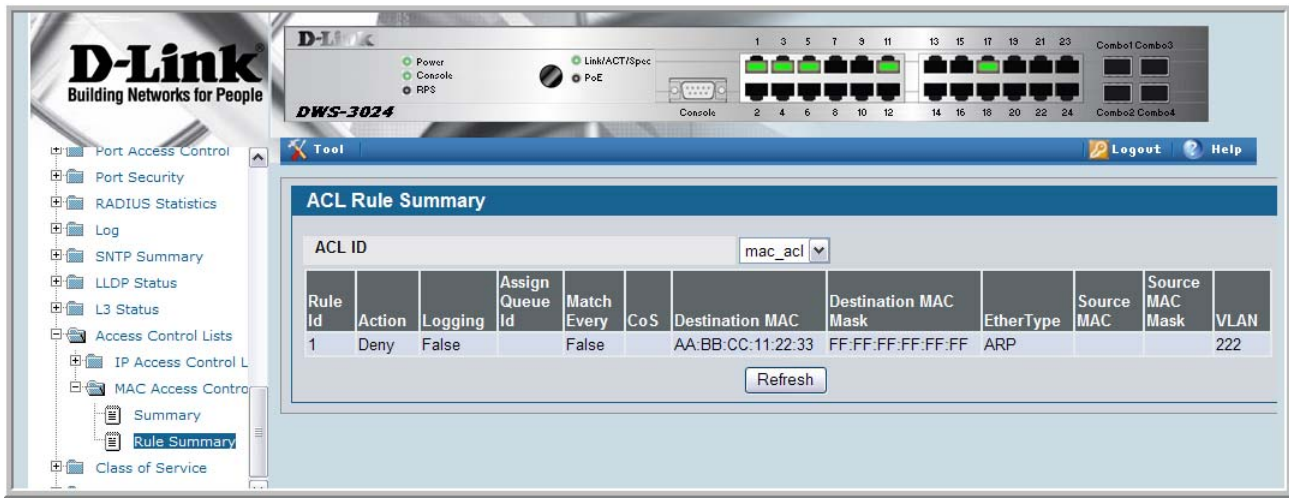


Figure 53. MAC ACL Summary

Figure 54. MAC ACL Rule Summary



IP ACL Web Pages

The following figures show the pages available to view and configure standard and extended IP ACL settings.

Figure 55. IP ACL Configuration Page - Create a New IP ACL

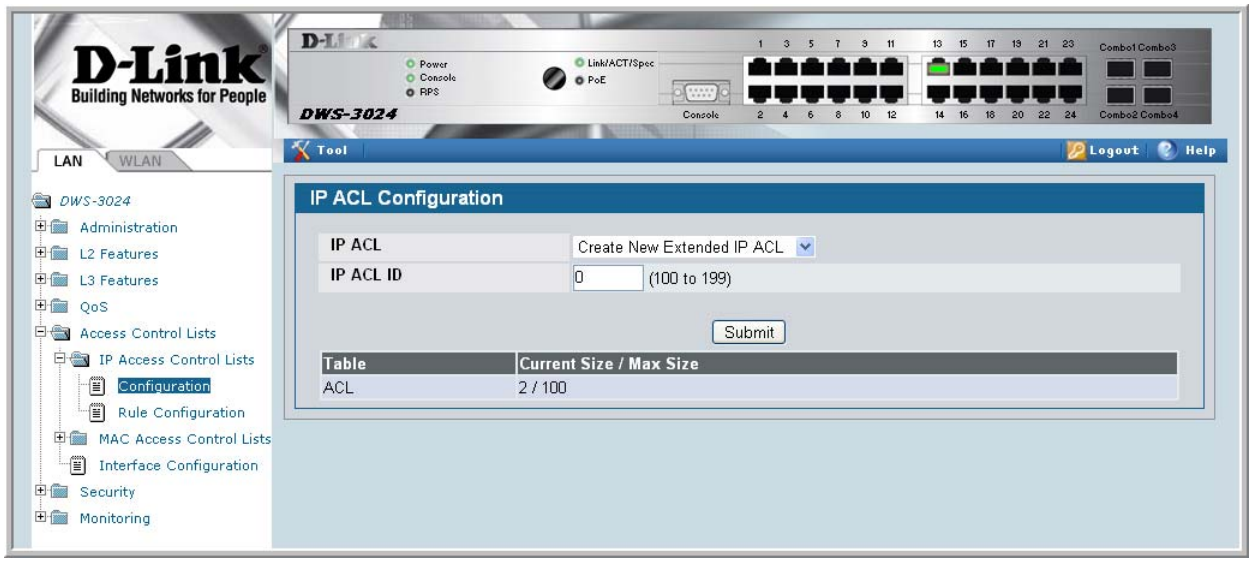


Figure 56. IP ACL Configuration Page - Create a Rule and Assign an ID

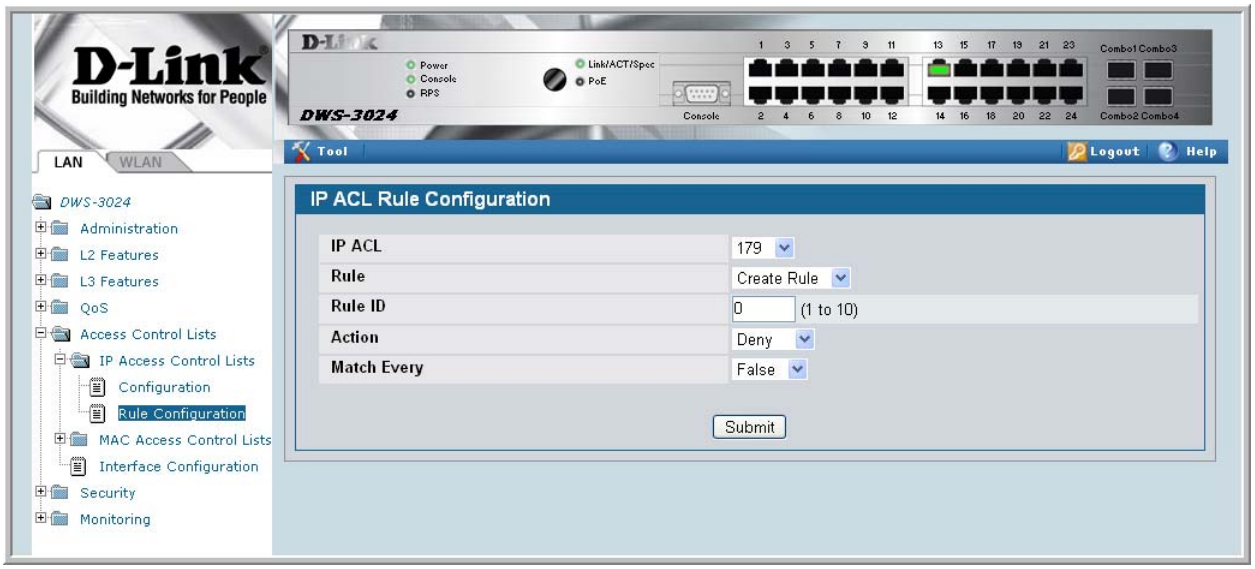


Figure 57. IP ACL Rule Configuration Page - Rule with Protocol and Source IP Configuration

Figure 58. Attach IP ACL to an Interface

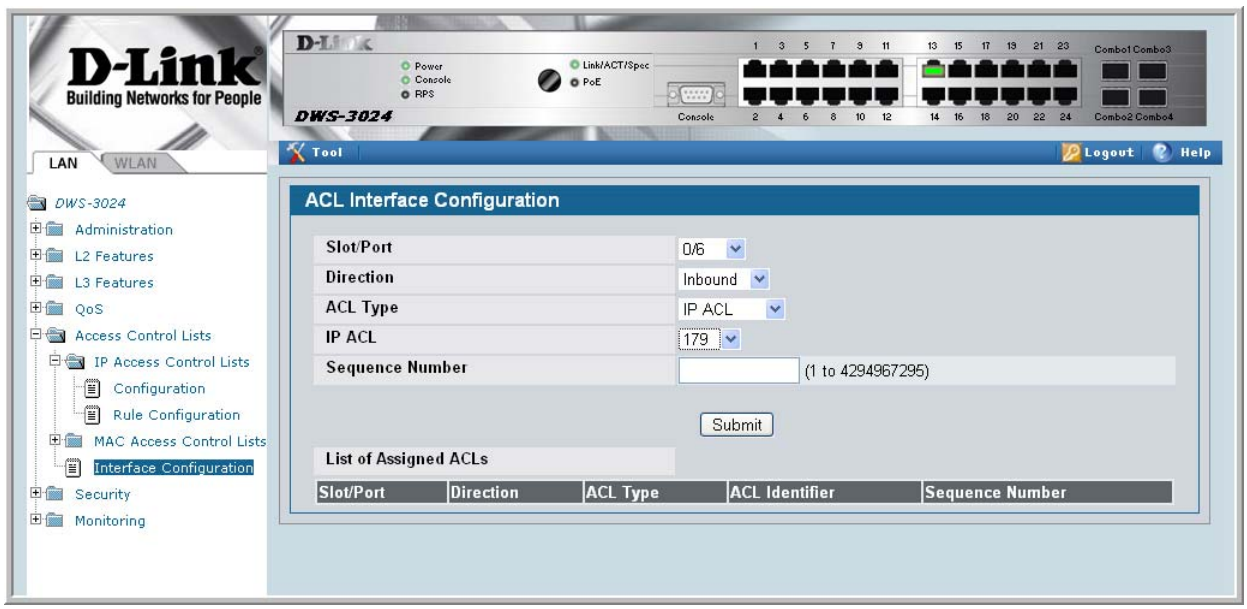
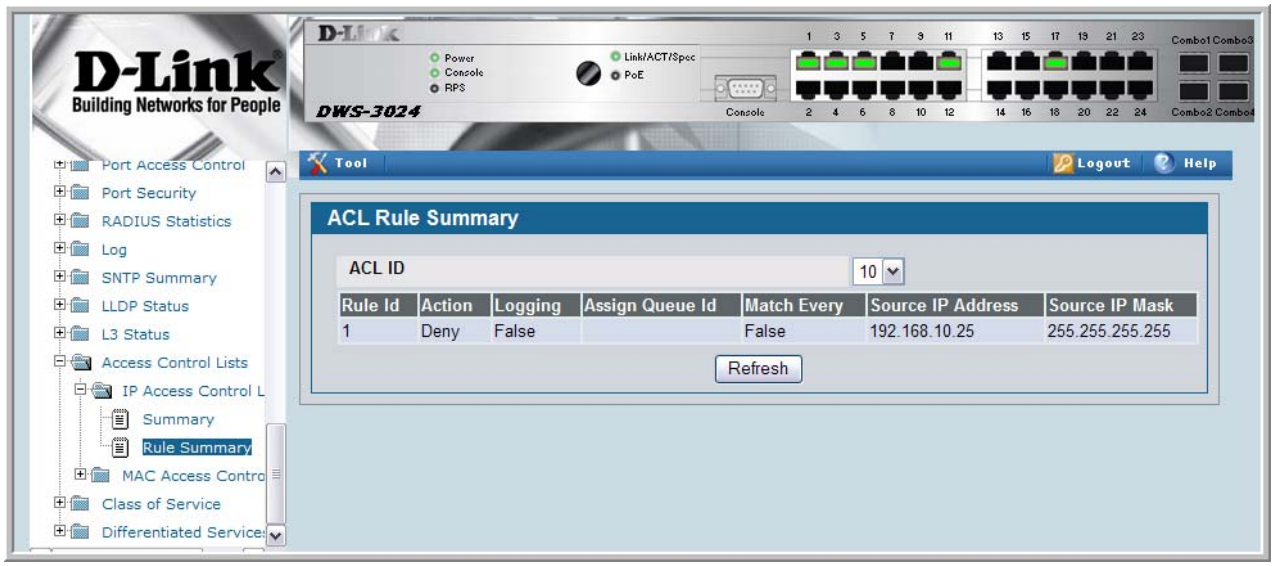


Figure 59. IP ACL Summary

Figure 60. IP ACL Rule Summary



17

Class of Service Queuing

The Class of Service (CoS) feature lets you give preferential treatment to certain types of traffic over others. To set up this preferential treatment, you can configure the ingress ports, the egress ports, and individual queues on the egress ports to provide customization that suits your environment.

The level of service is determined by the egress port queue to which the traffic is assigned. When traffic is queued for transmission, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in other queues for that port.

Some traffic is classified for service (i.e., packet marking) before it arrives at the switch. If you decide to use these classifications, you can map this traffic to egress queues by setting up a CoS Mapping table.

Ingress Port Configuration

Each ingress port on the switch has a default priority value (set by configuring VLAN Port Priority in the Switching sub-menu) that determines the egress queue its traffic gets forwarded to. Packets that arrive without a priority designation, or packets from ports you have identified as “untrusted,” get forwarded according to this default.

Trusted and Untrusted Ports/CoS Mapping Table

The first task for ingress port configuration is to specify whether traffic arriving on a given port is “trusted” or “untrusted.”

A trusted port means that the system will accept at face value a priority designation within arriving packets. You can configure the system to trust priority designations based on one of the following fields in the packet header:

- 802.1 Priority - values 0-7
- IP DSCP - values 0-63
- IP Precedence - values 0-7

You can also configure an ingress port as untrusted, where the system ignores priority designations of incoming packets and sends the packet to a queue based on the ingress port’s default priority.

CoS Mapping Table for Trusted Ports

Mapping is from the designated field values on trusted ports' incoming packets to a traffic class priority (actually a CoS traffic queue). The trusted port field-to-traffic class configuration entries form the Mapping Table the switch uses to direct ingress packets from trusted ports to egress queues.

Egress Port Configuration - Traffic Shaping

For slot/port interfaces, you can specify the shaping rate for the port, which is an upper limit of the transmission bandwidth used, specified as a percentage of the maximum link speed.

Queue Configuration

For each queue, you can specify:

- Minimum bandwidth guarantee
- Scheduler type - strict/weighted - Strict priority scheduling gives an absolute priority, with highest priority queues always sent first, and lowest priority queues always sent last. Weighted scheduling requires a specification of priority for each queue relative to the other queues, based on their minimum bandwidth values
- Queue management - tail drop

Queue Management Type

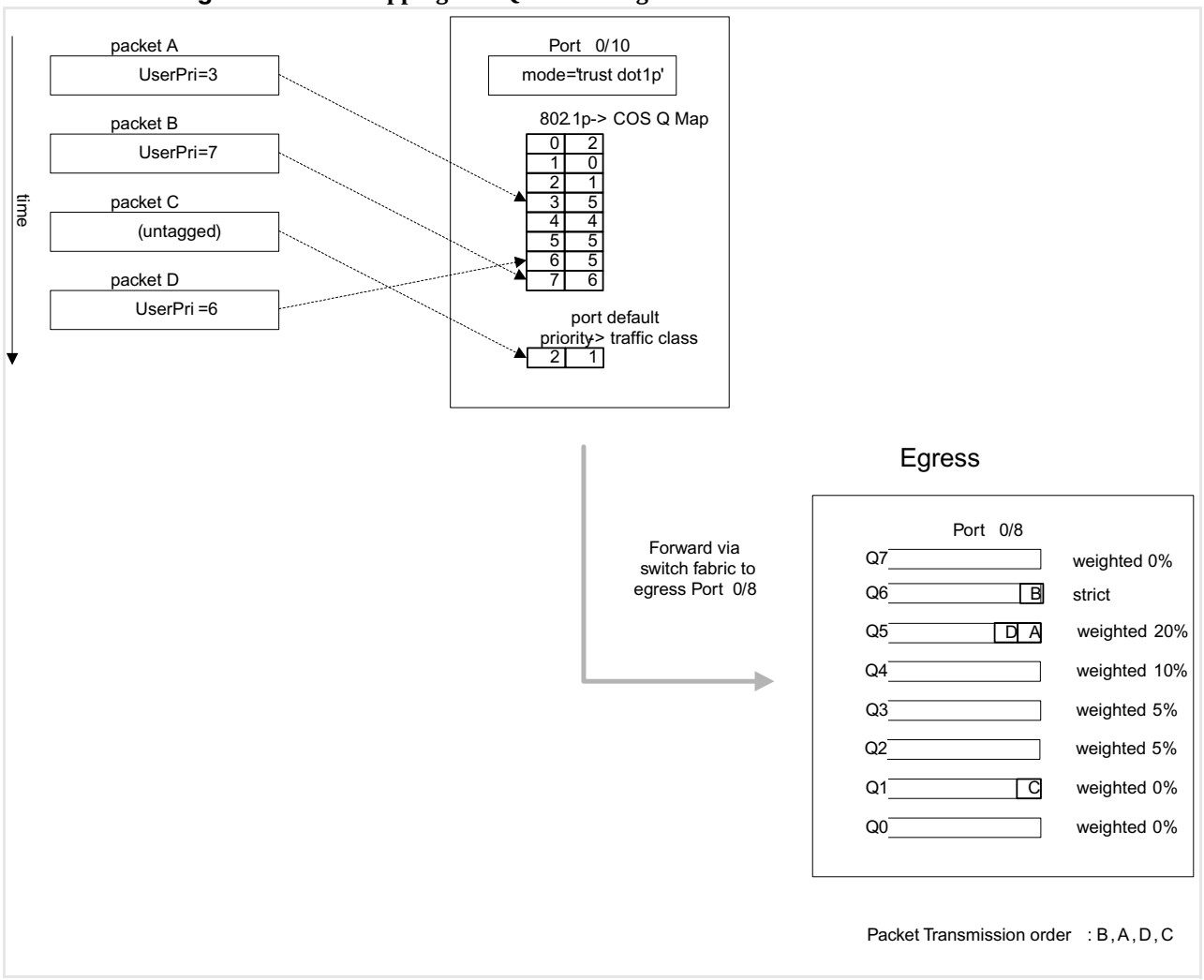
The D-Link DWS-3000 switch supports the tail drop method of queue management. This means that any packet forwarded to a full queue is dropped regardless of its importance.

CLI Examples

Figure 61 illustrates the network operation as it relates to CoS mapping and queue configuration.

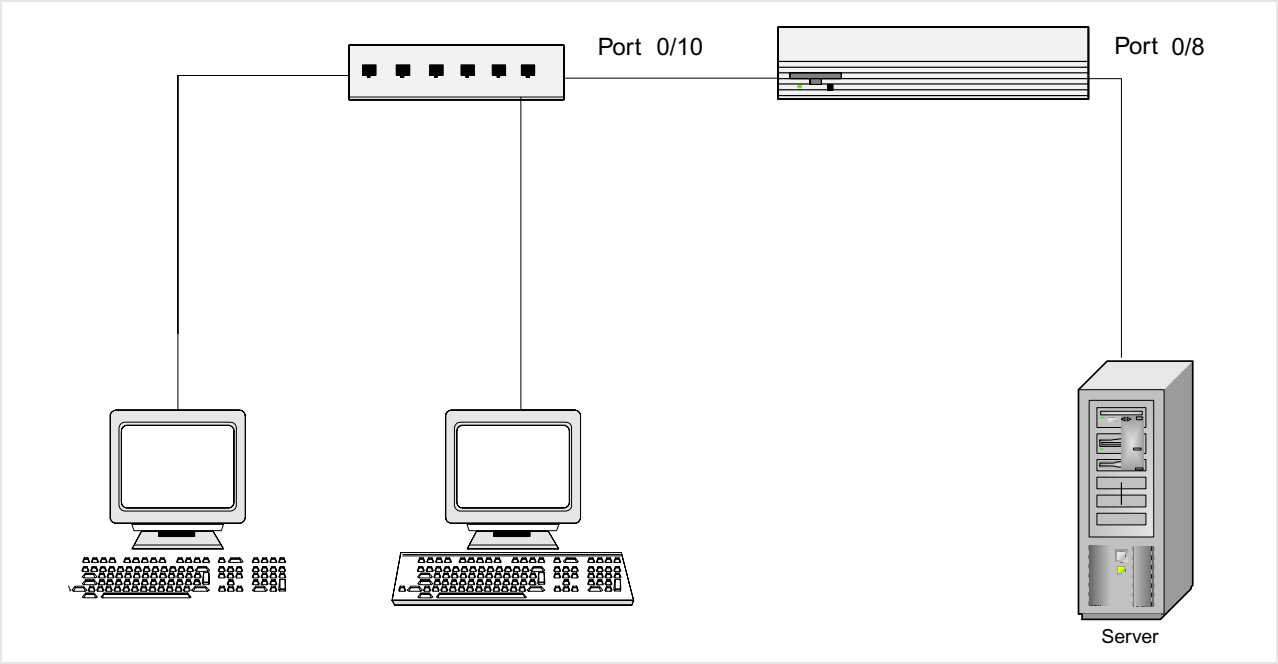
Four packets arrive at the ingress port 0/10 in the order A, B, C, and D. You've configured port 0/10 to trust the 802.1p field of the packet, which serves to direct packets A, B, and D to their respective queues on the egress port. These three packets utilize port 0/10's 802.1p to COS Mapping Table. In this case, the 802.1p user priority 3 was set up to send the packet to queue 5 instead of the default queue 3. Since packet C does not contain a VLAN tag, the 802.1p user priority does not exist, so Port 0/10 relies on its default port priority - 2 - to direct packet C to egress queue 1.

Figure 61. CoS Mapping and Queue Configuration



Continuing this example, you configured the egress Port 0/8 for strict priority on queue 6, and a set a weighted scheduling scheme for queues 5-0. Assuming queue 5 has a higher weighting than queue 1 (relative weight values shown as a percentage, with 0% indicating the bandwidth is not guaranteed), the queue service order is 6 followed by 5 followed by 1. Assuming each queue unloads all packets shown in the diagram, the packet transmission order as seen on the network leading out of Port 0/8 is B, A, D, C. Thus, packet B, with its higher user precedence than the others, is able to work its way through the device with minimal delay and is transmitted ahead of the other packets at the egress port.

Figure 62. CoS Configuration Example System Diagram



You will configure the ingress interface uniquely for all cos-queue and VLAN parameters.

```
configure
        interface  0/10
                classofservice trust dot1p
                classofservice dot1p-mapping 6 3
                vlan priority 2
        exit
        interface  0/8
                cos-queue min-bandwidth 0 0 5 5 10 20 40 0
                cos-queue strict 6
        exit
exit
```

You can also set traffic shaping parameters for the interface. If you wish to shape the egress interface for a sustained maximum data rate of 80 Mbps (assuming a 100Mbps link speed), you would add a simple configuration line expressing the shaping rate as a percentage of link speed.

```
configure
        interface  0/8
                traffic-shape 80
        exit
exit
```


Web Examples

The following web pages are used for the Class of Service feature.

Figure 63. 802.1p Priority Mapping Page

Figure 64. CoS Trust Mode Configuration Page

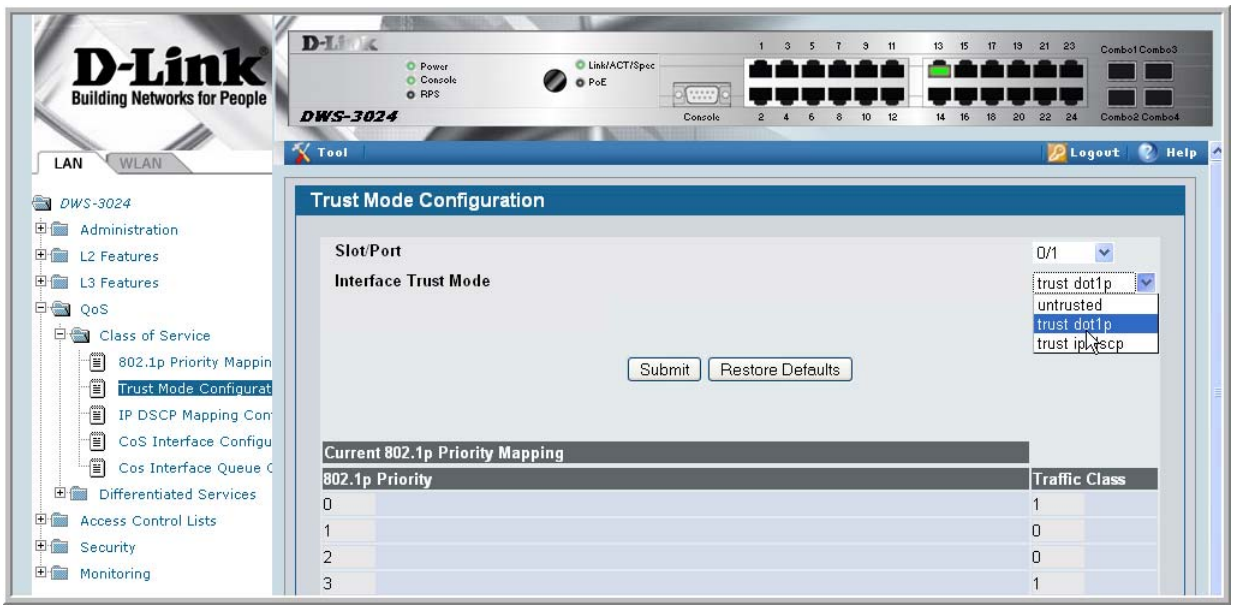


Figure 65. IP DSCP Mapping Configuration Page

Figure 66. CoS Interface Configuration Page

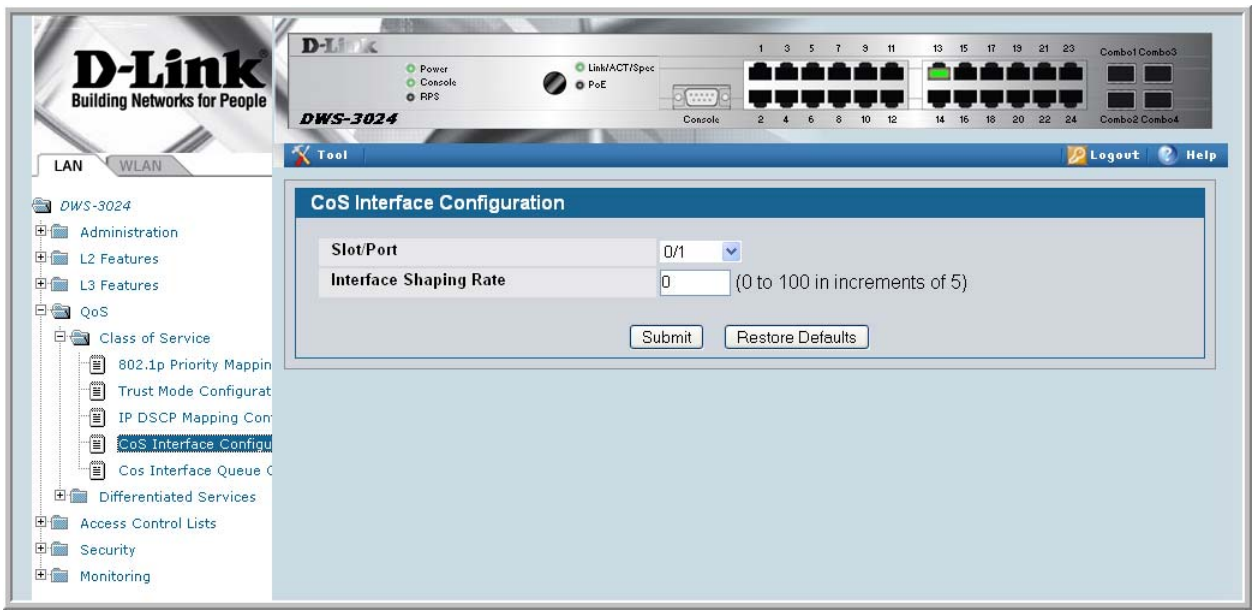


Figure 67. CoS Interface Queue Configuration Page

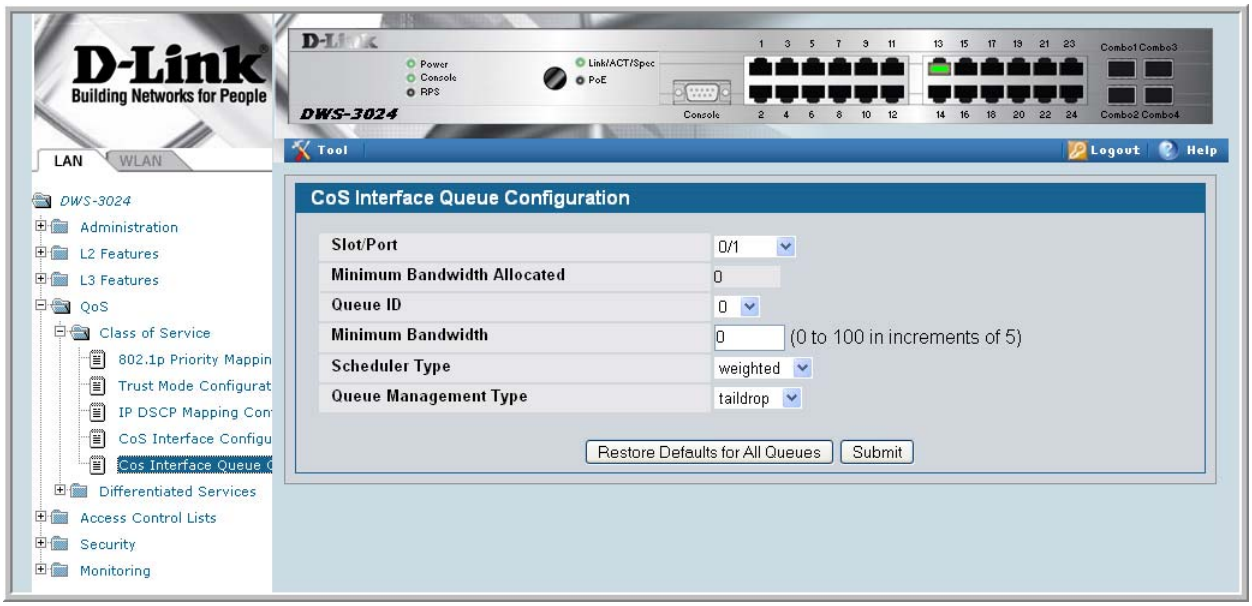
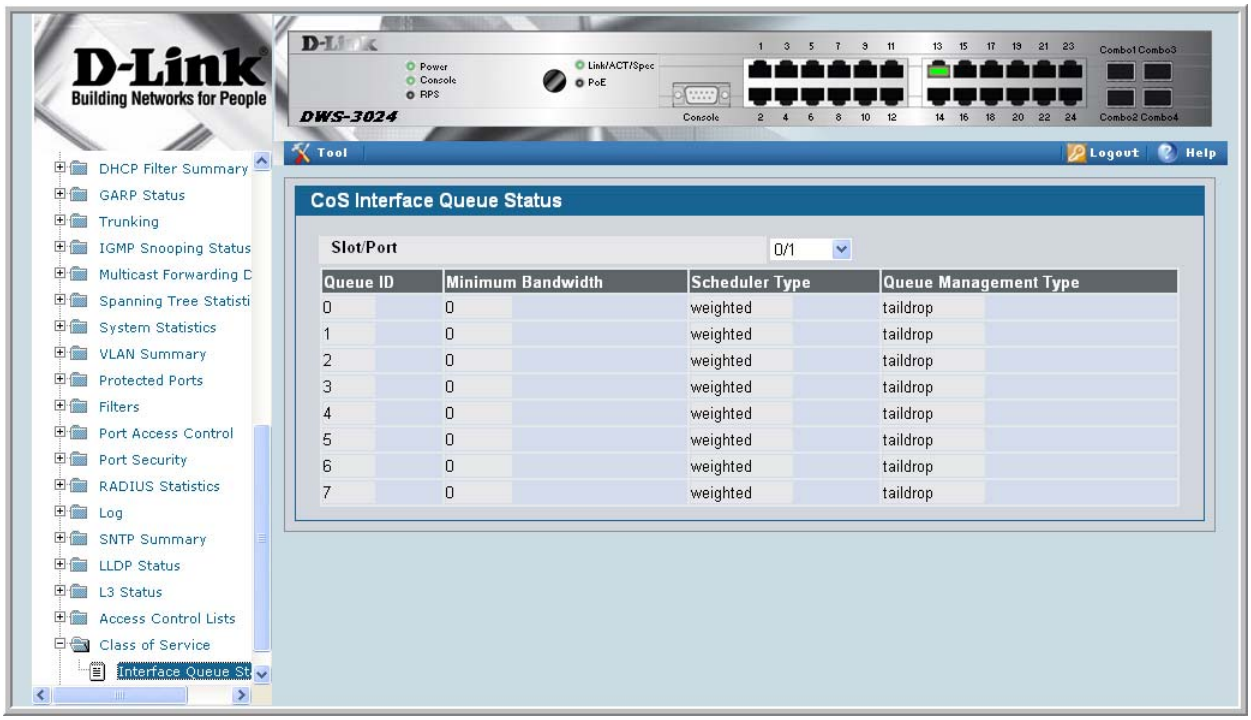


Figure 68. CoS Interface Queue Status Page



18

Differentiated Services

Differentiated Services (DiffServ) is one technique for implementing Quality of Service (QoS) policies. Using DiffServ in your network allows you to directly configure the relevant parameters on the switches and routers rather than using a resource reservation protocol. This section explains how to configure the Unified Switch to identify which traffic class a packet belongs to, and how it should be handled to provide the desired quality of service. As implemented on the Unified Switch, DiffServ allows you to control what traffic is accepted and what traffic is discarded.

Traffic to be processed by the DiffServ feature requires an IP header if the system uses IP Precedence or IP DSCP marking.

How you configure DiffServ support on a DWS-3000 switch varies depending on the role of the switch in your network:

- **Edge device –** An edge device handles ingress traffic, flowing towards the core of the network, and egress traffic, flowing away from the core. An edge device segregates inbound traffic into a small set of traffic classes, and is responsible for determining a packet's classification. Classification is primarily based on the contents of the Layer 3 and Layer 4 headers, and is recorded in the Differentiated Services Code Point (DSCP) added to a packet's IP header.
- **Interior node –** A switch in the core of the network is responsible for forwarding packets, rather than for classifying them. It decodes the DSCP in an incoming packet, and provides buffering and forwarding services using the appropriate queue management algorithms.

Before configuring DiffServ on a particular DWS-3000 switch, you must determine the QoS requirements for the network as a whole. The requirements are expressed in terms of rules, which are used to classify inbound traffic on a particular interface. The D-Link DWS-3000 switch does not support DiffServ in the outbound direction.

During configuration, you define DiffServ rules in terms of classes, policies and services:

- **Class –** A class consists of a set of rules that identify which packets belong to the class. Inbound traffic is separated into traffic classes based on Layer 2, Layer 3, and Layer 4 header data. One class type is supported, **All,** which specifies that every match criterion defined for the class must be true for a match to occur.
- **Policy –** Defines the QoS attributes for one or more traffic classes. An example of an attribute is the ability to mark a packet at ingress. The D-Link DWS-3000 switch supports the ability to assign traffic classes to output CoS queues.

The Unified Switch supports the **Traffic Conditioning Policy** type which is associated with an inbound traffic class and specifies the actions to be performed on packets meeting the class rules:

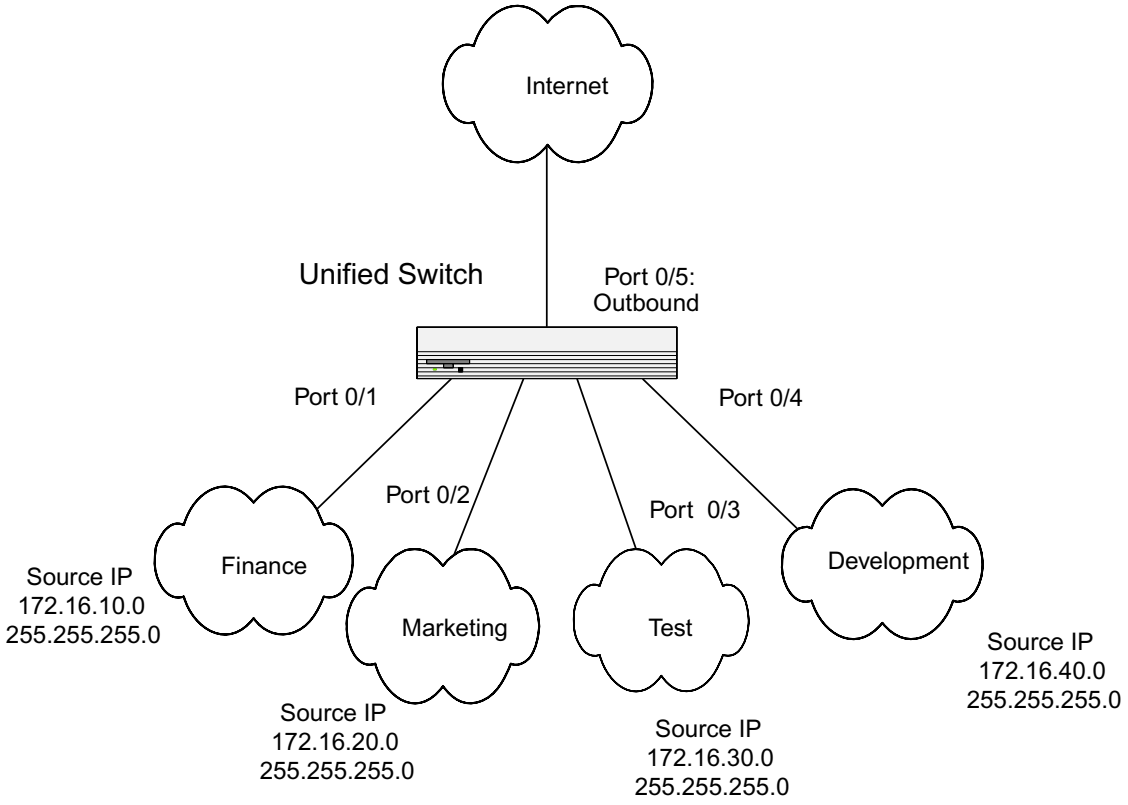
- Marking the packet with a given DSCP, IP precedence, or CoS
- Policing packets by dropping or re-marking those that exceed the class's assigned data rate
- Counting the traffic within the class

- **Service –** Assigns a policy to an interface for inbound traffic.

CLI Example

This example shows how a network administrator can provide equal access to the Internet (or other external network) to different departments within a company. Each of four departments has its own Class B subnet that is allocated 25% of the available bandwidth on the port accessing the Internet.

Figure 69. DiffServ Internet Access Example Network Diagram



DiffServ Inbound Configuration

1. Ensure DiffServ operation is enabled for the switch.

```
config
 diffserv
```


2. Create a DiffServ class of type “all” for each of the departments, and name them. Define the match criteria -- Source IP address -- for the new classes.

```
class-map match-all finance_dept
 match srcip 172.16.10.0 255.255.255.0
exit

class-map match-all marketing_dept
 match srcip 172.16.20.0 255.255.255.0
exit

class-map match-all test_dept
 match srcip 172.16.30.0 255.255.255.0
exit

class-map match-all development_dept
 match srcip 172.16.40.0 255.255.255.0
exit
```

3. Create a DiffServ policy for inbound traffic named 'internet_access', adding the previously created department classes as instances within this policy.

   This policy uses the assign-queue attribute to put each department's traffic on a different egress queue. This is how the DiffServ inbound policy connects to the CoS queue settings established below.

```
policy-map internet_access in
 class finance_dept
   assign-queue 1
 exit
 class marketing_dept
   assign-queue 2
 exit
 class test_dept
   assign-queue 3
 exit
 class development_dept
   assign-queue 4
 exit
exit
```

4. Attach the defined policy to interfaces 0/1 through 0/4 in the inbound direction

```
interface 0/1
 service-policy in internet_access
exit
interface 0/2
 service-policy in internet_access
exit
interface 0/3
 service-policy in internet_access
exit
interface 0/4
 service-policy in internet_access
exit
```

5. Set the CoS queue configuration for the (presumed) egress interface 0/5 such that each of queues 1, 2, 3 and 4 get a minimum guaranteed bandwidth of 25%. All queues for this interface use weighted round robin scheduling by default. The DiffServ inbound policy designates that these queues are to be used for the departmental traffic through the assign-

queue attribute. It is presumed that the switch will forward this traffic to interface 0/5 based on a normal destination address lookup for internet traffic.

```
interface 0/5
 cos-queue min-bandwidth 0 25 25 25 25 0 0 0
exit
exit
```

Adding Color-Aware Policing Attribute

Policing in the DiffServ feature uses either “color blind” or “color aware” mode. Color blind mode ignores the coloration (marking) of the incoming packet. Color aware mode takes into consideration the current packet marking when determining the policing outcome. An auxiliary traffic class is used in conjunction with the policing definition to specify a value for one of the DSCP or IP Precedence fields designating the incoming color value to be used as the conforming color.

The following commands show how to add a color aware policing attribute to the finance_dept class.

1. Add a new class to serve as the auxiliary traffic class. The match condition for the class must be either IP Precedence or IP DSCP. In this example, the match condition is IP Precedence with a value of 2.

   ```
   class-map match-all color_class
    match ip precedence 2
   exit
   ```

2. Before adding the color aware mode, you must configure policing for the finance_dept class.

   The following commands first configure simple policing with a conforming data rate of 10000 Kbps, a burst size of 100, a conform action of send, and a violate action of drop. After the policing is configured, the color aware attribute is configured. The color-aware attribute cannot be configured before policing.

   ```
   policy-map internet_access
    class finance_dept
          police-simple 100000 100 conform-action transmit
          violate-action drop

          conform-color color_class
   ```


3. View information about the DiffServ policy and class configuration. In the following example, the interface specified is interface 0/1. The policy is attached to interfaces 0/1 through 0/4.

```
(DWS-3024) #show diffserv service 0/1 in

DiffServ Admin Mode.......................... Enable
Interface.................................... 0/1
Direction.................................... In
Operational Status........................... Up
Policy Name.................................. internet_access

Class Name................................... finance_dept
Assign Queue................................. 1
Policing Style............................... Police Simple
Committed Rate............................... 100000
Committed Burst Size......................... 100
Conform Action............................... Send
Non-Conform Action........................... Drop
Conform Color Class.......................... color_class
Conform Color Mode........................... Aware IP Precedence
Conform Color IP Precedence Value............ 2

Class Name................................... marketing_dept
Assign Queue................................. 2

Class Name................................... test_dept
Assign Queue................................. 3

Class Name................................... development_dept
Assign Queue................................. 4
```

Using the Web Interface to Configure Diffserv

Access the DiffServ configuration pages from the **LAN > QoS > Differentiated Services** folder. The following DiffServ pages are available:

- DiffServ Configuration
- Class Configuration
- Policy Configuration
- Policy Class Definition
- Service Configuration

View information about the DiffServ classes, policies and services from the **LAN > Monitoring > Differentiated Services** folder. The following DiffServ pages are available:

- Class Summary
- Policy Summary
- Policy Attribute Summary
- Service Summary
- Service Statistics
- Service Detailed Statistics

The following figures shows all of the DiffServ configuring and monitoring pages. The figures also show how to perform the DiffServ example by using the Web Interface.

Figure 70. DiffServ Configuration

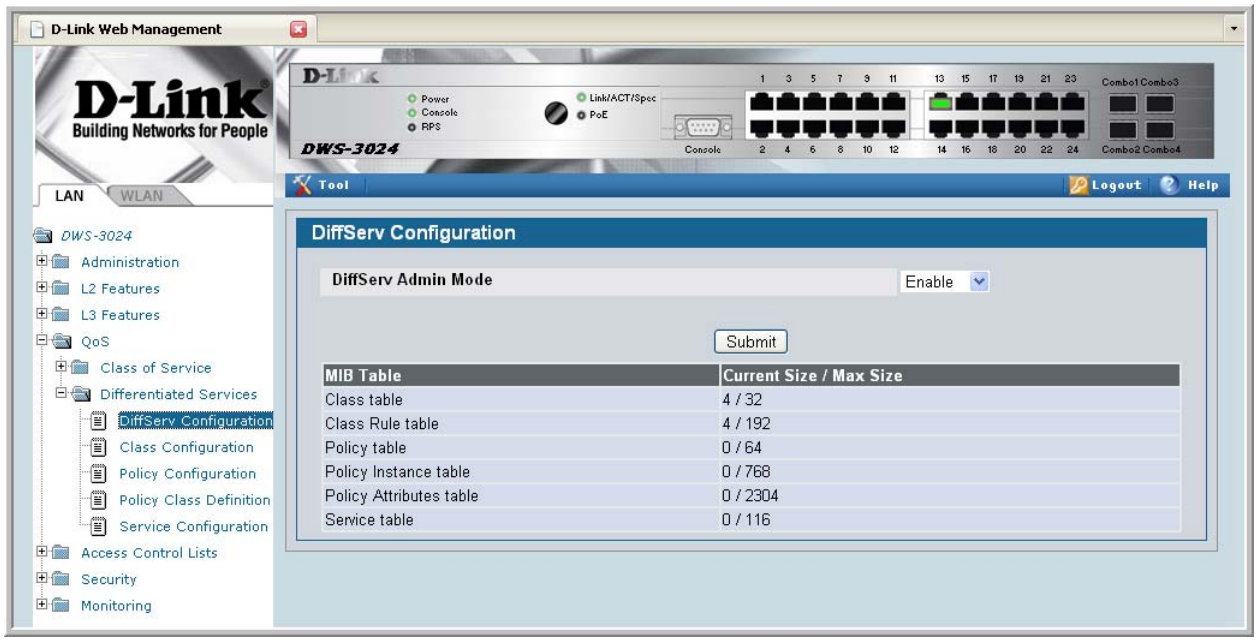


Figure 71. DiffServ Class Configuration

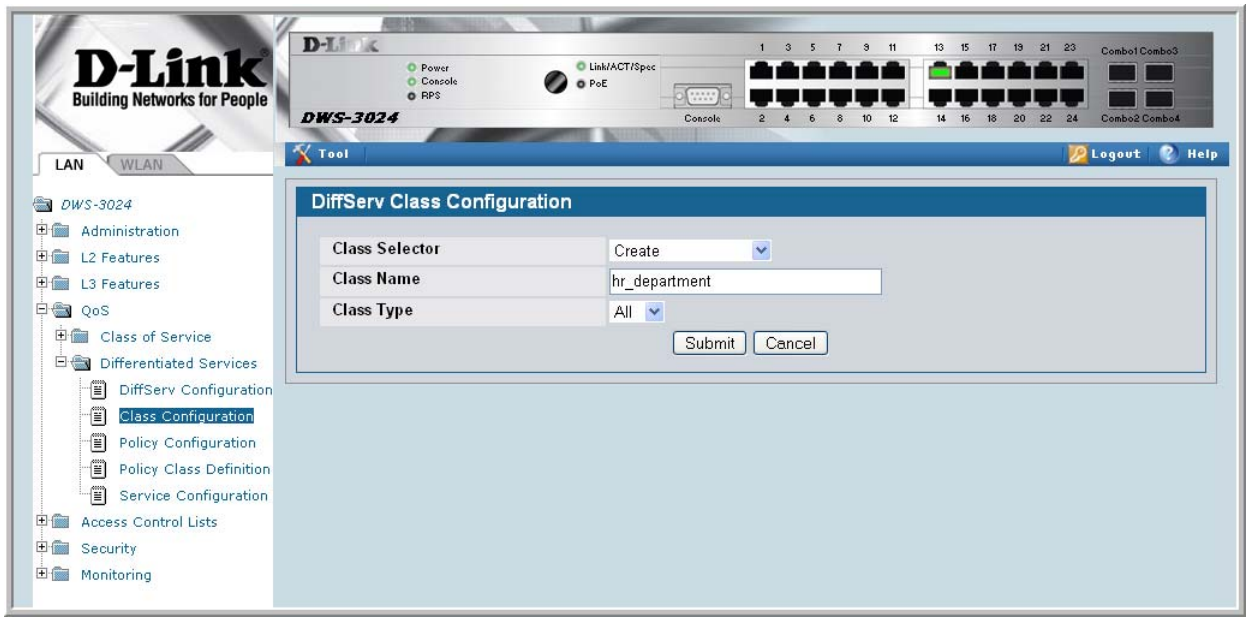


Figure 72. DiffServ Class Configuration - Add Match Criteria

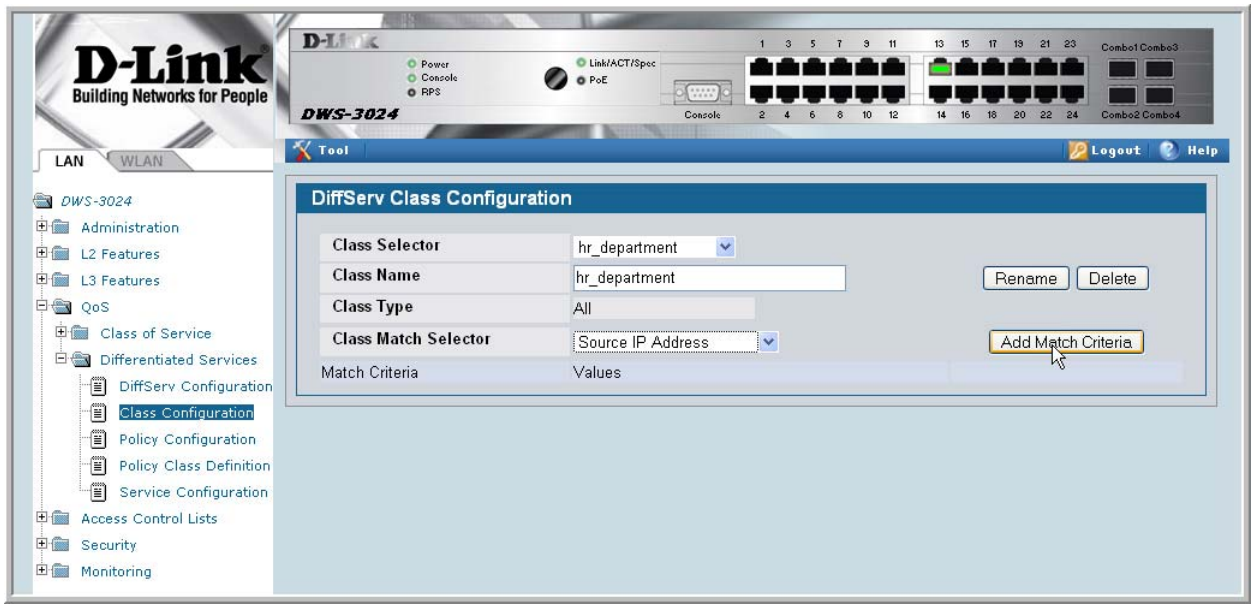


Figure 73. Source IP Address

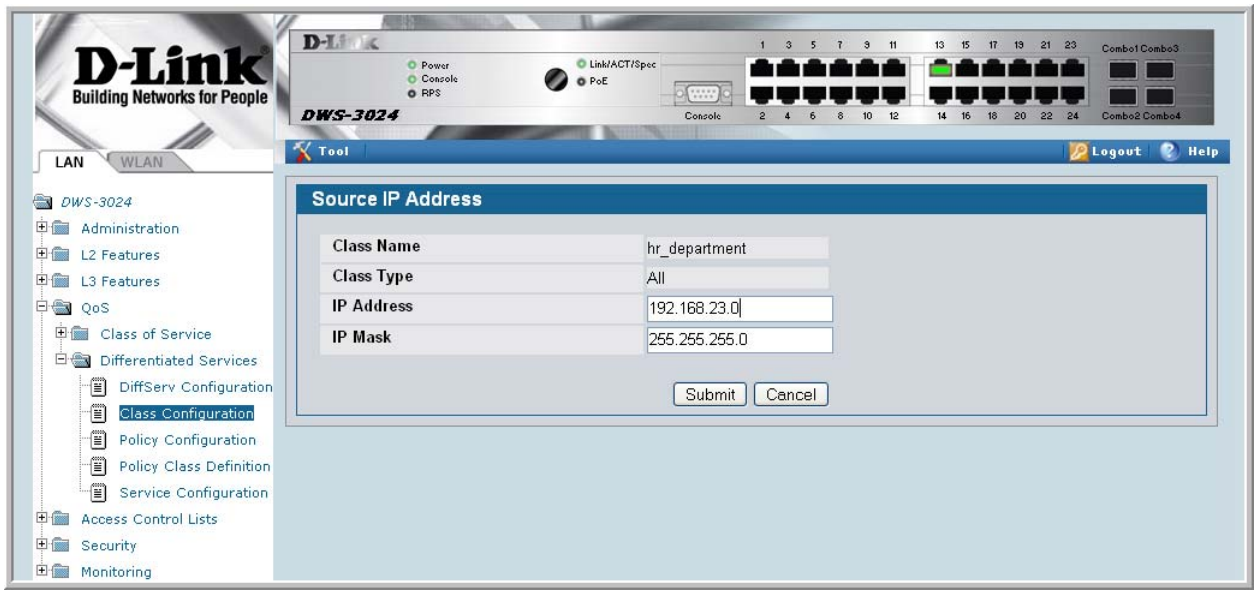


Figure 74. DiffServ Class Configuration

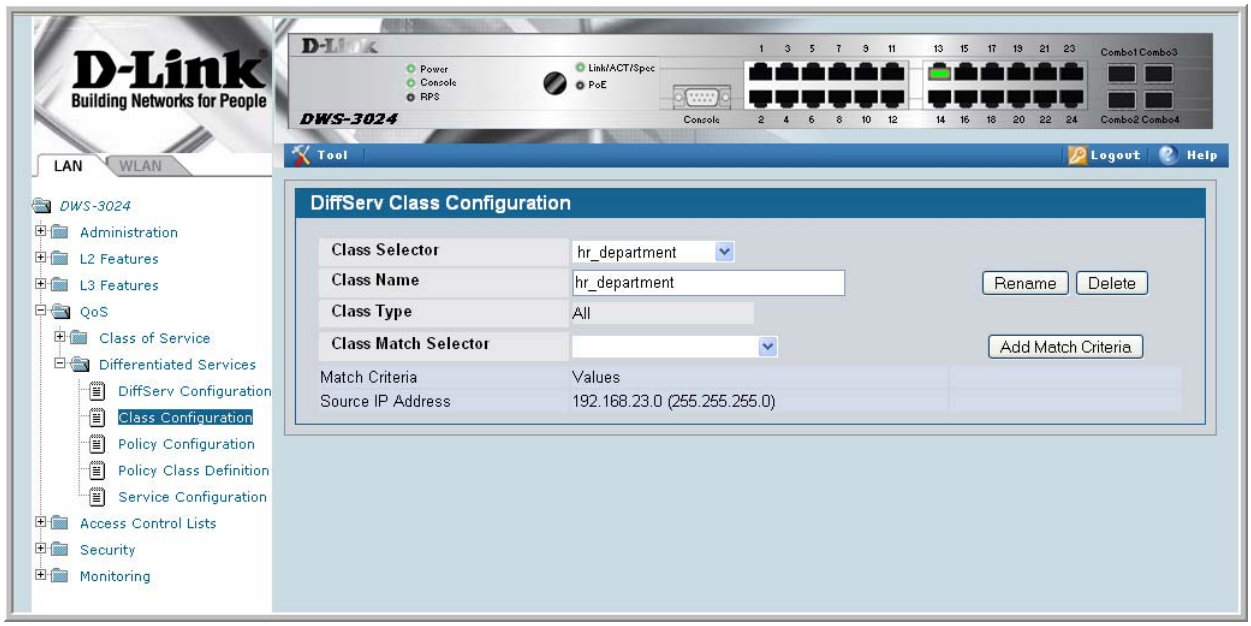


Figure 75. DiffServ Class Summary

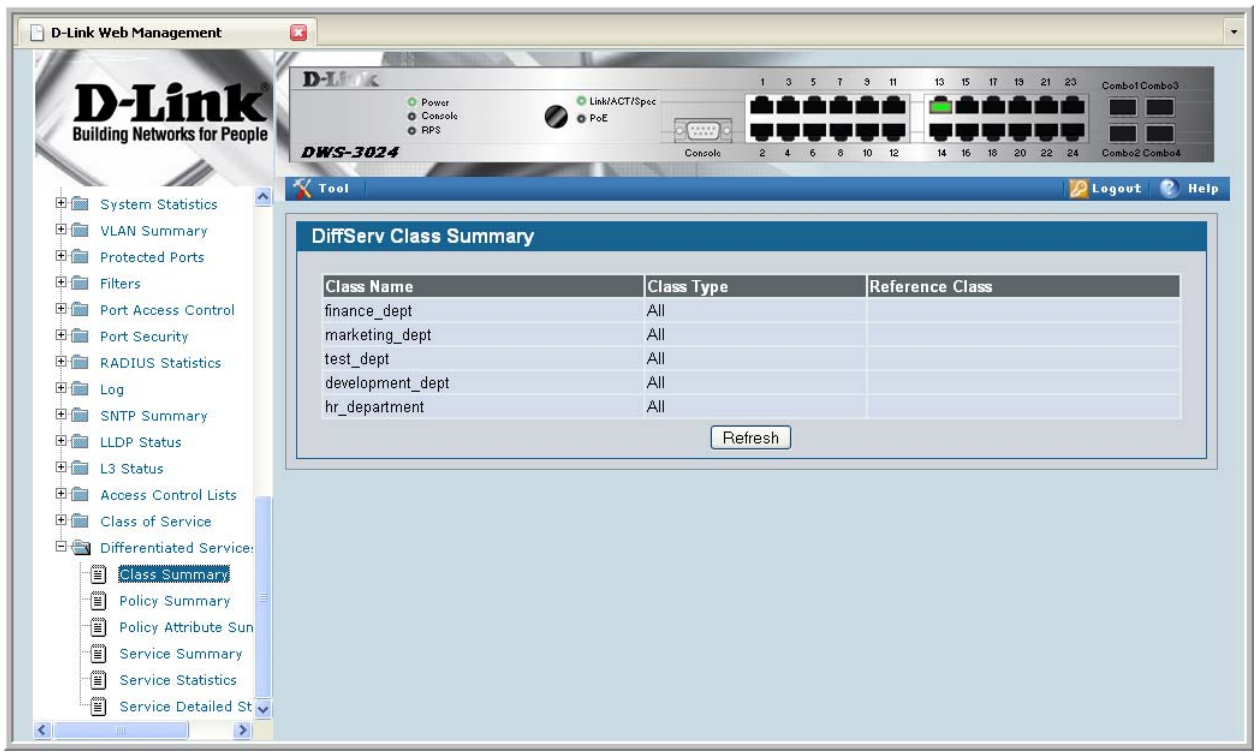


Figure 76. DiffServ Policy Configuration

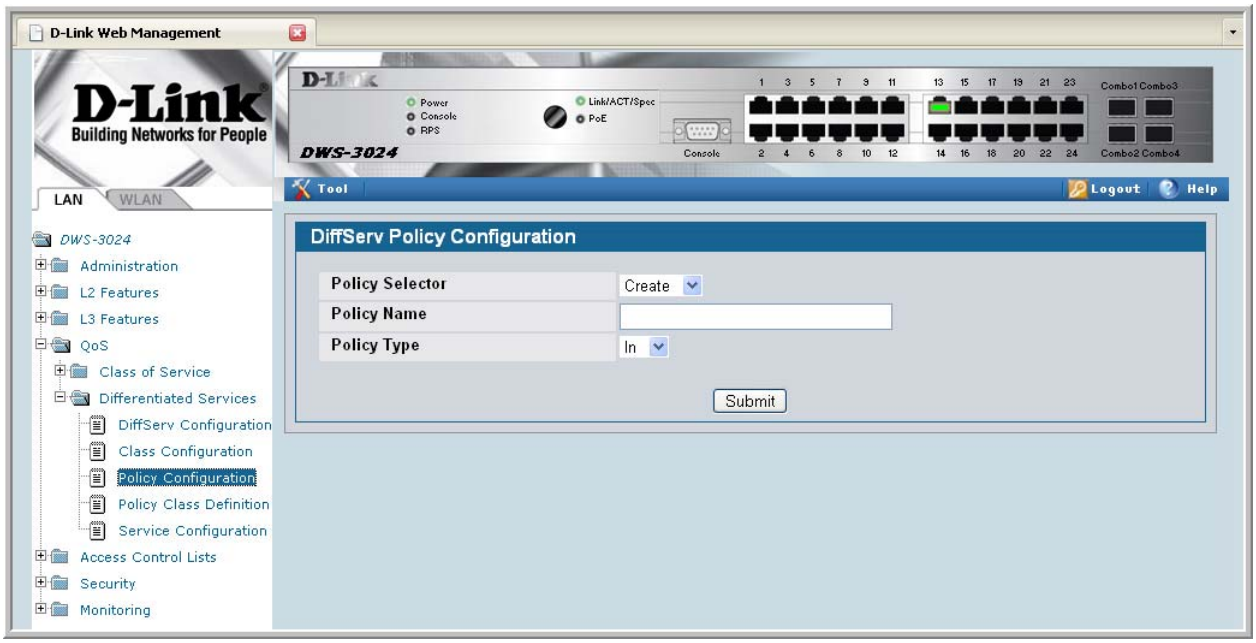


Figure 77. DiffServ Policy Configuration

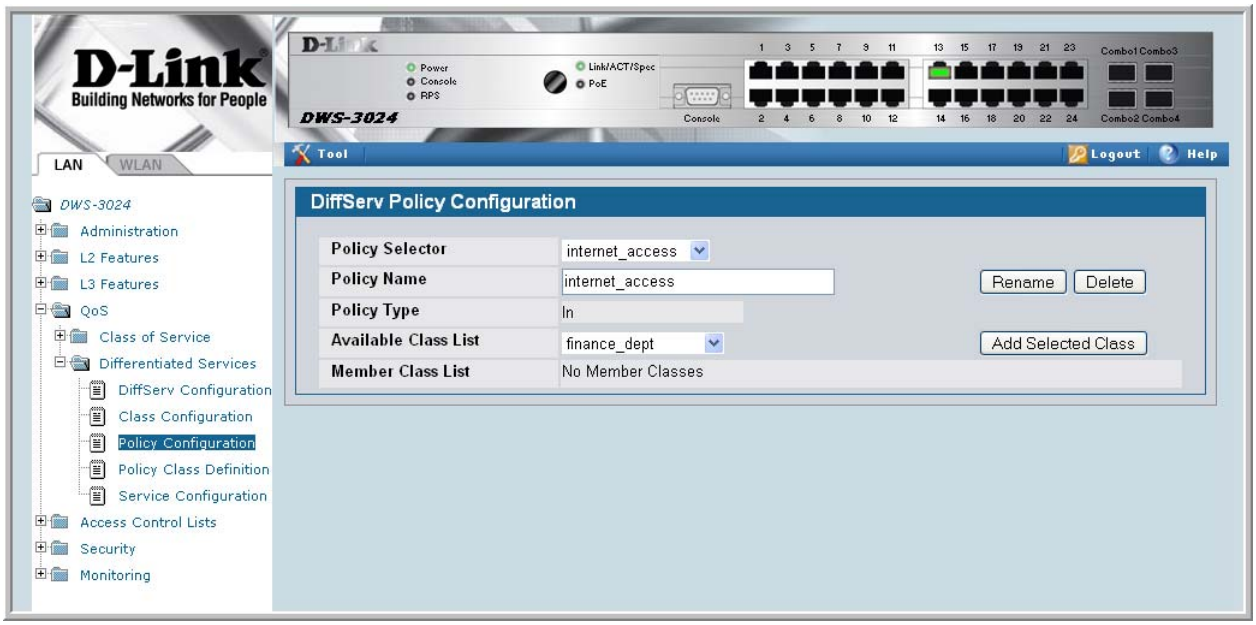


Figure 78. DiffServ Policy Class Definition

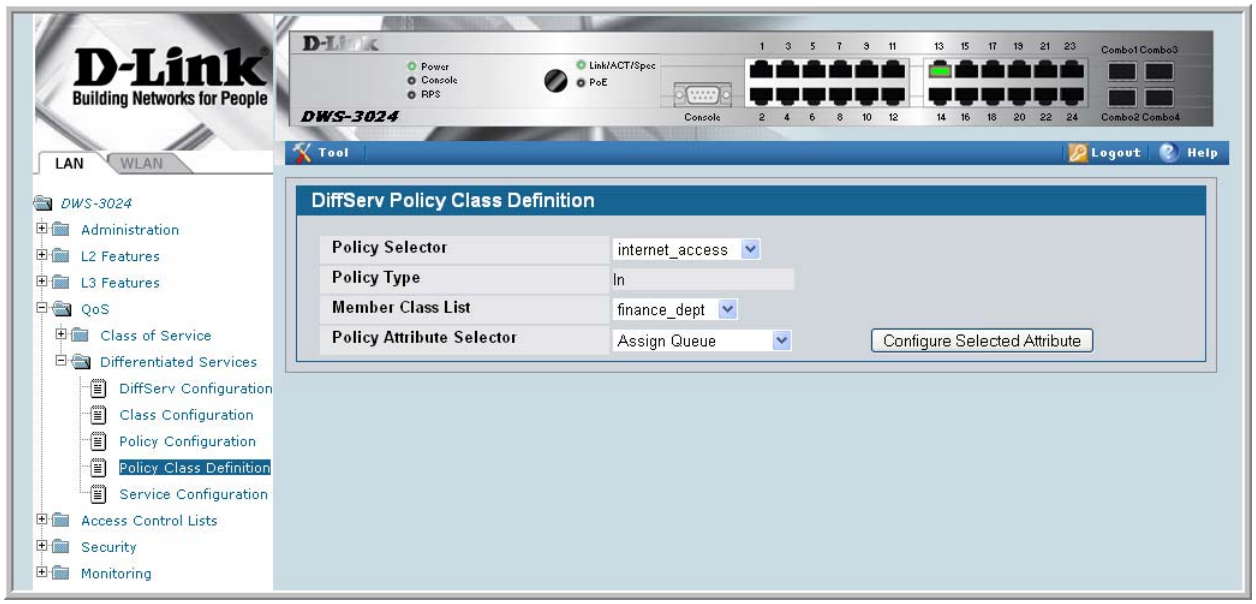


Figure 79. Assign Queue

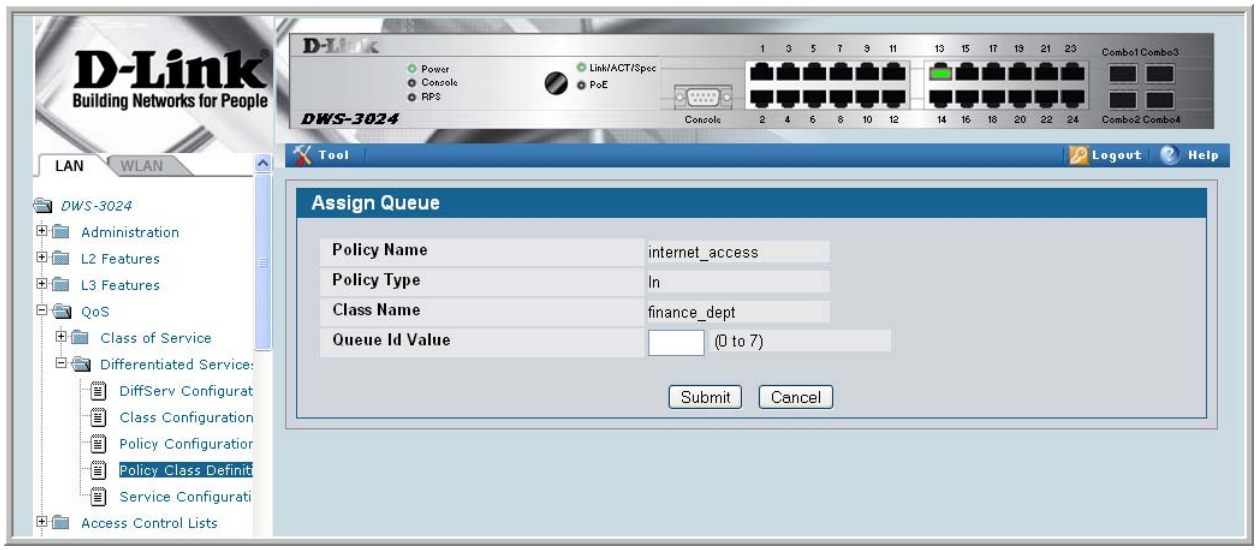


Figure 80. DiffServ Policy Summary

Figure 81. DiffServ Policy Attribute Summary

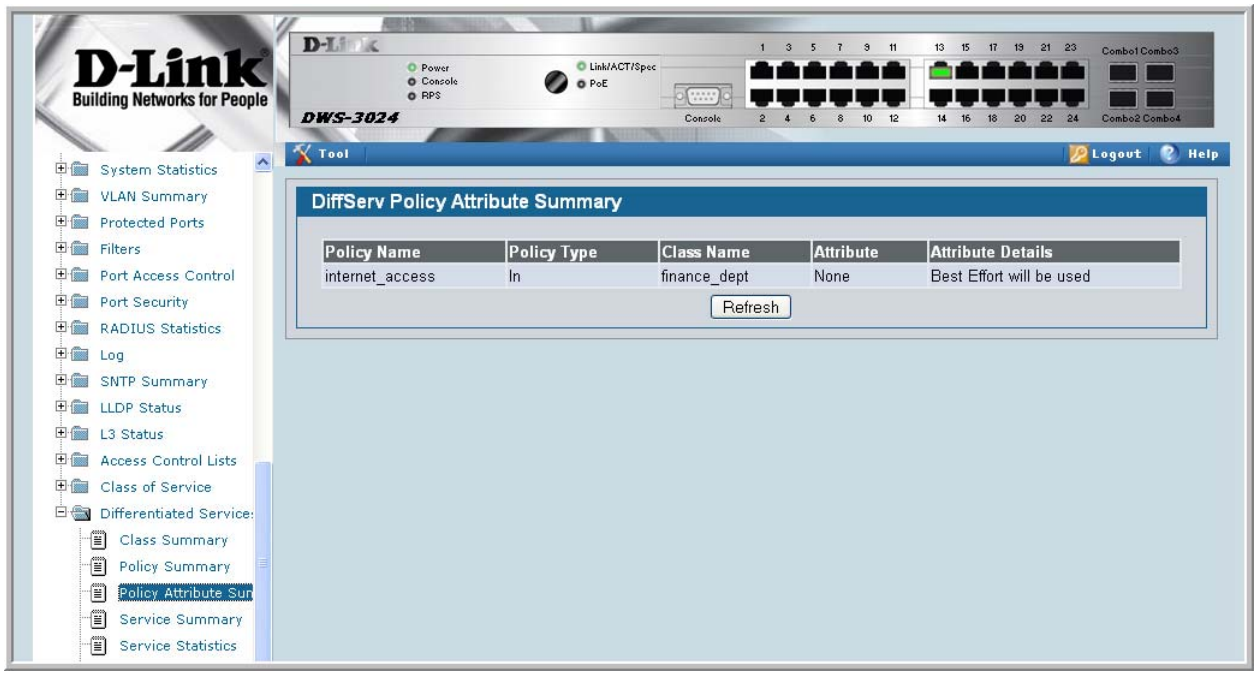


Figure 82. DiffServ Service Configuration

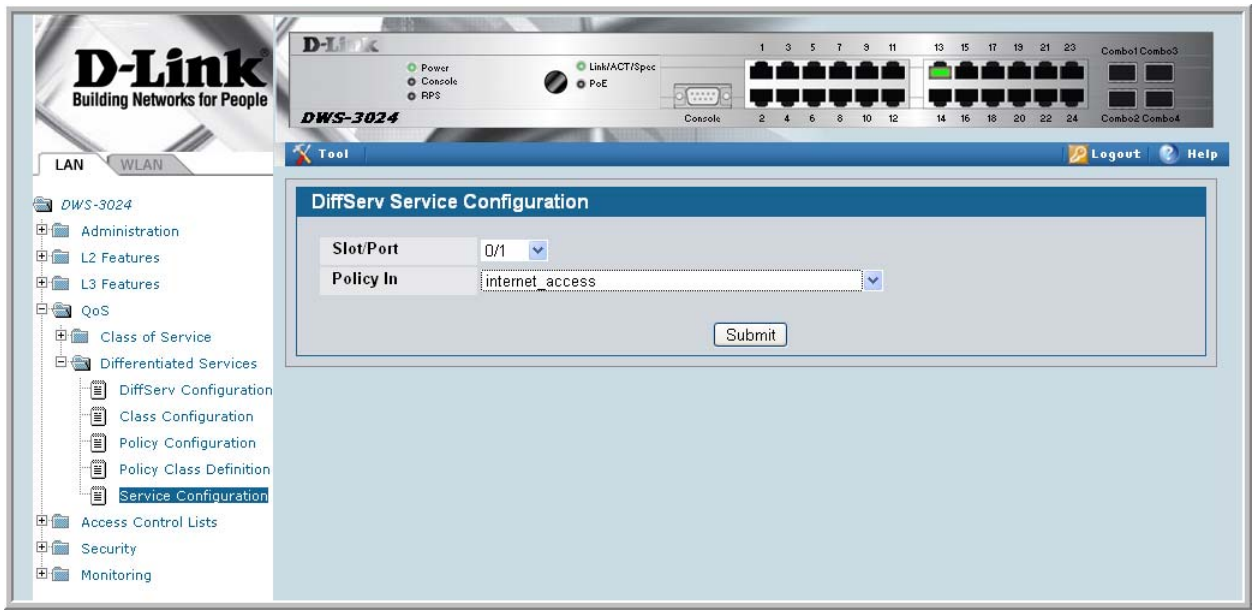
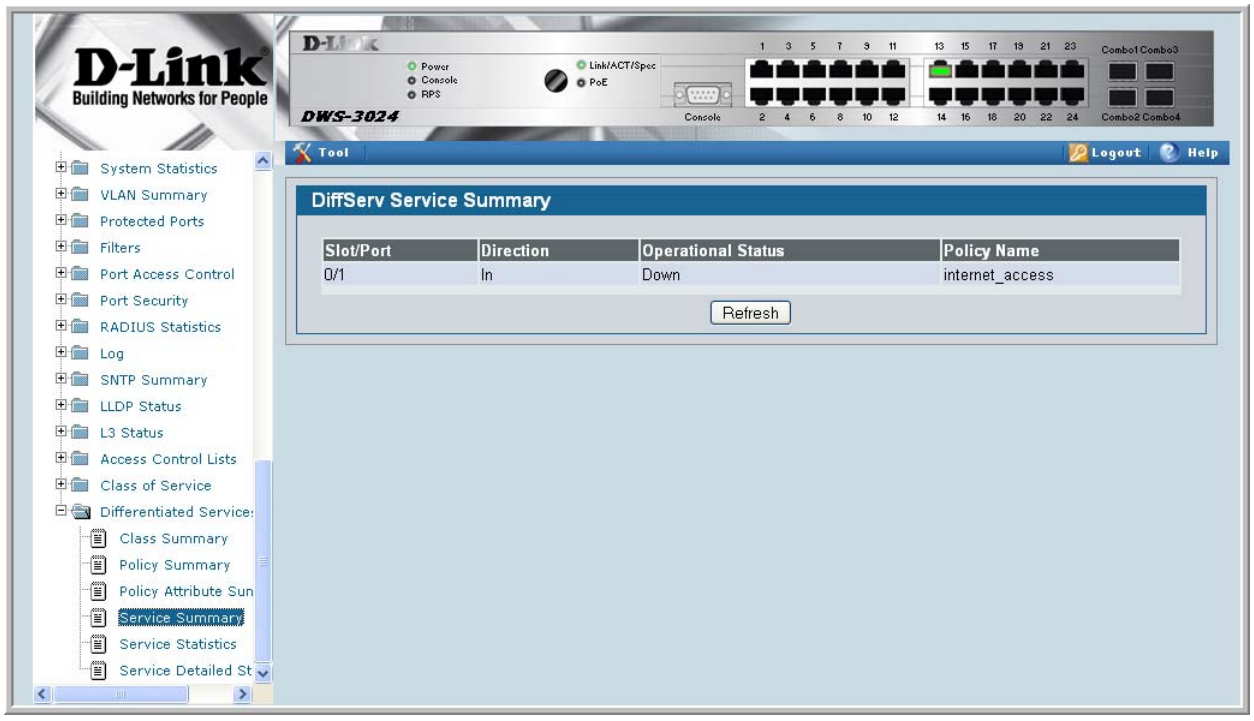


Figure 83. DiffServ Service Summary

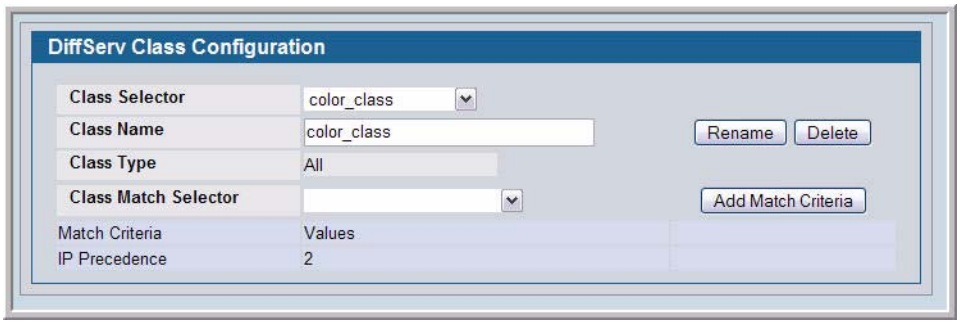


Configuring the Color-Aware Attribute by Using the Web

The following screens show the additional steps to take to configure the finance_dept class with a color-aware attribute.

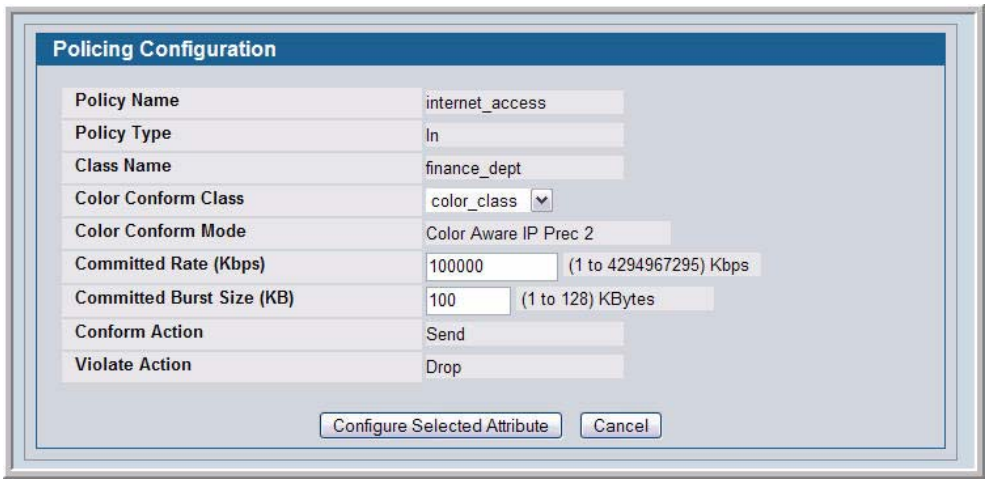
1. Add a new class to serve as the auxiliary traffic class.
   A. From the Class Selector menu on the DiffServ Class Configuration page, select **Create**.
   B. After the screen refreshes, enter color_class in the Class field.
   C. Select **All** as the Class Type.
   D. Click **Submit**.

   The screen refreshes, and the Class Match Selector field appears. The match condition for the class must be either IP Precedence or IP DSCP. In this example, the match condition is IP Precedence with a value of 2.
2. From the Class Match Selector field, select IP Precedence and click **Add Match Criteria**.
3. From the Precedence Value menu on the IP Precedence page, select **2**, and then click **Submit**.



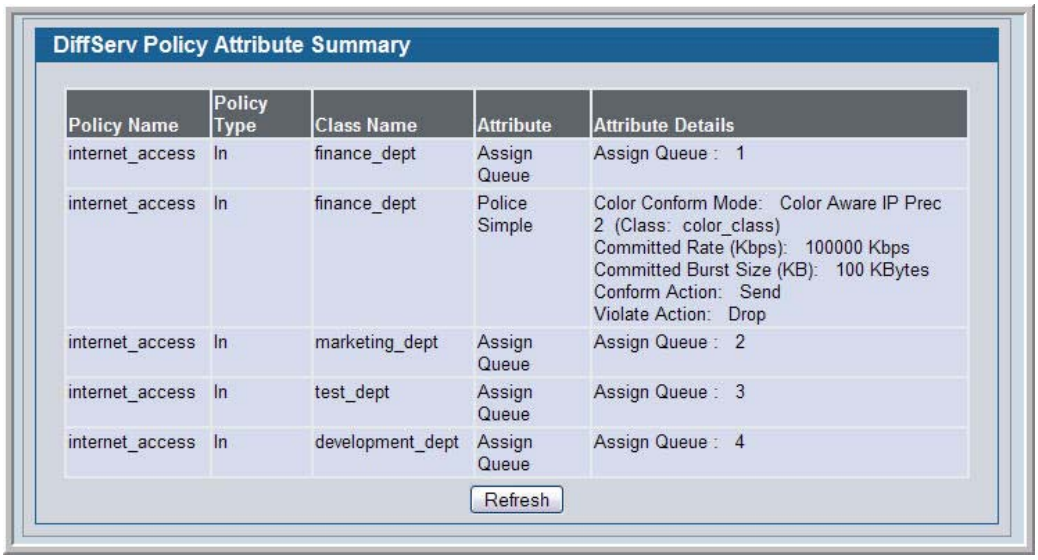
4. Navigate to the Policy Class Definition page to configure the additional policy attributes for the finance_dept class.
   A. Make sure **Police Simple** is selected from the Policy Attribute Selector menu, and then click **Configure Selected Attribute**.
   B. From the Color Mode field on the Policing Attributes page, select **Color Aware**, and then click **Confirm**.

C. After the screen refreshes, enter values for the Committed Rate and Committed Burst Size fields.



D. Click **Configure Selected Attribute**.

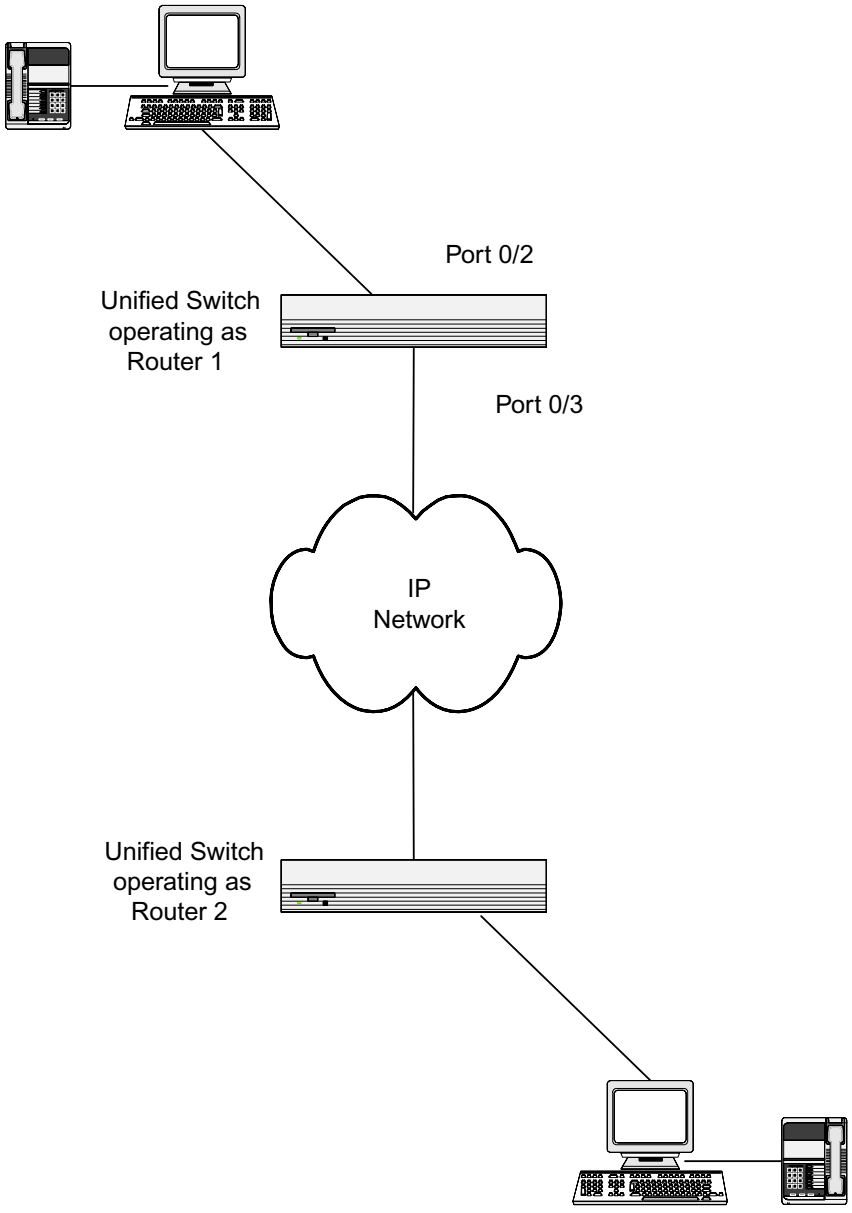
The DiffServ Policy Attribute Summary page appears so you can view information about all of the policies and their attributes configured on the system.



DiffServ for VoIP Configuration Example

One of the most valuable uses of DiffServ is to support Voice over IP (VoIP). VoIP traffic is inherently time-sensitive: for a network to provide acceptable service, a guaranteed transmission rate is vital. This example shows one way to provide the necessary quality of service: how to set up a class for UDP traffic, have that traffic marked on the inbound side, and then expedite the traffic on the outbound side. The configuration script is for Router 1 in the accompanying diagram: a similar script should be applied to Router 2.

Figure 84. DiffServ VoIP Example Network Diagram



Configuring DiffServ VoIP Support Example

Enter Global Config mode. Set queue 5 on all ports to use strict priority mode. This queue shall be used for all VoIP packets. Activate DiffServ for the switch.

```
config
  cos-queue strict 5
  diffserv
```

Create a DiffServ classifier named 'class_voip' and define a single match criterion to detect UDP packets. The class type “match-all” indicates that all match criteria defined for the class must be satisfied in order for a packet to be considered a match.

```
class-map match-all class_voip
 match protocol udp
exit
```

Create a second DiffServ classifier named 'class_ef' and define a single match criterion to detect a DiffServ code point (DSCP) of 'EF' (expedited forwarding). This handles incoming traffic that was previously marked as expedited elsewhere in the network.

```
class-map match-all class_ef
 match ip dscp ef
exit
```

Create a DiffServ policy for inbound traffic named 'pol_voip', then add the previously created classes 'class_ef' and 'class_voip' as instances within this policy.

This policy handles incoming packets already marked with a DSCP value of 'EF' (per 'class_ef' definition), or marks UDP packets per the 'class_voip' definition) with a DSCP value of 'EF'. In each case, the matching packets are assigned internally to use queue 5 of the egress port to which they are forwarded.

```
policy-map pol_voip in
 class class_ef
   assign-queue 5
 exit
 class class_voip
   mark ip-dscp ef
   assign-queue 5
 exit
exit
```

Attach the defined policy to an inbound service interface.

```
interface 0/3
 service-policy in pol_voip
exit
```

```
exit
```


19

RADIUS

Making use of a single database of accessible information – as in an Authentication Server – can greatly simplify the authentication and management of users in a large network. One such type of Authentication Server supports the Remote Authentication Dial In User Service (RADIUS) protocol as defined by RFC 2865.

For authenticating users prior to access, the RADIUS standard has become the protocol of choice by administrators of large accessible networks. To accomplish the authentication in a secure manner, the RADIUS client and RADIUS server must both be configured with the same shared password or “secret”. This “secret” is used to generate one-way encrypted authenticators that are present in all RADIUS packets. The “secret” is never transmitted over the network.

RADIUS conforms to a secure communications client/server model using UDP as a transport protocol. It is extremely flexible, supporting a variety of methods to authenticate and statistically track users. RADIUS is also extensible, allowing for new methods of authentication to be added without disrupting existing functionality.

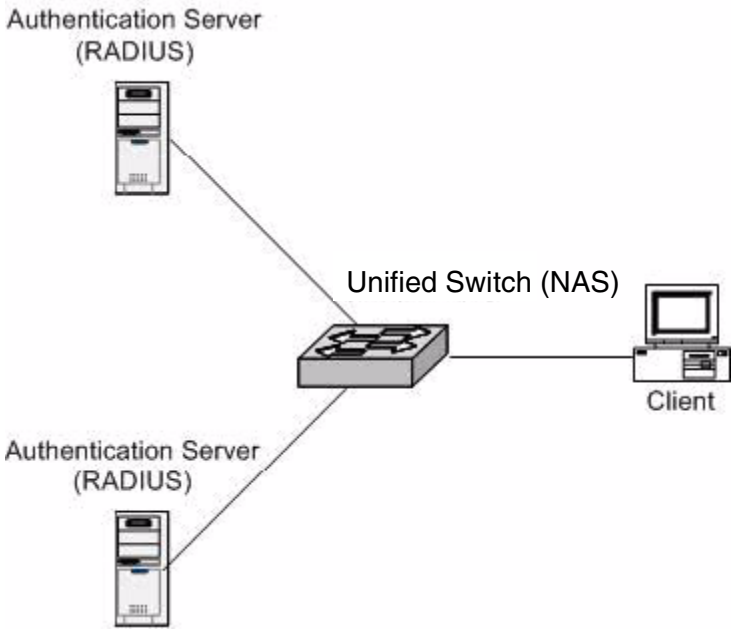
As a user attempts to connect to a functioning RADIUS supported network, a device referred to as the Network Access Server (NAS) or switch/router first detects the contact. The NAS or user-login interface then prompts the user for a name and password. The NAS encrypts the supplied information and a RADIUS client transports the request to a pre-configured RADIUS server. The server can authenticate the user itself, or make use of a back-end device to ascertain authenticity. In either case a response may or may not be forthcoming to the client. If the server accepts the user, it returns a positive result with attributes containing configuration information. If the server rejects the user, it returns a negative result. If the server rejects the client or the shared “secrets” differ, the server returns no result. If the server requires additional verification from the user, it returns a challenge, and the request process begins again.

RADIUS Configuration Example

This example configures two RADIUS servers at 10.10.10.10 and 11.11.11.11. Each server has a unique shared secret key. The shared secrets are configured to be *secret1* and *secret2* respectively. The server at 10.10.10.10 is configured as the primary server. A new authentication list, called radiusList, is created which uses RADIUS as the primary authentication method, and local authentication as a backup method in the event that the

RADIUS server cannot be contacted. This authentication list is then associated with the default login.

Figure 85. RADIUS Servers in a DWS-3000 Network



When a user attempts to log in, the switch prompts for a username and password. The switch then attempts to communicate with the primary RADIUS server at 10.10.10.10. Upon successful connection with the server, the login credentials are exchanged over an encrypted channel. The server grants or denies access, which the switch honors, and either allows or does not allow the user to access the switch. If neither of the two servers can be contacted, the switch searches its local user database for the user.

Configuring RADIUS by Using CLI Commands

The following CLI commands perform the configuration described in the example.

```
config
        radius server host auth 10.10.10.10
        radius server key auth 10.10.10.10
                secret1
                secret1
        radius server host auth 11.11.11.11
        radius server key auth 11.11.11.11
                secret2
                secret2
        radius server primary 10.10.10.10
        authentication login radiusList radius local
        users defaultlogin radiusList
exit
```


Configuring RADIUS by Using the Web Interface

The following Web screens show how to perform the configuration described in the example.

Figure 86. Add a RADIUS Server

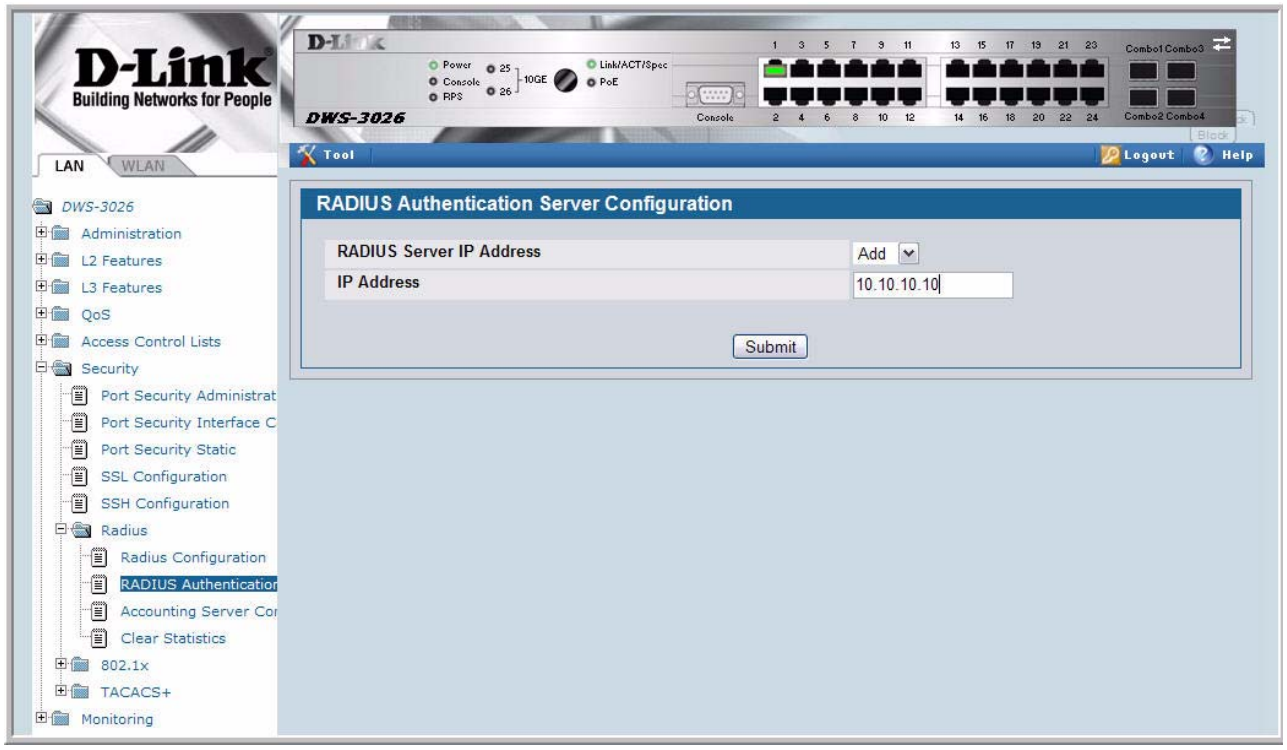


Figure 87. Configuring the RADIUS Server

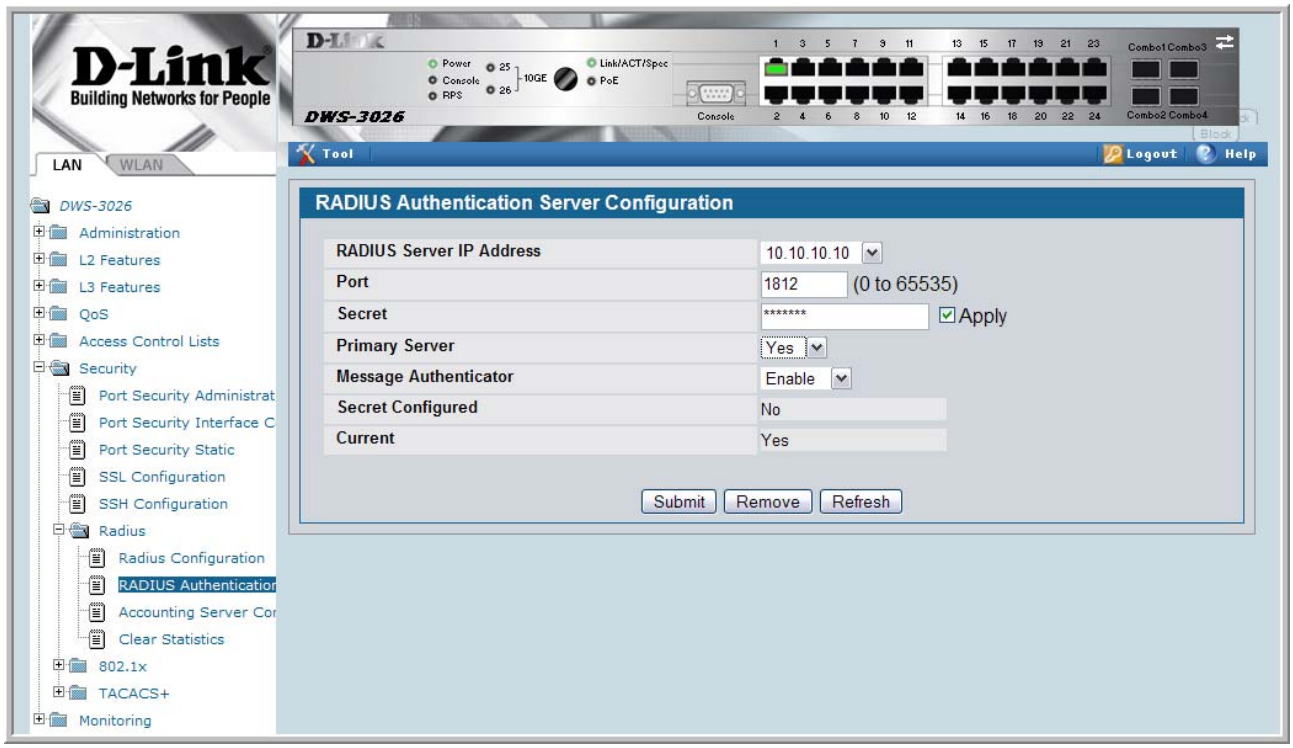


Figure 88. Create an Authentication List

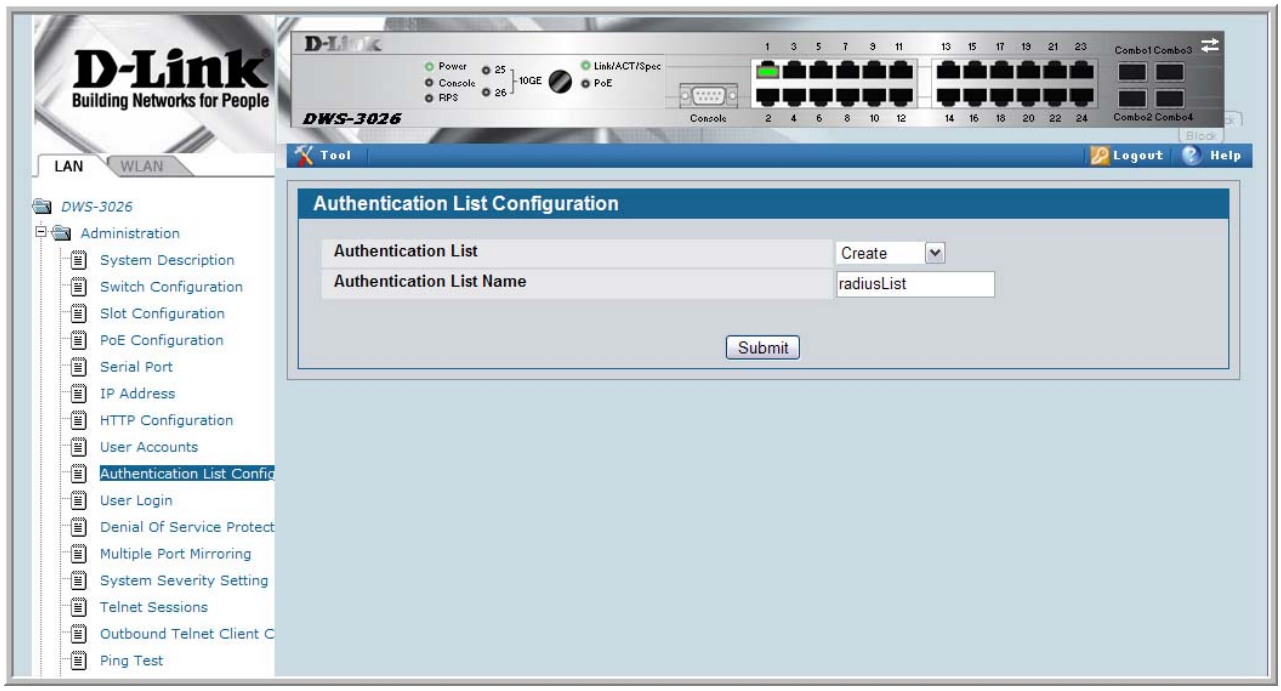


Figure 89. Configure the Authentication List

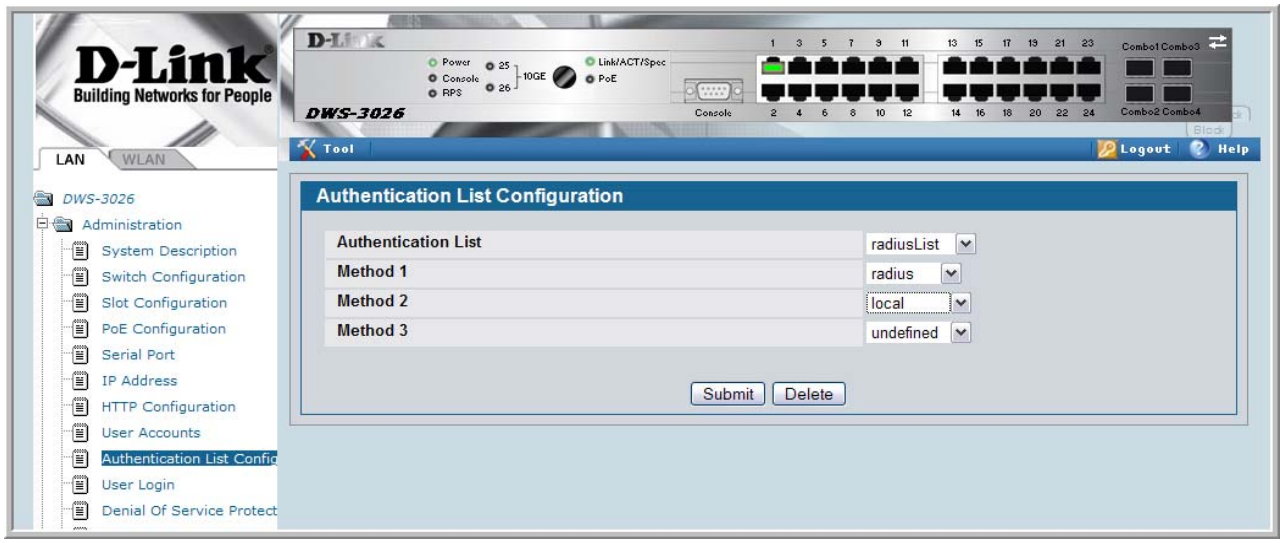
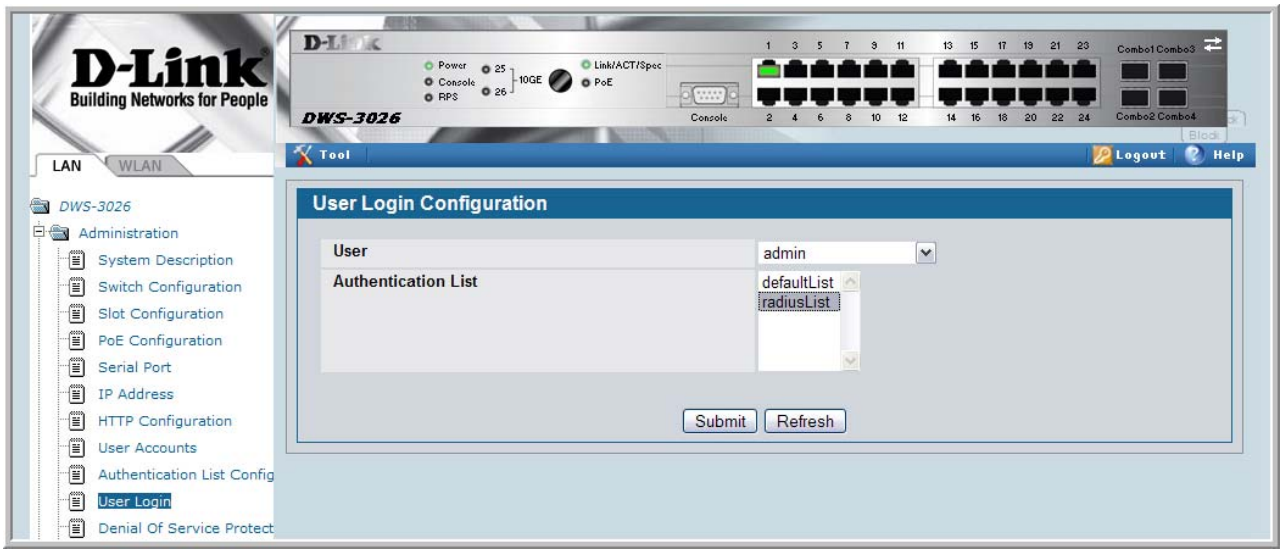


Figure 90. Set the User Login



20

TACACS+

TACACS+ (Terminal Access Controller Access Control System) provides access control for networked devices via one or more centralized servers. Similar to RADIUS, this protocol simplifies authentication by making use of a single database that can be shared by many clients on a large network. TACACS+ is based on the TACACS protocol described in RFC1492. TACACS+ uses TCP to ensure reliable delivery and a shared key configured on the client and daemon server to encrypt all messages.

After you configure TACACS+ as the authentication method for user login, the NAS (Network Access Server) prompts for the user login credentials and requests services from the DWS-3000 TACACS+ client. The client then uses the configured list of servers for authentication, and provides results back to the NAS. You can configure the TACACS+ server list with one or more hosts defined via their network IP address. You can also assign each a priority to determine the order in which the TACACS+ client will contact them. TACACS+ contacts the server when a connection attempt fails or times out for a higher priority server.

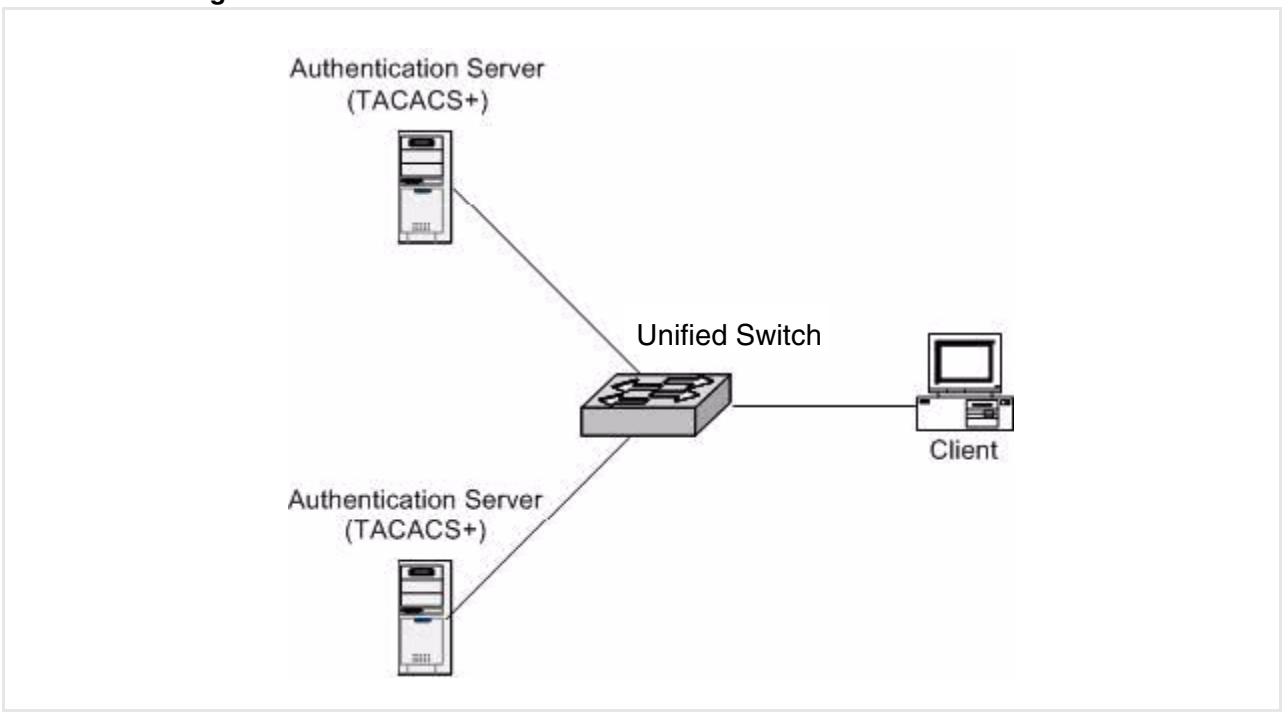
You can configure each server host with a specific connection type, port, timeout, and shared key, or you can use global configuration for the key and timeout.

Like RADIUS, the TACACS+ server can do the authentication itself, or redirect the request to another back-end device. All sensitive information is encrypted and the shared secret is never passed over the network - it is used only to encrypt the data.

TACACS+ Configuration Example

This example configures two TACACS+ servers at 10.10.10.10 and 11.11.11.11. Each server has a unique shared secret key. The server at 10.10.10.10 has a default priority of 0, the highest priority, while the other server has a priority of 2. A new authentication list called tacacsList is created which uses TACACS+ to authenticate, and uses local authentication as a backup method. This authentication list is then associated with the default login.

Figure 91. DWS-3000 with TACACS+



When a user attempts to log into the switch, the NAS or switch prompts for a user name and password. The switch attempts to communicate with the highest priority configured TACACS+ server at 10.10.10.10. Upon successful connection with the server, the switch and server exchange the login credentials over an encrypted channel. The server then grants or denies access, which the switch honors, and either allows or does not allow the user to gain access to the switch. If neither of the two servers can be contacted, the switch searches its local user database for the user.

Configuring TACACS+ by Using CLI Commands

The following CLI commands perform the configuration described in the example.

```
config
        tacacs-server host 10.10.10.10
                key tacacs1
        exit
        tacacs-server host 11.11.11.11
                key tacacs2
                priority 2
        exit
        authentication login tacacsList tacacs local
        users defaultlogin tacacsList
exit
```


Configuring TACACS+ by Using the Web Interface

The following Web screens show how to perform the configuration described in the example.

Figure 92. Add a TACACS+ Server

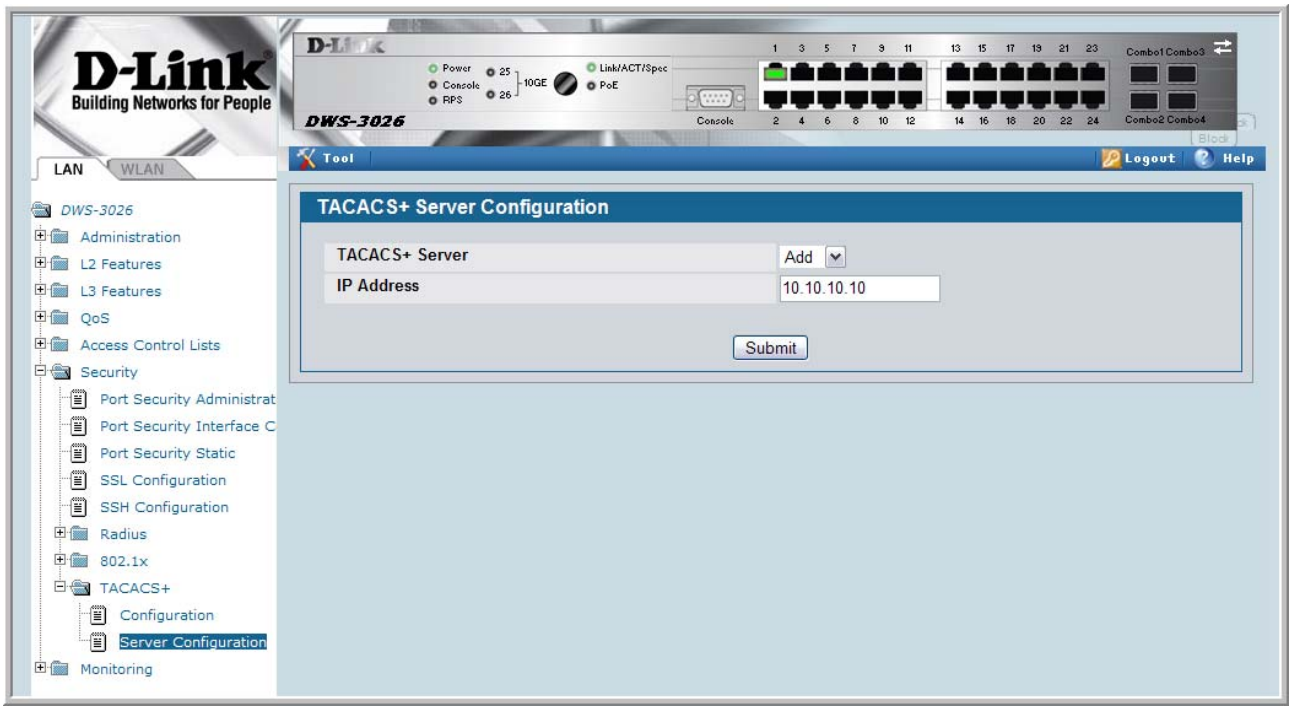


Figure 93. Configuring the TACACS+ Server

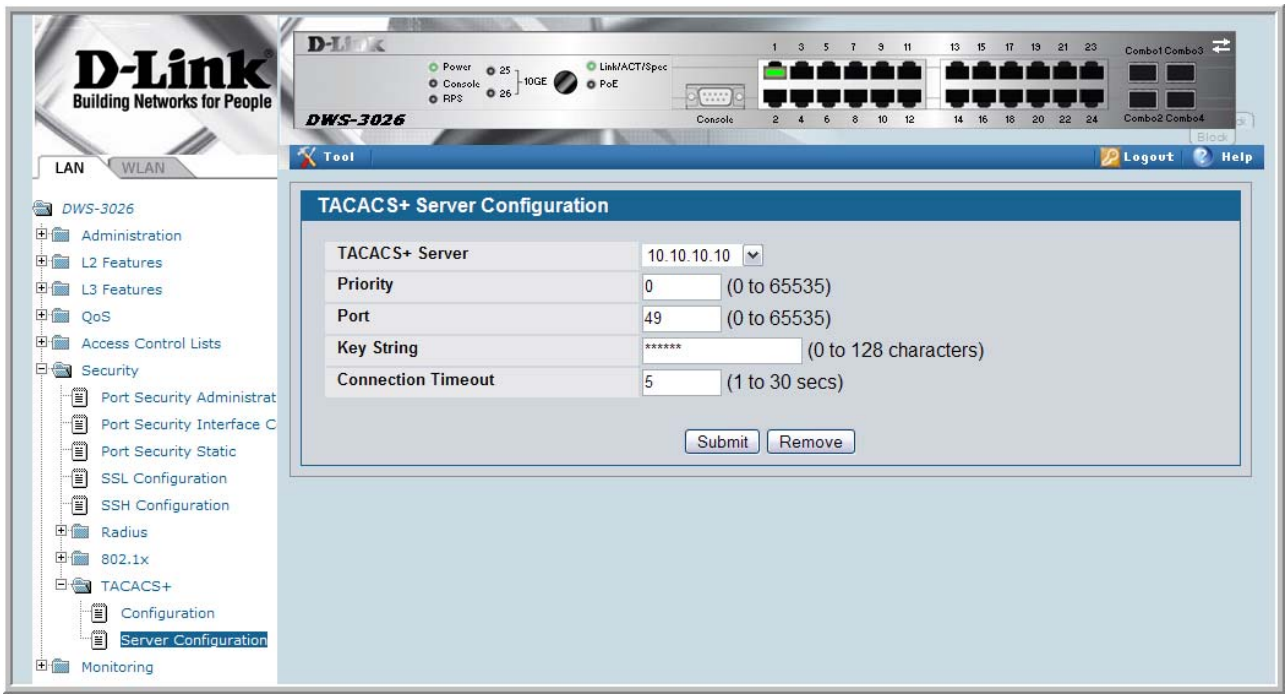


Figure 94. Create an Authentication List (TACACS+)

Figure 95. Configure the Authentication List (TACACS+)

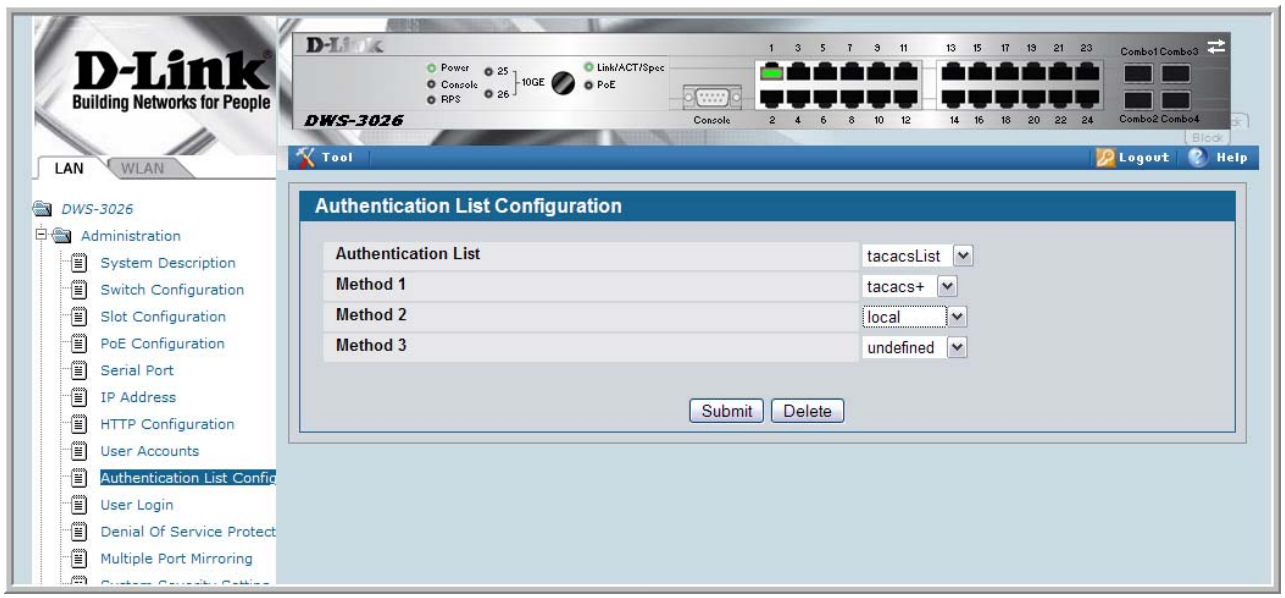
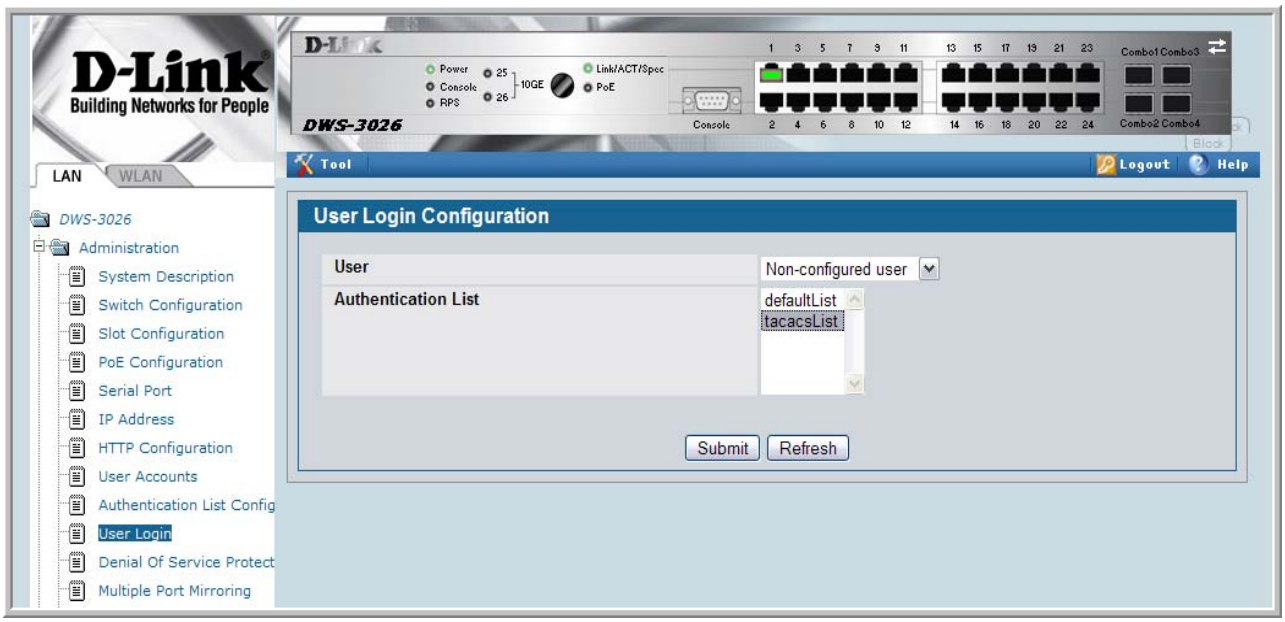


Figure 96. Set the User Login (TACACS+)



21

DHCP Filtering

This section describes the Dynamic Host Configuration Protocol (DHCP) Filtering feature.

Overview

DHCP filtering provides security by filtering untrusted DHCP messages. An untrusted message is a message that is received from outside the network or firewall, and that can cause traffic attacks within network.

You can use DHCP Filtering as a security measure against unauthorized DHCP servers. A known attack can occur when an unauthorized DHCP server responds to a client that is requesting an IP address. The unauthorized server can configure the gateway for the client to be equal to the IP address of the server. At that point, the client sends all of its IP traffic destined to other networks to the unauthorized machine, giving the attacker the possibility of filtering traffic for passwords or employing a ‘man-in-the-middle’ attack.

DHCP filtering works by allowing the administrator to configure each port as a trusted or untrusted port. The port that has the authorized DHCP server should be configured as a trusted port. Any DHCP responses received on a trusted port will be forwarded. All other ports should be configured as untrusted. Any DHCP (or BootP) responses received on the ingress side will be discarded.

Limitations

- Port Channels (LAGs) — If an interface becomes a member of a LAG, DHCP filtering is no longer operationally enabled on the interface. Instead, the interface follows the configuration of the LAG port. End user configuration for the interface remains unchanged. When an interface is no longer a member of a LAG, the current end user configuration for that interface automatically becomes effective.
- Mirroring — If an interface becomes a probe port, DHCP filtering can no longer become operationally enabled on the interface. End user configuration for the interface remains unchanged. When an interface no longer acts as a probe port, the current end user configuration for that interface automatically becomes effective.

CLI Examples

The commands shown below show examples of configuring DHCP Filtering for the switch and for individual interfaces.

Example #1: Enable DHCP Filtering for the Switch

This example

```
config
     ip dhcp filtering
     exit
exit
```

Example #2: Enable DHCP Filtering for an Interface

```
config
     interface 0/11
           ip dhcp filtering trust
           exit
     exit
```

Example #3: Show DHCP Filtering Configuration

```
show ip dhcp filtering

Switch DHCP Filtering is Enabled

Interface Trusted
--------- -----------
0/1       No
0/2       No
0/3       No
0/4       No
0/5       No
0/6       No
0/7       No
0/8       No
0/9       No
0/10      No
0/11      Yes
0/12      No
0/13      No
0/14      No
0/15      No
```

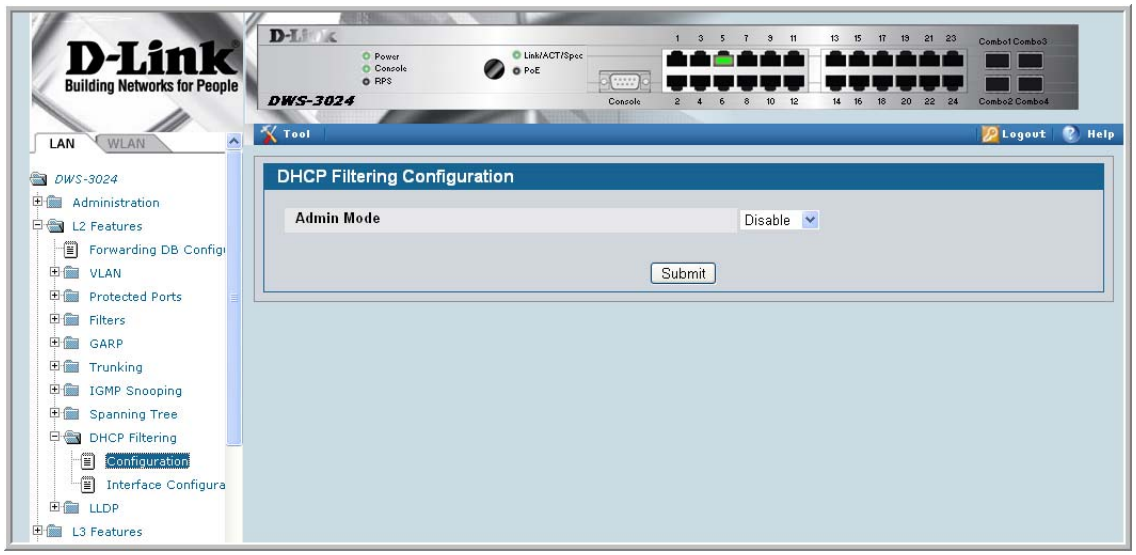
Web Examples

From the Web interface, you can perform the following DHCP Filtering tasks:

- Enable or disable administration mode on the switch
- Enable or disable the DHCP Filtering trust mode on specific interfaces
- View the interface binding information for DHCP Filtering

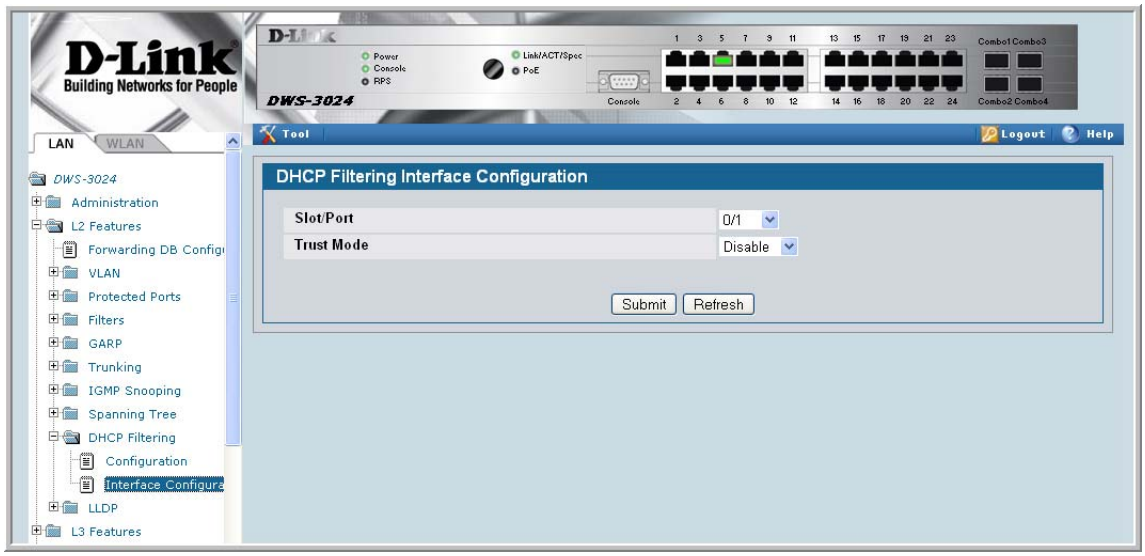
Use the DHCP Filtering Configuration page to configure the DHCP Filtering admin mode on the switch.

Figure 97. DHCP Filtering Configuration



Use the DHCP Filtering Interface Configuration page to configure DHCP Filtering on specific interfaces.

Figure 98. DHCP Filtering Interface Configuration



To view the DHCP Filtering settings on each interface, use the DHCP Filter Binding Information page under **LAN > Monitoring > DHCP Filter Summary**.

Figure 99. DHCP Filter Binding Information

22

Traceroute

This section describes the Traceroute feature.

Use Traceroute to discover the routes that packets take when traveling on a hop-by-hop basis to their destination through the network.

- Maps network routes by sending packets with small Time-to-Live (TTL) values and watches the ICMP time-out announcements
- Command displays all L3 devices
- Can be used to detect issues on the network
- Tracks up to 20 hops
- Default UDP port uses 33343 unless modified in the traceroute command

NOTE: You can execute Traceroute with CLI commands only — there is no Web interface for this feature.

CLI Example

The following shows an example of using the traceroute command to determine how many hops there are to the destination. The command output shows each IP address the packet passes through and how long it takes to get there. In this example, the packet takes 16 hops to reach its destination.

```
(DWS-3024)                          #traceroute ?
<ipaddr>                            Enter IP address.
(DWS-3024)                          #traceroute 216.109.118.74 ?
<cr>                                Press Enter to execute the command.
<port>                              Enter port no.

(DWS-3024)                          #traceroute 216.109.118.74

Tracing route over a maximum of 20 hops

 1  10.254.24.1        40 ms       9 ms      10 ms
 2  10.254.253.1       30 ms      49 ms      21 ms
 3  63.237.23.33       29 ms      10 ms      10 ms
 4  63.144.4.1         39 ms      63 ms      67 ms
 5  63.144.1.141       70 ms      50 ms      50 ms
 6  205.171.21.89      39 ms      70 ms      50 ms
 7  205.171.8.154      70 ms      50 ms      70 ms
 8  205.171.8.222      70 ms      50 ms      80 ms
 9  205.171.251.34     60 ms      90 ms      50 ms
10  209.244.219.181    60 ms      70 ms      70 ms
11  209.244.11.9       60 ms      60 ms      50 ms
12  4.68.121.146       50 ms      70 ms      60 ms
13  4.79.228.2         60 ms      60 ms      60 ms
14  216.115.96.185    110 ms      59 ms      70 ms
15  216.109.120.203    70 ms      66 ms      95 ms
16  216.109.118.74     78 ms     121 ms      69 ms
```


23

Configuration Scripting

Configuration Scripting allows you to generate a text-formatted script file that shows the current configuration of the system. You can generate multiple scripts and upload and apply them to more than one switch.

Overview

Configuration Scripting:

- Provides scripts that can be uploaded and downloaded to the system.
- Provides flexibility to create command configuration scripts.
- Can be applied to several switches.
- Can save up to ten scripts or 500K of memory.
- Provides List, Delete, Apply, Upload, Download.
- Provides script format of one CLI command per line.

Considerations

- Total number of scripts stored on the system is limited by NVRAM/FLASH size.
- Application of scripts is partial if script fails. For example, if the script executes five of ten commands and the script fails, the script stops at five.
- Scripts cannot be modified or deleted while being applied.
- Validation of scripts checks for syntax errors only. It does not validate that the script will run.

CLI Examples

The following are examples of the commands used for the Configuration Scripting feature.

Example #1: script

```
(DWS-3024) #script ?

apply       Applies configuration script to the switch.
delete      Deletes a configuration script file from the switch.
```

```
list        Lists all configuration script files present on the
            switch.
show        Displays the contents of configuration script.
validate    Validate the commands of configuration script.
```

Example #2: script list and script delete

```
(DWS-3024) #script list

Configuration Script Name     Size(Bytes)
--------------------------    -----------
basic.scr                            93
running-config.scr                 3201

2 configuration script(s) found.
1020706 bytes free.

(DWS-3024)                    #script delete basic.scr

Are you sure you want to delete the configuration script(s)? (y/n) y

1 configuration script(s) deleted.
```

Example #3: script apply running-config.scr

```
(DWS-3024) #script apply running-config.scr

Are you sure you want to apply the configuration script? (y/n) y

The systems has unsaved changes.
Would you like to save them now? (y/n) y

Configuration Saved!
```

Example #4: show running-config

Use this command to capture the running configuration into a script.

```
(DWS-3024)#show running-config running-config.scr

Config script created successfully.

(DWS-3024)#script list

Configuration Script Name     Size(Bytes)
--------------------------    ----------
running-config.scr            3201

1 configuration script(s) found.
1020799 bytes free.
```


Example #5: copy nvram: script

Use this command to upload a configuration script.

```
(DWS-3024) #copy nvram: script running-config.scr
tftp://192.168.77.52/running-config.scr

Mode..................... TFTP
Set TFTP Server IP.......... 192.168.77.52
TFTP Path................... ./
TFTP Filename............... running-config.scr
Data Type................... Config Script
Source Filename............. running-config.scr

Are you sure you want to start? (y/n) y

File transfer operation completed successfully.
```

Example #6: script validate running-config.scr

```
(DWS-3024)#script validate running-config.scr
serviceport protocol none
network protocol dhcp
no network javamode
vlan database
exit
configure
exit
logging buffered
logging host 192.168.77.151

Configuration script 'running-config.scr' validated.

(DWS-3024)  #script apply running-config.scr

Are you sure you want to apply the configuration script? (y/n) y
The system has unsaved changes.
Would you like to save them now? (y/n) y
Configuration Saved!
```

Example #7: Validate another Configuration Script

```
(DWS-3024) #script validate default.scr

network parms 172.30.4.2 255.255.255.0 0.0.0.0
vlan database
exit
configure
lineconfig
exit
spanning-tree configuration name 00-18-00-00-00-10
interface 0/1
exit
interface 0/2
exit
interface 0/3
exit
... continues through interface 0/26 ...
exit
exit
Configuration script 'default.scr' validation succeeded.
```


24

Outbound Telnet

This section describes the Outbound Telnet feature.

Overview

Outbound Telnet:

- Feature establishes an outbound telnet connection between a device and a remote host.
- When a telnet connection is initiated, each side of the connection is assumed to originate and terminate at a “Network Virtual Terminal” (NVT).
- Server and user hosts do not maintain information about the characteristics of each other’s terminals and terminal handling conventions.
- Must use a valid IP address.

CLI Examples

The following are examples of the commands used in the Outbound Telnet feature.

Example #1: show network

```
(DWS-3024) >telnet 192.168.77.151
Trying 192.168.77.151...
(DWS-3024)
User:admin
Password:
(DWS-3024)>enable
Password:

(DWS-3024)#show network

IP Address.............................192.168.77.151
Subnet Mask............................255.255.255.0
Default Gateway........................192.168.77.127
Burned In MAC Address..................00:10:18.82.04:E9
Locally Administered MAC Address.........00:00:00:00:00:00
MAC Address Type.......................Burned In
Network Configuration Protocol Current...DHCP
Management VLAN ID.....................1
Web Mode...............................Enable
Java Mode .............................Disable
```

Example #2: show telnet

```
(DWS-3024)#show telnet

Outbound Telnet Login Timeout (minutes).........5
Maximum Number of Outbound Telnet Sessions.....5
Allow New Outbound Telnet Sessions.............Yes
```

Example #3: transport output telnet

```
(DWS-3024) (Config)#lineconfig ?

<cr>                    Press Enter to execute the command.

(DWS-3024) (Config)#lineconfig

(DWS-3024) (Line)#transport ?

input                   Displays the protocols to use to connect to a
                        specific line of the router.
output                  Displays the protocols to use for outgoing
                        connections from a line.

(DWS-3024) (Line)#transport output ?

telnet                  Allow or disallow new telnet sessions.

(DWS-3024) (Line)#transport output telnet ?

<cr>                    Press Enter to execute the command.

(DWS-3024) (Line)#transport output telnet

(DWS-3024) (Line)#
```

Example #4: session-limit and session-timeout

```
(DWS-3024) (Line)#session-limit ?
```



```
<0-5>                    Configure the maximum number of outbound telnet
                         sessions allowed.

(DWS-3024) (Line)#session-limit 5

(DWS-3024) (Line)#session-timeout ?

<1-160>                  Enter time in minutes.

(DWS-3024) (Line)#session-timeout 15
```

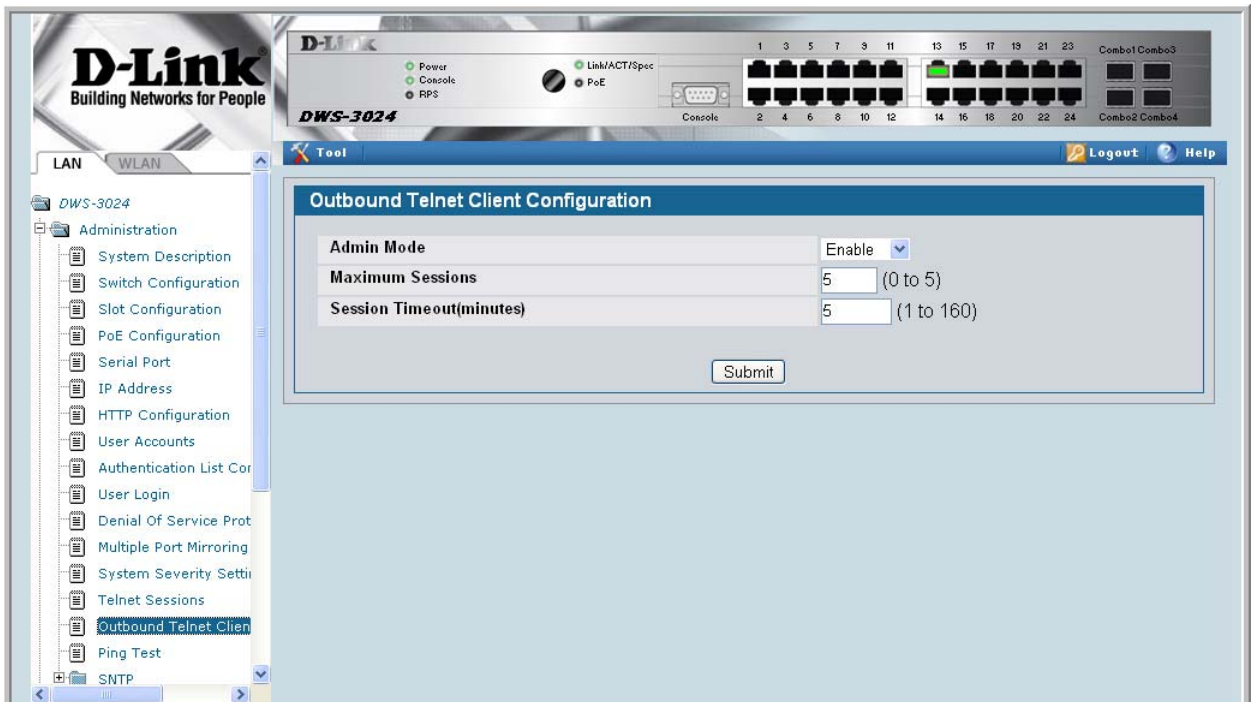
Web Example

You can set up the Outbound Telnet session through the Web interface.

You can:

- Enable or disable administration mode
- Set how many sessions you want
- Set the session time outs

Figure 100. Telnet Session Configuration



25

Pre-Login Banner

This section describes the Pre-Login Banner feature.

Overview

Pre-Login Banner:

- Allows you to create message screens when logging into the CLI Interface
- By default, no Banner file exists
- Banner can be uploaded or downloaded
- File size cannot be larger than 2K

The Pre-Login Banner feature is only for the CLI interface.

CLI Example

To create a Pre-Login Banner, follow these steps:

1. On your PC, using Notepad or another text editor, create a banner.txt file that contains the banner to be displayed.

```
DWS-3000 switch Login Banner - Unauthorized access is punishable by
law.
```

2. Transfer the file from the PC to the switch using TFTP

```
(DWS-3024) #copy tftp://192.168.77.52/banner.txt nvram:clibanner

Mode.....................................TFTP
Set TFTP Server IP.......................192.168.77.52
TFTP Path................................./
TFTP Filename............................banner.txt
Data Type................................Cli Banner

Are you sure you want to start? (y/n) y

CLI Banner file transfer operation completed successfully!

(DWS-3024) #exit

(DWS-3024) >logout

DWS-3000 switch Login Banner - Unauthorized access is punishable by
law.
User:
```

Note: The command “no clibanner” removes the banner from the switch.

26

Simple Network Time Protocol (SNTP)

This section describes the Simple Network Time Protocol (SNTP) feature.

Overview

SNTP:

- Used for synchronizing network resources
- Adaptation of NTP
- Provides synchronized network timestamp
- Can be used in broadcast or unicast mode
- SNTP client implemented over UDP which listens on port 123

CLI Examples

The following are examples of the commands used in the SNTP feature.

Example #1: show sntp

```
(DWS-3024) #show sntp ?

<cr>                    Press Enter to execute the command.
client                  Display SNTP Client Information.
server                  Display SNTP Server Information.
```

Example #2: show sntp client

```
(DWS-3024) #show sntp client

Client Supported Modes:  unicast broadcast
SNTP Version:            4
Port:                    123
Client Mode:             unicast
Unicast Poll Interval:   6
Poll Timeout (seconds):  5
Poll Retry:              1
```

Example #3: show sntp server

```
(DWS-3024) #show sntp server

Server IP Address:        81.169.155.234
Server Type:              ipv4
Server Stratum:           3
Server Reference Id:      NTP Srv: 212.186.110.32
Server Mode:              Server
Server Maximum Entries:   3
Server Current Entries:   1

SNTP Servers
------------

IP Address:               81.169.155.234
Address Type:             IPV4
Priority:                 1
Version:                  4
Port:                     123
Last Update Time:         MAY 18 04:59:13 2005
Last Attempt Time:        MAY 18 11:59:33 2005
Last Update Status:       Other
Total Unicast Requests:   1111
Failed Unicast Requests:  361
```

Example #4: configure sntp

```
(DWS-3024)(Config) #sntp ?

broadcast                 Configure SNTP client broadcast parameters.
client                    Configure the SNTP client parameters.
server                    Configure SNTP server parameters.
unicast                   Configure SNTP client unicast parameters.
```

Example #5: configure sntp client mode

```
(DWS-3024) (Config) #sntp client mode broadcast ?

<cr>                      Press Enter to execute the command.

(DWS-3024) (Config) #sntp client mode unicast ?

<cr>                      Press Enter to execute the command.

(DWS-3024)(Config)#sntp broadcast client poll-interval ?

<6-10>                    Enter value in the range (6 to 10). Poll
                          interval is 2^(value) in seconds.
```


Example #6: configuring sntp server

```
(DWS-3024)(Config) #sntp server 192.168.10.234 ?

<cr>                    Press Enter to execute the command.
<1-3>                   Enter SNTP server priority from 1 to 3.
```

Example #7: configure sntp client port

```
(DWS-3024)(Config) #sntp client port 1 ?

<cr>                    Press Enter to execute the command.
<6-10>                  Enter value in the range (6 to 10). Poll
                        interval is 2^(value) in seconds.
```

Web Interface Examples

The following are examples of Web Interface pages used in the SNTP feature.

Figure 101. SNTP Global Configuration Page

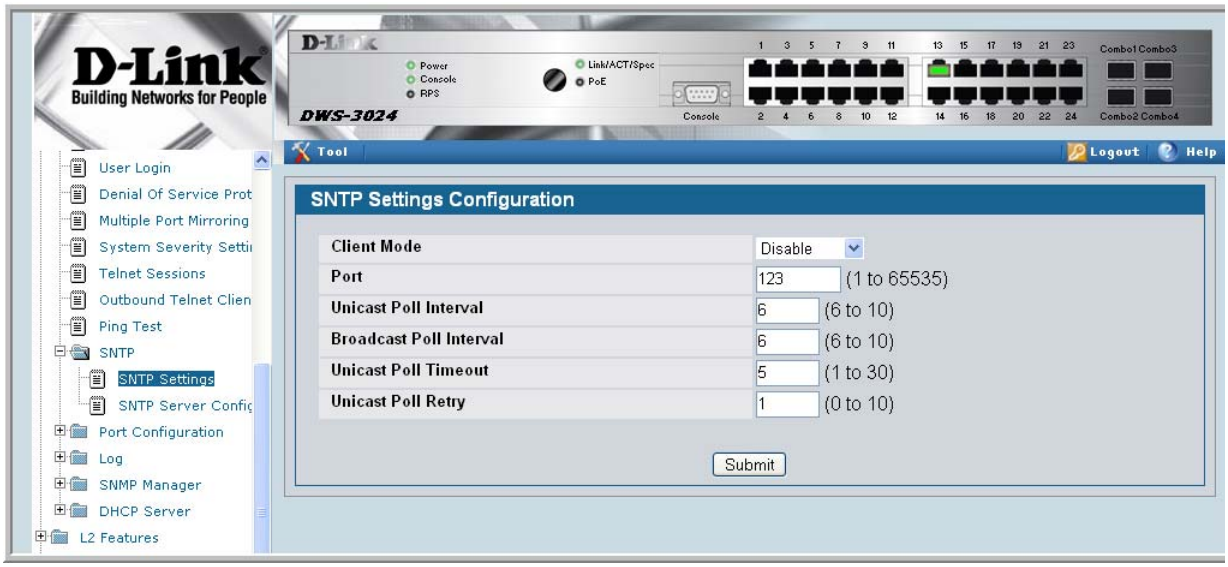


Figure 102. SNTP Global Status Page

Figure 103. SNTP Server Configuration Page

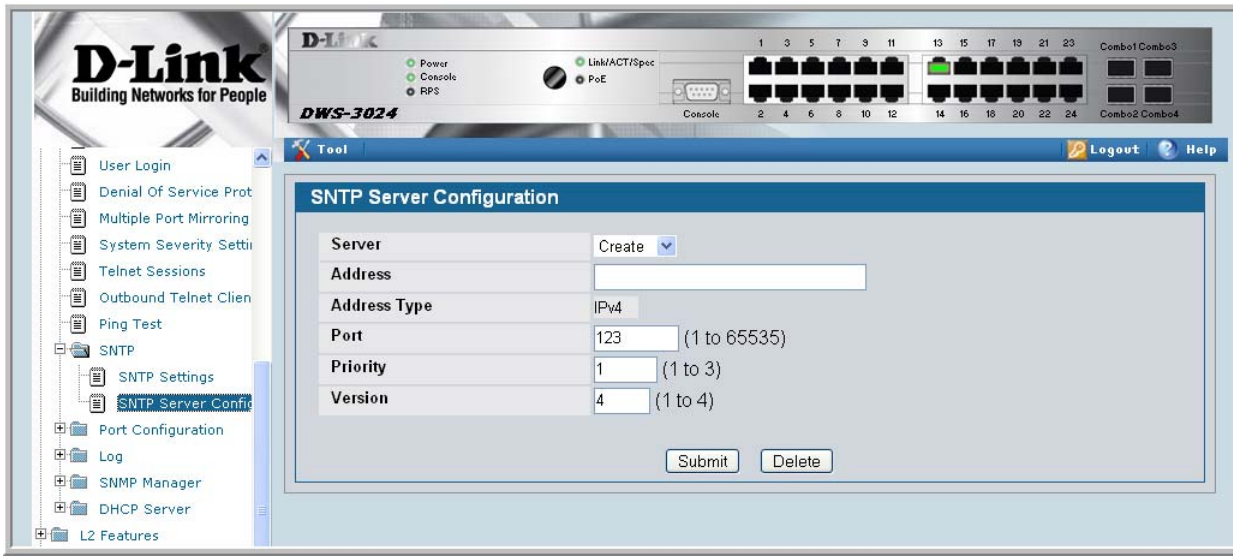
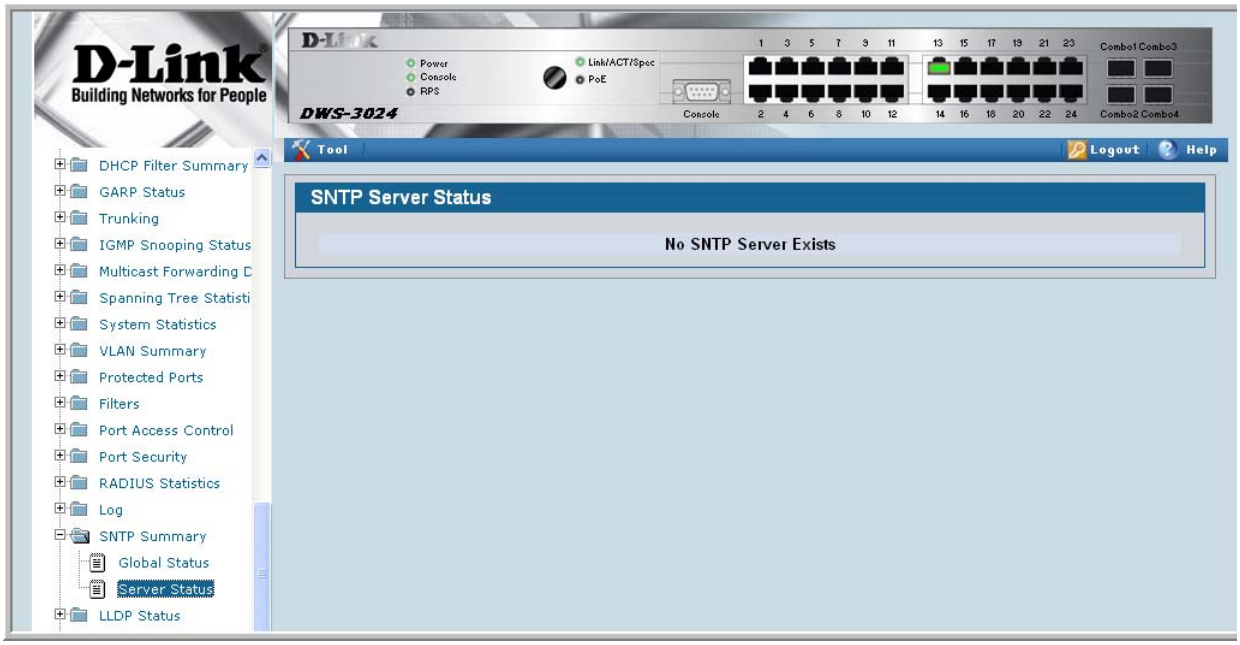


Figure 104. SNTP Server Status Page



27

Syslog

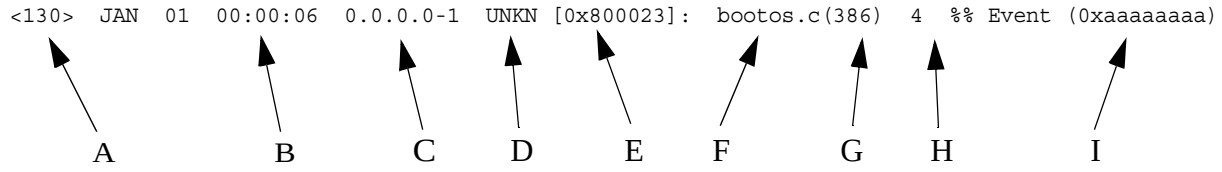
This section provides information about the Syslog feature.

Overview

Syslog:

- Allows you to store system messages and/or errors
- Can store to local files on the switch or a remote server running a syslog daemon
- Method of collecting message logs from many systems

Interpreting Log Files



A. Priority
B. Timestamp
C. Stack ID
D. Component Name
E. Thread ID
F. File Name
G. Line Number
H Sequence Number
I. Message

CLI Examples

The following are examples of the commands used in the Syslog feature.

Example #1: show logging

```
(DWS-3024) #show logging

Logging Client Local Port     :          514
CLI Command Logging           :           disabled
Console Logging               :          disabled
Console Logging Severity Filter:         alert
Buffered Logging              :          enabled

Syslog Logging                :          enabled

Log Messages Received         :          66
Log Messages Dropped          :          0
Log Messages Relayed          :          0
```

Example #2: show logging buffered

```
(DWS-3024) #show logging buffered ?

<cr>                      Press Enter to execute the command.

(DWS-3024) #show logging buffered

Buffered (In-Memory) Logging  :          enabled
Buffered Logging Wrapping Behavior:      On
Buffered Log Count            :          66
```

```
<6> Nov 29 13:31:38 0.0.0.0-1 UNKN[292290880]: sysapi.c(1280) 3 %% sysapiCfgFile
sSeparate: CRC check failed. 0x0 read and 0xce0a37e0 calculated
<6> Nov 29 13:31:38 0.0.0.0-1 UNKN[292290880]: sysapi.c(1131) 4 %% could not sep
arate SYSAPI_CONFIG_FILENAME
<2> Nov 29 13:31:42 0.0.0.0-1 UNKN[292290880]: bootos.c(332) 5 %% Event(0xaaaaaa
aa)
<6> Nov 29 13:31:49 0.0.0.0-1 UNKN[296038472]: sysapi.c(1912) 6 %% Building defa
ults for file log.cfg version 1
<6> Nov 29 13:32:12 0.0.0.0-1 UNKN[295813352]: edb.c(360) 7 %% EDB Callback: Uni
t Join: 1.
<6> Nov 29 13:32:12 0.0.0.0-1 UNKN[293358784]: sysapi.c(1912) 8 %% Building defa
ults for file simCfgData.cfg version 3
```


Example #3: show logging traplogs

```
(DWS-3024) #show logging traplogs

Number of Traps Since Last Reset.............. 16
Trap Log Capacity............................. 256
Number of Traps Since Log Last Viewed.......... 0

Log System Up Time           Trap
--- ----------------------- ---------------------------------------
  0 6 days 20:22:35          Failed User Login: Unit: 1 User ID:
  1 6 days 19:19:58          Multiple Users: Unit: 0 Slot: 3 Port: 1
  2 5 days 23:31:27          Multiple Users: Unit: 0 Slot: 3 Port: 1
  3 5 days 19:21:51          Multiple Users: Unit: 0 Slot: 3 Port: 1
  4 2 days 23:16:32          Link Down: Unit: 0 Slot: 1 Port: 2
  5 2 days 23:16:03          Link Down: Unit: 0 Slot: 1 Port: 1
  6 2 days 19:49:28          Multiple Users: Unit: 0 Slot: 3 Port: 1
  7 2 days 18:20:56          Multiple Users: Unit: 0 Slot: 3 Port: 1
  8 2 days 17:10:41          Multiple Users: Unit: 0 Slot: 3 Port: 1
  9 2 days 00:55:42          Multiple Users: Unit: 0 Slot: 3 Port: 1
 10 2 days 00:55:38          Failed User Login: Unit: 1 User ID: admin
 11 2 days 00:20:12          Multiple Users: Unit: 0 Slot: 3 Port: 1
```

Example 4: show logging hosts

```
(DWS-3024) #show logging hosts ?

<cr>                       Press Enter to execute the command.

(DWS-3024) #show logging hosts

Index     IP Address       Severity   Port     Status
-----  -----------------  ----------  ----  -------------
1      192.168.21.253     critical    514   Active
```

Example #5: logging port configuration

```
(DWS-3024)                          #config

(DWS-3024) (Config)#logging ?

buffered                Buffered (In-Memory) Logging Configuration.
cli-command             CLI Command Logging Configuration.
console                 Console Logging Configuration.
host                    Enter IP Address for Logging Host
syslog                  Syslog Configuration.

(DWS-3024) (Config)#logging host ?

<hostaddress>           Enter Logging Host IP Address
reconfigure             Logging Host Reconfiguration
remove                  Logging Host Removal

(DWS-3024) (Config)#logging host 192.168.21.253 ?

<cr>                    Press Enter to execute the command.
<port>                  Enter Port ID from 0 to 65535

(DWS-3024) (Config)#logging host 192.168.21.253 4 ?

<cr>                    Press Enter to execute the command.
<severitylevel>         Enter Logging Severity Level (emergency|0, alert|1,
                        critical|2, error|3, warning|4, notice|5, info|6,
                        debug|7).

(DWS-3024) (Config)#logging host 192.168.21.253 4 1 ?

<cr>                    Press Enter to execute the command.

(DWS-3024) (Config)#logging host 192.168.21.253 4 1

(DWS-3024) (Config)#exit

(DWS-3024) #show logging hosts

Index     IP Address      Port     Status
-----  -----------------  ----  -------------
1      192.168.21.253     4     Active
```


Web Examples

The following web pages are used with the Syslog feature.

Figure 105. Log - Syslog Configuration Page

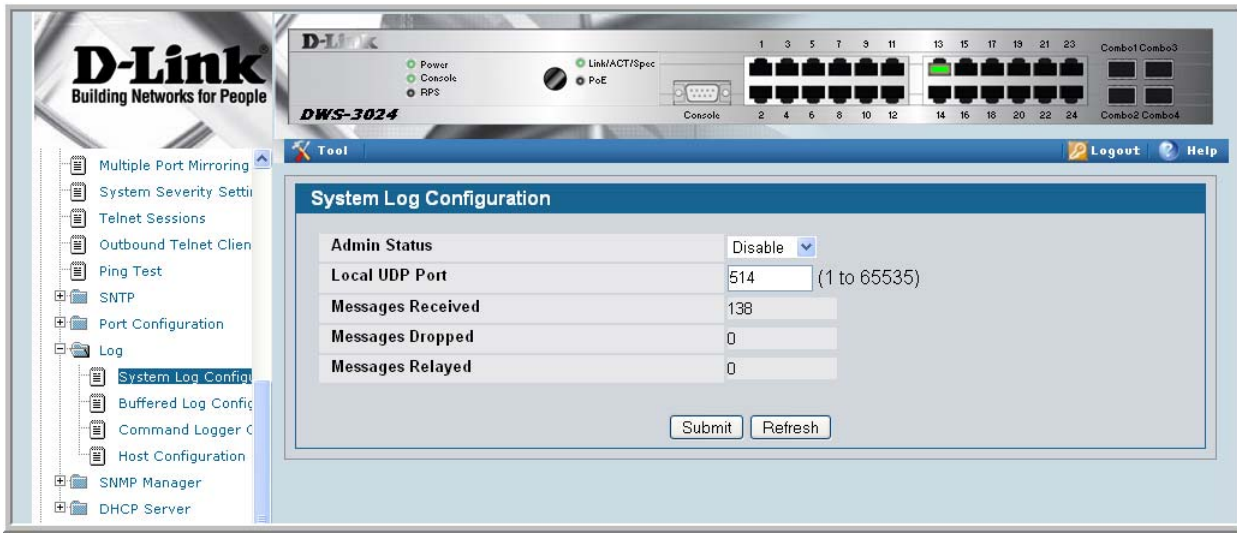


Figure 106. Buffered Log Configuration Page

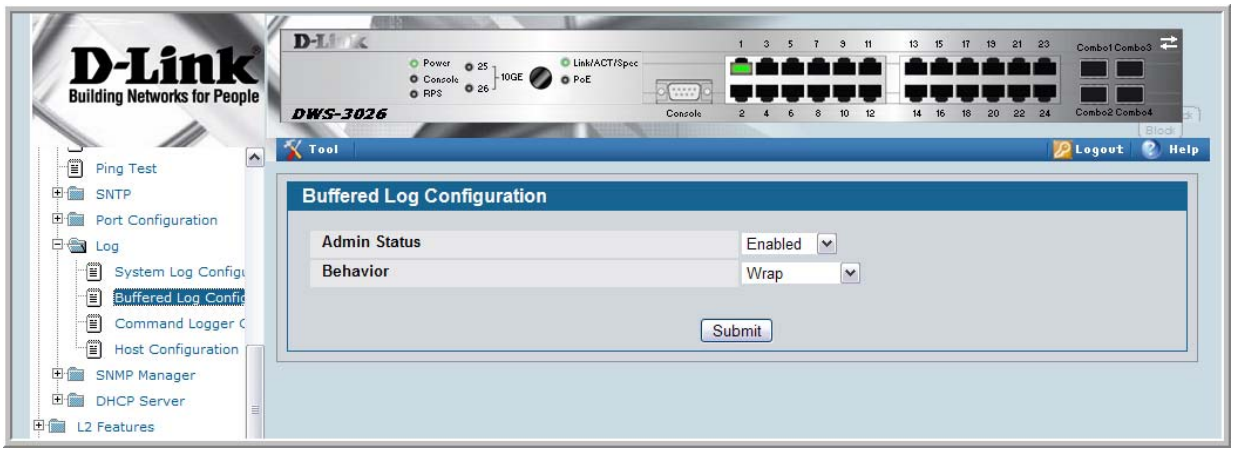


Figure 107. Log - Hosts Configuration Page - Add Host

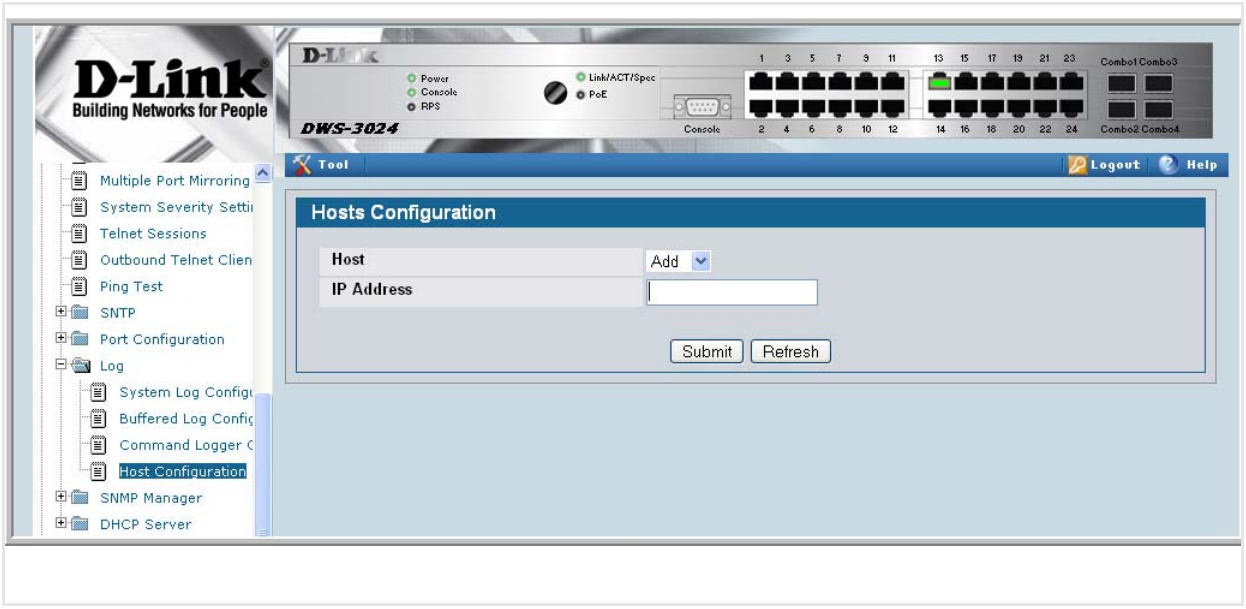
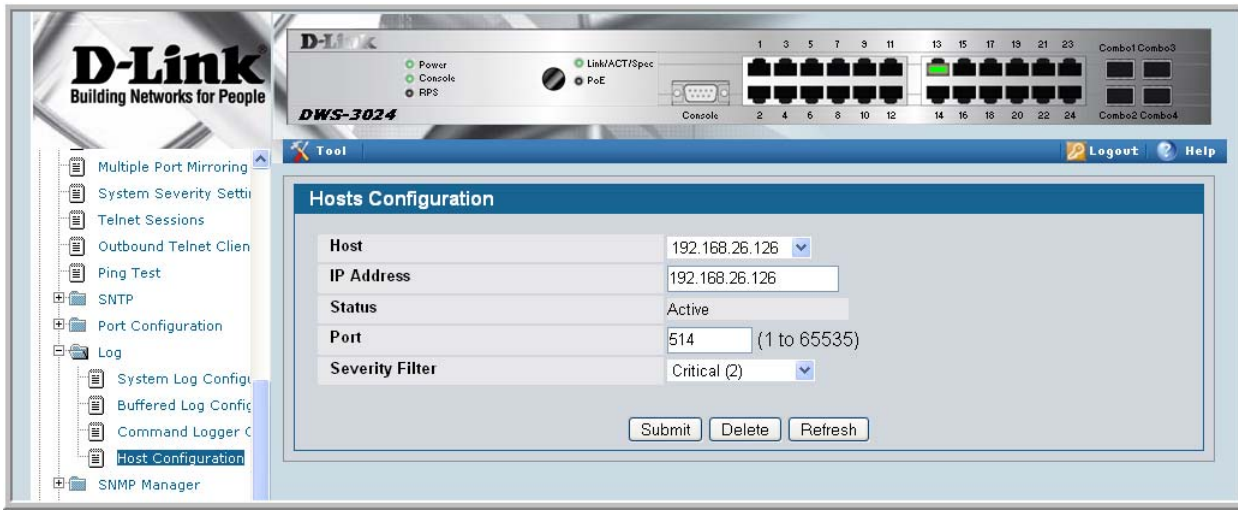


Figure 108. Log - Hosts Configuration Page



28

Port Description

The Port Description feature lets you specify an alphanumeric interface identifier that can be used for SNMP network management.

CLI Example

Use the commands shown below for the Port Description feature.

Example #1: Enter a Description for a Port

This example specifies the name “Test” for port 0/10:

```
config
     interface 0/10
          description Test
          exit
     exit
```

Example #2: Show the Port Description

```
show port description 0/10

Interface.......0/10
ifIndex.........10
Description.....Test
MAC Address.....00:00:00:01:00:02
Bit Offset Val..10
```

Configuring Port Description with the Web Interface

Use the following Web screen to enter Port Description information.

Figure 109. Port Configuration Screen - Set Port Description