Basic Router Commands and Tasks

Introduction

A large number of commands are available on Cisco routers, as well as many different protocols and features that can be used to establish a network. Navigating through Cisco IOS® Software can be confusing and intimidating for someone new to Cisco routers. This section will familiarize you with some of the basic router commands that are commonly used, as well as some typical router management tasks in the included labs.

Basic Cisco IOS Commands

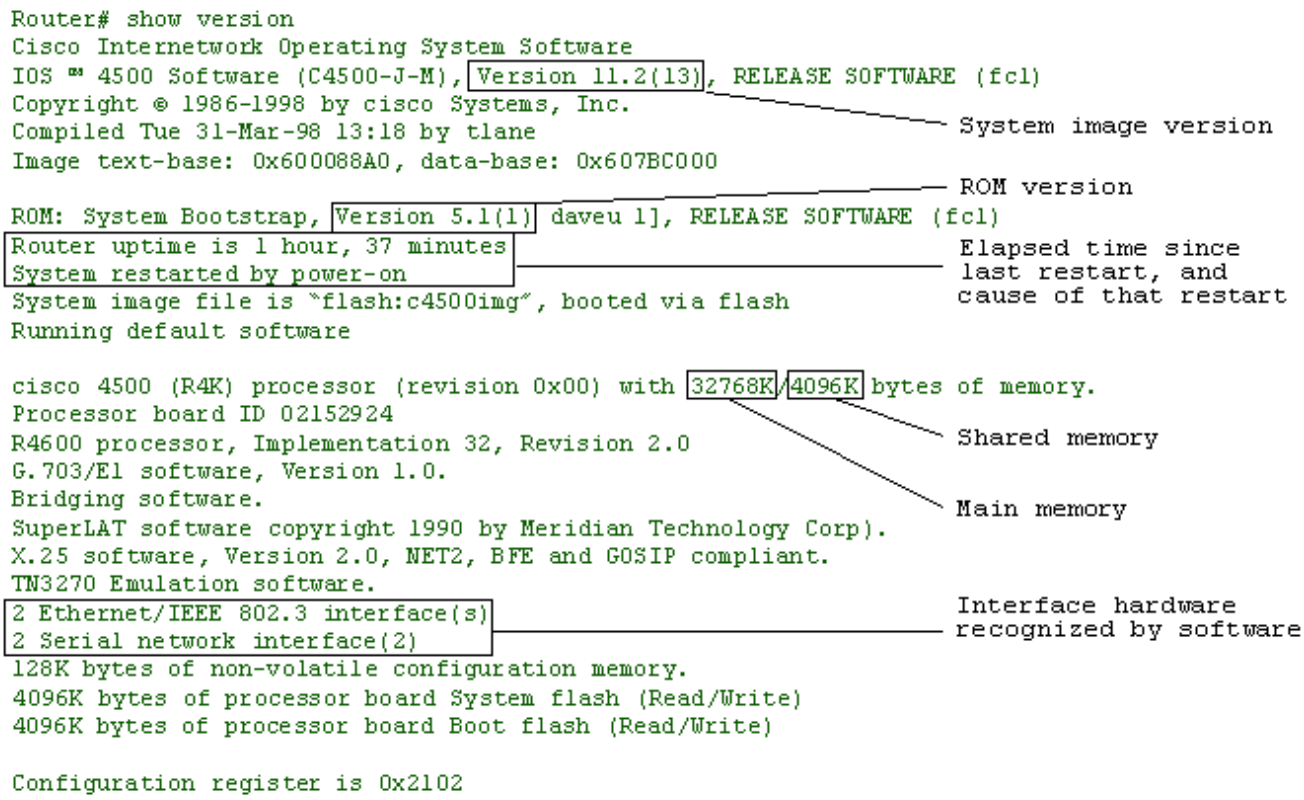
The following commands are used to gather information on a Cisco IOS Software-based router when attempting to learn basic information about a router, or possibly troubleshooting protocol-independent problems:

- **show version**
- **show running-config**
- **show interfaces**
- **show logging**
- **show tech-support**

Let's examine these commands further to see how they can be used to obtain valuable information.

show version

You will use the **show version** command in the simulation environment. This command displays the configuration of the system hardware, the software version, and the names and sources of configuration files and the boot images. This command also displays information about how the system was last started and how long the router has been running since that start. Sample output from the **show version** command follows:



System Image Version and ROM Version

This information indicates the running version of the Cisco IOS Software. This software has many different versions of the Cisco IOS Software, each of which supports a variety of features. The version of Cisco IOS Software on the router plays a major role in dictating the capabilities and services of the router.

Router Uptime and System Restart

The router uptime can be checked to make sure the router has been in continuous operation since it was last restarted. If the uptime is inconsistent with the last known router maintenance, the router may have restarted because of problems with the electrical circuit it is connected to, or because of problems with the router itself. The "System restarted by" line displays a log of how the system was last booted, whether by normal system startup or because of a system error. The following display is an example of a system error that is generally the result of an attempt by the router to access a nonexistent address:

```
System restarted by bus error at PC 0xC4CA, address 0x210C0C0
```

Interface Hardware Inventory

The interface hardware inventory should include all interface processors installed in the router. If any interfaces that are installed in the router do not show up in the inventory, there may be hardware problems with the interface processor itself, or the router may be running a version of the Cisco IOS Software that does not support that interface type.

Shared Memory

This is the memory the interface processors use for buffering packets. As the name suggests, all the interface processors in a router share this memory, and performance problems can result if there is not enough. It may be necessary to upgrade the memory if such an issue occurs.

Main Memory

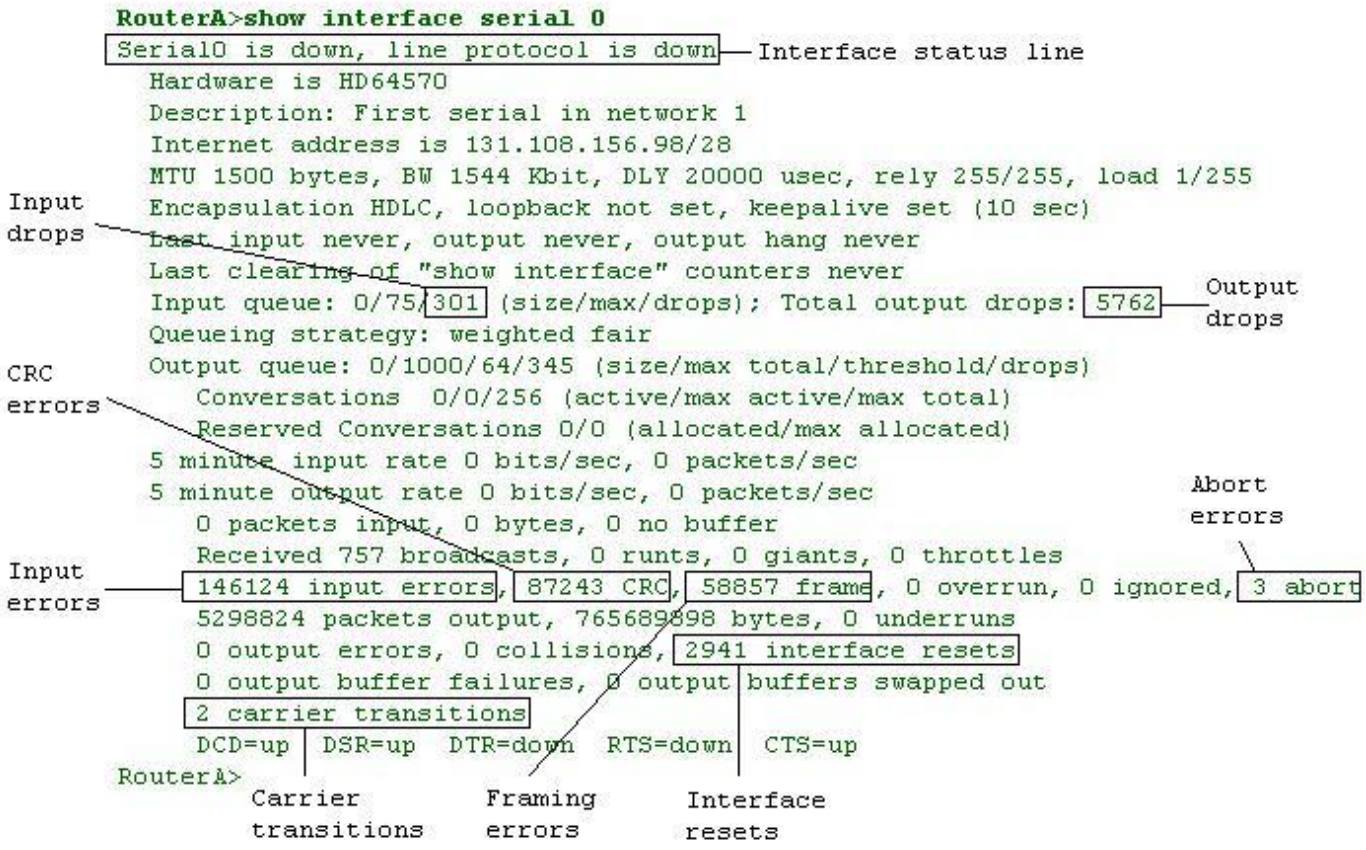
This memory is used to store the running configuration and all routing tables. In extremely large networks, it is possible for the routing tables to get so large they exceed the main memory capacity. When this happens, the router will crash. It may be necessary to upgrade the memory if such an issue occurs.

show running-config

All the commands that are entered on a router are stored in the current running configuration that is maintained in RAM. This command can be very useful when gathering basic information or troubleshooting because it allows the user to verify the commands that have been administered on the router. You will use the **show running-config** command in the simulation labs.

show interfaces

You will use the **show interfaces** command in the practice labs. This command displays statistics for the network interfaces. Sample output from the **show interfaces** command is shown below. Because your display will depend on the type and number of interface cards in your router, only a portion of the display is shown, in this case for a serial interface.



NetBit: Click on the Netbit icon to the right to view an animation about Cyclic Redundancy Check (CRC).

Interface and Line Protocol Status

The interface and line protocol status output gives information related to the physical state of the interface (the first part of the output) and shows the state of messages at the data link level (the second part of the output, following the comma).

When an interface is operating and communicating correctly, there is only one possible status output:

- Serial *x* is up, line protocol is up

Remember that this output is meant to correspond to the serial interface output shown above. If an Ethernet interface were being examined, the output would obviously change accordingly to "Ethernet *x* is up, line protocol is up."

You can identify five possible problem states in the interface status line of the **show interfaces serial** display:

- Serial *x* is down, line protocol is down
  - This state indicates a cable or interface problem. The remote end may be administratively shut down, a situation that could cause both ends to go down. To bring an interface up, use the *no* form of the shutdown command under the interface configuration mode.
- Serial *x* is up, line protocol is down
  - This state is often attributed to a clocking or framing problem. Check to make sure that clocking has been set on the correct end, keepalives are being sent correctly, and the encapsulation type on both ends match.
- Serial *x* is up, line protocol is up (looped)
  - This state indicates that a loop exists in the circuit. This problem could be associated with an existing loopback interface.
- Serial *x* is up, line protocol is down (disabled)
  - This state often indicates a hardware problem and may be associated with a telephone company service problem.
- Serial *x* is administratively down, line protocol is down
  - This state indicates that the shutdown command has been administered on the interface. To bring the interface up, use the **no shutdown** command under interface configuration mode.

Output Drops

Output drops appear in the output of the **show interfaces serial** command when the system is attempting to hand off a packet to a transmit buffer but no buffers are available.

NOTE: Output drops are acceptable under certain conditions. For instance, if a link is known to be overused (with no way to remedy the situation), it is often considered preferable to drop packets rather than holding them, particularly for protocols that support flow control and can retransmit data, such as TCP/IP.

NetBit: Click on the Netbit icon to the right to view an animation about buffering.

Input Drops

Input drops appear in the output of the **show interfaces serial** EXEC command when too many packets from that interface are still being processed in the system.

Input Errors

If input errors appear in the **show interfaces serial** output, they have several possible sources. The most likely sources are related to physical layer issues, including bad hardware, a noisy line, a bad connection, or incorrect equipment. Other potential causes include noisy lines and incorrect data conversion.

NOTE: Any input error value for cyclic redundancy check (CRC) errors, framing errors, or aborts above one percent of the total interface traffic suggests some kind of link problem that should be isolated and repaired.

Interface Resets

Interface resets that appear in the output of the **show interfaces serial** EXEC command are the result of missed keepalive packets. Interface resets may occur because of issues such as congestion on the line, a bad line, or faulty equipment.

Carrier Transitions

Carrier transitions appear in the output of the **show interfaces serial** EXEC command whenever there is an interruption in the carrier signal (such as an interface reset at the remote end of a link). Carrier transitions may be caused by physical changes to the line (cable unplugged or damaged) or by faulty equipment.

show logging

This command displays the state of syslog error and event logging, including host addresses, and whether console logging is enabled. This command also displays Simple Network Management Protocol (SNMP) configuration parameters and protocol activity.

```
Router# show logging
Syslog logging: enabled
     Console logging: disabled
     Monitor logging: level debugging, 266 messages logged.
     Trap logging: level informational, 266 messages logged.
     Logging to 192.180.2.238
SNMP logging: disabled, retransmission after 30 seconds
    0 messages logged
```

The following table describes significant fields shown in the command display.

Field	Description
Syslog Logging	When enabled, system logging messages are sent to a UNIX host that acts as a syslog server; that is, it captures and saves the messages.
Console Logging	If enabled, this field states the level; otherwise, it displays disabled.
Monitor Logging	This shows the minimum level of severity required for a log message to be sent to a monitor terminal (not the console).
Trap Logging	This field gives the minimum level of severity required for a log message to be sent to a syslog server.
SNMP Logging	This field shows whether SNMP logging is enabled and the number of messages logged, and the retransmission interval.

show tech-support

Use this command to help collect general information about the router when you are reporting a problem to the Cisco Technical Assistance Center (TAC). This command displays the equivalent of the following show commands:

- **show version**
- **show running-config**
- **show controllers**
- **show stacks**
- **show interfaces**
- **show buffers**
- **show processes memory**
- **show processes cpu**

The output of most of these commands is of use only to your technical support representative.

Basic Router Management Tasks

Although most configurations on a Cisco Router will probably occur when a network is initially being set up or an upgrade or enhancement is being performed, you may encounter some basic maintenance tasks during routine interaction with a router. A list of some of the common router management tasks are below. The simulation labs that follow will reinforce your understanding of these tasks by walking you through each of these procedures.

- Providing a router hostname
- Setting up passwords
- Disabling DNS lookup
- Setting up logging
- Setting timestamps for logging and debugging
- Defining console, auxiliary, and virtual terminal settings
- Setting up a Comm Server to access your routers more easily
- Handling password recovery
- Downloading a software image from a TFTP server
- File management tasks
- Cisco Discovery Protocol

Password Recovery

For security purposes, passwords are often configured on Cisco routers to restrict access. This password can be forgotten or lost and it may need to be recovered to gain access to the router. The process for recovering a lost password varies from platform to platform, because there are many different types of Cisco products. Several password recovery techniques for different Cisco products can be found on Cisco.com by searching on the words "password recovery."

Though the actual password-recovery processes for different routers may vary, each procedure follows the following basic steps:

1. Configure the router to boot up without reading the configuration memory (nonvolatile RAM, or NVRAM). This is sometimes called the "test system mode."
2. Reboot the system.
3. Access enable mode (this can be done without a password if you are in test system mode).
4. View or change the password, or erase the configuration.
5. Reconfigure the router to boot up and read the NVRAM as it normally does.
6. Reboot the system.

! **NOTE:** Some password recovery requires a terminal to issue a BREAK signal; you must be familiar with how your terminal or PC terminal emulator issues this signal. Several break sequences for different platforms and setups are provided on Cisco.com by searching on the words "break sequence."

NetBit: To view a NetBit on how to complete password recovery on a Cisco 2600 Router, click on the NetBit icon to the right.

Cisco Discovery Protocol

The Cisco Discovery Protocol (formerly known as CDP) is a proprietary, media- and protocol-independent protocol that runs on all Cisco manufactured equipment, including routers, bridges, access servers, and switches. With Cisco Discovery Protocol, network management applications can learn the device type and the Simple Network Management Protocol (SNMP) agent address of neighboring devices. This enables applications to send SNMP queries to neighboring devices.

Cisco Discovery Protocol essentially allows administrators to gain basic information about all other devices attached to a Cisco device. The type of information that can be obtained using Cisco Discovery Protocol includes the hostname, platform (type of device),

and capabilities of attached devices. Cisco Discovery Protocol can also be used to obtain the network address of the interface of an attached device.

Cisco Discovery Protocol runs on all media that support Subnetwork Access Protocol (SNAP), LAN, Frame Relay, and ATM media. Cisco Discovery Protocol runs over the data link layer only. Therefore, two systems that support different network-layer protocols can learn about each other.

Each device configured for Cisco Discovery Protocol sends periodic messages to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime, information, which indicates the length of time a receiving device should hold Cisco Discovery Protocol information before discarding it.

The section that follows outlines some of the basic Cisco IOS® commands related to Cisco Discovery Protocol. A lab is provided, later in this module, to give you some experience configuring and using Cisco Discovery Protocol in a network environment.

Basic Cisco IOS Commands Related to Cisco Discovery Protocol

To set the frequency of Cisco Discovery Protocol transmissions and the hold time for Cisco Discovery Protocol packets, perform the following tasks in global configuration mode:

Task	Command
Specify frequency of transmission of Cisco Discovery Protocol updates.	**cdp timer *seconds***
Specify the amount of time a receiving device should hold the information sent by your device before discarding it.	**cdp holdtime *seconds***

Cisco Discovery Protocol is enabled by default. To disable Cisco Discovery Protocol and later reenable it, perform the following tasks in global configuration mode:

Task	Command
Disable Cisco Discovery Protocol.	**no cdp run**
Enable Cisco Discovery Protocol.	**cdp run**

Cisco Discovery Protocol is enabled by default on the router and is also enabled by default on all supported interfaces to send and receive Cisco Discovery Protocol information. To disable and later reenable Cisco Discovery Protocol on an interface, perform the following tasks in interface configuration mode:

Task	Command
Disable Cisco Discovery Protocol on an interface.	**no cdp enable**
Enable Cisco Discovery Protocol on an interface.	**cdp enable**

To monitor and maintain CDP on your device, perform the following tasks in privileged EXEC mode:

Task	Command
Reset the traffic counters to zero.	**clear cdp counters**
Delete the Cisco Discovery Protocol table of information about neighbors.	**clear cdp table**
Display global information such as frequency of transmissions and the hold time for packets being transmitted.	**show cdp**
Display information about a specific neighbor. Display can be limited to protocol or version information.	**show cdp entry *entry-name* [*protocol* | *version*]**
Display information about interfaces on which Cisco Discovery Protocol is enabled.	**show cdp interface [*type number*]**
Display information about neighbors. The display can be limited to neighbors on a specific interface, and expanded to provide more-detailed information.	**show cdp neighbors [*type number*] [*detail*]**
Display Cisco Discovery Protocol counters, including the number of packets sent and received and checksum errors.	**show cdp traffic**
Display information about the types of debugging that are enabled for your router.	**show debugging**

What's Next

Now that you have explored some of the commands related to basic router settings and gathered information, let's look at the **show version** of some routers to obtain more information about them. Continue with Lab: Router Basics.