



## Initial Configuration

---


This chapter describes how to initially configure switches so they can be accessed by other devices. This chapter includes the following sections:

- [Starting a Switch in the Cisco MDS 9000 Family, page 4-2](#)
- [Initial Setup Routine, page 4-2](#)
- [Accessing the Switch, page 4-13](#)
- [Assigning a Switch Name, page 4-14](#)
- [Where Do You Go Next?, page 4-14](#)
- [Verifying the Module Status, page 4-14](#)
- [Configuring Date and Time, page 4-15](#)
- [Management Interface Configuration, page 4-20](#)
- [Telnet Server Connection, page 4-22](#)
- [Working with Configuration Files, page 4-23](#)
- [Deleting Files, page 4-29](#)
- [Accessing Remote File Systems, page 4-29](#)
- [Deleting Files, page 4-29](#)
- [Configuring Console Settings, page 4-30](#)
- [Configuring COM1 Settings, page 4-31](#)
- [Configuring Modem Connections, page 4-32](#)
- [CDP Configuration, page 4-36](#)

# Starting a Switch in the Cisco MDS 9000 Family

The following procedure is a review of the tasks you should have completed during hardware installation, including starting up the switch. These tasks must be completed before you can configure the switch.

Before you can configure a switch, follow these steps:

- 
- Step 1** Verify the following physical connections for the new Cisco MDS 9000 Family switch:
- The console port is physically connected to a computer terminal (or terminal server).
  - The management 10/100 Ethernet port (mgmt0) is connected to an external hub, switch, or router.
- Refer to the *Cisco MDS 9000 Family Hardware Installation Guide* (for the required product) for more information.
-  **Tip** Save the host ID information for future use (for example, to enable licensed features). The host ID information is provided in the Proof of Purchase document that accompanies the switch.
- 
- Step 2** Verify that the default console port parameters are identical to those of the computer terminal (or terminal server) attached to the switch console port:
- 9600 baud
  - 8 data bits
  - 1 stop bit
  - No parity
- Step 3** Power on the switch. The switch boots automatically and the `switch#` prompt appears in your terminal window.
- 

## Initial Setup Routine

The first time that you access a switch in the Cisco MDS 9000 Family, it runs a setup program that prompts you for the IP address and other configuration information necessary for the switch to communicate over the supervisor module Ethernet interface. This information is required to configure and manage the switch.

**Note**

The IP address can only be configured from the CLI. When you power up the switch for the first time assign the IP address. After you perform this step, the Cisco MDS 9000 Family Fabric Manager can reach the switch through the console port.

---

## Preparing to Configure the Switch

Before you configure a switch in the Cisco MDS 9000 Family for the first time, you need the following information:

- Administrator password, including:
  - Changing the default password (admin) for the administrator.
  - Creating an additional login account and password.
- SNMPv3 user name and authentication password.
- SNMP community string.
- Switch name—This is your switch prompt.
- IP address for the switch's management interface—The management interface can be an out-of-band Ethernet interface or an in-band Fibre Channel interface.
- Subnet mask for the switch's management interface.
- IP addresses, including:
  - Destination prefix, destination prefix subnet mask, and next hop IP address, if you want to enable IP routing. Also, provide the IP address of the default network.
  - Otherwise, provide an IP address of the default gateway.
- DNS IP address (optional).
- Default domain name (optional).
- SSH service on the switch—To enable this service, select the type of SSH key (dsa/rsa/rsa1) and number of key bits (768 to 2048).
- NTP server IP address (optional).

**Note**

---

Be sure to configure the IP route, the IP default network address, and the IP default gateway address to enable SNMP access. If IP routing is enabled, the switch uses the IP route and the default network IP address. If IP routing is disabled, the switch uses the default gateway IP address.

---

## Default Login

All Cisco MDS 9000 Family switches have the network administrator as a default user (admin) and a default password (admin). You can change the default password, if required, during the initial setup process. You cannot change the default user at any time.

During the initial setup process, you have the option to configure one additional user in the network administrator role. If you change the administrator password during the initial setup process and subsequently forget this new password, you have the option to recover this password.

See the [“Role-Based CLI Authorization” section on page 16-18](#) for information on default roles and permissions and see the [“Recovering Administrator Password” section on page 16-26](#) for information on changing the administrator password.

## Setup Options

The setup scenario differs based on the subnet to which you are adding the new switch. You must configure a switch in the Cisco MDS 9000 Family with an IP address to enable management connections from outside of the switch.

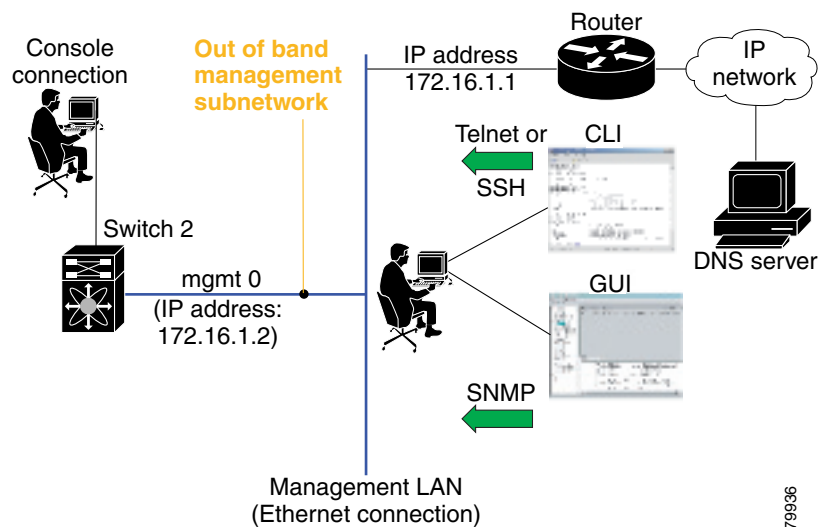


### Note

Some concepts such as out-of-band management and in-band management are briefly explained here. These concepts are explained in more detail in subsequent chapters.

- Out-of-band management—This feature provides a connection to the network through a supervisor module front panel Ethernet port (see [Figure 4-1](#)).
- In-band management—This feature provides IP over Fibre Channel (IPFC) to manage the switches. The in-band management feature is transparent to the network management system (NMS). Instead of conventional Ethernet physical media, switches in the Cisco MDS 9000 Family use IPFC as the transport mechanism (see [Figure 4-1](#) and [Chapter 20, “Configuring IP Services”](#)).

**Figure 4-1 Management Access to Switches**



79936

## Assigning Setup Information

This section describes how to initially configure the switch for both out-of-band and in-band management.



### Note

Press **Ctrl-C** at any prompt to skip the remaining configuration options and proceed with what is configured until that point.



### Tip

If you do not wish to answer a previously configured question, or if you wish to skip answers to any questions, press **Enter**. If a default answer is not available (for example, switch name), the switch uses what was previously configured and skips to the next question.

## Configuring Out-of-Band Management



### Note

You can configure both in-band and out-of-band configuration together by entering **Yes** in both [Step 11](#) and [Step 12](#) in the following procedure.

To configure the switch for first time out-of-band access, follow these steps:

**Step 1** Power on the switch. Switches in the Cisco MDS 9000 Family boot automatically.

**Step 2** Enter **yes** to enter the setup mode.

This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

Press Enter incase you want to skip any dialog. Use ctrl-c at anytime to skip away remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): **yes**

The setup utility guides you through the basic configuration process. Press **Ctrl-C** at any prompt to end the configuration process.

**Step 3** Enter the new password for the administrator (admin is the default).

Enter the password for admin: **admin**

**Step 4** Enter **yes** (no is the default) to create additional accounts.

Create another login account (yes/no) [n]: **yes**

While configuring your initial setup, you can create an additional user account (in the network-admin role) besides the administrator's account. See the [“Role-Based CLI Authorization”](#) section on [page 16-18](#) for information on default roles and permissions.

a. Enter the user login ID.

Enter the user login ID: *user\_name*

b. Enter the user password.

Enter the password for user\_name: *user-password*

**Step 5** Enter **yes** (yes is the default) to create an SNMPv3 account.

Configure SNMPv3 Management parameters (yes/no) [y]: **yes**

**a.** Enter the user name (admin is the default).

SNMPv3 user name [admin]: **admin**

**b.** Enter the SNMPv3 password (minimum of eight characters).

SNMPv3 user authentication password: *admin\_pass*




---

**Note** By default, if the admin password is at least eight characters, then the SNMP authentication password is the same as the admin password (at least eight characters). If the admin password is less than eight characters, then you need to provide a new password for SNMP. The admin password can have a minimum of one character, but the SNMP authentication password must have a minimum of eight characters.

---

**Step 6** Enter **yes** (no is the default) to configure read-only or read-write SNMP community string.

Configure read-only SNMP community string (yes/no) [n]: **yes**

**a.** Enter the SNMP community string.

SNMP community string: *snmp\_community*

**Step 7** Enter a name for the switch.




---

**Note** The switch name is limited to 32 alphanumeric characters.

---

Enter the switch name: *switch\_name*

**Step 8** Enter **yes** (yes is the default) to configure out-of-band management.

Continue with Out-of-band (mgmt0) management configuration? [yes/no]: **yes**

**a.** Enter the mgmt0 IP address.

Mgmt0 IP address: *ip\_address*

**b.** Enter the mgmt0 subnet mask.

Mgmt0 IP netmask: *subnet\_mask*

**Step 9** Enter **no** (no is the default) at the in-band management configuration prompt.

Continue with in-band (VSAN1) management configuration? (yes/no) [no]: **no**

**Step 10** Enter **yes** (yes is the default) to enable IP routing capabilities.

Enable the ip routing capabilities? (yes/no) [y]: **yes**

**Step 11** Enter **yes** (yes is the default) to configure a static route (recommended).

Configure static route: (yes/no) [y]: **yes**

**a.** Enter the destination prefix.

Destination prefix: *dest\_prefix*

**b.** Type the destination prefix mask.

Destination prefix mask: *dest\_mask*

- c. Type the next hop IP address.

Next hop ip address: *next\_hop\_address*




---

**Note** Be sure to configure the IP route, the IP default network address, and the IP default gateway address to enable SNMP access. If IP routing is enabled, the switch uses the IP route and the default network IP address. If IP routing is disabled, the switch uses the default gateway IP address.

---

- Step 12** Enter **yes** (yes is the default) to configure the default network (recommended).

Configure the default-network: (yes/no) [y]: **yes**

- a. Enter the default network IP address.




---

**Note** The default network address is the destination prefix provided earlier in Step 11 a.

---

Default network IP address: *dest\_prefix*

- Step 13** Enter **yes** (yes is the default) to configure the default gateway (recommended).

Configure the default-gateway: (yes/no) [y]: **yes**

- a. Enter the default gateway IP address.

IP address of the default-gateway: *default\_gateway*

- Step 14** Enter **yes** (yes is the default) to configure the DNS IP address.

Configure the DNS IP address? (yes/no) [y]: **yes**

- a. Enter the DNS IP address.

DNS IP address: *name\_server*

- Step 15** Enter **yes** (default is no) to configure the default domain name.

Configure the default domain name? (yes/no) [n]: **yes**

- a. Enter the default domain name.

Default domain name: *domain\_name*

- Step 16** Enter **yes** (yes is the default) to enable Telnet service.

Enable the telnet service? (yes/no) [y]: **yes**

- Step 17** Enter **yes** (no is the default) to enable the SSH service.

Enabled SSH service? (yes/no) [n]: **yes**

- Step 18** Enter the SSH key type (see the “[Generating the SSH Host Key Pair](#)” section on page 16-28) that you would like to generate.

Type the SSH key you would like to generate (dsa/rsa/rsal)? **dsa**

- Step 19** Enter the number of key bits within the specified range.

Enter the number of key bits? (512 to 2048): **768**

**Step 20** Enter **yes** (no is the default) to configure the NTP server.

```
Configure NTP server? (yes/no) [n]: yes
```

a. Enter the NTP server IP address.

```
NTP server IP address: ntp_server_IP_address
```

**Step 21** Enter **shut** (shut is the default) to configure the default switchport interface to the shut state.

```
Configure default switchport interface state (shut/noshut) [shut]: shut
```



**Note**

The management ethernet interface is not shut down at this point—only the Fibre Channel, iSCSI, FCIP, and Gigabit Ethernet interfaces are shut down.

**Step 22** Enter **on** (on is the default) to configure the switchport trunk mode.

```
Configure default switchport trunk mode (on/off/auto) [on]: on
```

**Step 23** Enter **deny** (deny is the default) to deny a default zone policy configuration.

```
Configure default zone policy (permit/deny) [deny]: deny
```

Denies traffic flow to all members of the default zone.

**Step 24** Enter **no** (no is the default) to disable a full zoneset distribution (see the [“Zone Set Distribution” section on page 13-11](#)).

```
Enable full zoneset distribution (yes/no) [n]: no
```

Disables the switch-wide default for the full-zoneset distribution feature.

**Step 25** Enter **no** (no is the default) to disable FC ID persistence in all VSANs in the switch (see the [“Enabling Persistent FC IDs” section on page 24-9](#)).

```
Enable FCID persistence in all the VSANs on this switch (yes/no) [n]: no
```

Disables FC ID persistence in all VSANs in the switch.

You see the new configuration.

**Step 26** Review and edit the configuration that you have just entered.

**Step 27** Enter **no** (no is the default) if you are satisfied with the configuration.

The following configuration will be applied:

```
username admin password admin_pass role network-admin
username user_name password user_pass role network-admin
snmp-server user admin network-admin auth md5 admin_pass priv admin_pass
snmp-server community snmp_community ro
switchname switch
interface mgmt0
  ip address ip_address subnet_mask
  no shutdown
ip routing
ip route dest_prefix dest_mask dest_address
ip default-network dest_prefix
ip default-gateway default_gateway
ip name-server name_server
ip domain-name domain_name
telnet server enable
ssh key dsa 768 force
ssh server enable
ntp server ipaddr ntp_server
no system default switchport shutdown
```



```

system default switchport trunk mode auto
no zone default-zone permit vsan 1-4093
no zoneset distribute full vsan 1-4093
no fcdomain fcid persistent global-enable

```

Would you like to edit the configuration? (yes/no) [n]: **no**

**Step 28** Enter **yes** (yes is default) to use and save this configuration:

Use this configuration and save it? (yes/no) [y]: **yes**



### Caution

If you do not save the configuration at this point, none of your changes are updated the next time the switch is rebooted. Type **yes** in order to save the new configuration. This ensures that the kickstart and system boot images are also automatically configured (see [Chapter 6, “Software Images”](#)).

## In-Band Management Configuration

The in-band management logical interface is VSAN 1. This management interface uses the Fibre Channel infrastructure to transport IP traffic. An interface for VSAN 1 is created on every switch in the fabric. Each switch should have its VSAN 1 interface configured with an IP address in the same subnetwork. A default route that points to the switch providing access to the IP network should be configured on every switch in the Fibre Channel fabric (see [Chapter 9, “Configuring and Managing VSANs”](#)).



### Note

You can configure both in-band and out-of-band configuration together by entering **Yes** in both [Step 11](#) and [Step 12](#) in the following procedure.

To configure a switch for first time in-band access, follow these steps:

**Step 1** Power on the switch. Switches in the Cisco MDS 9000 Family boot automatically.

**Step 2** Enter **yes** to enter the setup mode.

```

---- Basic System Configuration Dialog ----
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

```

```

Press Enter incase you want to skip any dialog. Use ctrl-c at anytime
to skip away remaining dialogs.

```

Would you like to enter the basic configuration dialog (yes/no): **yes**

The setup utility guides you through the basic configuration process. Press **Ctrl-C** from any prompt to end the configuration process.

**Step 3** Enter the new password (admin is the default) for the administrator.

```

Enter the password for admin: new_password

```

**Step 4** Enter **no** (no is the default) if you do not wish to create additional accounts.

```

Create another login account (yes/no) [no]: no

```

**Step 5** Enter **yes** (yes is the default) to create an SNMPv3 account.

Configure SNMPv3 Management parameters (yes/no) [y]: **yes**

**a.** Enter the user name (admin is the default).

SNMPv3 user name [admin]: *user\_name*

By default, the SNMP user name is admin.

**b.** Enter the SNMPv3 password (minimum of eight characters).

SNMPv3 user authentication password [admin\_pass]: *admin\_pass*




---

**Note** By default, if the admin password is at least eight characters, then the SNMP authentication password is the same as the admin password (at least eight characters). If the admin password is less than eight characters, then you need to provide a new password for SNMP. The admin password can have a minimum of one character, but the SNMP authentication password must have a minimum of eight characters.

---

**Step 6** Configure read-only or read-write SNMP community string.

**a.** Enter **no** (no is the default) to avoid configuring read-only SNMP community string.

Configure read-only SNMP community string (yes/no) [n]: **no**

**b.** Enter **no** (no is the default) to configure read-only SNMP community string.

Configure read-only SNMP community string (yes/no) [n]: **yes**

**c.** Enter the SNMP community string.

SNMP community string: *snmp\_community*

**Step 7** Enter a name for the switch.




---

**Note** The switch name is limited to 32 alphanumeric characters.

---

Enter the switch name: *switch\_name*

**Step 8** Enter **no** (yes is the default) at the configuration prompt to configure out-of-band management.

Continue with Out-of-band (mgmt0) management configuration? [yes/no]: **no**

**Step 9** Enter **yes** (no is the default) at the in-band management configuration prompt.

Continue with in-band (VSAN1) management configuration? (yes/no) [no]: **yes**

**a.** Enter the VSAN 1 IP address.

VSAN1 IP address: *ip\_address*

**b.** Enter the subnet mask.


VSAN1 IP net mask: *subnet\_mask*

**Step 10** Enter **yes** (yes is the default) to enable IP routing capabilities.

Enable ip routing capabilities? (yes/no) [y]: **yes**

**Step 11** Enter **no** (yes is the default) to configure a static route.

Configure static route: (yes/no) [y]: **no**

- Step 12** Enter **yes** (yes is the default) to configure the default network.  
Configure the default-network: (yes/no) [y]: **no**
- Step 13** Enter **yes** (yes is the default) to configure the default gateway.  
Configure the default-gateway: (yes/no) [y]: **yes**
- a.** Enter the default gateway IP address.  
IP address of the default-gateway: default\_gateway
- Step 14** Enter **no** (yes is the default) to configure the DNS IP address.  
Configure the DNS IP address? (yes/no) [y]: **no**
- Step 15** Enter **no** (no is the default) to skip the default domain name configuration.  
Configure the default domain name? (yes/no) [n]: **no**
- Step 16** Enter **no** (yes is the default) to disable Telnet service.  
Enable the telnet service? (yes/no) [y]: **no**
- Step 17** Enter **yes** (no is the default) to enable the SSH service.  
Enabled SSH service? (yes/no) [n]: **yes**
- Step 18** Enter the SSH key type (see the [“Generating the SSH Host Key Pair”](#) section on page 16-28) that you would like to generate.  
Type the SSH key you would like to generate (dsa/rsa/rsa1)? **rsa**
- Step 19** Enter the number of key bits within the specified range.  
Enter the number of key bits? (512 to 1024): **1024**
- Step 20** Enter **no** (no is the default) to configure the NTP server.  
Configure NTP server? (yes/no) [n]: **no**
- Step 21** Enter **shut** (shut is the default) to configure the default switchport interface to the shut state.  
Configure default switchport interface state (shut/noshut) [shut]: **shut**
-  **Note** The management ethernet interface is not shut down at this point—only the Fibre Channel, iSCSI, FCIP, and Gigabit Ethernet interfaces are shut down.
- Step 22** Enter **on** (on is the default) to configure the switchport trunk mode.  
Configure default switchport trunk mode (on/off/auto) [on]: **on**
- Step 23** Enter **deny** (deny is the default) to deny a default zone policy configuration.  
Configure default zone policy (permit/deny) [deny]: **deny**
- Denies traffic flow to all members of the default zone.
- Step 24** Enter **no** (no is the default) to disable a full zoneset distribution (see the [“Zone Set Distribution”](#) section on page 13-11).  
Enable full zoneset distribution (yes/no) [n]: **no**
- Disables the switch-wide default for the full-zoneset distribution feature.

- Step 25** Enter **no** (no is the default) to disable FC ID persistence in all VSANs in the switch (see the “[Enabling Persistent FC IDs](#)” section on page 24-9).

```
Enable FCID persistence in all the VSANs on this switch (yes/no) [n]: no
```

Disables FC ID persistence in all VSANs in the switch.

You see the new configuration.

- Step 26** Review and edit the configuration that you have just entered.

- Step 27** Enter **no** (no is the default) if you are satisfied with the configuration.

The following configuration will be applied:

```
username admin password admin_pass role network-admin
snmp-server user snmp_user network-admin auth md5 snmp_pass priv snmp_pass
snmp-server community snmp_community rw
switchname switch
interface vsan1
  ip address ip_address subnet_mask
  no shutdown
ip default-gateway default_gateway
no telnet server enable
ssh key rsa 1024 force
ssh server enable
no system default switchport shutdown
system default switchport trunk mode auto
no zone default-zone permit vsan 1-4093
no zoneset distribute full vsan 1-4093
no fcdomain fcid persistent global-enable
```

```
Would you like to edit the configuration? (yes/no) [n]: no
```

- Step 28** Enter **yes** (yes is default) to use and save this configuration.

```
Use this configuration and save it? (yes/no) [y]: yes
```



#### Caution

If you do not save the configuration at this point, none of your changes are updated the next time the switch is rebooted. Type **yes** in order to save the new configuration. This ensures that the kickstart and system boot images are also automatically configured (see [Chapter 6, “Software Images”](#)).

## Using the setup Command

To make changes to the initial configuration at a later time, you can issue the **setup** command in EXEC mode.

```
switch# setup
---- Basic System Configuration Dialog ----
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup always assumes a predefined defaults irrespective
of the current system configuration when invoked from CLI.
```

```
Press Enter incase you want to skip any dialog. Use ctrl-c at anytime
to skip away remaining dialogs.
```

```
Would you like to enter the basic configuration dialog (yes/no): yes
```

The setup utility guides you through the basic configuration process.

# Accessing the Switch

After initial configuration, you can access the switch in one of three ways (see [Figure 4-2](#)):

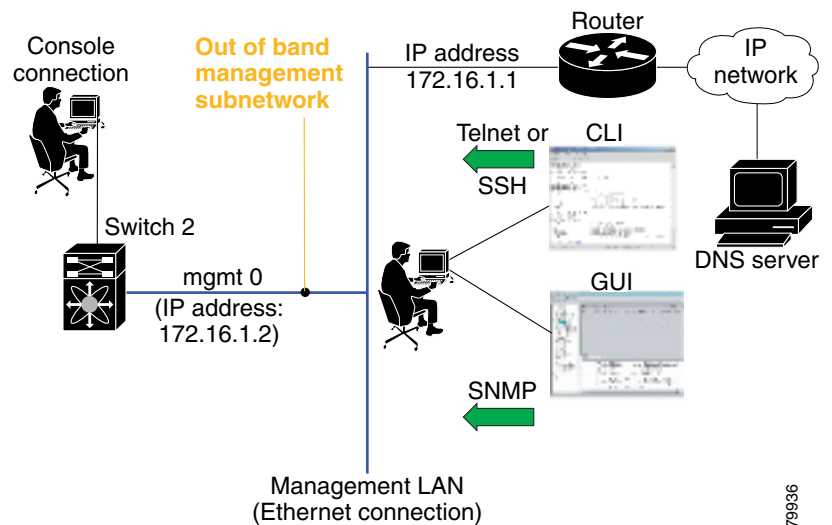
- In-band IP (IPFC) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use SNMP to connect to a Cisco MDS 9000 Fabric Manager application.
- Out-of-band (10/100BASE-T Ethernet) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use SNMP to connect to a Cisco MDS 9000 Fabric Manager application.



**Note** To use the Cisco Fabric Manager, refer to the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.

- Serial console access—You can use a serial port connection to access the CLI.

**Figure 4-2** Switch Access Options



## Assigning a Switch Name

Each switch in the fabric requires a unique name. You can assign names to easily identify the switch by its physical location, its SAN association, or the organization to which it is deployed. The assigned name is displayed in the command-line prompt. The switch name is limited to 32 alphanumeric characters.



### Note

This guide refers to a switch in the Cisco MDS 9000 Family as *switch*, and it uses the `switch#` prompt.

To change the name of the switch, follow these steps:

	Command	Purpose
Step 1	<code>switch# config t</code>	Enters configuration mode.
Step 2	<code>switch(config)# switchname myswitch1</code> <code>myswitch1(config)#</code>	Changes the switch name prompt as specified.
Step 3	<code>myswitch1(config)# no switchname</code> <code>switch(config)#</code>	Reverts the switch name prompt to its default (switch#).

## Where Do You Go Next?

After reviewing the default configuration, you can change it or perform other configuration or management tasks. The initial setup can only be performed at the CLI. However, you can continue to configure other software features, or access the switch after initial configuration by using either the CLI or the Device Manager and Fabric Manager applications.

To use the Cisco MDS 9000 Fabric Manager, refer to the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.

## Verifying the Module Status

Before you begin configuring the switch, you need to ensure that the modules in the chassis are functioning as designed. To verify the status of a module at any time, issue the **show module** command in EXEC mode. A sample output of the **show module** command follows:

```
switch# show module
Mod  Ports  Module-Type                               Model                               Status
---  -
1    0      Caching Services Module                 DS-X9560-SMAP                      ok
2    8      IP Storage Services Module               DS-X9308-SMIP                      ok <-----IPS-8 module
4    16     2x1GE IPS, 14x1/2Gbps FC Module         DS-X9216i-K9-SUP                   ok <-----MPS-14/2 module
5    0      Supervisor/Fabric-1                     DS-X9530-SF1-K9                    active *
6    0      Supervisor/Fabric-1                     DS-X9530-SF1-K9                    ha-standby
9    4      IP Storage Services Module               DS-X9304-SMIP                      ok <-----IPS-4 module

Mod  Sw          Hw          World-Wide-Name(s) (WWN)
---  -
1    2.0(1)     0.201      20:41:00:0b:fd:44:68:c0 to 20:48:00:0b:fd:44:68:c0
2    2.0(0.196) 0.206      20:41:00:0b:fd:44:68:c0 to 20:48:00:0b:fd:44:68:c0
4    2.0(1)     0.201      20:c1:00:05:30:00:07:1e to 20:d0:00:05:30:00:07:1e
5    2.0(1)     0.0        --
6    2.0(1)     0.0        --
9    2.0(1)     0.1        22:01:00:05:30:00:07:1e to 22:04:00:05:30:00:07:1e
```

```

Mod      Application Image Description      Application Image Version
-----
1        svc-node1                          2.0(1)
1        svc-node2                          2.0(1)

```

```

Mod  MAC-Address(es)      Serial-Num
---
1    00-05-30-01-49-c2 to 00-05-30-01-4a-46  JAB073907EP
2    00-05-30-00-9d-d2 to 00-05-30-00-9d-de  JAB064605a2
4    00-05-30-01-7f-32 to 00-05-30-01-7f-38  JAB081405AM
5    00-05-30-00-2c-4e to 00-05-30-00-2c-52  JAB06350B1M
6    00-05-30-00-19-66 to 00-05-30-00-19-6a  JAB073705GL
9    00-0d-bc-2f-d6-00 to 00-0d-bc-2f-d6-08  JAB080804TN

```

\* this terminal session

If the status is OK or active, you can continue with your configuration (see [Chapter 7, “Managing Modules”](#)).

## Configuring Date and Time

Switches in the Cisco MDS 9000 Family use Universal Coordinated Time (UTC), which is the same as Greenwich Mean Time (GMT). To change the default time on the switch, issue the **clock** command from EXEC mode.

```
switch# clock set <HH:MM:SS> <DD> <Month in words> <YYYY>
```

For example:

```
switch# clock set 15:58:09 23 September 2002
Mon Sep 23 15:58:09 UTC 2002
```

Where *HH* represents hours in military format (15 for 3 p.m.), *MM* is minutes (58), *SS* is seconds (09), *DD* is the date (23), *Month* is the month in words (September), and *YYYY* is the year (2002).



### Note

The **clock** command changes are saved across system resets.

## Configuring the Time Zone

You can specify a time zone for the switch.

To specify the local time without the daylight savings feature, follow these steps:

	Command	Purpose
Step 1	switch# <b>config t</b>	Enters configuration mode.
Step 2	switch(config)# <b>clock timezone</b> <timezone name> <-23 to 23 hours offset from UTC time> <0 to 50 minutes offset from UTC>  Example: switch(config)# <b>clock timezone PST -8 0</b>	Sets the time zone with a specified name, specified hours, and specified minutes.  This example sets the time zone to Pacific Standard Time (PST) and offsets the UTC time by negative eight hours and 0 minutes.
Step 3	switch(config)# <b>exit</b> switch#	Returns to EXEC mode.
Step 4	switch# <b>show clock</b>	Verifies the time zone configuration.
Step 5	switch# <b>show run</b>	Displays changes made to the time zone configuration along with other configuration information.

## Adjusting for Daylight Saving Time

Following U.S. standards, you can have the switch advance the clock one hour at 2:00 a.m. on the first Sunday in April and move back the clock one hour at 2:00 a.m. on the last Sunday in October. You can also explicitly specify the start and end dates and times and whether or not the time adjustment recurs every year.

To enable the daylight saving time clock adjustment according to the U.S. rules, follow these steps:

	Command	Purpose
Step 1	switch# <b>config t</b>	Enters configuration mode.
Step 2	switch(config)# <b>clock timezone</b> <i>timezone_name hour_offset_from_UTC minute_offset_from_UTC</i>  Example: switch(config)# <b>clock timezone PST -8 0</b> switch(config)# <b>no clock timezone</b>	Offsets the time zone as specified.  This example set the Pacific standard offset time as negative 8 hours and 0 minutes.
		Disables the time zone adjustment feature.



	Command	Purpose
<b>Step 3</b>	<pre>switch(config)# clock summer-time daylight_timezone_name start_week start_day start_month start_time end_week end_day end_month end_time daylight_offset_inminutes</pre> <p>Example:</p> <pre>switch(config)# clock summer-time PDT 1 Sun Apr 02:00 5 Sun Oct 02:00 60 switch(config)#</pre>	<p>Sets the daylight savings time for a specified time zone.</p> <p>The start and end values are as follows:</p> <ul style="list-style-type: none"> <li>• Week ranging from 1 through 5</li> <li>• Day ranging from Sunday through Saturday</li> <li>• Month ranging from January through December</li> </ul> <p>The daylight offset ranges from 1 through 1440 minutes which are added to the start time and deleted time from the end time.</p> <p>This example adjusts the daylight savings time for the Pacific daylight time by 60 minutes starting the first Sunday in April at 2 a.m. and ending the last Sunday in October at 2 a.m.</p>
	<pre>switch(config)# no clock summer-time</pre>	Disables the daylight saving time adjustment feature.
<b>Step 4</b>	<pre>switch(config)# exit switch#</pre>	Returns to EXEC mode.
<b>Step 5</b>	<pre>switch# show clock</pre>	Verifies the time zone configuration.

## NTP Configuration

A Network Time Protocol (NTP) server provides a precise time source (radio clock or atomic clock) to synchronize the system clocks of network devices. NTP is transported over User Datagram Protocol UDP/IP. All NTP communications use UTC. An NTP server receives its time from a reference time source, such as a radio clock or atomic clock, attached to the time. NTP distributes this time across the network.

In a large enterprise network, having one time standard for all network devices is critical for management reporting and event logging functions when trying to correlate interacting events logged across multiple devices. Many enterprise customers with extremely mission-critical networks maintain their own stratum-1 NTP source.

Time synchronization happens when several frames are exchanged between clients and servers. The switches in client mode know the address of one or more NTP servers. The servers act as the time source and receive client synchronization requests.

By configuring an IP address as a peer, the switch will obtain and provide time as required. The peer is capable of providing time on its own and is capable of having a server configured. If both these instances point to different time servers, your NTP service is more reliable. Thus, even if the active server link is lost, you can still maintain the right time due to the presence of the peer.



### Tip

If an active server fails, a configured peer helps in providing the NTP time. Provide a direct NTP server association and configure a peer to ensure backup support if the active server fails.

If you only configure a peer, the most accurate peer takes on the role of the NTP server and the other peer(s) act as a peer(s). Both machines end at the right time if they have the right time source or if they point to the right NTP source.

## Configuring NTP

To configure NTP in a server association, follow these steps:

	Command	Purpose
Step 1	switch# <b>confi g t</b>	Enters configuration mode.
Step 2	switch(config)# <b>ntp server 10.10.10.10</b> switch(config)#	Forms a server association with a server.
Step 3	switch(config)# <b>ntp peer 10.20.10.0</b> switch(config)#	Forms a peer association with a peer. You can specify multiple associations.
Step 4	switch(config)# <b>exit</b> switch#	Returns to EXEC mode.
Step 5	switch# <b>copy running-config startup-config</b>	Saves your configuration changes to NVRAM.  <b>Tip</b> This is one instance where you can save the configuration as a result of an NTP configuration change. You can issue this command at any time.
Step 6	switch# <b>show ntp peers</b>  ----- Peer IP Address                      Serv/Peer ----- 10.20.10.2                              Server 10.20.10.0                              Peer	Displays the configured server and peer associations.  <b>Note</b> A domain name is resolved only when you have a DNS server configured.

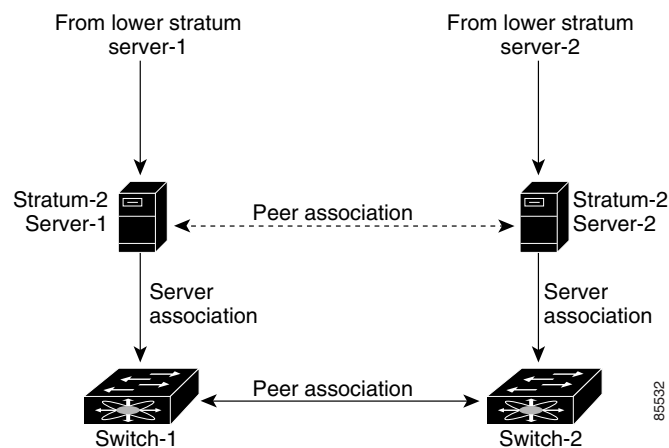
## NTP Configuration Guidelines

The following guidelines apply to all NTP configurations:

- You should have a peer association with another switch only when you are sure that your clock is reliable (which means that you are a client of a reliable NTP server).
- A peer configured alone takes on the role of a server and should be used as backup. If you have two servers, then you can have several switches point to one server, and the remaining switches to the other server. Then you would configure peer association between these two sets. This forces the clock to be more reliable.
- If you only have one server, it's better for all the switches to have a client association with that server.

Not even a server down time will affect well-configured switches in the network. [Figure 4-3](#) displays a network with two NTP stratum 2 servers and two switches.

**Figure 4-3 NTP Peer and Server Association**



In this configuration, the switches were configured as follows:

- Stratum 2 Server 1
  - IP address -10.10.10.10
  - Stratum-2 Server-2
  - IP address -10.10.10.9
- Switch 1
  - Switch IP address -10.10.10.1
- NTP configuration
  - NTP server 10.10.10.10
  - NTP peer 10.10.10.2
- Switch 2
  - Switch IP address -10.10.10.2
  - NTP configuration
  - NTP server 10.10.10.9
  - NTP peer 10.10.10.1

# Management Interface Configuration

On director class switches, a single IP address is used to manage the switch. The active supervisor module's management (mgmt0) interface uses this IP address. The mgmt0 interface on the standby supervisor module remains in an inactive state and cannot be accessed until a switchover happens. After a switchover, the mgmt0 interface on the standby supervisor module becomes active and assumes the same IP address as the previously active supervisor module.

The management interface on the switch allows multiple simultaneous Telnet or SNMP sessions. You can remotely configure the switch through the management interface, but first you must configure some IP parameters (IP address, subnet mask) so that the switch is reachable. You can manually configure the management interface from the CLI.

The management port (mgmt0) is autosensing and operates in full duplex mode at a speed of 10/100 Mbps. The speed and mode cannot be configured.



## Note

Before you begin to configure the management interface manually, obtain the switch's IP address and IP subnet mask. Also make sure the console cable is connected to the console port.

## Obtaining Remote Management Access

In some cases, a switch interface might be administratively shut down. You can check the status of an interface at any time by using the **show interface mgmt 0** command.

To obtain remote management access, follow these steps:

	Command	Command
Step 1	switch# <b>config terminal</b> switch(config)#	Enters configuration mode. You can also abbreviate the command to <b>config t</b> .
Step 2	switch(config)# <b>interface mgmt 0</b>	Enters the interface configuration mode on the specified interface (mgmt0).  You can use the management Ethernet interface on the switch to configure the management interface.
Step 3	switch(config)# <b>ip address 1.1.1.0 255.255.255.0</b>	Enters the IP address and IP subnet mask for the interface specified in Step 2.
Step 4	switch(config-if)# <b>no shutdown</b>	Enables the interface.
Step 5	switch(config-if)# <b>exit</b>	Returns to configuration mode.
Step 6	switch(config)# <b>ip default-gateway 1.1.1.1</b>	Configures the default gateway address.

## Using the force Option

When you try to shut down a management interface (mgmt0), a follow-up message confirms your action before performing the operation. You can use the **force** option to bypass this confirmation. The following example shuts down the interface without using the **force** option:

```
switch# config t
switch(config)# interface mgmt 0
switch(config-if)# shutdown
Shutting down this interface will drop all telnet sessions.
```

Do you wish to continue (y/n)? **y**

The following example shuts down the interface using the **force** option:

```
switch# config t
switch(config)# interface mgmt 0
switch(config-if)# shutdown force
```



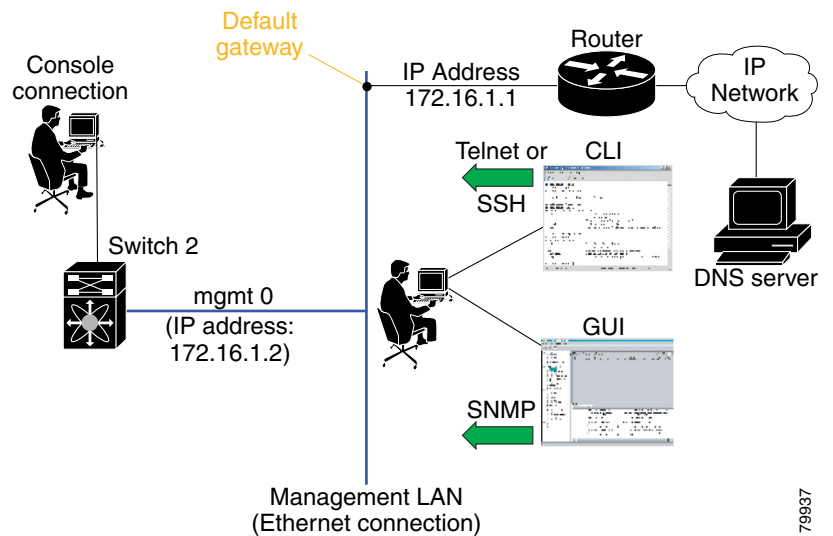
**Note**

You need to explicitly configure a default gateway to connect to the switch and send IP packets or add a route for each subnet.

## Default Gateway Configuration

The supervisor module sends IP packets with unresolved destination IP addresses to the default gateway (see [Figure 4-4](#)).

**Figure 4-4** Default Gateway



79937

## Configuring the Default Gateway

To configure the IP address of the default gateway, follow these steps:

	Command	Purpose
Step 1	switch# <b>config t</b>	Enters configuration mode.
Step 2	switch(config)# <b>ip default-gateway 172.16.1.1</b>	Configures the 172.16.1.1 IP address.

## Telnet Server Connection

The Telnet server is enabled by default on all switches in the Cisco MDS 9000 Family. If you require a secure SSH connection, you need to disable the default Telnet connection and then enable the SSH connection (see the “[Enabling SSH Service](#)” section on page 16-27).



### Note

For information on connecting a terminal to the supervisor module console port, refer to the *Cisco MDS 9200 Series Hardware Installation Guide* or the *Cisco MDS 9500 Series Hardware Installation Guide*.



### Tip

A maximum of 16 sessions are allowed in any Cisco MDS 9216 Switch or in any switch in the Cisco MDS 9500 Series.

Make sure the terminal is connected to the switch and that the switch and terminal are both powered on.

## Disabling a Telnet Connection

To disable Telnet connections to the switch, follow these steps:

	Command	Purpose
Step 1	switch# <b>config t</b>	Enters configuration mode.
Step 2	switch(config)# <b>no telnet server enable</b> updated	Disables the Telnet server.
	switch(config)# <b>telnet server enable</b> updated	Enables the Telnet server to return a Telnet connection from a secure SSH connection.

# Working with Configuration Files

Configuration files can contain some or all of the commands needed to configure one or more switches. For example, you might want to download the same configuration file to several switches that have the same hardware configuration so that they have identical module and port configurations.

This section describes how to work with configuration files and has the following topics:

- [Displaying Configuration Files, page 4-23](#)
- [Downloading Configuration Files to the Switch, page 4-23](#)
- [Saving the Configuration, page 4-26](#)
- [Copying Files, page 4-26](#)
- [Backing Up the Current Configuration, page 4-27](#)
- [Rolling Back to a Previous Configuration, page 4-27](#)

## Displaying Configuration Files

Use the **show running-config** command to view the running configuration file.

```
switch# show running-config
Building Configuration ...
 interface port-channel 98
interface fc1/1
 interface fc1/2
interface mgmt0
ip address 172.22.95.112 255.255.255.0
no shutdown
vsan database
vsan 2
clock summer-time Pacific 1 Sun Apr 02:00 5 Sun Oct 02:00 60
switchname switch112
```

Use the **show startup-config** command to view the startup configuration file.

```
switch# show startup-config
 interface port-channel 98
 interface fc1/1
channel-group 98 force
no shutdown
 interface mgmt0
ip address 172.22.95.112 255.255.255.0
boot system system-237; ep-41
boot kickstart boot-237 ep-41
ip domain-name cisco.com
```

## Downloading Configuration Files to the Switch

You can configure a switch in the Cisco MDS 9000 Family by using configuration files you create or download from another switch. In addition, you can store configuration files on a bootflash device on the supervisor module and you can configure the switch using a configuration stored on an external CompactFlash disk.

Before you begin downloading a configuration file using a remote server, do the following:

- Ensure the configuration file to be downloaded is in the correct directory on the remote server.

- Ensure that the permissions on the file are set correctly. Permissions on the file should be set to world-read.
- Ensure the switch has a route to the remote server. The switch and the remote server must be in the same subnetwork if you do not have a router or default gateway to route traffic between subnets. Check connectivity to the remote server using the **ping** command.

## From a Remote Server

To configure a switch in the Cisco MDS 9000 Family using a configuration file downloaded from a remote server using TFTP, FTP, SCP, or SFTP, follow these steps:

- 
- Step 1** Log into the switch through the console port or through a Telnet or SSH session.
- Step 2** Configure the switch using the configuration file downloaded from the remote server using the **copy <scheme> :// <server address> system:running-config** command, where *scheme* is TFTP, FTP, SCP, or SFTP.

The configuration file downloads and the commands are executed as the file is parsed line by line.

---

Use the following command to download a configuration file from a remote server to the running configuration.

```
switch# copy <scheme>://<url> system:running-config
```

## From an External Flash (slot0:)



### Note

The physical media must be inserted into slot0: after you log into the switch.

---

To configure a switch in the Cisco MDS 9000 Family using a configuration file stored on an external CompactFlash disk, follow these steps:

- 
- Step 1** Log into the switch through the console port or through a Telnet or SSH session.
- Step 2** Locate the configuration file using the **cd** and **dir** commands. (See the [“Copying Files” section on page 4-26.](#))
- Step 3** Configure the switch using the configuration file stored on the external CompactFlash disk using the **copy <source file> system:running-config** command.

The commands are executed as the file is parsed line by line.

---

Use the following command to download a configuration file from an external CompactFlash to the running configuration:

```
switch copy slot0:dns-config.cfg system:running-config
```



## To a Remote Server

To save a configuration file to a remote server such as TFTP, FTP, SCP, or SFTP, follow these steps:

- 
- Step 1** Log into the switch through the console port or through a Telnet or SSH session.
  - Step 2** Save the configuration using the **copy system:running-config <scheme> :// <url>** command, where *scheme* is TFTP, FTP, SCP, or SFTP.
  - Step 3** Specify the IP address or host name of the remote server and the name of the file to download.  
The configuration file is saved to the remote server.
- 

Use the following command to save a running configuration file to a remote server:

```
switch# copy system:running-config <scheme>://<url>
```

Use the following command to save a startup configuration file to a remote server:

```
switch# copy nvram:startup-config <scheme>://<url>
```

## To an External CompactFlash Disk

To save a configuration file on an external CompactFlash disk, follow these steps:

- 
- Step 1** Log into the switch through the console port or through a Telnet session.
  - Step 2** Locate the configuration file using the **cd** and **dir** commands. (See the “Copying Files” section on [page 4-26](#).)
  - Step 3** Save the configuration file using the **copy system:running-config <destination file>** command.  
The configuration file is saved to the CompactFlash disk.
- 

Use the following command to save a running configuration file to an external CompactFlash disk:

```
switch# copy system:running-config slot0:dns-config.cfg
```

Use the following command to save a startup configuration file to an external CompactFlash disk:

```
switch# copy nvram:startup-config slot0:dns-config.cfg
```

## Saving the Configuration

After you have created a configuration, you save the configuration using the following **copy** command:

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

The **copy running-config startup-config** command is an alias to the previous command and is used frequently throughout this guide.

## Copying Files

The syntax for the **copy** command follows and is explained in [Table 4-1](#).

```
switch# copy <scheme>://<username@><server>/<file name>
<scheme>://<username@><server>/<file name>
```

**Table 4-1** copy Command Syntax

Scheme	Server	File Name
bootflash	sup-active sup-standby sup-1 or module-5 sup-2 or module-6 sup-local sup-remote	User-specified
slot0	—	User-specified
volatile	—	User-specified
nvram	—	startup-config or snapshot-config
system	—	running-config
tftp <sup>1</sup>	IP address or DNS name	User-specified
ftp		
scp (secure copy)		
sftp		
core	slot-number	Process identifier number

1. When downloading and uploading files, a TFTP limitation restricts a TFTP client to a 32 MB file size and some TFTP servers to a 16 MB file size.

- This example shows how to copy a file from the active supervisor module's (sup-1 in slot 5) bootflash to the standby supervisor module's (sup-2 in slot 6) bootflash.

```
switch# copy bootflash:system_image bootflash://sup-2/system_image
```

- This example shows how to overwrite the contents of an existing configuration in NVRAM.

```
switch# copy nvram:snapshot-config nvram:startup-config
```

```
Warning: this command is going to overwrite your current startup-config.
Do you wish to continue? {y/n} [y] y
```

- This example shows how to copy a running configuration to the bootflash: directory.  
switch# `copy system:running-config bootflash:my-config`
- This example shows how to copy a system image file from the SCP server to bootflash.  
switch# `copy scp://user@10.1.7.2/system-image bootflash:system-image`
- This example shows how to copy a script file from the SFTP server to the volatile: directory.  
switch# `copy sftp://172.16.10.100/myscript.txt volatile:myscript.txt`

**Note**

Use the `show version image` command to verify if the downloaded images are valid.

## Backing Up the Current Configuration

Before installing or migrating to any software configuration, back up the startup configuration.

- This example shows how to create a snapshot of the startup configuration in a predefined location on the switch (binary file).  
switch# `copy nvram:startup-config nvram:snapshot-config`
- This example shows how to back up the startup configuration copy in the bootflash: file system (ASCII file).  
switch# `copy nvram:startup-config bootflash:my-config`
- This example shows how to back up the startup configuration to the TFTP server (ASCII file).  
switch# `copy nvram:startup-config tftp://172.16.10.100/my-config`
- This example shows how to back up the running configuration to the bootflash: file system (ASCII file).  
switch# `copy system:running-config bootflash:my-config`

## Rolling Back to a Previous Configuration

All switch configurations reside in the internal bootflash: file system. If your internal bootflash: file system is corrupted, you could potentially lose your configuration. Save and back up your configuration file periodically.

- This example shows how to roll back to a snapshot copy of a previously saved running configuration (binary file).  
switch# `copy nvram:snapshot-config nvram:startup-config`

**Note**

You can issue a rollback command only when a snapshot is already created. Otherwise, you will receive the `No snapshot-config found` error message.

- This example shows how to roll back to a configuration copy that was previously saved in the bootflash: file system (ASCII file).  
switch# `copy bootflash:my-config nvram:startup-config`

**Note**

Each time a **copy running-config startup-config** command is issued, a binary file is created and the ASCII file is updated. A valid binary configuration file reduces the overall boot time significantly. A binary file cannot be uploaded, but its contents can be used to overwrite the existing startup configuration. The **write erase** command clears the binary file.

## Restoring the Configured Redundancy Mode

**Tip**

If you configure the **combined** mode as the redundancy mode for power supplies on a Cisco MDS 9509 switch, exert care when using the **write erase** and **reload** command sequence before rolling back to a saved configuration.

By issuing the **write erase** command and the **reload** command, you restore the switch settings to their factory defaults. This sequence also restores the redundancy mode setting for the power supplies back to the **redundant** mode (default).

Depending on the type of power supply, the input voltage, and the number of modules (line cards) in the chassis, the redundancy mode may prevent the line cards from being powered on after a system reboot (see the “[Configuring Power Supplies](#)” section on page 8-6). If you use this sequence, the commands that apply to the powered down line cards will not be enforced on the switch (and will not be part of its running configuration).

If using the **write erase** and **reload** command sequence before rolling back to a saved configuration, follow these steps:

- 
- Step 1** Manually change (if originally configured) the **redundant** mode configuration to **combined** mode.
  - Step 2** Wait until all modules are back online—the module status displays `ok` in response to the **show module** command.
  - Step 3** Roll back to the saved configuration (see the “[Rolling Back to a Previous Configuration](#)” section on page 4-27).
- 

## Downgrading from a Higher Release

Use the **install all** command to gracefully reload the switch and handle configuration conversions. When downgrading any switch in the Cisco MDS 9000 Family, avoid using the **reload** command.

For example, to revert to Cisco MDS SAN-OS Release 1.0(4) or 1.0(3a) from Release 1.x, follow these steps:

- 
- Step 1** Save the configuration using the **copy running-config startup-config** command.
  - Step 2** Issue the **install all** command to downgrade the software (see the “[Performing an Automated Upgrade](#)” section on page 6-5).
-

# Accessing Remote File Systems

To access contents of the standby supervisor module (remote), follow these steps:

**Step 1** Verify if the standby supervisor module has sufficient space for new image files.

```
switch# dir bootflash://sup-remote
12198912   Aug 27 17:21:10 2003  bootflash:boot-39a
12198912   Aug 27 16:29:18 2003  bootflash:m9500-sflek9-kickstart-mzg.1.3.0.39a.bin
1921922    Sep 14 19:58:12 2003  aOldImage
1864931    Apr 29 12:41:50 2003  bOldImage
1864931    Apr 29 12:41:59 2003  dplug2
  12288    Apr 18 20:23:11 2003  lost+found/
12097024   Nov 21 16:34:18 2003  m9500-sflek9-kickstart-mz.1.3.1.1.bin
41574014   Nov 21 16:34:47 2003  m9500-sflek9-mz.1.3.1.1.bin
  1024     Oct 28 20:24:59 2003  newer-fs/
2021518    Oct 11 15:49:41 2003  plugin-69a

Usage for bootflash://sup-remote
102081536 bytes used
82478080 bytes free
184559616 bytes total
```

**Step 2** Delete files, if required, to make more space for the new image files.

```
switch# del aOldImage
```

## Deleting Files

Assuming you are already in the bootflash: directory, use the **delete** command as follows:

- This example shows how to delete a file from the bootflash: directory.  

```
switch# delete dns_config.cfg
```
- This example shows how to delete a file from an external CompactFlash (slot0).  

```
switch# delete slot0:dns_config.cfg
```
- This example shows how to delete the file named test from the Flash card inserted in slot 0.  

```
switch# delete slot0:test
Delete slot0:test? [confirm]
```
- This example shows how to delete the entire my-dir directory and all its contents.  

```
switch# delete bootflash:my-dir
```

# Configuring Console Settings

A console port is an asynchronous serial port that enables switches in the Cisco MDS 9000 Family to be set up for initial configuration through a standard RS-232 port with an RJ-45 connector. Any device connected to this port must be capable of asynchronous transmission. Connection to a terminal requires a terminal emulator to be configured as 9600 baud, 8 data bits, 1 stop bit, no parity.



## Caution

The console baud rate automatically reverts to the default rate (9600) after any BIOS upgrade.

To configure the console port parameters from the console terminal, follow these steps:

	Command	Command
Step 1	switch# <b>config terminal</b> switch(config)#	Enters configuration mode.
Step 2	switch(config)# <b>line console</b> switch(config-console)#	Enters the line console configuration mode.
Step 3	switch(config-console)# <b>speed</b> <b>9600</b>	Configures the port speed for the serial console. The default console baud rate is 9600 baud. The valid range is between 110 and 115,200 bps (110, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, 28800, 38400, 57600, 115200). Be sure to specify one of these exact values.
Step 4	switch(config-console)# <b>databits 8</b>	Configures the data bits for the console connection. The default is 8 data bits and the valid range is between 5 and 8 data bits.
Step 5	switch(config-console)# <b>stopbits 1</b>	Configures the stop bits for the console connection. The default is 1 stop bit and the valid values are 1 or 2 stop bits.
Step 6	switch(config-console)# <b>parity</b> <b>none</b>	Configures the parity for the console connection. The default is no parity and the valid values are even or odd parity.

## Verifying the Console Configuration

Use the **show line console** command to verify the configured console settings. This command also displays problems that may have occurred along with the other registration statistics.

```
switch# show line console
line Console:
  Speed:          9600 bauds
  Databits:       8 bits per byte
  Stopbits:       1 bit(s)
  Parity:         none
  Modem In:       Enable
  Modem Init-String -
    default : ATE0Q1&D2&C1S0=1\015
  Statistics:     tx:12842    rx:366    Register Bits:RTS|CTS|DTR|DSR|CD|RI
```

## Configuring COM1 Settings

A COM1 port is a RS-232 port with a DB-9 interface that enables you to connect to an external serial communication device such as a modem. Connection to a terminal requires the terminal emulator to be configured as 9600 baud, 8 data bits, 1 stop bit, no parity.

To configure the COM1 port parameters, follow these steps:

	Command	Command
Step 1	switch# <b>config terminal</b> switch(config)#	Enters configuration mode.
Step 2	switch(config)# <b>line com1</b> switch(config-com1)#	Enters the COM1 port configuration mode.
Step 3	switch(config-com1)# <b>speed 9600</b>	Configures the port speed for the COM1 connection. The default console baud rate is 9600 baud. The valid range is between 110 and 115,200 bps (110, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, 28800, 38400, 57600, 115200). Be sure to specify one of these exact values.  <b>Note</b> This configuration depends on the incoming speed of the modem connected to COM1.
Step 4	switch(config-com1)# <b>databits 8</b>	Configures the data bits for the COM1 connection. The default is 8 data bits and the valid range is between 5 and 8 data bits.
Step 5	switch(config-com1)# <b>stopbits 1</b>	Configures the stop bits for the COM1 connection. The default is 1 stop bits and the valid values are 1 or 2 stop bits.
Step 6	switch(config-com1)# <b>parity none</b>	Configures the parity for the COM1 connection. The default is no parity and the valid values are even or odd parity.
Step 7	switch(config-com1)# <b>no flowcontrol hardware</b>	Disables hardware flow control. By default, hardware flow control is enabled on all switches in the Cisco 9000 Family. When enabled, this option is useful in protecting data loss at higher baud rates.  <b>Note</b> This option is only available through the COM1 port.

## Verifying the COM1 Configuration

Use the **show line com1** command to verify the configured COM1 settings. This command also displays problems that may have occurred along with the other registration statistics.

```
switch# show line com1
line Aux:
  Speed:          9600 bauds
  Databits:       8 bits per byte
  Stopbits:       1 bit(s)
  Parity:         none
  Modem In:       Enable
  Modem Init-String -
    default : ATE0Q1&D2&C1S0=1\015
  Statistics:     tx:17      rx:0      Register Bits:RTS|DTR
```

# Configuring Modem Connections

Modems can only be configured if you are connected to the console or COM1 ports. A modem connection to a switch in the Cisco MDS 9000 Family does not affect switch functionality.



## Note

If you plan on connecting a modem to the console port or the COM1 port of a switch in the Cisco MDS 9000 Family, refer to the *Cisco MDS 9216 Switch Hardware Installation Guide* or the *Cisco MDS 9500 Series Hardware Installation Guide*. COM1 ports are not available on switches in the Cisco MDS 9100 Series. Refer to the *Cisco MDS 9100 Series Hardware Installation Guide*.

## Guidelines to Configure Modems



## Tip

We recommend you use the COM1 port to connect the modem from a Cisco MDS 9216 switch or from any director in the Cisco MDS 9500 Family.

The following guidelines apply to modem configurations:

- The following Cisco modems were tested to work in the Cisco SAN-OS environment:
  - MultiTech MT2834BA (<http://www.multitech.com/PRODUCTS/Families/MultiModemII/>)
  - Hayes Accura V.92 (<http://www.hayesmicro.com/Products/accura-prod-v92.htm>)
- Connect the modem before attempting to configure the modem.
- Do not connect a modem to the console port while the system is booting.

Follow the procedure specified in the “[Initializing a Modem in a Powered on Switch](#)” section on [page 4-35](#).

## Enabling Modem Connections

To configure a modem connection through the COM1 port, follow these steps:

	Command	Command
Step 1	switch# <b>config t</b> switch(config)#	Enters configuration mode.
Step 2	switch(config)# <b>line com1</b> switch(config-com1)#	Enters the COM1 port configuration mode.
Step 3	switch(config-com1)# <b>modem in</b>	Enables the COM1 port to only connect to a modem.
	switch(config-com1)# <b>no modem in</b>	Disables (default) the current modem from executing its functions.



To configure a modem connection through the console port, follow these steps:

	Command	Command
Step 1	switch# <b>confi g t</b> switch(config)#	Enters configuration mode.
Step 2	switch(config)# <b>line console</b> switch(config-console)#	Enters the console port configuration mode.
Step 3	switch(config-console)# <b>modem in</b>	Enables the console port to only connect to a modem.
	switch(config-console)# <b>no modem in</b>	Disables (default) the current modem from executing its functions.

## Configuring the Initialization String

Switches in the Cisco MDS 9500 Family and the Cisco MDS 9216 switch have a default initialization string (`ATE0Q1&D2&C1S0=1\015`) to detect connected modems. The default string detects connected modems supported by Cisco Systems. The default string contents are as follows:

- AT—Attention
- E0 (required)—No echo
- Q1—Result code on
- &D2—Normal data terminal ready (DTR) option
- &C1—Enable tracking the state of the data carrier.
- S0=1—Pick up after one ring
- \015 (required)—carriage return in octal

You may retain the default string or change it to another string (80 character limit) using the **user-input** option. This option is provided if you prefer to use a modem that is not supported or tested by Cisco systems. If you change the string, the changes you make are permanent and remain in effect unless you change them again. Rebooting the system or restarting the CLI does not change the modem initialization string. The switch is not affected even if the modem is not functioning.



### Tip

We recommend you use the default initialization string. If the required options are not provided in the user-input string, the initialization string is not processed.

The modem initialization string usage depends on the modem state when the switch boots:

- If the modem is already attached to the switch during boot-up, the default initialization string is written to the modem (see the [“Configuring the Default Initialization String”](#) section on page 4-34).
- If the modem is not attached to the switch during boot-up, then attach the modem as outlined in the *Cisco MDS 9000 Family Hardware Installation Guide* (depending on the product), and follow the procedure provided in this section (see the [“Configuring a User-Specified Initialization String”](#) section on page 4-34).



### Note

You can perform the configuration specified in this section only if you are connected to the console port or the COM1 port.

## Configuring the Default Initialization String

To configure the default initialization string through the COM1 port, follow these steps:

	Command	Command
Step 1	switch# <b>config t</b> switch(config)#	Enters configuration mode.
Step 2	switch(config)# <b>line com1</b> switch(config-com1)#	Enters the COM1 port configuration mode.
Step 3	switch(config-com1)# <b>modem init-string default</b>	Writes the default initialization string to the modem.

To configure the default initialization string through the console port, follow these steps:

	Command	Command
Step 1	switch# <b>config t</b> switch(config)#	Enters configuration mode.
Step 2	switch(config)# <b>line com1</b> switch(config-console)#	Enters the console port configuration mode.
Step 3	switch(config-console)# <b>modem init-string default</b>	Writes the default initialization string to the modem.

## Configuring a User-Specified Initialization String

To configure a user-specified initialization string through the COM1 port, follow these steps:

	Command	Command
Step 1	switch# <b>config terminal</b> switch(config)#	Enters configuration mode.
Step 2	switch(config)# <b>line com1</b> switch(config-com1)#	Enters the COM1 port configuration mode.
Step 3	switch(config-com1)# <b>modem set-string user-input ATE0Q1&amp;D2&amp;C1S0=3\015</b>	Assigns the user-specified initialization string to its corresponding profile.
		<b>Note</b> You must first set the user-input string, before initializing the string.
	switch(config-com1)# <b>no modem set-string</b>	Reverts the configured initialization string to the factory default string.
Step 4	switch(config-com1)# <b>modem init-string user-input</b>	Writes the user-specified initialization string to the modem.

To configure a user-specified initialization string through the console port, follow these steps:

	Command	Command
Step 1	switch# <b>config terminal</b> switch(config)#	Enters configuration mode.
Step 2	switch(config)# <b>line com1</b> switch(config-console)#	Enters the console port configuration mode.

	Command	Command
Step 3	switch(config-console)# <b>modem set-string user-input ATE0Q1&amp;D2&amp;C1S0=3\015</b>	Assigns the user-specified initialization string to its corresponding profile.  <b>Note</b> You must first set the user-input string, before initializing the string.
	switch(config-console)# <b>no modem set-string</b>	Reverts the configured initialization string to the factory default string.
Step 4	switch(config-console)# <b>modem init-string user-input</b>	Writes the user-specified initialization string to the modem.

## Initializing a Modem in a Powered on Switch

When a switch is already powered on and the modem is later connected to either the console port or the COM1 port, you can initialize the modem using the **modem connect line** command in EXEC mode. You can specify the **com1** option if the modem is connected to the COM1 port, or the **console** option if the modem is connected to the console.

To connect a modem to a switch that is already powered on, follow these steps.

- 
- Step 1** Wait until the system has completed the boot sequence and the system image is running.
  - Step 2** Connect the modem to the switch as specified in the *Cisco MDS 9216 Switch Hardware Guide* or the *Cisco MDS 9500 Series Hardware Installation Guide*.
  - Step 3** Initialize the modem using the **modem connect line** command in EXEC mode.
- 

## Verifying the Modem Configuration

Use the **show line** command to verify the configured modem settings.

```
switch# show line
line Console:
  Speed:          9600 bauds
  Databits:       8 bits per byte
  Stopbits:       1 bit(s)
  Parity:         none
  Modem In:       Enable
  Modem Init-String -
    default : ATE0Q1&D2&C1S0=1\015
  Statistics:     tx:12842    rx:366    Register Bits:RTS|CTS|DTR|DSR|CD|RI
line Aux:
  Speed:          9600 bauds
  Databits:       8 bits per byte
  Stopbits:       1 bit(s)
  Parity:         none
  Modem In:       Enable
  Modem Init-String -
    default : ATE0Q1&D2&C1S0=1\015
  Statistics:     tx:17      rx:0      Register Bits:RTS|DTR
```

# CDP Configuration

The Cisco Discovery Protocol (CDP) is an advertisement protocol used by Cisco devices to advertise itself to other Cisco devices in the same network. CDP runs on the data link layer and is independent of Layer 3 protocols. Cisco devices that receive the CDP packets cache the information to make it accessible through the CLI and SNMP.

CDP is supported on the management Ethernet interface on the supervisor module and the Gigabit Ethernet interface on the IPS module. The CDP daemon is restartable and switchable. The running and startup configurations are available across restarts and switchovers.

CDP version 1 (v1) and version 2 (v2) are supported in Cisco MDS 9000 Family switches. CDP packets with any other version number are silently discarded when received.

When the interface link is established, CDP is enabled by default and three CDP packets are sent at one-second intervals. Following this, the CDP frames are sent at the globally-configured refresh interval.

## Configuring the CDP

To globally disable the CDP, follow these steps:

	Command	Command
Step 1	switch# <b>config terminal</b> switch(config)#	Enters configuration mode.
Step 2	switch(config)# <b>no cdp enable</b> Operation in progress. Please check global parameters switch(config-console)#	Disables the CDP protocol on the switch. When CDP is disabled on an interface, one packet is sent to clear out the switch state with each of the receiving devices.
	switch(config)# <b>cdp enable</b> Operation in progress. Please check global parameters switch(config)#	Enables (default) the CDP protocol on the switch. When CDP is enabled on an interface, one packet is sent immediately. Subsequent packets are sent at the configured refresh time.

To disable the CDP protocol on a specific interface, follow these steps:

	Command	Command
Step 1	switch# <b>config terminal</b> switch(config)#	Enters configuration mode.
Step 2	switch(config)# <b>interface gigbitethernet 8/8</b> switch(config-if)#	Configures the Gigabit Ethernet interface for the module in slot 8 port 8.
Step 3	switch(config-if)# <b>no cdp enable</b> Operation in progress. Please check interface parameters switch(config-console)#	Disables the CDP protocol on the selected interface. When CDP is disabled on an interface, one packet is sent to clear out the switch state with each of the receiving devices.
	switch(config-if)# <b>cdp enable</b> Operation in progress. Please check interface parameters switch(config)#	Enables (default) the CDP protocol on the selected interface. When CDP is enabled on an interface, one packet is sent immediately. Subsequent packets are sent at the configured refresh time.

To globally configure the refresh time interval for the CDP protocol, follow these steps:

	Command	Command
Step 1	switch# <b>config terminal</b> switch(config)#	Enters configuration mode.
Step 2	switch(config)# <b>cdp timer 100</b> switch(config)#	Sets the refresh time interval in seconds. The default is 60 seconds and the valid range is from 5 to 255 seconds.
	switch(config)# <b>no cdp timer 100</b> switch(config)#	Reverts the refresh time interval to the factory default of 60 seconds.

To globally configure the hold time advertised in CDP packets, follow these steps:

	Command	Command
Step 1	switch# <b>config terminal</b> switch(config)#	Enters configuration mode.
Step 2	switch(config)# <b>cdp holdtime 200</b> switch(config)#	Sets the hold time advertised in CDP packets in seconds. The default is 180 seconds and the valid range is from 10 to 255 seconds.
	switch(config)# <b>no cdp holdtime 200</b> switch(config)#	Reverts the hold time to the factory default of 180 seconds.

To globally configure the CDP version, follow these steps:

	Command	Command
Step 1	switch# <b>config terminal</b> switch(config)#	Enters configuration mode.
Step 2	switch(config)# <b>cdp advertise v1</b> switch(config)#	Sets the CDP version to be used. The default is version 2 (v2). The valid options are v1 and v2.
	switch(config)# <b>no advertise v1</b> switch(config)#	Reverts the version to the factory default of v2.

## Clearing CDP Configurations

Use the **clear cdp counters** command to clear CDP traffic counters for all interfaces. You can issue this command for a specified interface or for all interfaces (management and Gigabit Ethernet interfaces).

```
switch# clear cdp counters
switch#
```

Use the **clear cdp table** command to clear neighboring CDP entries for all interfaces. You can issue this command for a specified interface or for all interfaces (management and Gigabit Ethernet interfaces).

```
switch# clear cdp table interface gigabitethernet 4/1
switch#
```

## Displaying CDP Protocol Settings

Use the **show cdp** command to display CDP entries. See Examples 4-1 to 4-11.

### Example 4-1 Displays All CDP Capable Interfaces and Parameters

```
switch# show cdp all
GigabitEthernet4/1 is up
  CDP enabled on interface
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet4/8 is down
  CDP enabled on interface
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
mgmt0 is up
  CDP enabled on interface
  Sending CDP packets every 100 seconds
  Holdtime is 200 seconds
```

### Example 4-2 Displays All CDP Neighbor Entries

```
switch# show cdp entry all
-----
Device ID:069038747(Kiowa3)
Entry address(es):
  IP Address: 172.22.92.5
Platform: WS-C5500, Capabilities: Trans-Bridge Switch
Interface: mgmt0, Port ID (outgoing port): 5/22
Holdtime: 136 sec

Version:
WS-C5500 Software, Version McpSW: 2.4(3) NmpSW: 2.4(3)
Copyright (c) 1995-1997 by Cisco Systems

Advertisement Version: 1
```

### Example 4-3 Displays the Specified CDP Neighbor

```
switch# show cdp entry name 0
-----
Device ID:0
Entry address(es):
  IP Address: 0.0.0.0
Platform: DS-X9530-SF1-K9, Capabilities: Host
Interface: GigabitEthernet4/1, Port ID (outgoing port): GigabitEthernet4/1
Holdtime: 144 sec

Version:
1.1(0.144)

Advertisement Version: 2
Duplex: full
```

**Example 4-4 Displays Global CDP Parameters**

```
switch# show cdp global
Global CDP information:
  CDP enabled globally
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
```

**Example 4-5 Displays CDP Parameters for the Management Interface**

```
switch# show cdp interface mgmt 0
mgmt0 is up
  CDP enabled on interface
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

**Example 4-6 Displays CDP Parameters for the Gigabit Ethernet Interface**

```
switch# show cdp interface gigabitethernet 4/1
GigabitEthernet4/1 is up
  CDP enabled on interface
  Sending CDP packets every 80 seconds
  Holdtime is 200 seconds
```

**Example 4-7 Displays CDP Neighbors (in brief)**

```
switch# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID          Local Intrfce  Hldtme  Capability  Platform          Port ID
0                  Gig4/1         135     H           DS-X9530-SF1-    Gig4/1
069038732(Kiowa2  mgmt0         132     T S         WS-C5500          8/11
069038747(Kiowa3  mgmt0         156     T S         WS-C5500          6/20
069038747(Kiowa3  mgmt0         158     T S         WS-C5500          5/22
```

**Example 4-8 Displays CDP Neighbors (in detail)**

```
switch# show CDP neighbor detail
-----
Device ID:0
Entry address(es):
  IP Address: 0.0.0.0
Platform: DS-X9530-SF1-K9, Capabilities: Host
Interface: GigabitEthernet4/1, Port ID (outgoing port): GigabitEthernet4/1
Holdtime: 162 sec

Version:
1.1(0.144)

Advertisement Version: 2
Duplex: full
-----
Device ID:069038732(Kiowa2)
Entry address(es):
  IP Address: 172.22.91.5
Platform: WS-C5500, Capabilities: Trans-Bridge Switch
Interface: mgmt0, Port ID (outgoing port): 8/11
Holdtime: 132 sec
```

```
Version:
WS-C5500 Software, Version McpSW: 2.4(3) NmpSW: 2.4(3)
Copyright (c) 1995-1997 by Cisco Systems
Advertisement Version: 1
```

**Example 4-9 Displays the Specified CDP Neighbor (in detail)**

```
switch# show cdp neighbors interface gigabitethernet 4/1 detail
-----
Device ID:0
Entry address(es):
  IP Address: 0.0.0.0
Platform: DS-X9530-SF1-K9, Capabilities: Host
Interface: GigabitEthernet4/1, Port ID (outgoing port): GigabitEthernet4/1
Holdtime: 144 sec

Version:
1.1(0.144)

Advertisement Version: 2
Duplex: full
```

**Example 4-10 Displays CDP Traffic Statistics for the Management Interface**

```
switch# show cdp traffic interface mgmt 0
-----
Traffic statistics for mgmt0
Input Statistics:
  Total Packets: 1148
  Valid CDP Packets: 1148
    CDP v1 Packets: 1148
    CDP v2 Packets: 0
  Invalid CDP Packets: 0
    Unsupported Version: 0
    Checksum Errors: 0
    Malformed Packets: 0
Output Statistics:
  Total Packets: 2329
    CDP v1 Packets: 1164
    CDP v2 Packets: 1165
  Send Errors: 0
```

**Example 4-11 Displays CDP Traffic Statistics for the Gigabit Ethernet Interface**

```
switch# show cdp traffic interface gigabitethernet 4/1
-----
Traffic statistics for GigabitEthernet4/1
Input Statistics:
  Total Packets: 674
  Valid CDP Packets: 674
    CDP v1 Packets: 0
    CDP v2 Packets: 674
  Invalid CDP Packets: 0
    Unsupported Version: 0
    Checksum Errors: 0
    Malformed Packets: 0

Output Statistics:
  Total Packets: 674
    CDP v1 Packets: 0
    CDP v2 Packets: 674
  Send Errors: 0
```