Data Center Switch Software (DCSS)

Administrator's Guide

61700558F1MC-31B

August, 2018

Table of Contents

List of Tables

Trademarks

Any brand names and product names included in this manual are trademarks, registered trademarks, service marks, or trade names of their respective holders.

To the Holder of this Manual

The contents of this manual are current as of the date of publication. ADTRAN reserves the right to change the contents without prior notice.

In no event will ADTRAN be liable for any special, incidental, or consequential damages or for commercial losses even if ADTRAN has been advised thereof as a result of issue of this publication.

Be advised that certain security risks are inherent in the use of any telecommunications or networking equipment, including but not limited to, toll fraud, Denial of Service (DoS) attacks, loss or theft of data, and the unauthorized or illegal use of said equipment. ADTRAN OFFERS NO WARRANTIES, EITHER EXPRESSED OR IMPLIED, REGARDING THE PREVENTION, DETECTION, OR DETERRENCE OF TOLL FRAUD, NETWORKING ATTACKS, OR UNAUTHORIZED, ILLEGAL, OR IMPROPER USE OF ADTRAN EQUIPMENT OR SOFTWARE. THEREFORE, ADTRAN IS NOT LIABLE FOR ANY LOSSES OR DAMAGES RESULTING FROM SUCH FRAUD, ATTACK, OR IMPROPER USE, INCLUDING, BUT NOT LIMITED TO, HUMAN AND DATA PRIVACY, INTELLECTUAL PROPERTY, MATERIAL ASSETS, FINANCIAL RESOURCES, LABOR AND LEGAL COSTS. Ultimately, the responsibility for securing your telecommunication and networking equipment rests with you, and you are encouraged to review documentation regarding available security measures, their configuration and implementation, and to test such features as is necessary for your network.

Software Licensing Agreement

Each ADTRAN product contains a single license for ADTRAN supplied software. Pursuant to the Licensing Agreement, you may: (a) use the software on the purchased ADTRAN device only and (b) keep a copy of the software for backup purposes. This Agreement covers all software installed on the system, as well as any software available on the ADTRAN website. In addition, certain ADTRAN systems may contain additional conditions for obtaining software upgrades.

ADTRAN®
901 Explorer Boulevard
P.O. Box 140000
Huntsville, AL 35814-4000
Phone: (256) 963-8000
www.adtran.com
61700558F1MC-31B

Service and Warranty

For information on the service and warranty of ADTRAN products, visit the ADTRAN website at http://www.adtran.com/support.

Export Statement

An Export License is required if an ADTRAN product is sold to a Government Entity outside of the EU+8 (Austria, Australia, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland and the United Kingdom). This requirement is per DOC/BIS ruling G030477 issued 6/6/03. This product also requires that the Exporter of Record file a semi-annual report with the BXA detailing the information per EAR 740.17(5)(e)(2).

DOC - Department of Commerce
BIS - Bureau of Industry and Security
BXA - Bureau of Export Administration

About This Document

Purpose and Audience

This guide describes the DCSS software features and provides configuration examples for many of the features. DCSS software runs on a variety of platforms and is ideal for Layer 2/3 switching solutions in the data center.

The information in this guide is intended for any of the following individuals:

- System administrators who are responsible for configuring and operating a network using DCSS software
- Software engineers who are integrating DCSS software into a router or switch product
- Level 1 and/or Level 2 Support providers

To obtain the greatest benefit from this guide, you should have an understanding of the base software and should have read the specification for your networking device platform. You should also have basic knowledge of Ethernet and networking concepts.

Document Organization

This guide contains the following sections:

- Section 1: “DCSS Features,” on page 10 provides an overview of the features that DCSS software supports.
- Section 2: “Getting Started with Switch Configuration,” on page 17 contains information about the boot process, initial system configuration and user interface access.
- Section 3: “Configuring Switch Management Features,” on page 30 describes how to perform typical system maintenance tasks, such as installing a new image.

- Section 4: "Configuring Switching Features," on page 42 describes how to manage and monitor some of the key Layer 2 switching features, such as VLANs and spanning tree protocol (STP).
- Section 5: "Configuring Routing," on page 60 provides summary information and configuration examples for some of the Layer 3 routing features that DCSS software supports.

Document Conventions

The following conventions may be used in this document:

Table 1: Typographical Conventions

Symbol	*Description*	*Example*
Blue Text	Hyperlinked text.	See "About This Document" on page 8.
`courier font`	Command or command-line text	`show network`
`italic courier font`	Variable value. You must replace the italicized text with an appropriate value, which might be a name or number.	*`value`*
[] square brackets	Optional parameter.	`[value]`
{ } curly braces	Required parameter values. You must select a parameter from the list or range of choices.	`{choice1 | choice2}`
| Vertical bar	Separates the mutually exclusive choices.	`choice1 | choice2`
[{ }] Braces within square brackets	Optional parameter values. Indicates a choice within an optional element.	`[{choice1 | choice2}]`

Supported features

The following list of features is supported on the ADTRAN 1748F. Any other commands or features available in the product are untested and are used at your own risk. ADTRAN Support recommends not using untested commands or features.

- Basic Layer 2 and Layer 3 VLANs (VLAN port-assignments, IP addressing)
- Layer 3 Static Routing/Switching
- LLDP
- LLDP med
- IP DHCP helper (DHCP forwarding)
- SNMP
- SNTP
- Rapid Spanning Tree
- DNS-Client
- Console/SSH/Telnet Access
- Static LACP
- Logging, debug, and Show Commands associated with the above feature set

Section 1: DCSS Features

This section provides a brief overview of the supported DCSS features. The features are categorized as follows:

- “Management Features” on page 10
- “Switching Features” on page 13
- “Routing Features” on page 16
- “Getting Started with Switch Configuration” on page 17

Management Features

This section describes the management features DCSS software supports. For additional information and configuration examples for some of these features, see Section 3: “Configuring Switch Management Features”.

Management Options

You can use the following methods to manage the switch:

- Use a telnet client, SSH client, or a direct console connection to access the CLI. The CLI syntax and semantics conform as much as possible to common industry practice.
- Use a network management system (NMS) to manage and monitor the system through SNMP. The switch supports SNMP v1/v2c/v3 over the UDP/IP transport protocol.

Management of Basic Network Information

The DHCP client on the switch allows the switch to acquire information such as the IP address and default gateway from a network DHCP server. You can also disable the DHCP client and configure static network information. Other configurable network information includes a Domain Name Server (DNS), host name to IP address mapping, and a default domain name.

Dual Software Images

The switch can store up to two software images. The dual image feature allows you to upgrade the switch without deleting the older software image. You designate one image as the active image and the other image as the backup image.

Warm Reboot

The Warm Reboot feature reduces the time it takes to reboot the switch thereby reducing the traffic disruption in the network during a switch reboot. For a typical switch, the traffic disruption is reduced from about two minutes for a cold reboot to about 20 seconds for a warm reboot.

SNMP Alarms and Trap Logs

The system logs events with severity codes and timestamps. The events are sent as SNMP traps to a trap recipient list.

Log Messages

The switch maintains in-memory log messages as well as persistent logs. You can also configure remote logging so that the switch sends log messages to a remote log server. You can also configure the switch to send log messages to a configured SMTP server. This allows you to receive the log message in an e-mail account of your choice. Switch auditing messages, CLI command logging, and SNMP logging can be enabled or disabled.

System Time Management

You can configure the switch to obtain the system time and date through a remote Simple Network Time Protocol (SNTP) server, or you can set the time and date locally on the switch. You can also configure the time zone and information about time shifts that might occur during summer months.

Note: The manually-configured local clock settings are not retained across a system reset if the platform does not include a Real Time Clock (RTC).

Source IP Address Configuration

Syslog, TACACS, SNTP, sFlow, SNMP Trap, RADIUS, and DNS Clients allow the IP Stack to select the source IP address while generating the packet. This feature provides an option for the user to select an interface for the source IP address while the management protocol transmits packets to management stations. The source address is specified for each protocol.

Core Dump

The core dump feature provides the ability to retrieve the state from a crashed box such that it can be then loaded into a debugger and have that state re-created there.

Core Dump File Handling

A core dump file can be transferred to a debugger using several methods, depending on the supported switch interfaces and capabilities:

- Via a USB connection (if supported)
- Stored locally on flash (if it is of sufficient size) and accessed from a remote system via NFS.
- Transferred via FTP to a remote FTP server.

Because the size of the core dump file can be several hundred megabytes, the file is compressed using the bzip2 compression technique available in BusyBox. Compression is enabled by default and can be enabled/disabled using the CLI.

Kernel Core Dump

The kernel core dump feature enables the system to perform a warm reboot into a new kernel in reserved memory, allowing the current state of the operating kernel to be captured for analysis. This feature is available only on Ubuntu Linux distributions of the DCSS software.

Switching Features

This section describes the Layer 2 switching features DCSS software supports. For additional information and configuration examples for some of these features, see Section 4: “Configuring Switching Features,” on page 42.

VLAN Support

VLANs are collections of switching ports that comprise a single broadcast domain. Packets are classified as belonging to a VLAN based on either the VLAN tag or a combination of the ingress port and packet contents. Packets sharing common attributes can be groups in the same VLAN. DCSS software is in full compliance with IEEE 802.1Q VLAN tagging.

Switchport Modes

The switchport mode feature helps to minimize the potential for configuration errors. The feature also makes VLAN configuration easier by reducing the amount of commands needed for port configuration. For example, to configure a port connected to an end user, the administrator can configure the port in Access mode. Ports connected to other switches can be configured in Trunk mode. VLAN assignments and tagging behavior are automatically configured as appropriate for the connection type.

A third switchport mode, General mode, provides no configuration restrictions and allows the administrator to configure the port with custom VLAN settings.

Spanning Tree Protocol (STP)

Spanning Tree Protocol (IEEE 802.1D) is a standard requirement of Layer 2 switches that allows bridges to automatically prevent and resolve L2 forwarding loops. The STP feature supports a variety of per-port settings including path cost, priority settings, Port Fast mode, STP Root Guard, Loop Guard, TCN Guard, and Auto Edge. These settings are also configurable per-LAG.

Rapid Spanning Tree

Rapid Spanning Tree Protocol (RSTP) detects and uses network topologies to enable faster spanning tree convergence after a topology change, without creating forwarding loops. The port settings supported by STP are also supported by RSTP.

Bridge Protocol Data Unit (BPDU) Guard

Spanning Tree BPDU Guard is used to disable the port in case a new device tries to enter the already existing topology of STP. Thus devices, which were originally not a part of STP, are not allowed to influence the STP topology.

BPDU Filtering

When spanning tree is disabled on a port, the BPDU Filtering feature allows BPDU packets received on that port to be dropped. Additionally, the BPDU Filtering feature prevents a port in Port Fast mode from sending and receiving BPDUs. A port in Port Fast mode is automatically placed in the forwarding state when the link is up to increase convergence time.

Link Aggregate Control Protocol (LACP)

Link Aggregate Control Protocol (LACP) uses peer exchanges across links to determine, on an ongoing basis, the aggregation capability of various links, and continuously provides the maximum level of aggregation capability achievable between a given pair of systems. LACP automatically determines, configures, binds, and monitors the binding of ports to aggregators within the system.

Auto-MDI/MDIX Support

Your switch supports auto-detection between crossed and straight-through cables. Media-Dependent Interface (MDI) is the standard wiring for end stations, and the standard wiring for hubs and switches is known as Media-Dependent Interface with Crossover (MDIX).

Auto Negotiation

Auto negotiation allows the switch to advertise modes of operation. The auto negotiation function provides the means to exchange information between two switches that share a point-to-point link segment, and to automatically configure both switches to take maximum advantage of their transmission capabilities.

The switch enhances auto negotiation by providing configuration of port advertisement. Port advertisement allows the system administrator to configure the port speeds that are advertised.

Static and Dynamic MAC Address Tables

You can add static entries to the switch’s MAC address table and configure the aging time for entries in the dynamic MAC address table. You can also search for entries in the dynamic table based on several different criteria.

Link Layer Discovery Protocol (LLDP)

The IEEE 802.1AB defined standard, Link Layer Discovery Protocol (LLDP), allows the switch to advertise major capabilities and physical descriptions. This information can help you identify system topology and detect bad configurations on the LAN.

Link Layer Discovery Protocol (LLDP) for Media Endpoint Devices

The Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) provides an extension to the LLDP standard for network configuration and policy, device location, Power over Ethernet management, and inventory management.

DHCP Layer 2 Relay

This feature permits Layer 3 Relay agent functionality in Layer 2 switched networks. The switch supports L2 DHCP relay configuration on individual ports, link aggregation groups (LAGs) and VLANs.

Management and Control Plane ACLs

This feature provides hardware-based filtering of traffic to the CPU. An optional 'management' feature is available to apply the ACL on the CPU port. Currently, control packets like BPDU are dropped because of the implicit 'deny all' rule added at the end of the list. To overcome this rule, you must add rules that allow the control packets.

Support for user-defined simple rate limiting rule attributes for inbound as well as outbound traffic is also available. This attribute is supported on all QoS capable interfaces - physical, lag, and control-plane. Outbound direction is only supported on platforms with an Egress Field Processor (EFP).

Routing Features

This section describes the layer-3 routing features DCSS software supports. For additional information and configuration examples for some of these features, see Section 5: “Configuring Routing,” on page 60.

VLAN Routing

DCSS software supports VLAN routing. You can also configure the software to allow traffic on a VLAN to be treated as if the VLAN were a router port.

IP Configuration

The switch IP configuration settings to allow you to configure network information for VLAN routing interfaces such as IP address and subnet mask, MTU size, and ICMP redirects. Global IP configuration settings for the switch allow you to enable or disable the generation of several types of ICMP messages and enable or disable the routing mode.

ARP Table Management

You can create static Address Resolution Protocol (ARP) entries and manage many settings for the dynamic ARP table, such as age time for entries, retries, and cache size.

BOOTP/DHCP Relay Agent

The switch BOOTP/DHCP Relay Agent feature relays BOOTP and DHCP messages between DHCP clients and DHCP servers that are located in different IP subnets.

IP Helper and UDP Relay

The IP Helper and UDP Relay features provide the ability to relay various protocols to servers on a different subnet.

Routing Table

The routing table displays information about the routes that have been dynamically learned. You can configure static and default routes and route preferences. A separate table shows the routes that have been manually configured.

Section 2: Getting Started with Switch Configuration

Accessing the Switch Command-Line Interface

The command-line interface (CLI) provides a text-based way to manage and monitor the switch features. You can access the CLI by using a direct connection to the console port or by using a Telnet or SSH client.

To access the switch by using Telnet or Secure Shell (SSH), the switch must have an IP address configured on either the service port or the network interface, and the management station you use to access the device must be able to ping the switch IP address. DHCP is enabled by default on the service port. It is disabled on the network interface.

Connecting to the Switch Console

To connect to the switch and configure or view network information, use the following steps:

1. Using a straight-through modem cable, connect a VT100/ANSI terminal or a workstation to the console (serial) port.

   If you attached a PC, Apple, or UNIX workstation, start a terminal-emulation program, such as HyperTerminal or TeraTerm.

2. Configure the terminal-emulation program to use the following settings:
   - Baud rate: 9600 bps
   - Data bits: 8
   - Parity: none
   - Stop bit: 1
   - Flow control: none

3. Power on the switch.

   For information about the boot process, including how to access the boot menu, see “Booting the Switch” on page 21.

   After the system completes the boot cycle, the `User:` prompt appears.

4. At the `User:` prompt, type `admin` and press ENTER. The `Password:` prompt appears.

5. There is no default password. Press ENTER at the password prompt if you did not change the default password.

   After a successful login, the screen shows the system prompt, for example `(Routing) >`.

6. At the `(Routing) >` prompt, enter `enable` to enter the Privileged EXEC command mode.

7. There is no default password to enter Privileged EXEC mode. Press ENTER at the password prompt if you did not change the default password.

   The command prompt changes to `(Routing) #`.

8. To view service port network information, type `show serviceport` and press ENTER.

```
(Routing) #show serviceport

Interface Status............................... Up
IP Address..................................... 10.27.21.33
Subnet Mask.................................... 255.255.252.0
Default Gateway................................ 10.27.20.1
IPv6 Administrative Mode....................... Enabled
IPv6 Prefix is ................................ fe80::210:18ff:fe82:157c/64
Configured IPv4 Protocol....................... DHCP
Configured IPv6 Protocol....................... None
IPv6 AutoConfig Mode........................... Disabled
Burned In MAC Address.......................... 00:10:18:82:15:7C
```

By default, the DHCP client on the service port is enabled. If your network has a DHCP server, then you need only to connect the switch service port to your management network to allow the switch to acquire basic network information.

Accessing the Switch CLI Through the Network

Remote management of the switch is available through the service port or through the network interface. To use telnet, SSH, or SNMP for switch management, the switch must be connected to the network, and you must know the IP or IPv6 address of the management interface. The switch has no IP address by default. The DHCP client on the service port is enabled, and the DHCP client on the network interface is disabled.

After you configure or view network information, configure the authentication profile for telnet or SSH and physically and logically connect the switch to the network, you can manage and monitor the switch remotely. You can also continue to manage the switch through the terminal interface via the console port.

Using the Service Port or Network Interface for Remote Management

The service port is a dedicated Ethernet port for out-of-band management. ADTRAN recommends that you use the service port to manage the switch. Traffic on this port is segregated from operational network traffic on the switch ports and cannot be switched or routed to the operational network. Additionally, if the production network is experiencing problems, the service port still allows you to access the switch management interface and troubleshoot issues. Configuration options on the service port are limited, which makes it difficult to accidentally cut off management access to the switch.

Alternatively, you can choose to manage the switch through the production network, which is known as in-band management. Because in-band management traffic is mixed in with production network traffic, it is subject to all of the filtering rules usually applied on a switched/routed port such as ACLs and VLAN tagging. You can access the in-band network management interface through a connection to any front-panel port.

Configuring Service Port Information

To disable DHCP/BOOTP and manually assign an IPv4 address, enter:

```
serviceport protocol none
serviceport ip ipaddress netmask [gateway]
```

For example, `serviceport ip 192.168.2.23 255.255.255.0 192.168.2.1`

To disable DHCP/BOOTP and manually assign an IPv6 address and (optionally) default gateway, enter:

```
serviceport protocol none
serviceport ipv6 address address/prefix-length [eui64]
serviceport ipv6 gateway gateway
```

To view the assigned or configured network address, enter:

```
show serviceport
```

To enable the DHCP client on the service port, enter:

```
serviceport protocol dhcp
```

To enable the BOOTP client on the service port, enter:

```
serviceport protocol bootp
```

Configuring the In-Band Network Interface

To use a DHCP server to obtain the IP address, subnet mask, and default gateway information, enter:

```
network protocol dhcp.
```

To use a BOOTP server to obtain the IP address, subnet mask, and default gateway information, enter:

```
network protocol bootp.
```

To manually configure the IPv4 address, subnet mask, and (optionally) default gateway, enter:

```
network parms ipaddress netmask [gateway],
```

For example, `network parms 192.168.2.23 255.255.255.0 192.168.2.1`

To manually configure the IPv6 address, subnet mask, and (optionally) default gateway, enter:

```
network ipv6 address address/prefix-length [eui64]
network ipv6 gateway gateway
```

To view the network information, enter:

```
show network.
```

To save these changes so they are retained during a switch reset, enter the following command:

```
copy system:running-config nvram:startup-config
```

Booting the Switch

When the power is turned on with the local terminal already connected, the switch goes through Power-On Self-Test (POST). POST runs every time the switch is initialized and checks hardware components to determine if the switch is fully operational before completely booting.

If a critical problem is detected, the program flow stops. If POST passes successfully, a valid executable image is loaded into RAM.

POST messages are displayed on the terminal and indicate test success or failure.

To view the text that prints to the screen during the boot process, complete the following steps:

1. Make sure that the serial cable is connected to the terminal.
2. Connect the power supply to the switch.
3. Power on the switch.

   As the switch boots, the boot-up test first counts the switch memory availability and then continues to boot.
4. During boot, you can use the Utility menu, if necessary, to run special procedures. To enter the Boot menu, press **2** within the first five seconds after the following message appears.

   ```
   Select startup mode.  If no selection is made within 5 seconds,
   the FASTPATH Application will start automatically...

   FASTPATH Startup -- Main Menu

   1 - Start FASTPATH Application
   2 - Display Utility Menu
   Select (1, 2):
   ```

   For information about the Boot menu, see ““Utility Menu Functions” on page 22."
5. If you do not start the boot menu, the operational code continues to load.

After the switch boots successfully, the User login prompt appears and you can use the local terminal to begin configuring the switch. However, before configuring the switch, make sure that the software version installed on the switch is the latest version.

Utility Menu Functions

Note: Utility menu functions vary on different platforms. The following example might not represent the options available on your platform.

You can perform many configuration tasks through the Utility menu, which can be invoked after the first part of the POST is completed.

To display the Utility menu, boot the switch observe the output that prints to the screen. After various system initialization information displays, the following message appears:

```
FASTPATH Startup Rev: 8.2

Select startup mode.  If no selection is made within 5 seconds,
the FASTPATH Application will start automatically...

FASTPATH Startup -- Main Menu

1 - Start FASTPATH Application
2 - Display Utility Menu
Select (1, 2):
```

Press press **2** within five seconds to start the Utility menu. If you do not press 2, the system loads the operational code.

After you press **2** the following information appears:

```
FASTPATH Startup -- Utility Menu

 1  - Start FASTPATH Application
 2  - Load Code Update Package
 3  - Load Configuration
 4  - Select Serial Speed
 5  - Retrieve Error Log
 6  - Erase Current Configuration
 7  - Erase Permanent Storage
 8  - Select Boot Method
 9  - Activate Backup Image
10  - Start Diagnostic Application
11  - Reboot
12 - Rease All Configuration Files

 Q  - Quit from FASTPATH Startup

Select option (1-12 or Q):
```

The following sections describe the Utility menu options.

1 – Start DCSS Application

Use option 1 to resume loading the operational code. After you enter 1, the switch exits the Startup Utility menu and the switch continues the boot process.

2 – Load Code Update Package

Use option 2 to download a new software image to the switch to replace a corrupted image or to update, or upgrade the system software.

The switch is preloaded with DCSS software, so these procedures are needed only for upgrading or downgrading to a different image.

You can use any of the following methods to download the image:

- TFTP
- XMODEM
- YMODEM
- ZMODEM

If you use TFTP to download the code, the switch must be connected to the network, and the code to download must be located on the TFTP server.

When you use XMODEM, YMODEM, or ZMODEM to download the code, the code must be located on an administrative system that has a console connection to the switch.

Use the following procedures to download an image to the switch by using TFTP:

1. From the Utility menu, select **2** and press ENTER.

   The switch creates a temporary directory and prompts you to select the download method:

   ```
   Creating tmpfs filesystem on tmpfs for download...done.
   Select Mode of Transfer (Press T/X/Y/Z for TFTP/XMODEM/YMODEM/ZMODEM) []:
   ```
2. Enter **T** to download the image from a TFTP server to the switch.
3. Enter the IP address of the TFTP server where the new image is located, for example:

   ```
   Enter Server IP []:192.168.1.115
   ```
4. Enter the desired IP address of the switch management interface, for example:

   ```
   Enter Host IP []192.168.1.23
   ```

Note: The switch uses the IP address, subnet mask, and default gateway information you specify for the TFTP download process only. The switch automatically reboots after the process completes, and this information is not saved.

5. Enter the subnet mask associated with the management interface IP address or press ENTER to accept the default value, which is 255.255.255.0.
6. Optionally, enter the IP address of the default gateway for the switch management interface, for example:

   ```
   Enter Gateway IP []192.168.1.1
   ```

7. Enter the filename, including the file path (if it is not in the TFTP root directory), of the image to download, for example:

   ```
   Enter Filename[]images/image0630.stk
   ```

8. Confirm the information you entered and enter **y** to allow the switch to contact the TFTP server.

   After the download completes, you are prompted to reboot the switch. The switch loads the image during the next boot cycle.

Use the following procedures to download an image to the switch by using XMODEM, YMODEM, or ZMODEM.

1. From the Utility menu, select **2** and press ENTER.

   The switch creates a temporary directory and prompts you to select the download method:

   ```
   Creating tmpfs filesystem on tmpfs for download...done.
   Select Mode of Transfer (Press T/X/Y/Z for TFTP/XMODEM/YMODEM/ZMODEM) []:
   ```

2. Specify the protocol to use for the download.
   - Enter **X** to download the image by using the XMODEM file transfer protocol.
   - Enter **Y** to download the image by using the YMODEM file transfer protocol.
   - Enter **Z** to download the image by using the ZMODEM file transfer protocol.

3. When you are ready to transfer the file from the administrative system, enter **y** to continue.

   ```
   Do you want to continue? Press(Y/N): y
   ```

4. From the terminal or terminal emulation application on the administrative system, initiate the file transfer.

   For example, if you use HyperTerminal, use the following procedures:

   a. From the **HyperTerminal** menu bar, click **Transfer** > **Send File**.

      The **Send File** window displays.

   b. Browse to the file to download and click **Open** to select it.

   c. From the **Protocol:** field, select the protocol to use for the file transfer.

   d. Click **Send**.

   After you start the file transfer, the software is downloaded to the switch, which can take several minutes. The terminal emulation application might display the loading process progress.

5. After software downloads, you are prompted to reboot the switch. The switch loads the image during the next boot cycle.

3 – Load Configuration

Use option **3** to download a new configuration that will replace the saved system configuration file. You can use any of the following methods to download the configuration file:

- TFTP
- XMODEM
- YMODEM
- ZMODEM

Use the following procedures to download a configuration file to the switch.

1. From the Utility menu, select **3** and press ENTER.
2. Enter T to download the text-based configuration file to the switch.
3. Specify the protocol to use for the download.
4. Respond to the prompts to begin the file transfer.

   The configuration file download procedures are very similar to the software image download procedures. For more information about the prompts and how to respond, see "2 – Load Code Update Package" on page 23.

4 – Select Serial Speed

Use option **4** to change the baud rate of the serial interface (console port) on the switch. When you select option **4**, the following information displays:

```
1 - 2400
2 - 4800
3 - 9600
4 - 19200
5 - 38400
6 - 57600
7 - 115200
8 - Exit without change
Select option (1-8):
```

To set the serial speed, enter the number that corresponds to the desired speed.

Note: The selected baud rate takes effect immediately.

5 – Retrieve Error Log

Use option **5** to retrieve the error log that is stored in nonvolatile memory and upload it from the switch to your ASCII terminal or administrative system. You can use any of the following methods to copy the error log to the system:

- TFTP
- XMODEM
- YMODEM
- ZMODEM

Use the following procedures to upload the error log from the switch:

1. From the Utility menu, select **5** and press ENTER.
2. Specify the protocol to use for the download.
3. Respond to the prompts to begin the file transfer.

   If you use TFTP to upload the file from the switch to the TFTP server, the prompts and procedures very similar to the steps described for the TFTP software image download. For more information about the prompts and how to respond, see "2 – Load Code Update Package" on page 23.

   If you use XMODEM, YMODEM, or ZMODEM to transfer the file, configure the terminal or terminal emulation application with the appropriate settings to receive the file. For example, if you use HyperTerminal, click **Transfer** > **Receive File, and then specify where to put the file and which protocol to use.**

6 – Erase Current Configuration

Use option **6** to clear changes to the startup-config file and reset the system to its factory default setting. This option is the same as executing the `clear config` command from Privileged EXEC mode. You are not prompted to confirm the selection.

7 – Erase Permanent Storage

Use option **7** to completely erase the switch software application, any log files, and any configurations. The boot loader and operating system are not erased. Use this option only if a file has become corrupt and your are unable to use option **2**, Load Code Update Package, to load a new image onto the switch. After you erase permanent storage, you must download an image to the switch; otherwise, the switch will not be functional.

8 – Select Boot Method

Use option **8** to specify whether the system should boot from the image stored on the internal flash, from an image over the network, or from an image over the serial port. By default, the switch boots from the flash image.

To boot over the network, the image must be located on a TFTP server that can be accessed by the switch. To boot from the serial port, the switch must be connected through the console port to a terminal or system with a terminal emulator. The image must be located on the connected device.

If you select option **8**, the following menu appears:

```
Current boot method: FLASH
1 - Flash Boot
2 - Network Boot
3 - Serial Boot
4 - Exit without change
Select option (1-4):
```

If you select a new boot method, the switch uses the selected method for the next boot cycle.

9 – Activate Backup Image

Use option **9** to activate the backup image. The active image becomes the backup when you select this option. When you exit the Startup Utility and resume the boot process, the switch loads the image that you activated, but ADTRAN recommends that you reload the switch so it can perform an entire boot cycle with the newly active image.

After you activate the backup image, the following information appears.

```
Image image1 is now active.
Code update instructions found!
Extracting kernel and rootfs from image1
Copying kernel/rootfs uimage to boot flash area
Activation complete
image1 activated -- system reboot recommended!
Reboot? (Y/N):
```

Enter **y** to reload the switch.

10 – Start Diagnostic Application

Option **10** is for field support personnel only. Access to the diagnostic application is password protected.

11 – Reboot

Use option **11** to restart the boot process.

12 – Erase All Configuration Files

Use option **12** to clear changes to the startup-config file and the factory-defaults file and reset the system to its factory default (compile-time) setting. You are not prompted to confirm the selection.

Understanding the User Interfaces

DCSS software includes a set of comprehensive management functions for configuring and monitoring the system by using one of the following methods:

- Command-Line Interface (CLI)
- Simple Network Management Protocol (SNMP)
- RESTful API Interface
- RESTCONF Interface

These standards-based management methods allows you to configure and monitor the components of the DCSS software. The method you use to manage the system depend on your network size and requirements, and on your preference.

Note: Not all features are supported on all hardware platforms, so some CLI commands and object identifiers (OIDs) might not available on your platform.

Using the Command-Line Interface

The command-line interface (CLI) is a text-based way to manage and monitor the system. You can access the CLI by using a direct serial connection or by using a remote logical connection with telnet or SSH.

The CLI groups commands into modes according to the command function. Each of the command modes supports specific software commands. The commands in one mode are not available until you switch to that particular mode, with the exception of the User EXEC mode commands. You can execute the User EXEC mode commands in the Privileged EXEC mode.

To display the commands available in the current mode, enter a question mark (?) at the command prompt. To display the available command keywords or parameters, enter a question mark (?) after each word you type at the command prompt. If there are no additional command keywords or parameters, or if additional parameters are optional, the following message appears in the output:

```
<cr>                     Press Enter to execute the command
```

For more information about the CLI, see the *DCSS CLI Command Reference.*

The *DCSS CLI Command Reference* lists each command available from the CLI by the command name and provides a brief description of the command. Each command reference also contains the following information:

- The command keywords and the required and optional parameters.
- The command mode you must be in to access the command.
- The default value, if any, of a configurable setting on the device.

The `show` commands in the document also include a description of the information that the command shows.

Using SNMP

SNMP is enabled by default. The `show sysinfo` command displays the information you need to configure an SNMP manager to access the switch. You can configure SNMP groups and users that can manage traps that the SNMP agent generates.

DCSS uses both standard public MIBs for standard functionality and private MIBs that support additional switch functionality. All private MIBs begin with a “-” prefix. The main object for interface configuration is in -SWITCHING-MIB, which is a private MIB. Some interface configurations also involve objects in the public MIB, IF-MIB.

SNMPv3

SNMP version 3 (SNMPv3) adds security and remote configuration enhancements to SNMP. DCSS has the ability to configure SNMP server, users, and traps for SNMPv3. Any user can connect to the switch using the SNMPv3 protocol, but for authentication and encryption, you need to configure a new user profile. To configure a profile by using the CLI, see the SNMP section in the *DCSS CLI Command Reference*.

Section 3: Configuring Switch Management Features

Managing Images and Files

DCSS-based switches maintain several different types of files on the flash file system. Table 2 describes the files that you can manage. You use the `copy` command to copy a source file to a destination file. The copy command may permit the following actions (depending on the file type):

- Copy a file from the switch to a remote server.
- Copy a file from a remote server to the switch.
- Overwrite the contents of the destination file with the contents of the source file.

Table 2: Files to Manage

File	*Description*
active	The switch software image that has been loaded and is currently running on the switch.
backup	A second software image that is currently not running on the switch.
startup-config	Contains the software configuration that loads during the boot process.
running-config	Contains the current switch configuration.
factory-defaults	Contains the software configuration that can be used to load during the boot process or after clearing the configuration.
backup-config	An additional configuration file that serves as a backup. You can copy the startup-config file to the backup-config file.
fastpath.cfg	A binary configuration file.
Configuration script	Text file with CLI commands. When you apply a script on the switch, the commands are executed and added to the running-config.
CLI Banner	Text file containing the message that displays upon connecting to the switch or logging on to the switch by using the CLI.
Log files	Trap, error, or other log files that provide Provides various information about events that occur on the switch.

Table 2: Files to Manage (Cont.)

File	***Description***
SSH key files	Contains information to authenticate SSH sessions. The switch supports the following files for SSH: • SSH-1 RSA Key File • SSH-2 RSA Key File (PEM Encoded) • SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded) ***Note:*** If you use the CLI to manage the switch over an SSH connection, you must copy the appropriate key files to the switch.
IAS Users	List of Internal Authentication Server (IAS) users for IEEE 802.1X authentication. You can configure the switch to use the local IAS user database for port-based authentication instead of using a remote server, such as a RADIUS server.

Supported File Management Methods

For most file types, you can use any of the following protocols to download files from a remote system to the switch or to upload files from the switch to a remote system:

- FTP
- TFTP
- SFTP
- SCP
- XMODEM
- YMODEM
- ZMODEM

Note: The IAS Users file can be copied from a remote server to the switch only by using FTP, TFTP, SFTP, or SCP.

Uploading and Downloading Files

To use FTP, TFTP, SFTP, or SCP for file management, you must provide the IP address of the remote system that is running the appropriate server (FTP, TFTP, SFTP, or SCP). Make sure there is a route from the switch to the remote system. You can use the `ping` command from the CLI to verify that a route exists between the switch and the remote system.

If you are copying a file from the remote system to the switch, be sure to provide the correct path to the file (if the file is **not** in the root directory) and the correct file name.

Managing Switch Software (Images)

The switch can maintain two software images: the active image and the backup image. When you copy a new image from a remote system to the switch, you can specify whether to save it as the active or backup image. The downloaded image overwrites the image that you specify. If you save the new image as the active image, the switch continues to operate using the current (old) image until you reload the switch. Once the switch reboots, it loads with the new image. If you download the new image as the backup image, the file overwrites the current backup image, if it exists. To load the switch with the backup image, you must first set it as the active image and then reload the switch. The image that was previously the active image becomes the backup image after the switch reloads.

If you activate a new image and reload the switch, and the switch is unable to complete the boot process due to a corrupt image or other problem, you can use the boot menu to activate the backup image. You must be connected to the switch through the console port to access the boot menu.

To create a backup copy of the firmware on the switch, copy the active image to the backup image. You can also copy an image to a file on a remote server.

Managing Configuration Files

Configuration files contain the CLI commands that change the switch from its default configuration. The switch can maintain three separate configuration files: startup-config, running-config, and backup-config. The switch loads the startup-config file when the switch boots. Any configuration changes that take place after the boot process completes are written to the running-config file. The backup-config file does not exist until you explicitly create one by copying an existing configuration file to the backup-config file or downloading a backup-config file to the switch.

You can also create configuration scripts, which are text files that contains CLI commands.

When you apply (run) a configuration script on the switch, the commands in the script are executed in the order in which they are written as if you were typing them into the CLI. The commands that are executed in the configuration script are added to the running-config file.

You might upload a configuration file from the switch to a remote server for the following reasons:

- To create a backup copy
- To use the configuration file on another switch
- To manually edit the file

You might download a configuration file from a remote server to the switch for the following reasons:

- To restore a previous configuration
- To load the configuration copied from another switch
- To load the same configuration file on multiple switches

Use a text editor to open a configuration file and view or change its contents.

Editing and Downloading Configuration Files

Each configuration file contains a list of executable CLI commands. The commands must be complete and in a logical order, as if you were entering them by using the switch CLI.

When you download a startup-config or backup-config file to the switch, the new file replaces the previous version. To change the running-config file, you execute CLI commands either by typing them into the CLI or by applying a configuration script with the `script apply` command.

Saving the Running Configuration

Changes you make to the switch configuration while the switch is operating are written to the running-config. These changes are not automatically written to the startup-config. When you reload the switch, the startup-config file is loaded. If you reload the switch (or if the switch resets unexpectedly), any settings in the running-config that were not explicitly saved to the startup-config are lost. You must save the running-config to the startup-config to ensure that the settings you configure on the switch are saved across a switch reset.

To save the running-config to the startup-config from the CLI, use the `write memory` command.

File and Image Management Configuration Examples

This section contains the following examples:

- “Upgrading the Firmware” on page 34
- “Managing Configuration Scripts” on page 36

Upgrading the Firmware

This example shows how to download a firmware image to the switch and activate it. The TFTP server in this example is PumpKIN, an open source TFTP server running on a Windows system.

- TFTP server IP address: 10.27.65.112
- File path: \image
- File name: icos_1206.stk

Use the following steps to prepare the download, and then download and upgrade the switch image.

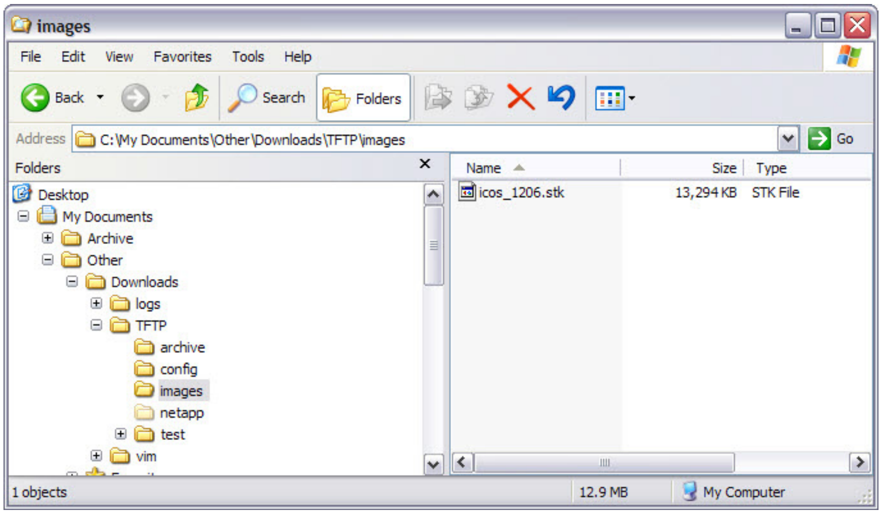
1. Check the connectivity between the switch and the TFTP server.

```
(Routing) #ping 10.27.65.112
 Pinging 10.27.65.112 with 0 bytes of data:

Reply From 10.27.65.112: icmp_seq = 0. time= 5095 usec.

----10.27.65.112 PING statistics----
1 packets transmitted, 1 packets received, 0% packet loss
round-trip (msec) min/avg/max = 5/5/5
```

2. Copy the image file to the appropriate directory on the TFTP server. In this example, the TFTP root directory is `C:\My Documents\Other\Downloads\TFTP`, so the file path is `images.`



Address: C:\My Documents\Other\Downloads\TFTP\images

Name	Size	Type
icos_1206.stk	13,294 KB	STK File

3. View information about the current image.

```
(Routing) #show bootvar
Image Descriptions
active : default image
 backup :

 Images currently available on Flash
--------------------------------------------------------------------
 unit      active      backup     current-active        next-active
--------------------------------------------------------------------
1    I.12.5.1  11.21.16.52           I.12.5.1           I.12.5.1
```

4. Download the image to the switch. After you execute the `copy` command, you must verify that you want to start the download. The image is downloaded as the backup image.

```
(Routing) #copy tftp://10.27.65.112/images/icos_1206.stk backup

Mode........................................... TFTP
Set Server IP.................................. 10.27.65.112
Path........................................... images/
Filename....................................... icos_1206.stk
Data Type...................................... Code
Destination Filename........................... backup

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n)y
```

5. After the transfer completes, activate the new image so that it becomes the active image after the switch resets.

```
(Routing) #boot system backup
Activating image backup ..
```

6. View information about the current image.

```
(Routing) #show bootvar
Image Descriptions

 active : default image
 backup :

 Images currently available on Flash
--------------------------------------------------------------------
 unit      active     backup         current-active    next-active
--------------------------------------------------------------------
 1         I.12.5.1   11.21.16.52    I.12.5.1          I.12.6.2
```

7. Copy the running configuration to the startup configuration to save the current configuration to NVRAM.

```
(Routing) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

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

Configuration Saved!
```

8. Reset the switch to boot the system with the new image.

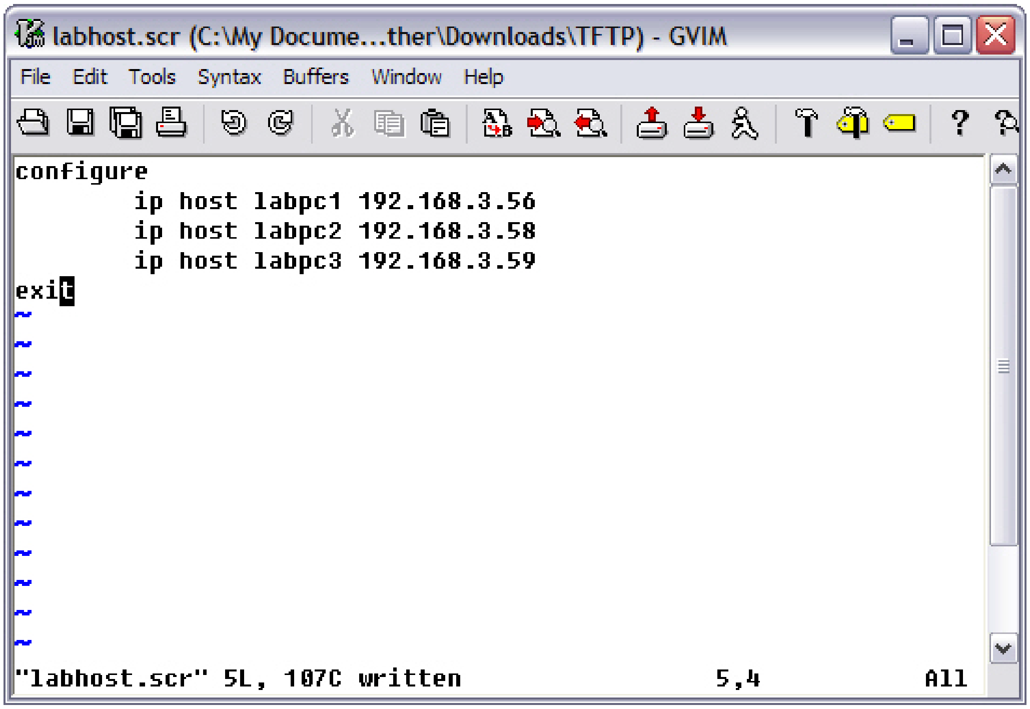
```
(Routing) #reload
Are you sure you want to continue? (y/n)y
Reloading all switches...
```

Managing Configuration Scripts

This example shows how to create a configuration script that adds three host name-to-IP address mappings to the host table.

To configure the switch:

1. Open a text editor on an administrative computer and type the commands as if you were entering them by using the CLI.


labhost.scr (C:\My Docume...ther\Downloads\TFTP) - GVIM
File Edit Tools Syntax Buffers Window Help

```
configure
        ip host labpc1 192.168.3.56
        ip host labpc2 192.168.3.58
        ip host labpc3 192.168.3.59
exit
"labhost.scr" 5L, 107C written                    5,4          All
```

2. Save the file with an *.scr extension and copy it to the appropriate directory on your TFTP server.
3. Download the file from the TFTP server to the switch.

```
(Routing) #copy tftp://10.27.65.112/labhost.scr nvram:script labhost.scr

Mode........................................... TFTP
Set Server IP.................................. 10.27.65.112
Path........................................... ./
Filename....................................... labhost.scr
Data Type...................................... Config Script
Destination Filename........................... labhost.scr

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n)
```

4. After you confirm the download information and the script successfully downloads, it is automatically validated for correct syntax.

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

135 bytes transferred

Validating configuration script...
configure
exit
configure
ip host labpc1 192.168.3.56

ip host labpc2 192.168.3.58

ip host labpc3 192.168.3.59

Configuration script validated.
File transfer operation completed successfully.
```

5. Run the script to execute the commands.

```
(Routing) #script apply labhost.scr

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

configure
exit
configure
ip host labpc1 192.168.3.56

ip host labpc2 192.168.3.58sj

ip host labpc3 192.168.3.59

Configuration script 'labhost.scr' applied.
```

6. Verify that the script was successfully applied.

```
(Routing) #show hosts
..
.
.
Configured host name-to-address mapping:
Host                     Addresses
------------------------  ------------------------
labpc1                   192.168.3.56
labpc2                   192.168.3.58
labpc3                   192.168.3.59
```

Downloading a Core Dump

The core dump file can be downloaded using the following methods:

- NFS
- TFTP
- FTP

On systems that have gigabytes of flash storage, the core dump file can also be copied to flash.

Using NFS to Download a Core Dump

Use the following commands to download a core dump file via NFS:

```
(Routing) #config
(Routing) (Config)#exception protocol nfs
(Routing) (Config)#exception dump nfs 192.168.1.10://home/nfs_test
(Routing) (Config)#show exception

Coredump file name............................. ASDF
Coredump filename uses hostname................ TRUE
Coredump filename uses time-stamp.............. TRUE
NFS mount point................................ 192.168.1.10://home/nfs_test
TFTP server IP................................. 10.27.9.99
File path...................................... ./.
Protocol....................................... nfs
Switch-chip-register...........................TRUE
(Routing) (Config)#

(Routing) #write core test

The configured protocol nfs test PASS
(Routing) #
```

Using TFTP or FTP to Download a Core Dump

Use the following commands to download a core dump file via TFTP. To use FTP, substitute `ftp` for `tftp` in the commands.

```
(Routing) #config
(Routing) (Config)#exception protocol tftp
(Routing) (Config)#exception dump tftp-server 192.168.1.2
(Routing) (Config)#show exception

Coredump file name............................. core
Coredump filename uses hostname................ FALSE
Coredump filename uses time-stamp.............. TRUE
TFTP server IP................................. 192.168.1.2
File path...................................... ./.
Protocol....................................... tftp
Switch-chip-register...........................FALSE
```

```
(Routing) (Config)#

(Routing) #write core test
The configured protocol tftp test PASS
(Routing) #
```

Enabling Kernel Core Dump

Note: This feature is available only on Ubuntu Linux distributions of the DCSS software.

The kernel core dump feature enables the system to perform a warm reboot into a new kernel in reserved memory, allowing the current state of the operating kernel to be captured for post-mortem analysis. This feature involves configuring the underlying operating system to enable the Linux kexec feature. The kernel-dump feature is implemented as a set of bash scripts in either a RPM or DEB package that can be used with or without the DCSS application running. It provides a convenient method to invoke the “crash” console kernel debugging utility without requiring complex user configuration. This provides the necessary handling to allow debugging of the DCSS customized Linux kernel. This feature is available only on platforms with Intel x86-class CPUs running standard Ubuntu Linux.

The following commands can be executed in Global Config mode to enable the kernel-dump feature, which is disabled by default, and to configure the path for storing kernel-dump files:

```
(Routing) #config
(Routing) (Config)#exception kernel-dump
(Routing) (Config)#exception kernel-dump path path
```

You use the following commands in Privileged Exec mode to show kernel-dump settings, show the list of saved kernel dumps, and show the dmesg log from a particular kernel dump.

```
(Routing) #show exception kernel-dump
(Routing) #show exception kernel-dump list
(Routing) #show exception kernel-dump log record number
```

See the *DCSS CLI Command Reference* for a complete list of commands.

Setting the System Time

The switch uses the system clock to provide time stamps on log messages. Additionally, some show commands include the time in the command output. For example, the `show users login-history` command includes a Login Time field. The system clock provides the information for the Login Time field.

You can configure the system time manually, or you can configure the switch to obtain the time by using a Simple Network Time Protocol (SNTP) server. A network SNTP server can provide more accurate switch clock time synchronization than manually-configured time.

Note: The manually-configured local clock settings are not retained across a system reset if the platform does not include a Real Time Clock (RTC).

The SNTP client on the switch can request the time from an SNTP server on the network (unicast), or you can allow the switch to receive SNTP broadcasts. Requesting the time from a unicast SNTP server is more secure. Use this method if you know the IP address of the SNTP server on your network. If you allow the switch to receive SNTP broadcasts, any clock synchronization information is accepted, even if it has not been requested by the device. This method is less secure than polling a specified SNTP server.

The switch also supports the following time configuration settings:

- Time Zone —Allows you to specify the offset from Coordinated Universal Time (UTC), which is also known as Greenwich Mean Time (GMT).
- Summer Time/Daylight Saving Time (DST)— In some regions, the time shifts by one hour in the fall and spring. The switch supports manual entry of one-time or recurring shifts in the time.

Manual Time Configuration

The example in this section shows how to manually configure the time, date, time zone, and summer time settings for a switch in Hyderabad, India.

1. Set the time. The system clock uses a 24-hour clock, so 6:23 PM is entered as 18:23:00.

```
(Routing) #configure
(Routing) (Config)#clock set 18:23:00
```

2. Set the date. In this example, the date is April 30, 2012.

```
(Routing) (Config)#clock set 04/30/2012
```

3. Configure the time zone. In this example, the time zone is India Standard Time (IST), which is UTC/GMT +5 hours and 30 minutes.

```
(Routing) (Config)#clock timezone 5 minutes 30 zone IST
```

4. Configure the offset for a hypothetical daylight saving time. In this example, the offset is one hour. It occurs every year on Sunday in the first week of April and ends the fourth Sunday in October. The start and end times are 2:30 AM, and the time zone is India Standard Summer Time (ISST).

```
(Routing) (Config)#clock summer-time recurring 1 sun apr 02:30 4 sun oct 02:30 offset 60 zone ISST
(Routing) (Config)#exit
```

5. View the clock settings.

```
(Routing) #show clock detail

20:30:07 ISST(UTC+6:30) Apr 30 2012
No time source

 Time zone:
 Acronym is IST
 Offset is UTC+5:30
```

```
Summertime:
Acronym is ISST
Recurring every year
Begins at first Sunday of Apr at 02:30
Ends at fourth Sunday of Oct at 02:30
offset is 60 minutes
```

Configuring SNTP

This example shows how to configure the system clock for a switch in New York City, which has a UTC/GMT offset of –5 hours.

1. Specify the SNTP server the client on the switch should contact. You can configure the IP address or host name of the SNTP server.

```
(Routing) #configure
(Routing) (Config)#sntp server time1.rtp.broadcom.com
```

2. Configure the UTC/GMT offset for the location.

```
(Routing) (Config)#clock timezone -5
```

3. Configure the time offset for DST.

```
(Routing) (Config)#clock summer-time recurring USA
```

4. Enable the SNTP client on the device in unicast mode.

```
(Routing) (Config)#sntp client mode unicast
```

5. View the time information.

```
(Routing) #show sntp

Last Update Time:                  Apr 27 16:42:23 2012
Last Unicast Attempt Time:         Apr 27 16:43:28 2012
Last Attempt Status:               Success

(Routing) #show clock

12:47:22 (UTC-4:00) Apr 27 2012
Time source is SNTP
```

Section 4: Configuring Switching Features

VLANs

By default, all switchports on the switch are in the same broadcast domain. This means when one host connected to the switch broadcasts traffic, every device connected to the switch receives that broadcast. All ports in a broadcast domain also forward multicast and unknown unicast traffic to the connected host. Large broadcast domains can result in network congestion, and end users might complain that the network is slow. In addition to latency, large broadcast domains are a greater security risk since all hosts receive all broadcasts.

Virtual Local Area Networks (VLANs) allow you to divide a broadcast domain into smaller, logical networks. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast, and like a router, it partitions the network into logical segments, which provides better administration, security, and management of multicast traffic.

Network administrators have many reasons for creating logical divisions, such as department or project membership. Because VLANs enable logical groupings, members do not need to be physically connected to the same switch or network segment. Some network administrators use VLANs to segregate traffic by type so that the time-sensitive traffic, like voice traffic, has priority over other traffic, such as data. Administrators also use VLANs to protect network resources. Traffic sent by authenticated clients might be assigned to one VLAN, while traffic sent from unauthenticated clients might be assigned to a different VLAN that allows limited network access.

When one host in a VLAN sends a broadcast, the switch forwards traffic only to other members of that VLAN. For traffic to go from a host in one VLAN to a host in a different VLAN, the traffic must be forwarded by a layer 3 device, such as a router. VLANs work across multiple switches, so there is no requirement for the hosts to be located near each other to participate in the same VLAN.

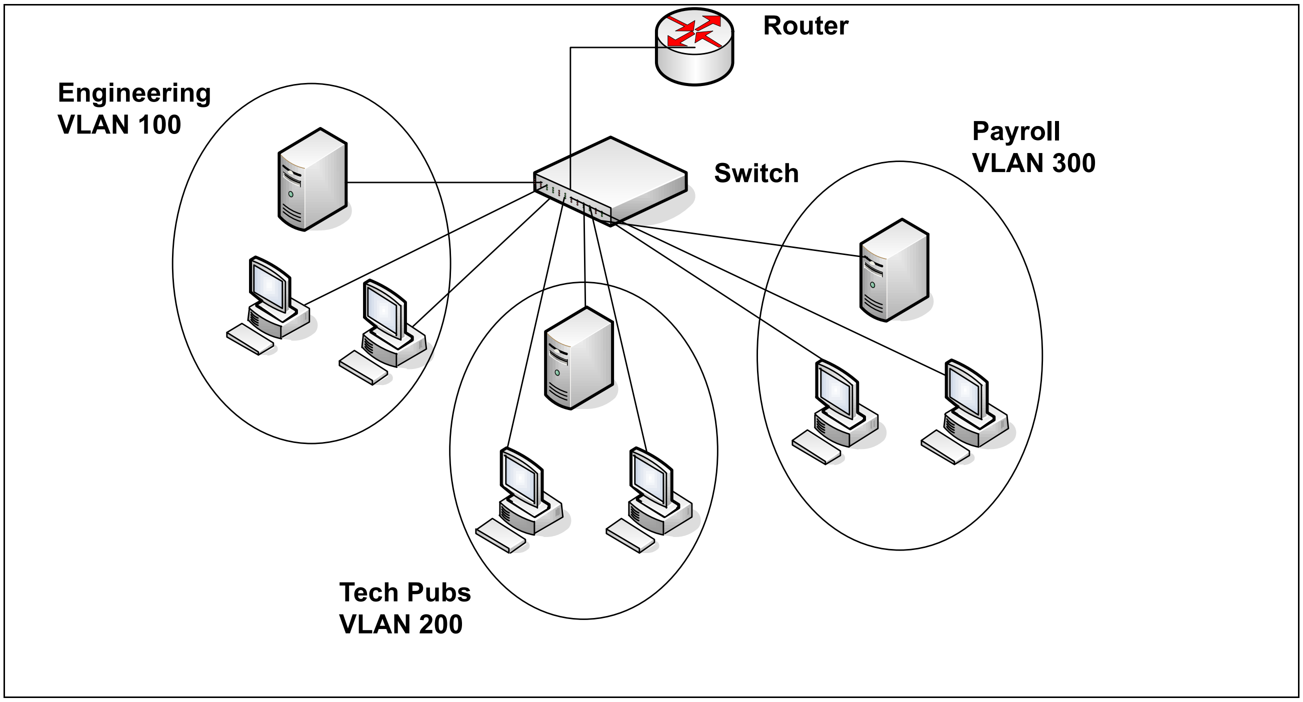
Note: DCSS software supports VLAN routing. When you configure VLAN routing, the switch acts as a layer 3 device and can forward traffic between VLANs. For more information, see “VLAN Routing” on page 60.

Each VLAN has a unique number, called the VLAN ID. The DCSS supports a configurable VLAN ID range of 2–4093. A VLAN with VLAN ID 1 is configured on the switch by default. You can associate a name with the VLAN ID. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN identifier is the Port VLAN ID (PVID) specified for the port that received the frame. For information about tagged and untagged frames, see "VLAN Tagging" on page 44.

DCSS supports adding individual ports and Link Aggregation Groups (LAGs) as VLAN members.

Figure 1 on page 43 shows an example of a network with three VLANs that are department-based. The file server and end stations for the department are all members of the same VLAN.

Figure 1: Simple VLAN Topology



In this example, each port is manually configured so that the end station attached to the port is a member of the VLAN configured for the port. The VLAN membership for this network is port-based or static.

VLAN Tagging

DCSS supports IEEE 802.1Q tagging. Ethernet frames on a tagged VLAN have a 4-byte VLAN tag in the header. VLAN tagging is required when a VLAN spans multiple switches, which is why trunk ports transmit and receive only tagged frames.

Tagging may be required when a single port supports multiple devices that are members of different VLANs. For example, a single port might be connected to an IP phone, a PC, and a printer (the PC and printer are connected via ports on the IP phone). IP phones are typically configured to use a tagged VLAN for voice traffic, while the PC and printers typically use the untagged VLAN.

When a port is added to a VLAN as an untagged member, untagged packets entering the switch are tagged with the PVID (also called the *native VLAN*) of the port. If the port is added to a VLAN as an untagged member, the port does not add a tag to a packet in that VLAN when it exits the port. Configuring the PVID for an interface is useful when untagged and tagged packets will be sent and received on that port and a device connected to the interface does not support VLAN tagging.

When ingress filtering is on, the frame is dropped if the port is not a member of the VLAN identified by the VLAN ID in the tag. If ingress filtering is off, all tagged frames are forwarded. The port decides whether to forward or drop the frame when the port receives the frame.

Default VLAN Behavior

One VLAN exists on the switch by default. The VLAN ID is 1, and all ports are included in the VLAN as access ports, which are untagged. This means when a device connects to any port on the switch, the port forwards the packets without inserting a VLAN tag. If a device sends a tagged frame to a port, the frame is dropped. Since all ports are members of this VLAN, all ports are in the same broadcast domain and receive all broadcast and multicast traffic received on any port.

When you add a new VLAN to the VLAN database, no ports are members. The configurable VLAN range is 2–4093. VLANs 4094 and 4095 are reserved.

Table 3 shows the default values or maximum values for VLAN features.

Table 3: VLAN Default and Maximum Values

Feature	***Value***
Default VLAN ID	1
VLAN Name	default
VLAN Range	2–4093
Frames accepted	Untagged Incoming untagged frames are classified into the VLAN whose VLAN ID is the currently configured PVID.
Frames sent	Untagged
Ingress Filtering	On
PVID	1

Table 3: VLAN Default and Maximum Values (Cont.)

Feature	*Value*
Double-VLAN tagging	Disabled If double-VLAN tagging is enabled, the default EtherType value is 802.1Q

VLAN Configuration Example

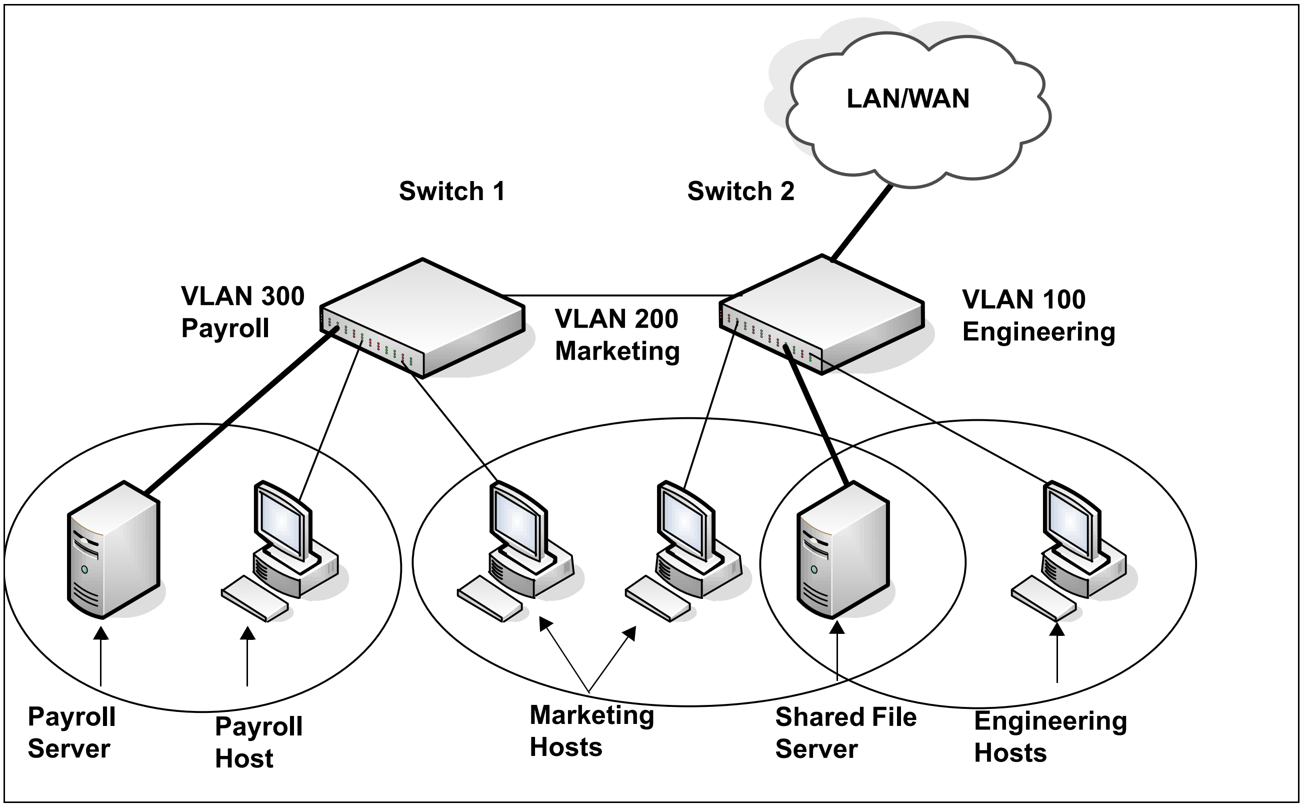
A network administrator wants to create the VLANs in Table 4:

Table 4: Example VLANs

VLAN ID	*VLAN Name*	*VLAN Type*	*Purpose*
100	Engineering	Port-based	All employees in the Engineering department use this VLAN. Confining this department's traffic to a single VLAN helps reduce the amount of traffic in the broadcast domain, which increases bandwidth.
200	Marketing	Port-based	All employees in the Marketing department use this VLAN.
300	Payroll	Port-based	The payroll department has sensitive traffic and needs its own VLAN to help keep that traffic private.

Figure 2 on page 46 shows the network topology for this example. As the figure shows, there are two switches, two file servers, and many hosts. One switch has an uplink port that connects it to a layer 3 device and the rest of the corporate network.

Figure 2: Network Topology for VLAN Configuration



The network in Figure 2 has the following characteristics:

- Each connection to a host represents multiple ports and hosts.
- The Payroll and File servers are connected to the switches through a LAG.
- Some of the Marketing hosts connect to Switch 1, and some connect to Switch 2.
- The Engineering and Marketing departments share the same file server.
- Because security is a concern for the Payroll VLAN, the ports and LAG that are members of this VLAN will accept and transmit only traffic tagged with VLAN 300.

Table 5 shows the port assignments on the switches.

Table 5: Switch Port Connections

Port/LAG	*Function*
Switch 1	
1	Connects to Switch 2
2–15	Host ports for Payroll
16–20	Host ports for Marketing
LAG1 (ports 21–24)	Connects to Payroll server
Switch 2	
1	Connects to Switch 1
2–10	Host ports for Marketing
11–30	Host ports for Engineering
LAG1 (ports 35–39)	Connects to file server
LAG2 (ports 40–44)	Uplink to router.

Configure the VLANs and Ports on Switch 1

Use the following steps to configure the VLANs and ports on Switch 1. None of the hosts that connect to Switch 1 use the Engineering VLAN (VLAN 100), so it is not necessary to create it on that switch.

To configure Switch 1:

1. Create VLANs 200 (Marketing), 300 (Payroll), and associate the VLAN ID with the appropriate name.

```
(Routing) #vlan database
(Routing) (Vlan)#vlan 200,300
(Routing) (Vlan)#vlan name 200 Marketing
(Routing) (Vlan)#vlan name 300 Payroll
(Routing) (Vlan)#exit
```

2. Assign ports 16–20 to the Marketing VLAN.

```
(Routing) #configure
(Routing) (Config)#interface 0/16-0/20
(Routing) (Interface 0/16-0/20)#vlan participation include 200
(Routing) (Interface 0/16-0/20)#exit
```

3. Assign ports 2–15 to the Payroll VLAN

```
(Routing) (Config)#interface 0/2-0/15
(Routing) (Interface 0/2-0/15)#vlan participation include 300
(Routing) (Interface 0/2-0/15)#exit
```

4. Assign LAG1 to the Payroll VLAN and configure the frames to always be transmitted tagged with a PVID of 300.

```
(Routing) (Config)#interface 3/1
(Routing) (Interface 3/1)#vlan participation include 300
(Routing) (Interface 3/1)#vlan tagging 300
(Routing) (Interface 3/1)#vlan pvid 300
(Routing) (Interface 3/1)#exit
```

5. Configure port 1 as a trunk port and add VLAN 200 and VLAN 300 as members. Trunk ports accept and transmits tagged frames only and have ingress filtering enabled.

```
(Routing) (Config)#interface 0/1
(Routing) (Interface 0/1)#vlan acceptframe vlanonly
(Routing) (Interface 0/1)#vlan participation include 200,300
(Routing) (Interface 0/1)#vlan participation exclude 1
(Routing) (Interface 0/1)#vlan tagging 200,300
(Routing) (Interface 0/1)#vlan ingressfilter
(Routing) (Interface 0/1)#exit
(Routing) (Config)#exit
```

6. To save the configuration so that it persists across a system reset, use the following command:

```
(Routing) #copy system:running-config nvram:startup-config
```

7. View the VLAN settings.

```
(Routing) #show vlan

VLAN ID VLAN Name                         VLAN Type
------- -------------------------------- -------------------
1       default                           Default
200     Marketing                         Static
300     Payroll                           Static

(Routing) #show vlan 300

VLAN ID: 300
VLAN Name: Payroll
VLAN Type: Static

Interface   Current   Configured   Tagging
----------  --------  -----------  --------
0/1         Include   Include      Tagged
0/2         Include   Include      Untagged
0/3         Include   Include      Untagged
0/4         Include   Include      Untagged
0/5         Include   Include      Untagged
--More-- or (q)uit
```

8. View the VLAN information for a port.

```
(Routing) #show vlan port 0/1

          Port       Port                Ingress    Ingress
          VLAN ID    VLAN ID  Acceptable  Filtering  Filtering Default
Interface Configured Current  Frame Types Configured Current   Priority
--------- ---------- -------- ----------- ---------- --------- --------
0/1       1          1        VLAN Only   Enable     Enable       0

Protected Port .............................. False
```

Configure the VLANs and Ports on Switch 2

Use the following steps to configure the VLANs and ports on Switch 2. Many of the procedures in this section are the same as procedures used to configure Switch 1. For more information about specific procedures, see the details and figures in the previous section.

Use the following steps to configure Switch 2:

1. Create the Engineering, Marketing, and Payroll VLANs.

   Although the Payroll hosts do not connect to this switch, traffic from the Payroll department must use Switch 2 to reach the rest of the network and Internet through the uplink port. For that reason, Switch 2 must be aware of VLAN 300 so that traffic is not rejected by the trunk port.

2. Configure ports 2-10 to participate in VLAN 200.
3. Configure ports 11–30 to participate in VLAN 100.
4. Configure LAG 1 to participate in VLAN 100 and VLAN 200.
5. Configure port 1 and LAG 2 as participants in ports and add VLAN 100, VLAN 200, and VLAN 300 that accept and transit tagged frames only.
6. Enable ingress filtering on port 1 and LAG 2.
7. If desired, copy the running configuration to the startup configuration.
8. View VLAN information for the switch and ports.

Switchport Modes

You can configure each port on an DCSS switch to be in one of the following modes:

- **Access**—Access ports are intended to connect end-stations to the system, especially when the end-stations are incapable of generating VLAN tags. Access ports support a single VLAN (the PVID). Packets received untagged are processed as if they are tagged with the access port PVID. Packets received that are tagged with the PVID are also processed. Packets received that are tagged with a VLAN other than the PVID are dropped. If the VLAN associated with an access port is deleted, the PVID of the access port is set to VLAN 1. VLAN 1 may not be deleted.
- **Trunk**—Trunk-mode ports are intended for switch-to-switch links. Trunk ports can receive both tagged and untagged packets. Tagged packets received on a trunk port are forwarded on the VLAN contained in the tag if the trunk port is a member of the VLAN. Untagged packets received on a trunk port are forwarded on the native VLAN. Packets received on another interface belonging to the native VLAN are transmitted untagged on a trunk port.
- **General**—General ports can act like access or trunk ports or a hybrid of both. VLAN membership rules that apply to a port are based on the switchport mode configured for the port.

Table 21-2 shows the behavior of the three switchport modes.

Table 6: Switchport Mode Behavior

Mode	*VLAN Membership*	*Frames Accepted*	*Frames Sent*	*Ingress Filtering*
Access	One VLAN	Untagged/Tagged	Untagged	Always On
Trunk	All VLANs that exist in the system (default)	Untagged/Tagged	Tagged and Untagged	Always On
General	As many as desired	Tagged or Untagged	Tagged or Untagged	On or Off

When a port is in General mode, all VLAN features are configurable. When ingress filtering is on, the frame is dropped if the port is not a member of the VLAN identified by the VLAN ID in the tag. If ingress filtering is off, all tagged frames are forwarded. The port decides whether to forward or drop the frame when the port receives the frame.

The following example configures a port in Access mode with a single VLAN membership in VLAN 10:

```
(Routing) #config
(Routing) (Config)#interface 0/5
(Routing) (Interface 0/5)#switchport mode access
(Routing) (Interface 0/5)#switchport access vlan 10
(Routing) (Interface 0/5)#exit
```

The **switchport trunk allowed vlan** command with the **add** keyword adds the list of VLANs that can receive and send traffic on the interface in tagged format when in trunking mode. Alternatively, the all keyword can be used to specify membership in all VLANs, the **remove** keyword can be used to remove membership. If this command is omitted, the port is a member of all configured VLANs. The native VLAN specifies the VLAN on which the port forwards untagged packets it receives.

The following example configures a port in Trunk mode.

```
(Routing) #config
(Routing) (Config)#interface 0/8
(Routing) (Interface 0/8)#switchport mode trunk
(Routing) (Interface 0/8)#switchport trunk allowed vlan add 10,20,30
(Routing) (Interface 0/8)#switchport trunk native vlan 100
(Routing) (Interface 0/8)#exit
```

The following commands configure a port in General mode.

```
(Routing) #config
(Routing) (Config)#interface 0/10
(Routing) (Interface 0/10)#switchport mode general
(Routing) (Interface 0/10)#exit
```

The General mode port can then be configured as a tagged or untagged member of any VLAN, as shown in "VLAN Configuration Example" on page 45.

Static Link Aggregation

Link aggregation can be configured as static. Static configuration is used when connecting the switch to an external Gigabit Ethernet switch that does not support LACP.

Configuring Static LAGs

The commands in this example show how to configure a static LAG on a switch. The LAG number is 3 (interface 1/3), and the member ports are 10, 11, 14, and 17.

Use the following steps to configure the switch:

1. Enter interface configuration mode for the ports that are to be configured as LAG members.

   ```
   (Routing) (Config)#interface 0/10-0/12,0/14,0/17
   ```

2. Add the ports to LAG 2 without LACP.

   ```
   (Routing) (Interface 0/10-0/12,0/14,0/17)#addport 1/3
   (Routing) (Interface 0/10-0/12,0/14,0/17)#exit
   (Routing) (Config)#exit
   ```

3. View information about LAG 2.

   ```
   (Routing) #show port-channel 3/3
   ```

```
Local Interface................................ 1/3
Channel Name................................... ch3
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Static
Port-channel Min-links......................... 1
Load Balance Option............................ 3
(Src/Dest MAC, VLAN, EType, incoming port)

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
0/10   actor/long    Auto      True
       partner/long
0/11   actor/long    Auto      False
       partner/long
0/12   actor/long    Auto      False
       partner/long
0/14   actor/long    Auto      False
       partner/long
0/17   actor/long    Auto      False
       partner/long
--More-- or (q)uit
```

Spanning Tree Protocol

Spanning Tree Protocol (STP) is a layer 2 protocol that provides a tree topology for switches on a bridged LAN. STP allows a network to have redundant paths without the risk of network loops. STP uses the spanning-tree algorithm to provide a single path between end stations on a network.

DCSS software supports Classic STP and Rapid STP.

Classic STP and Rapid STP

Classic STP provides a single path between end stations, avoiding and eliminating loops. The difference between the RSTP and the traditional STP (IEEE 802.1D) is the ability to configure and recognize full-duplex connectivity and ports which are connected to end stations, resulting in rapid transitioning of the port to the Forwarding state and the suppression of Topology Change Notifications.

STP Operation

The switches (bridges) that participate in the spanning tree elect a switch to be the root bridge for the spanning tree. The root bridge is the switch with the lowest bridge ID, which is computed from the unique identifier of the bridge and its configurable priority number. When two switches have an equal bridge ID value, the switch with the lowest MAC address is the root bridge.

After the root bridge is elected, each switch finds the lowest-cost path to the root bridge. The port that connects the switch to the lowest-cost path is the root port on the switch. The switches in the spanning tree also determine which ports have the lowest-path cost for each segment. These ports are the designated ports. Only the root ports and designated ports are placed in a forwarding state to send and receive traffic. All other ports are put into a blocked state to prevent redundant paths that might cause loops.

To determine the root path costs and maintain topology information, switches that participate in the spanning tree use Bridge Protocol Data Units (BPDUs) to exchange information.

Optional STP Features

DCSS software supports the following optional STP features:

- BPDU flooding
- Edge Port
- BPDU filtering
- Root guard
- Loop guard
- BPDU protection

BPDU Flooding

The BPDU flooding feature determines the behavior of the switch when it receives a BPDU on a port that is disabled for spanning tree. If BPDU flooding is configured, the switch will flood the received BPDU to all the ports on the switch which are similarly disabled for spanning tree.

Edge Port

The Edge Port feature reduces the STP convergence time by allowing ports that are connected to end devices (such as a desktop computer, printer, or file server) to transition to the forwarding state without going through the listening and learning states.

BPDU Filtering

Ports that have the Edge Port feature enabled continue to transmit BPDUs. The BPDU filtering feature prevents ports configured as edge ports from sending BPDUs.

If BPDU filtering is configured globally on the switch, the feature is automatically enabled on all operational ports where the Edge Port feature is enabled. These ports are typically connected to hosts that drop BPDUs. However, if an operational edge port receives a BPDU, the BPDU filtering feature disables the Edge Port feature and allows the port to participate in the spanning-tree calculation.

Enabling BPDU filtering on a specific port prevents the port from sending BPDUs and allows the port to drop any BPDUs it receives.

Root Guard

Enabling root guard on a port ensures that the port does not become a root port or a blocked port. When a switch is elected as the root bridge, all ports are designated ports unless two or more ports of the root bridge are connected together. If the switch receives superior STP BPDUs on a root-guard enabled port, the root guard feature moves this port to a root-inconsistent STP state, which is effectively equal to a listening state. No traffic is forwarded across this port. In this way, the root guard feature enforces the position of the root bridge.

When the STP mode is MSTP, the port may be a designated port in one MSTI and an alternate port in the CIST, etc. Root guard is a per port (not a per port per instance command) configuration, so all the MSTP instances this port participates in should not be in a root role.

Loop Guard

Loop guard protects a network from forwarding loops induced by BPDU packet loss. The reasons for failing to receive packets are numerous, including heavy traffic, software problems, incorrect configuration, and unidirectional link failure. When a non-designated port no longer receives BPDUs, the spanning-tree algorithm considers that this link is loop free and begins transitioning the link from blocking to forwarding. Once in forwarding state, the link may create a loop in the network.

Enabling loop guard prevents such accidental loops. When a port is no longer receiving BPDUs and the max age timer expires, the port is moved to a *loop-inconsistent blocking state*. In the loop-inconsistent blocking state, traffic is not forwarded so the port behaves as if it is in the blocking state. The port will remain in this state until it receives a BPDU. It will then transition through the normal spanning tree states based on the information in the received BPDU.

Note: Loop Guard should be configured only on non-designated ports. These include ports in alternate or backup roles. Root ports and designated ports should not have loop guard enabled so that they can forward traffic

BPDU Protection

When the switch is used as an access layer device, most ports function as edge ports that connect to a device such as a desktop computer or file server. The port has a single, direct connection and is configured as an edge port to implement the fast transition to a forwarding state. When the port receives a BPDU packet, the system sets it to non-edge port and recalculates the spanning tree, which causes network topology flapping. In normal cases, these ports do not receive any BPDU packets. However, someone may forge BPDU to maliciously attack the switch and cause network flapping.

BPDU protection can be enabled in RSTP to prevent such attacks. When BPDU protection is enabled, the switch disables an edge port that has received BPDU and notifies the network manager about it.

The PVRSTP side sends IEEE STP BPDUs corresponding to the VLAN 1 STP to the IEEE MAC address as untagged frames across the link. At the same time, SSTP BPDUs are sent as untagged frames. IEEE switches simply flood the SSTP BPDUs throughout VLAN 1. This facilitates PVRSTP connectivity in case there are other PVRSTP switches connected to the IEEE STP domain.

For non-native VLANs (VLANs 2–4093), the PVRSTP switch sends SSTP BPDUs, tagged with their VLAN number. The VLAN STP instances are multicast across the RSTP region, as if it were a hub switch.

The VLAN 1 STP instance of SW1 and SW2 are joined with the STP instance running in SW3. VLANs 2 and 3 consider the path across SW3 as another segment linking SW1 and SW2, and their SSTP information is multicast across SW3.

The bridge priority of SW1 and SW2 for VLAN1 instance is 32769 (bridge priority + VLAN identifier).

The bridge priority of SW3 is 32768, per the IEEE 802.w standard.

SW3 is selected as Root Bridge for the VLAN1 instance that is CST, and SW1 is selected as Root Bridge for VLAN2 and VLAN3 (based on the low MAC address of SW1).

STP Configuration Examples

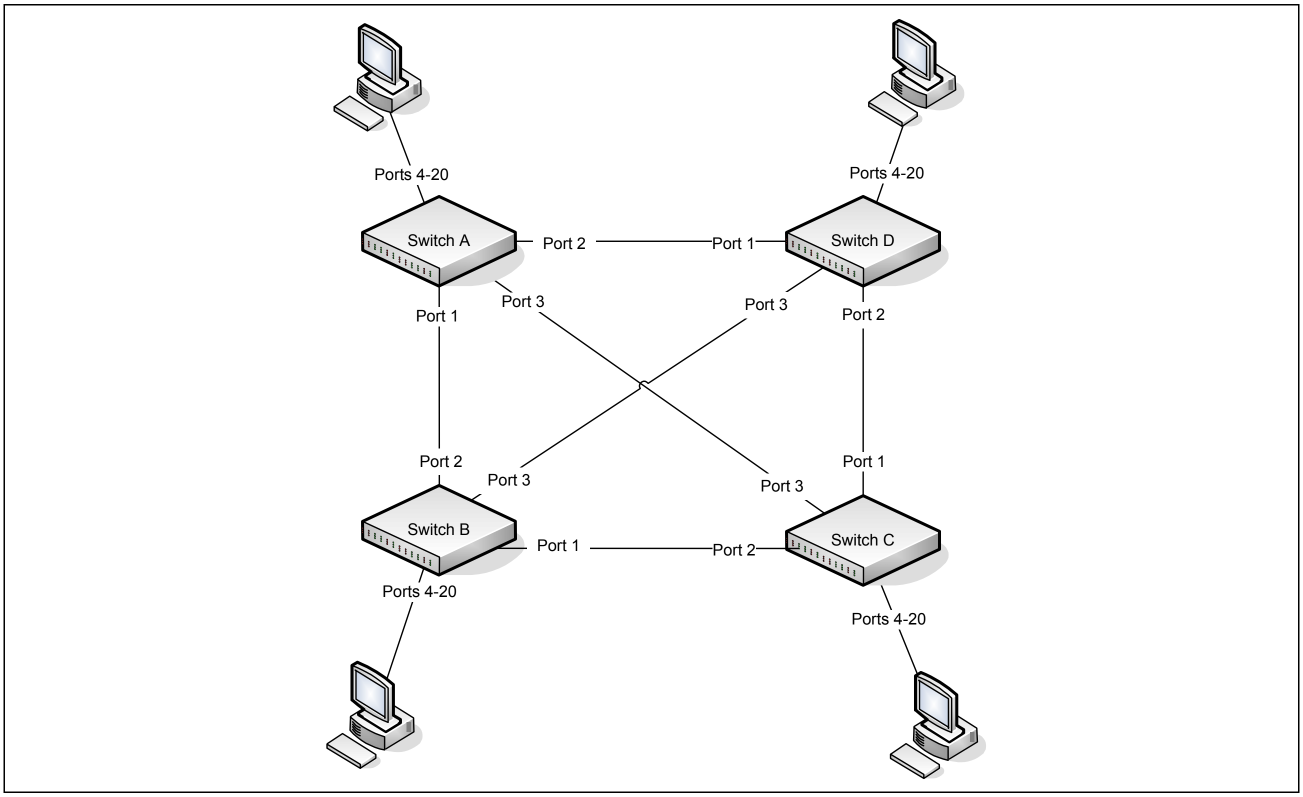
This section contains the following examples:

- "Configuring STP" on page 56
- "LLDP and LLDP-MED" on page 58

Configuring STP

This example shows a LAN with four switches. On each switch, ports 1, 2, and 3 connect to other switches, and ports 4–20 connect to hosts (in Figure 3, each PC represents 17 host systems).

Figure 3: STP Example Network Diagram



Of the four switches in Figure 3 on page 56, the administrator decides that Switch A is the most centrally located in the network and is the least likely to be moved or redeployed. For these reasons, the administrator selects it as the root bridge for the spanning tree. The administrator configures Switch A with the highest priority and uses the default priority values for Switch B, Switch C, and Switch D.

For all switches, the administrator also configures ports 4–17 in Port Fast mode because these ports are connected to hosts and can transition directly to the Forwarding state to speed up the connection time between the hosts and the network.

The administrator also configures Port Fast BPDU filtering and Loop Guard to extend STP's capability to prevent network loops. For all other STP settings, the administrator uses the default STP values.

Use the following steps to configure the switch:

1. Connect to Switch A and configure the priority to be higher (a lower value) than the other switches, which use the default value of 32768.

```
(Routing) #config
(Routing) (Config)#spanning-tree mst priority 0 8192
```

2. Configure ports 4–20 to be in Edge Port mode.

```
(Routing) (Config)#interface 0/4-0/20
(Routing) (Interface 0/4-0/20)#spanning-tree edgeport
(Routing) (Interface 0/4-0/20)#exit
```

3. Enable Loop Guard on ports 1–3 to help prevent network loops that might be caused if a port quits receiving BPDUs.

```
(Routing) (Config)#interface 0/1-0/3
(Routing) (Interface 0/1-0/3)#spanning-tree guard loop
(Routing) (Interface 0/1-0/3)#exit
```

4. Enable Port Fast BPDU Filter. This feature is configured globally, but it affects only access ports that have the Edge Port feature enabled.

```
(Routing) (Config)#spanning-tree bpdufilter default
```

5. Repeat Step 2 through Step 4 on Switch B, Switch C, and Switch D to complete the configuration.

LLDP and LLDP-MED

LLDP is a standardized discovery protocol defined by IEEE 802.1AB. It allows stations residing on an 802 LAN to advertise major capabilities physical descriptions, and management information to physically adjacent devices allowing a network management system (NMS) to access and display this information.

LLDP is a one-way protocol; there are no request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function. The transmit and receive functions can be enabled/disabled separately on each switch port.

LLDP-MED is an extension of the LLDP standard. LLDP-MED uses LLDP's organizationally-specific Type-Length-Value (TLV) extensions and defines new TLVs that make it easier for a VoIP deployment in a wired or wireless LAN/MAN environment. It also makes mandatory a few optional TLVs from LLDP and recommends not transmitting some TLVs.

The TLVs only communicate information; these TLVs do not automatically translate into configuration. An external application may query the MED MIB and take management actions in configuring functionality.

LLDP and LLDP-MED are used primarily in conjunction with network management tools to provide information about network topology and configuration, and to help troubleshoot problems that occur on the network. The discovery protocols can also facilitate inventory management within a company.

LLDP and the LLDP-MED extension are vendor-neutral discovery protocols that can discover devices made by numerous vendors. LLDP-MED is intended to be used on ports that connect to VoIP phones. Additional applications for LLDP-MED include device location (including for Emergency Call Service/E911) and Power over Ethernet management.

LLDP and Data Center Applications

DCBX uses TLV information elements over LLDP to exchange information, so LLDP must be enabled on the port to enable the information exchange.

Configuring LLDP

This example shows how to configure LLDP settings for the switch and to allow port 0/3 to transmit all LLDP information available.

Do the following steps to configure the switch:

1. Configure the transmission interval, hold multiplier, and reinitialization delay for LLDP PDUs sent from the switch.

```
(Routing) #configure
(Routing) (Config)#lldp timers interval 60 hold 5 reinit 3
```

2. Enable port 0/3 to transmit and receive LLDP PDUs.

```
(Routing) (Config)#interface 0/3
(Routing) (Interface 0/3)#lldp transmit
(Routing) (Interface 0/3)#lldp receive
```

3. Enable port 0/3 to transmit management address information in the LLDP PDUs and to send topology change notifications if a device is added or removed from the port.

   ```
   (Routing) (Interface 0/3)#lldp transmit-mgmt
   (Routing) (Interface 0/3)#lldp notification
   ```

4. Specify the TLV information to be included in the LLDP PDUs transmitted from port 0/3.

   ```
   (Routing) (Interface 0/3)#lldp transmit-tlv sys-name sys-desc sys-cap port-desc
   ```

5. Set the port description to be transmitted in LLDP PDUs.

   ```
   (Routing) (Interface 0/3)#description “Test Lab Port”
   ```

6. Exit to Privileged EXEC mode.

   ```
   (Routing) (Interface 0/3)# <CTRL + Z>
   ```

7. View global LLDP settings on the switch.

   ```
   (Routing) #show lldp

   LLDP Global Configuration

   Transmit Interval..................... 60 seconds
   Transmit Hold Multiplier.............. 5
   Reinit Delay.......................... 3 seconds
   Notification Interval................. 5 seconds
   ```

8. View summary information about the LLDP configuration on port 0/3.

   ```
   (Routing) #show lldp interface 0/3
   LLDP Interface Configuration

   Interface  Link    Transmit  Receive   Notify    TLVs     Mgmt
   ---------  ------  --------  --------  --------  -------  ----
   0/3        Down    Enabled   Enabled   Enabled   0,1,2,3  Y

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

9. View detailed information about the LLDP configuration on port 0/3.

   ```
   (Routing) #show lldp local-device detail 0/3

   LLDP Local Device Detail

   Interface: 0/3

   Chassis ID Subtype: MAC Address
   Chassis ID: 00:10:18:82:15:7B
   Port ID Subtype: MAC Address
   Port ID: 00:10:18:82:15:7D
   System Name:
   System Description: Broadcom Triumph2 56634 Development System - 48 GE, 4 TENGIG, I.12.5.1, Linux
   2.6.27.47
   Port Description: Test Lab Port
   System Capabilities Supported: bridge, router
   System Capabilities Enabled: bridge
   Management Address:
       Type: IPv4
       Address: 10.27.22.149
   ```

Section 5: Configuring Routing

Basic Routing and Features

DCSS software runs on multilayer switches that support static and dynamic routing. Table 7 describes some of the general routing features that you can configure on the switch. The table does not list supported routing protocols.

Table 7: IP Routing Features

Feature	***Description***
ICMP message control	You can configure the type of ICMP messages that the switch responds to as well as the rate limit and burst size.
Default gateway	The switch supports a single default gateway. A manually configured default gateway is more preferable than a default gateway learned from a DHCP server.
ARP table	The switch maintains an ARP table that maps an IP address to a MAC address. You can create static ARP entries in the table and manage various ARP table settings such as the aging time of dynamically-learned entries.
Routing table entries	You can configure the following route types in the routing table: • Default: The default route is the route the switch will use to send a packet if the routing table does not contain a longer matching prefix for the packet's destination. • Static: A static route is a route that you manually add to the routing table. • Static Reject: Packets that match a reject route are discarded instead of forwarded. The router may send an ICMP Destination Unreachable message.
Route preferences	The common routing table collects static, local, and dynamic (routing protocol) routes. When there is more than one route to the same destination prefix, the routing table selects the route with the best (lowest) route preference.

VLAN Routing

VLANs divide a single physical network (broadcast domain) into separate logical networks. To forward traffic across VLAN boundaries, a layer 3 device, such as router, is required. A switch running DCSS software can act as layer 3 device when you configure VLAN routing interfaces. VLAN routing interfaces make it possible to transmit traffic between VLANs while still containing broadcast traffic within VLAN boundaries. The configuration of VLAN routing interfaces makes inter-VLAN routing possible.

For each VLAN routing interface you can assign a static IP address, or you can allow a network DHCP server to assign a dynamic IP address.

When a port is enabled for bridging (L2 switching) rather than routing, which is the default, 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 router interface, the packet is routed. An inbound multicast packet is forwarded to all ports in the VLAN, plus the internal bridge-router interface, if it was received on a routed VLAN.

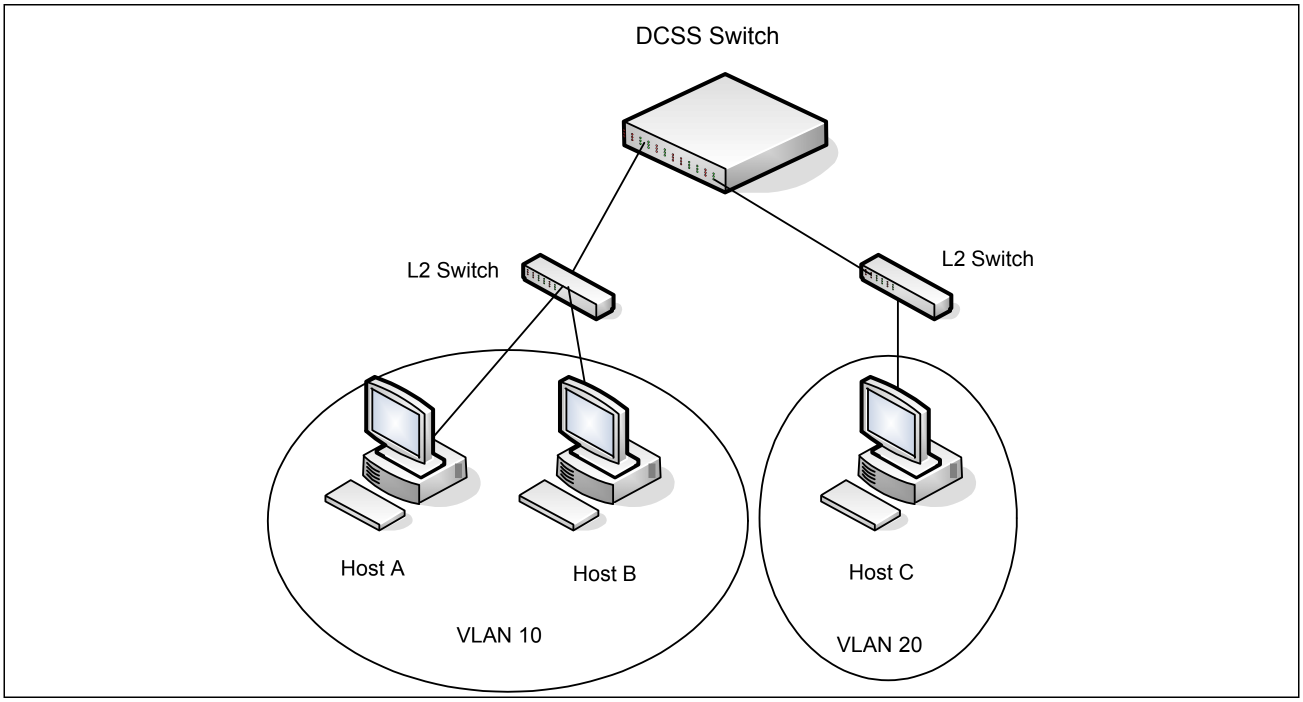
Since a port can be configured to belong to more than one VLAN, VLAN routing might be enabled for all of the VLANs on the port or for only some of the VLANs on the port. VLAN Routing can be used to allow more than one physical port to reside on the same subnet. It could also be used when a VLAN spans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

When To Configure VLAN Routing

VLAN routing is required when the switch is used as a layer 3 device. VLAN routing must be configured to allow the switch to forward IP traffic between subnets and allow hosts in different networks to communicate.

In Figure 4 the DCSS switch is configured as an L3 device and performs the routing functions for hosts connected to the L2 switches. For Host A to communicate with Host B, no routing is necessary. These hosts are in the same VLAN. However, for Host A in VLAN 10 to communicate with Host C in VLAN 20, the switch must perform inter-VLAN routing.

Figure 4: Inter-VLAN Routing

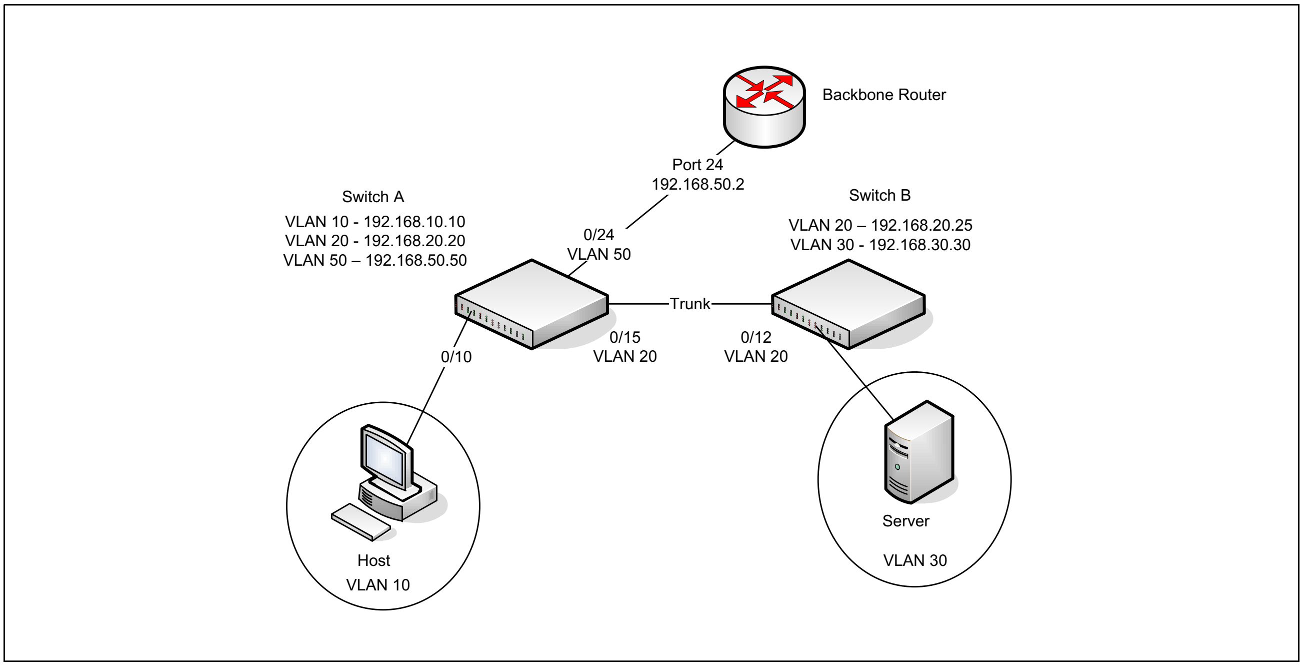


IP Routing Configuration Example

In this example, the switches are L3 switches with VLAN routing interfaces. VLAN routing is configured on Switch A and Switch B. This allows the host in VLAN 10 to communicate with the server in VLAN 30. A static route to the VLAN 30 subnet is configured on Switch A. Additionally, a default route is configured on Switch A so that all traffic with an unknown destination is sent to the backbone router through port 24, which is a member of VLAN 50. A default route is configured on Switch B to use Switch A as the default gateway. The hosts use the IP address of the VLAN routing interface as their default gateway.

This example assumes that all L2 VLAN information, such as VLAN creation and port membership, has been configured.

Figure 5: IP Routing Example Topology



Configuring Switch A

Do the following steps to configure Switch A.

1. Create the VLANs.

```
(Routing) #vlan database
(Routing) (Vlan)#vlan 10,20,30,50
```

2. Configure the VLANs for routing and assign the interface port numbers.

```
(Routing) (Vlan)#vlan routing 10 10
(Routing) (Vlan)#vlan routing 20 20
(Routing) (Vlan)#vlan routing 30 30
(Routing) (Vlan)#vlan routing 50 50
(Routing) (Vlan)#exit
```

3. View the interface names assigned to the VLAN routing interfaces.

```
(Routing) #show ip vlan

MAC Address used by Routing VLANs:   00:10:18:82:15:7E

           Logical
VLAN ID   Interface       IP Address       Subnet Mask
-------  -------------    ---------------  ---------------
10       4/10             0.0.0.0          0.0.0.0
20       4/20             0.0.0.0          0.0.0.0
30       4/30             0.0.0.0          0.0.0.0
50       4/50             0.0.0.0          0.0.0.0
```

4. Enable routing on the switch.

```
(Routing) #configure
(Routing) (Config)#ip routing
```

5. Assign an IP address to VLAN 10. This command also enables IP routing on the VLAN.

```
(Routing) (Config)#interface 4/10
(Routing) (Interface 4/10)#ip address 192.168.10.10 255.255.255.0
(Routing) (Interface 4/10)#exit
```

6. Assign an IP address to VLAN 20.

```
(Routing) (Config)#interface 4/20
(Routing) (Interface 4/20)#ip address 192.168.20.20 255.255.255.0
(Routing) (Interface 4/20)#exit
```

7. Assign an IP address to VLAN 50.

```
(Routing) (Config)#interface 4/50
(Routing) (Interface 4/50)#ip address 192.168.50.50 255.255.255.0
(Routing) (Interface 4/50)#exit
```

8. Configure a static route to the network that VLAN 30 is in, using the IP address of the VLAN 20 interface on Switch B as the next hop address.

```
(Routing) (Config)#ip route 192.168.30.0 255.255.255.0 192.168.20.25
```

9. Configure the backbone router interface as the default gateway.

```
(Routing) (Config)#ip route default 192.168.50.2
```

Configuring Switch B

Do the following steps to configure Switch B:

1. Create the VLANs.

```
(Routing) #vlan database
(Routing) (Vlan)#vlan 20,30
```

2. Configure the VLANs for routing.

```
(Routing) (Vlan)#vlan routing 20 20
```

```
(Routing) (Vlan)#vlan routing 30 30
(Routing) (Vlan)#exit
```

3. View the interface names assigned to the VLAN routing interfaces.

```
(Routing) #show ip vlan

MAC Address used by Routing VLANs:   00:10:18:82:15:7E

           Logical
VLAN ID   Interface        IP Address       Subnet Mask
-------  --------------  ---------------  ---------------
20       4/20             0.0.0.0          0.0.0.0
30       4/30             0.0.0.0          0.0.0.0
```

4. Enable routing on the switch.

```
(Routing) #configure
(Routing) (Config)#ip routing
```

5. Assign an IP address to VLAN 20. This command also enables IP routing on the VLAN.

```
(Routing) (Config)#interface 4/20
(Routing) (Interface 4/20)#ip address 192.168.20.25 255.255.255.0
(Routing) (Interface 4/20)#exit
```

6. Assign an IP address to VLAN 30. This command also enables IP routing on the VLAN.

```
(Routing) (Config)#interface 4/30
(Routing) (Interface 4/30)#ip address 192.168.30.30 255.255.255.0
(Routing) (Interface 4/30)#exit
```

7. Configure the VLAN 20 routing interface on Switch A as the default gateway so that any traffic with an unknown destination is sent to Switch A for forwarding.

```
(Routing) (Config)#ip route default 192.168.20.20
```

IP Helper

The IP Helper feature provides the ability for a router to forward configured UDP broadcast packets to a particular IP address. This allows applications to reach servers on non-local subnets. This is possible even when the application is designed to assume a server is always on a local subnet or when the application uses broadcast packets to reach the server (with the limited broadcast address 255.255.255.255, or a network directed broadcast address).

You can configure relay entries globally and on routing interfaces. Each relay entry maps an ingress interface and destination UDP port number to a single IPv4 address (the helper address). Multiple relay entries may be configured for the same interface and UDP port, in which case the relay agent relays matching packets to each server address. Interface configuration takes priority over global configuration. If the destination UDP port for a packet matches any entry on the ingress interface, the packet is handled according to the interface configuration. If the packet does not match any entry on the ingress interface, the packet is handled according to the global IP helper configuration.

You can configure discard relay entries. Discard entries are used to discard packets received on a specific interface when those packets would otherwise be relayed according to a global relay entry. Discard relay entries may be configured on interfaces, but are not configured globally.

Additionally, you can configure which UDP ports are forwarded. Certain UDP port numbers can be specified by name in the CLI, but you can also configure a relay entry with any UDP port number. You may configure relay entries that do not specify a destination UDP port. The relay agent assumes that these entries match packets with the UDP destination ports listed in Table 8 (the list of default ports).

Table 8: Default Ports - UDP Port Numbers Implied By Wildcard

Protocol	***UDP Port Number***
IEN-116 Name Service	42
DNS	53
NetBIOS Name Server	137
NetBIOS Datagram Server	138
TACACS Server	49
Time Service	37
DHCP	67
Trivial File Transfer Protocol	69

The system limits the number of relay entries to four times the maximum number of routing interfaces (512 relay entries). There is no limit to the number of relay entries on an individual interface, and no limit to the number of servers for a given {interface, UDP port} pair.

Certain configurable DHCP relay options do not apply to relay of other protocols. You may optionally set a maximum hop count or minimum wait time using the `bootpdhcprelay maxhopcount` and `bootpdhcprelay minwaittime` commands.

The relay agent relays DHCP packets in both directions. It relays broadcast packets from the client to one or more DHCP servers, and relays packets to the client that the DHCP server unicasts back to the relay agent. For other protocols, the relay agent only relays broadcast packets from the client to the server. Packets from the server back to the client are assumed to be unicast directly to the client. Because there is no relay in the return direction for protocols other than DHCP, the relay agent retains the source IP address from the original client packet. The relay agent uses a local IP address as the source IP address of relayed DHCP client packets.

When a switch receives a broadcast UDP packet on a routing interface, the relay agent verifies that the interface is configured to relay to the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise, the relay agent verifies that there is a global configuration for the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise the packet is not relayed.

Note: If the packet matches a discard relay entry on the ingress interface, the packet is not forwarded, regardless of the global configuration.

The relay agent relays packets that meet only the following conditions:

- The destination MAC address must be the all-ones broadcast address (FF:FF:FF:FF:FF:FF).
- The destination IP address must be the limited broadcast address (255.255.255.255) or a directed broadcast address for the receive interface.
- The IP time-to-live (TTL) must be greater than 1.
- The protocol field in the IP header must be UDP (17).
- The destination UDP port must match a configured relay entry.

Table 9 shows the most common protocols and their UDP port numbers and names that are relayed.

Table 9: UDP Port Allocations

UDP Port Number	***Acronym***	***Application***
7	Echo	Echo
11	SysStat	Active User
15	NetStat	NetStat
17	Quote	Quote of the day
19	CHARGEN	Character Generator
20	FTP-data	FTP Data
21	FTP	FTP
37	Time	Time
42	NAMESERVER	Host Name Server
43	NICNAME	Who is
53	DOMAIN	Domain Name Server
69	TFTP	Trivial File Transfer
111	SUNRPC	Sun Microsystems Rpc
123	NTP	Network Time
137	NetBiosNameService	NT Server to Station Connections

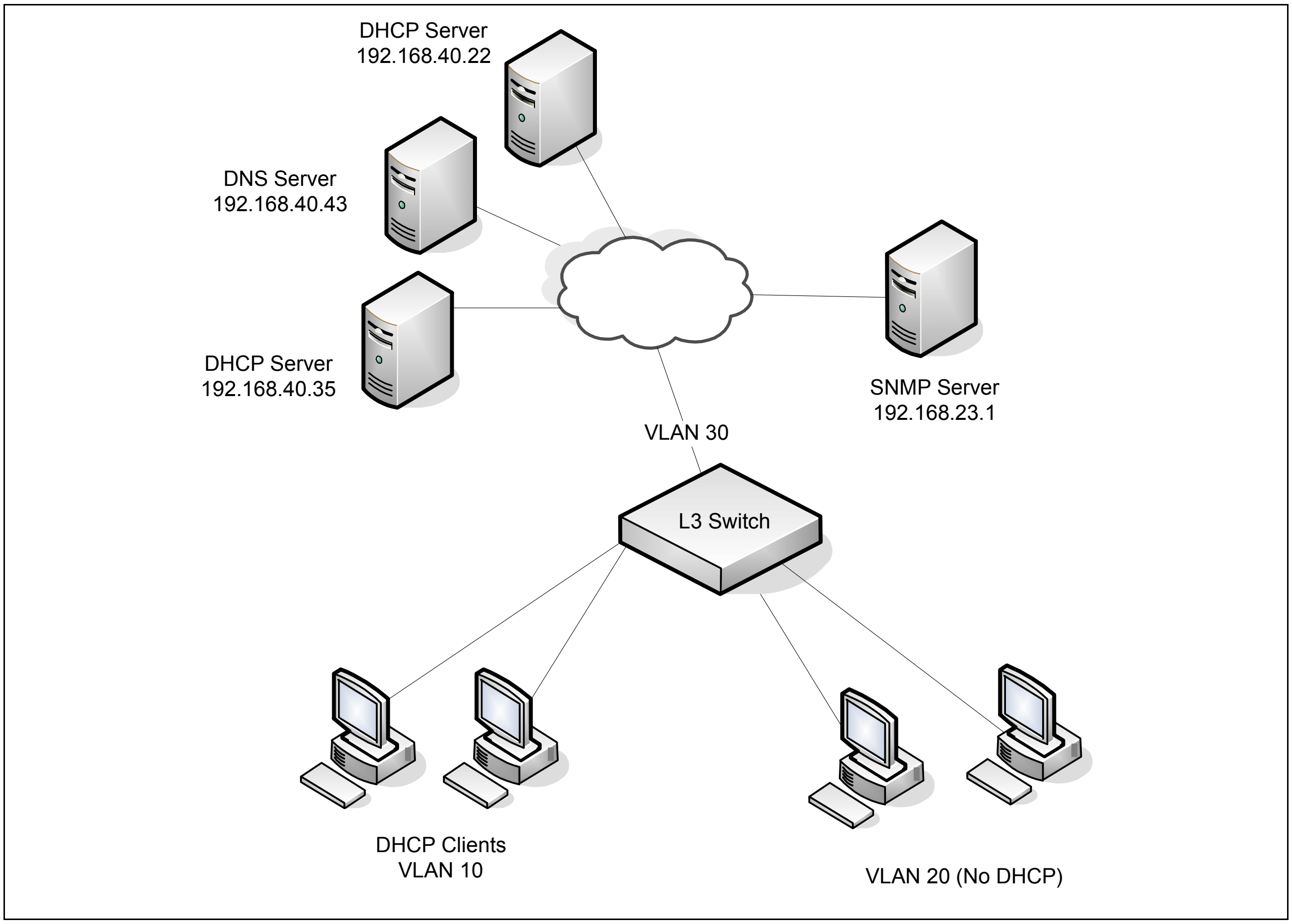
Table 9: UDP Port Allocations (Cont.)

UDP Port Number	Acronym	Application
138	NetBiosDatagramService	NT Server to Station Connections
139	NetBios	SessionServiceNT Server to Station Connections
161	SNMP	Simple Network Management
162	SNMP-trap	Simple Network Management Traps
513	who	Unix Rwho Daemon
514	syslog	System Log
525	timed	Time Daemon

Relay Agent Configuration Example

The example in this section shows how to configure the L3 relay agent (IP helper) to relay and discard various protocols.

Figure 6: L3 Relay Network Diagram



This example assumes that multiple VLAN routing interfaces have been created and configured with IP addresses.

Use the following steps to configure the switch:

1. Enable IP helper on the switch.

```
(Routing) #config
(Routing) (Config)#ip helper enable
```

2. Relay DHCP packets received on VLAN 10 to 192.168.40.35

```
(Routing) (Config)#interface 4/1
(Routing) (Interface 4/1)#ip helper-address 192.168.40.35 dhcp
```

3. Relay DNS packets received on VLAN 10 to 192.168.40.43

```
(Routing) (Interface 4/1)#ip helper-address 192.168.40.35 domain
(Routing) (Interface 4/1)#exit
```

4. Relay SNMP traps (port 162) received on VLAN 20 to 192.168.23.1

```
(Routing) (Config)#interface 4/2
(Routing) (interface 4/2)#ip helper-address 192.168.23.1 162
```

5. The clients on VLAN 20 have statically-configured network information, so the switch is configured to drop DHCP packets received on VLAN 20

```
(Routing) (Interface 4/2)#ip helper-address discard dhcp
(Routing) (Interface 4/2)#exit
```

6. Configure the switch so that DHCP packets received from clients in any VLAN other than VLAN 10 and VLAN 20 are relayed to 192.168.40.22.

Note: The following command is issued in Global Configuration mode, so it applies to all interfaces except VLAN 10 and VLAN 20. IP helper commands issued in Interface Configuration mode override the commands issued in Global Configuration Mode.

```
(Routing) (Config)#ip helper-address 192.168.40.22 dhcp
(Routing) (Config)#exit
```

7. Verify the configuration.

```
(Routing) #show ip helper-address

IP helper is enabled

Interface               UDP Port    Discard  Hit Count     Server Address
-------------------- ----------- ---------- ---------- ------------------
4/1                       domain         No          0      192.168.40.35
4/1                         dhcp         No          0      192.168.40.35
4/2                         dhcp        Yes          0
4/2                          162         No          0       192.168.23.1
Any                         dhcp         No          0      192.168.40.22
```

Appendix A: Terms and Acronyms

Table 10: Terms and Acronyms

Term	***Definition***
Access port	A port where native (i.e. unencapsulated) packets are associated with a DCVPN. May be a physical port or a LAG.
ACL	Access Control List
Adj-RIB-In	The collection of routing information received from peers
AS	Autonomous System
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BPDU	Bridge Protocol Data Unit
CBS	Committed Burst Size
CIR	Committed Information Rate
CLI	Command Line Interface
CN	Congestion Notification, IEEE 802.1Qau
CoA	Change of Authorization
CoS	Class of Service
CS	Class Selector (as in PHB)
DAC	Dynamic Authorization Client
DAS	Dynamic Authorization Server
DCB	Data Center Bridging
DCPDP	Dual Control Plane Detection Protocol
DCVPN	Data center virtual private network. This term can refer to the overall data center L2 over L3 tunneling feature, realized through VXLAN or NVGRE. This term may also be used to refer to the DC L2 over L3 tunnel application in DCSS.
DCVPN Gateway	A VXLAN or NVGRE gateway
Default Router	The legacy router. When the Virtual Routing feature is disabled only the Default Router is operational. When the Virtual Routing feature is enabled the Default Router supports all routing protocols and features, while the Virtual Routers support only a subset of features. Also the default router is configured via CLI without specifying the “vrf” keyword.
802.3ad	IEEE Std for Link Aggregation
DSCP	Differentiated Services Code Point
eBGP	Exterior Border Gateway Protocol
ECMP	Equal-Cost Multipath
ECN	Explicit Congestion Notification
ENode	FCoE End Node
ETS	Enhanced Transmission Selection, IEEE 802.1Qaz
FC	Fibre Channel
FCF	FCoE Forwarder

Table 10: Terms and Acronyms (Cont.)

Term	***Definition***
FCoE	Fibre Channel Over Ethernet
FDB	Forwarding Database
FIP	Fibre Channel Initialization Protocol
iBGP	Interior Border Gateway Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IP Interface	An interface configured as an IP interface rather than a layer 2 switching interface. An IP interface must be assigned one more IP addresses.
LACP	Link Aggregation Control Protocol
LAG	Link aggregation
LFDB	Label Forwarding Database
LSP	Label Switched Path
MAC	Media Access Control
MFDB	Multicast Forwarding Database
MIB	Management Information Base
VPC partner switch	DUT that is VPC unaware and forms one end of the LAG (with VPC aware switches on the other end)
VPC peer switches	DUTs that are VPC aware and pair to form one end of the LAG
VPC peer-link	Peer-Link between two MLAG peer switches
MAB	MAC Authentication Bypass. This feature provides 802.1x-unaware clients (such as printers and fax machines) controlled access to the network using the devices' MAC address as an identifier.
MPLS	Multi-Protocol Label Switching
MVR	Multicast VLAN Registration
NAS	Network Access Server
Network port (in DCVPN)	A port where DCVPN tunnels originate or terminate.
Non-redundant ports	Ports on the VPC aware switch that do not participate in VPC.
NSF	Non-stop forwarding
NVE	Network Virtualization Edge. NVGRE term for a device or software module that bridges between the overlay and underlay networks. Synonym for VTEP.
NVGRE	Network Virtualization using Generic Routing Encapsulation
PBS	Peak Burst Size
PDU	Protocol data unit
PFC	Priority-based Flow Control,
PIR	Peak Information Rate
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Services
RED	Random Early Discard
RFC	Request For Comments
Route Leaking	The ability to inject routes belonging to one VR instance into another.

Table 10: Terms and Acronyms (Cont.)

Term	*Definition*
RTO	Routing Table Object. The common routing table, or "RIB", which collects routes from all sources (local, static, dynamic) and determines the most preferred route to each destination.
SDM	Switch Database Management
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
Tenant	An organization for which one or more virtual networks has been provisioned.
Tenant System	A physical or virtual resource, such as a compute or storage device, that is assigned to a specific tenant.
TRILL	Transparent Interconnect of Lots of Links
UDP	User Datagram Protocol
UI	User Interface
Underlay network	IP network that carries tunnel encapsulated traffic from one VTEP/NVE to another.
VLAN	Virtual Local Area Network
VM	Virtual Machine. A virtualized end host.
VN	Virtual Network. The set of tunnels, VTEPs, and tenant systems forming a closed user group. For VXLAN, all traffic in a VN carries the same VNID. This document uses VN interchangeably with DCVPN.
VNID	Virtual network identifier. A 24-bit value that uniquely identifies a VXLAN segment.
VoIP	Voice over Internet Protocol
VPC	Virtual Port Channel
VR	Virtual Router
VR-aware	Whether the feature is aware of and works independently in each Virtual Router
VR instance	An instance of the virtual router
VRF	Virtual Routing and Forwarding (unless otherwise specified, VRF refers to VRF Lite solution in DCSS.
VRF Lite	VRF Without MPLS
VRID	Virtual Router Identifier
VRRP	Virtual Router Redundancy Protocol
VSID	Virtual Segment Subnet IdentifierD.ID. A 24-bit value used as a Virtual network identifier in NVGRE.
VTEP	Virtual Tunnel End Point. A device or module that does VXLAN tunnel initiation and termination. Synonym for NVE.
VXLAN	Virtual Extensible Local Area Network
WRED	Weighted Random Early Discard
ZTP	Zero-Touch Provisioning. This feature enables automatic installation of the Chef Client/Puppet Agent to support Auto Install functionality upon switch bootup.