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

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.

Step 1 Check that the switch is set for the correct AC (or DC) power voltages.

Refer to either the *Cisco MDS 9200 Series Hardware Installation Guide* or the *Cisco MDS 9500 Series Hardware Installation Guide* for correct power voltages.

Step 2 Connect the power cord(s) to the switch.

Step 3 Connect the console port to the switch.

Note The console port is an asynchronous (async) serial port; any device connected to this port must be capable of asynchronous transmission.

Before connecting the console port, check the terminal documentation to determine the baud rate. The baud rate of the terminal must match the default baud rate (9600 baud) of the console port. Set up the terminal as follows (see the "Configuring Line Console Settings" section on page 3-27):

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity

Step 4 Power on the switch. The switch boots automatically.

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 also required if you plan to configure and manage the switch.

Note The IP address must first be set up in CLI when the switch is powered up for the first time so the Cisco MDS 9000 Fabric Manager can reach the switch.

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—You have the option to create a new login account or overwrite a preexisting account 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.
- The following IP addresses:
  - 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—if you wish to enable this service, then 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 routing, 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. See the "Role-Based Authorization" section on page 14-3 for information of default roles and permissions.

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 "Recovering Administrator Password" section on page 14-12).

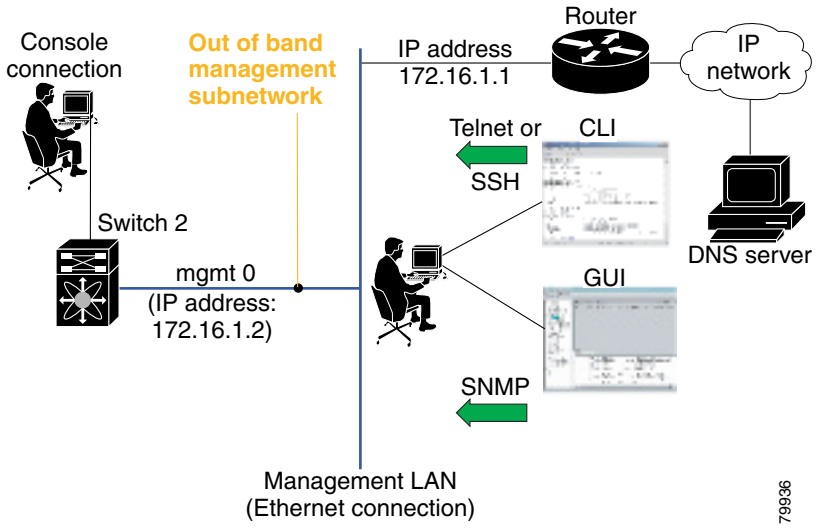
Setup Options

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 like 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 3-1).
- 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 3-1 and Chapter 16, "Configuring IP Services").

Figure 3-1 Management Access to Switches



Assigning Setup Information

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

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

Configuring Out-of-Band Management

Note If you wish to configure both in-band and out-of-band configuration together, enter **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.

```
---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Use ctrl-c to abort configuration dialog at any prompt.

Basic management setup configures only enough connectivity for
management of the system.

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

The setup utility guides you through the basic configuration process. Type **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 Authorization" section on page 14-3 for information of 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), if you wish 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 8 characters).

```
SNMPv3 user authentication password : admin_pass
```

Note If this password contains less than eight characters, you must enter a new password. The same password is also used for the SNMPv3 privacy.
By default if the admin password is at least 8 characters, then the SNMP authentication password will be same as admin password (at least 8 characters). If the admin password is less than 8 characters, then you need to provide a new password for SNMP.
The admin password can have a minimum of 1 character, but the SNMP authentication password must have a minimum of 8 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 and default-gateway capabilities.

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

a. 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 routing, 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.

b. 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 in Step 10 a above.

```
Default network IP address: dest_prefix
```

c. 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 11 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 12 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 13 Enter **yes** (yes is the default), to enable Telnet service.

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

Step 14 Enter **yes** (no is the default) to enable the SSH service.

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

Step 15 Enter the SSH key type (see Generating an SSH Host Key Pair, page 14-18) you would like to generate.

```
Type the SSH key you would like to generate (dsa/rsa/rsa1)? dsa
```

Step 16 Enter the number of key bits within the specified range.

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

Step 17 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 18 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
```

Step 19 Enter **on** (on is the default) to configure the switchport trunk mode.

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

Step 20 Enter **permit** (deny is the default) to permit a default zone policy.

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

Permits traffic to flow to all members of the default zone.

Step 21 Review and edit the configuration that you have just entered.

Step 22 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 ntp_server
  system default switchport shutdown
  system default switchport trunk mode on
  no zone default-zone permit vsan 1-4093

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

Step 23 Enter **yes** (yes is default) to use and save this configuration:

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

Caution If you do not save the configuration at this point, none of your changes will be updated the next time the switch is rebooted. Ensure to type **yes** in order to save the new configuration. This will ensure that the kickstart and system boot images are also automatically configured (see Chapter 5, “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 it's VSAN 1 interface configured with an IP address in the same subnetwork. A default route, pointing to the switch that provides access to the IP network should be configured on every switch in the Fibre Channel fabric (see Chapter 8, "Configuring and Managing VSANs").

Note If you wish to configure both in-band and out-of-band configuration together, enter **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. Use ctrl-c to abort configuration dialog at any prompt.

Basic management setup configures only enough connectivity for
management of the system.

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

The setup utility guides you through the basic configuration process. Type **Ctrl-c** from any prompt, to abort the configuration process.

Step 3 Enter the new password for the administrator.

```
Enter the password for admin: admin
```

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

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

Step 5 Enter **yes** (yes is the default), if you wish to create a SNMPv3 account.

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

a. Enter the user name.

```
SNMPv3 user name [admin]: user_name
```

By default, the SNMP user name is `admin`.

b. Enter the SNMPv3 password (minimum of 8 characters).

```
SNMPv3 user authentication password [admin_pass]: admin_pass
```

Note If this password contains less than eight characters, you must enter a new password. The same password is also used for the SNMPv3 privacy.
By default if the admin password is at least 8 characters, then the SNMP authentication password will be same as admin password (at least 8 characters). If the admin password is less than 8 characters, then you need to provide a new password for SNMP.
The admin password can have a minimum of 1 character, but the SNMP authentication password must have a minimum of 8 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 the default-gateway capabilities.

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

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

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

b. Enter **yes** (yes is the default) to configure the default network.

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

c. 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 11 Enter **No** (yes is the default) to configure the DNS IP address.

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

Step 12 Enter **no** (no is the default) to skip the default domain name configuration.

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

Step 13 Enter **no** (yes is the default), to disable Telnet service.

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

Step 14 Enter **yes** (no is the default) to enable the SSH service.

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

Step 15 Enter the SSH key type (see Generating an SSH Host Key Pair, page 14-18) you would like to generate.

```
Type the SSH key you would like to generate (dsa/rsa/rsa1)? rsa
```

Step 16 Enter the number of key bits within the specified range.

```
Enter the number of key bits? (512 to 1024): 1024
```

Step 17 Enter **no** (no is the default) to configure the NTP server.

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

Step 18 Enter **noshut** (shut is the default) to configure the default switchport interface to the up state.

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

Step 19 Enter **auto** (on is the default) to configure the switchport trunk mode automatically.

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

Step 20 Enter **deny** (deny is the default) to deny a default zone policy.

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

Step 21 Review and edit the configuration that you have just entered.

Step 22 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 deny vsan 1-4093
Would you like to edit the configuration? (yes/no): no
```

Step 23 Enter **yes** (yes is default) to use and save this configuration.

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

Caution If you do not save the configuration at this point, none of your changes will be updated the next time the switch is rebooted. Ensure to type **yes** in order to save the new configuration. This will ensure that the kickstart and system boot images are also automatically configured (see Chapter 5, "Software Images").

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.

Note The switch name is limited to 32 alphanumeric characters.

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

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

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

Assigning SNMP Switch Contact Information

Use the **snmp-server** command to set the contact information, switch location, and switch name. They are each limited to 32 characters (without spaces). Use the **no** form of the command to remove the system contact information. For more information on other **snmp-server** commands see the "SNMP Security" section on page 14-20

To configure contact information, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# snmp-server contact NewUser` `switch(config)#`	Assigns the contact name for the switch.
	`switch(config)# no snmp-server contact NewUser` `switch(config)#`	Deletes the contact name for the switch.
Step 3	`switch(config)# snmp-server location SanJose` `switch(config)#`	Assigns the switch location.
	`switch(config)# no snmp-server location SanJose` `switch(config)#`	Deletes the switch location.

Accessing the Switch

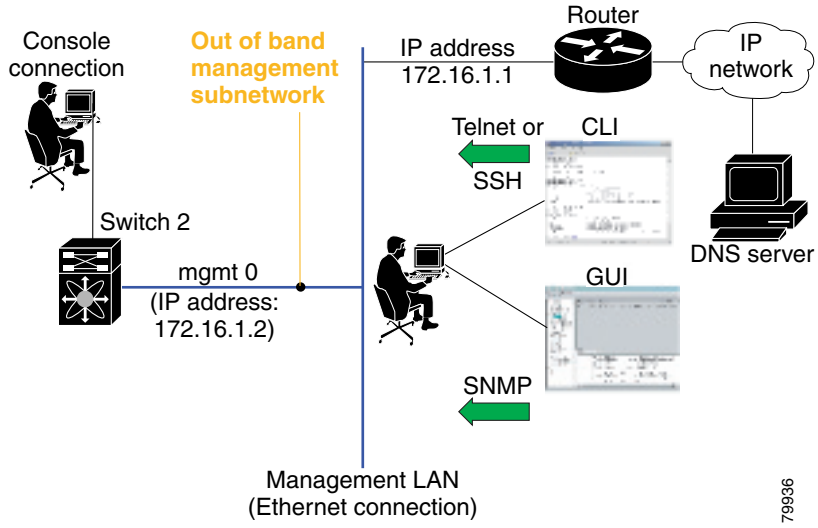
After initial configuration, you can access the switch in one of three ways (see Figure 3-2):

- 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 GUI.
- 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 GUI.

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

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

Figure 3-2 Switch Access Options



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 Element Manager and Fabric Manager GUIs.

To use the Cisco MDS 9000 Fabric Manager, refer to the *Cisco MDS 9000 Family Fabric Manager User 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
---  -----  -------------------------------- ------------------ ------------
3    16     1/2 Gbps FC Module               DS-X9016           ok
5    0      Supervisor/Fabric-1              DS-X9530-SF1-K9    active *
9    16     1/2 Gbps FC Module               DS-X9016           ok

Mod  Sw           Hw      World-Wide-Name(s) (WWN)
---  -----------  ------  --------------------------------------------------
3    1.0(1.22)    0.0     20:81:00:05:30:00:12:5e to 20:90:00:05:30:00:12:5e
5    1.0(1.22)    0.0     --
9    1.0(1.22)    0.0     22:01:00:05:30:00:12:5e to 22:10:00:05:30:00:12:5e

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
3    00-05-30-00-76-26 to 00-05-30-00-76-2a
5    00-05-30-00-53-ae to 00-05-30-00-53-b2
9    00-05-30-00-64-b6 to 00-05-30-00-64-ba

* this terminal session
```

If the status is OK or active, you can continue with your configuration (see Chapter 6, “Managing Modules”).

Configuring Time

Switches in the Cisco MDS 9000 Family use Coordinated Universal 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 12:07:50 23 September 2002
Mon Sep 23 12:07:50 UTC 2002
```

HH represents hours in military format (15 for 3 p.m.), *MM* is minutes (58), *SS* is seconds (09), *DD* is the date (02), *Month* is the month in words (August), 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 display the time.

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

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.

Step 2	`switch(config)# clock timezone <timezone name> <-23 to 23 hours offset from UTC time> <0 to 50 minutes offset from UTC>`
	
	Example:
	`switch(config)# clock timezone PST -8 0`
		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)# exit` `switch#`	Returns to EXEC mode.
Step 4	`switch# show clock`	Verifies the time zone configuration.
Step 5	`switch# show run`	Displays changes made to the time zone configuration along with other configuration information.

Setting the Daylight Saving Time Adjustment

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# config t`	Enters configuration mode.

Step 2	`switch(config)# clock timezone timezone_name hour_offset_from_UTC minute_offset_from_UTC`
	
	Example:
	`switch(config)# clock timezone PST -8 0`
		Offsets the time zone as specified.
		
		This example set the Pacific standard offset time as negative 8 hours and 0 minutes.

	`switch(config)# no clock timezone`	Disables the timezone adjustment feature.

	Command	Purpose

Step 3	`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*
	
	Example:
	`switch(config)# clock summer-time PDT 1 Sun Apr 02:00 5 Sun Oct 02:00 60`
	`switch(config)#`
		Sets the daylight savings time for a specified time zone.
		The start and end values are as follows:
		• week ranging from 1 through 5
		• day ranging from Sunday through Saturday
		• month ranging from January through December
		The daylight offset ranges from1 through 1440 minutes which are added to the start time and deleted time from the end time.
		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.

	`switch(config)# no clock summer-time`	Disables the daylight saving time adjustment feature.
Step 4	`switch(config)# exit` `switch#`	Returns to EXEC mode.
Step 5	`switch# show clock`	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 will be 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.

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

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ntp server 10.10.10.10` `switch(config)#`	Forms a server association with a server.
Step 3	`switch(config)# ntp peer 10.20.10.0` `switch(config)#`	Forms a peer association with a peer. You can specify multiple associations.
Step 4	`switch(config)# exit` `switch#`	Returns to EXEC mode.
Step 5	`switch# copy running-config startup-config`	Saves your configuration changes to NVRAM. **Tip** 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# show ntp peers`
	`----------------------------------------`
	`Peer IP Address Serv/Peer`
	`----------------------------------------`
	`10.20.10.2 Server`
	`10.20.10.0 Peer`
		Displays the configured server and peer associations.
		Note A domain name will be resolved only when you have a DNS server configured.

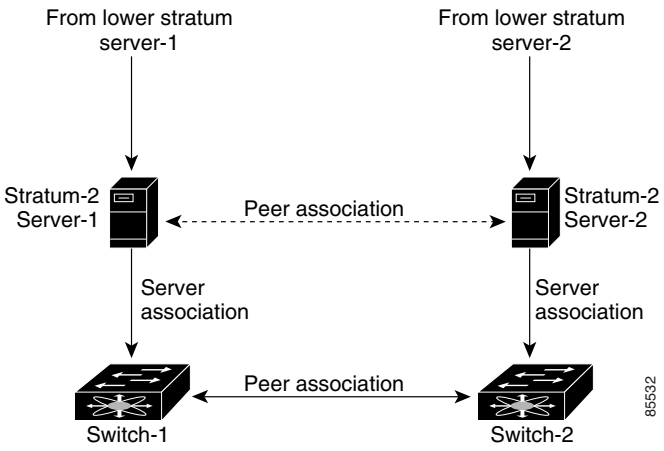
NTP Configuration Guidelines

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).
- Though a peer configured alone, will be the most accurate peer taking on the role of a server, the configured peer should be used more as a back-up support. If more than one server is present, you can have several switches point to one server, and the remaining to the another server, and then configure peer association between these two sets. This forces the clock more reliable.
- If you only have one server, it's better for all the switches have a client association with that server.

If the network is configured robustly, even a server down time will not affect well-configured switches in the network. Figure 3-3 displays a network with two NTP stratum 2 servers and two switches.

Figure 3-3 NTP Peer and Server Association



In this configuration, the switches were configured as explained below:

- 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

Configuring the Management Port

The management port on the switch allows multiple simultaneous Telnet or SNMP sessions.

You can remotely configure the switch through the management port, but first you must configure some IP parameters (IP address, subnet mask) so that the switch is reachable. You can manually configure the management port interface from the CLI.

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

To obtain remote management access using Telnet (CLI) or SNMP (GUI), follow these steps:

	Command	Command
Step 1	`switch# config terminal` `switch(config)#`	Enters configuration mode. You can also abbreviate the command to **config t**. The `switch(config)#` prompt indicates that you are in configuration mode.

Step 2	`switch(config)# interface` *type interface_string*
	`switch(config-if)#`
	Examples:
	`switch(config)# interface mgmt0`
	`switch(config-if)#`
		Enters the interface configuration mode on the specified interface.
		You can use the management Ethernet interface on the switch to configure the management interface.
		The `switch(config-if)#` prompt indicates that you are in the interface configuration mode.

Step 3	`switch(config)# ip address 1.1.1.0 255.255.255.0`	Enters the IP address and IP subnet mask for the interface specified in Step 2.
Step 4	`switch(config-if)# no shutdown`	Enables the interface.
Step 5	`switch(config-if)# exit` `switch#`	Returns to configuration mode.
Step 6	`switch(config)# ip default-gateway 1.1.1.1` `switch#`	Configures the default gateway address.
Step 7	`switch(config)# exit` `switch#`	Returns to EXEC mode.
Step 8	`switch# copy running-config startup-config`	Saves your configuration changes to the file system.

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** command.

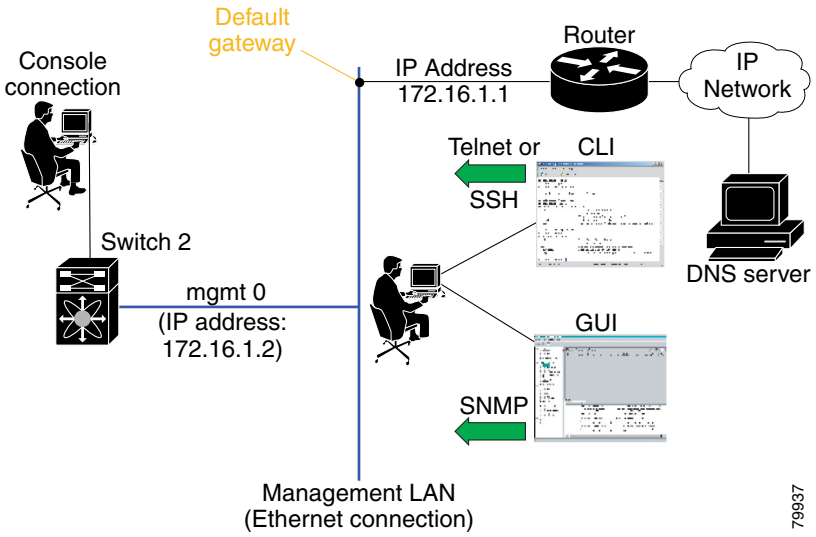
The management port (mgmt0) is autosensing and operates as full duplex mode and 100 Mbps speed. The speed and mode cannot be configured.

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.

Configuring Default Gateways

The supervisor module sends IP packets with unresolved destination IP addresses to the default gateway (see Figure 3-4).

Figure 3-4 Default Gateway



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

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ip default-gateway 1.1.1.4` `switch(config)#`	Configures the 1.1.1.4 IP address.

Disabling a Telnet Server

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 14-17).

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

Make sure the terminal is connected to the switch and that the switch and terminal are on. To allow Telnet connections to the switch, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# no telnet server enable` `updated`	Disables the Telnet server.
	`switch(config)# telnet server enable` `updated`	Enables the Telnet server if you wish to return a Telnet connection from a secure SSH connection.

Working with Configuration Files

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

Guidelines for Creating and Using 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.

Certain commands must be followed by a blank line in the configuration file. Without these blank lines, the commands might disconnect your Telnet session. Before disconnecting a session, the switch prompts you for confirmation. The blank line acts as a carriage return, which indicates a negative response to the prompt retaining the Telnet session.

Include a blank line after the following command in a configuration file:

```
interface mgmt0 disable
```

Viewing Configuration Files

To view the running configuration file, use the **show running-config** command:

```
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
```

To view the startup configuration file, use the **show startup-config** command:

```
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 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.
- 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 world-read.

Note See the "Copying Files" section on page 3-25.

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 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.

The *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 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
```

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

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

From an External CompactFlash Disk

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 session.

Step 2 Locate the configuration file using the **cd** and **dir** commands. (See the "Copying Files" section on page 3-25.)

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
```

Use the following command to download a configuration file from an external CompactFlash to the startup configuration.

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

To a Remote Server

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

Step 1 Log into the switch through the console port or through a Telnet session.

Step 2 Save the configuration using the **copy system: running-config <***scheme***> :// <***url***>** command.

Scheme can be 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 3-25.)

Step 3 Save the configuration file using the **copy system:running-config** <*source 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 system: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 3-1.

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

Table 3-1 copy Command Syntax

Scheme	Server	File Name
bootflash	active-sup standby-sup	User-specified
slot0	—	User-specified
volatile	—	User-specified
nvram	—	startup-config or snapshot-config
system	—	running-config
tftp[1]	IP address or DNS name	User-specified
ftp		
scp (secure copy)		
sftp		
core	—	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 bootflash to the standby supervisor module's bootflash.

```
switch# copy bootflash:active-sup/system.img bootflash:standby-sup/
```

Note Do not copy a file from an external source directly to the standby supervisor. You must copy from the external source to the active supervisor, and then copy the saved file to the standby supervisor.

- 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 create a running configuration copy in bootflash.

```
switch# copy system:running-config bootflash:my-config
```

- This example shows how to copy a system image file from the TFTP server to bootflash.

```
switch# copy tftp://172.16.10.100/system-237.img bootflash:system-237.img
```

- This example shows how to copy a script file from the SFTP server to volatile.

```
switch# copy sftp://172.16.10.100/myscript.txt volatile:myscript.txt
```

Rolling Back to a Previous Configuration

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

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

You can copy the configuration file to a TFTP server or to a local disk in ASCII format.

- This example shows how to roll back to a snapshot copy of a previously saved running configuration.

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

- This example shows how to create a running configuration copy in the bootflash: file system.

```
switch# copy system:running-config bootflash:my-config
```

- This example shows how to create a startup configuration copy in the bootflash: file system.

```
switch# copy nvram:startup-config bootflash:my-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 to match the new system image.

Deleting Files

To delete files on a Flash device, follow these steps:

	Command	Purpose
Step 1	`switch# delete [device:]filename`	Deletes files from a directory
Step 2	`switch# dir [device:][filename]`	Verifies the files are deleted.

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

```
switch# delete dns_config.cfg
switch#
```

- This example shows how to delete a file from an external CompactFlash (slot0):

```
switch# delete slot0:dns_config.cfg
switch#
```

Configuring Line Console Settings

Console ports on Cisco switches are set up for quick and easy access through any standard RS-232 data terminal equipment (DTE) device.

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

Note If you plan on connecting a modem to the console port of a switch in the Cisco MDS 9000 Family, first refer to the Console Port Issues section of the Modem-Router Connection Guide

Console Port Speed

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.

For the purposes of this document, the default console port speed of 9600 baud is assumed.

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

To configure console port speed, follow these steps:

	Command	Command
Step 1	`switch# config terminal` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# line console` `switch(config-console)#`	Enters the line console configuration mode.
Step 3	`switch(config-console)# speed 9600`	Configures the port speed for the serial console. the default is 9600 baud and the range is from 110 to 115,200 baud.

If you specify an invalid speed, you will receive the following error message:

```
switch(config-console)# speed 111
Error: 111 is not supported speed
Supported speed are 110, 150, 300,2400, 4800, 9600, 19200, 28800, 38400, 57600 (56K), and
115200
```

Device Control Parameters

Be sure to set the values for the device control parameters when setting up the terminal:

- 8 data bits
- 1 stop bit
- No parity

You can change these parameters to meet the requirements of the terminal or host to which you are attached.

To configure device control parameters, follow these steps:

	Command	Command
Step 1	`switch# config terminal` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# line console` `switch(config-console)#`	Enters the line console configuration mode.
Step 3	`switch(config-console)# databits 8` `switch(config-console)#`	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 4	`switch(config-console)# stopbits 1` `switch(config-console)#`	Configures the stop bits for the console connection. The default is 1 stop bits and the valid values are 1 or 2 stop bits.
Step 5	`switch(config-console)# parity none` `switch(config-console)#`	Configures the parity for the console connection. The default is no parity and the valid values even or odd parity.