Computers and Networks

Bucharest
- 2003 -

Router Components

External router configuration sources

In this section, you will learn about the router components that play a key role in the configuration process. Knowing which components are involved in the configuration process gives you a better understanding of how the router stores and uses your configuration commands. Being aware of the steps that take place during router initialization will help
you determine what and where problems may occur when you start up your router.
You can configure a router from many external locations, including the following:

- from the console terminal (a computer connected to the router through a console port) during its installation
-via modem by using the auxiliary port
-from Virtual Terminals 0-4, after it has been installed on the network
-from a TFTP server on the network

Internal router's configuration components

The internal architecture of the Cisco router supports components that play an important role in the startup process. Internal router configuration components are as follows:

RAM/DRAM -- stores routing tables,ARP cache, fast-switching cache,packet buffering (shared RAM), and packet hold queues; RAM also provides temporary and/or running memory for a router's configuration file while the router is powered; RAM content is lost during a power down or restart

NVRAM -- non-volatile RAM stores the router's backup/startup configuration file; NVRAM content is retained during power down or restart

Flash -- erasable, reprogrammable ROM that holds the operating system image and microcode; Flash memory enables software updates without removing and replacing

processor chips; Flash content is retained during power down o restart; Flash memory can store multiple versions of IOS software

ROM -- contains power-on diagnostics, a bootstrap program, and operating system software; software upgrades in ROM require removing and replacing pluggable chips on the CPU interfaces -- network connections on the motherboard or on separate interface modules, through which packets enter and exit a router.

RAM for working storage in the router

RAM is the working storage area for a router. When you turn a router on, the ROM executes a bootstrap program. This program performs some tests, and then loads the Cisco IOS software into memory. The command executive, or EXEC, is one part of the Cisco IOS software. EXEC receives and executes commands you enter for the router.

A router also uses RAM to store an active configuration file and tables of network maps and routing address lists. You can display the configuration file on a remote or console terminal. A saved version of this file is stored in NVRAM. It is accessed and loaded into main memory each time a router initializes. The configuration file contains global, process, and interface information that directly affects the operation of a router and its interface ports.

An operating system image cannot be displayed on a terminal screen. An image is usually executed from the main RAM and loaded from one of several input sources.

The operating software is organized into routines that handle the tasks associated with different protocols, such as data movement, table and buffer management, routing updates, and user command execution.

Router modes

Whether accessed from the console or by a Telnet session through a TTY port, a router can be placed in several modes. Each mode provides different functions:

-user EXEC mode -- This is look-only mode in which the user can view some information about the router, but can change nothing.

-privileged EXEC mode -- This mode supports the debugging and testing commands, detailed examination o the router, manipulation of configuration files, and access to

configuration modes.

- setup mode -- This mode presents an interactive prompted dialog at the console that helps the new user create a first-time basic configuration.

- global configuration mode -- This mode implements powerful one-line commands that perform simple configuration tasks.

-other configuration modes – Thes modes provide more detailed multiple-line configurations.

-RXBOOT mode -- This is the maintenance mode that you can use, among other things, to recover from lost passwords.

Router Show Commands

Examining router status by using router status commands

In this section, you will learn basic commands that you can issue to determine the current status of a router. These commands help you obtain vital information you need when monitoring and troubleshooting router operations.

It is important to be able to monitor the health and state of your router at any given time. Cisco routers have a series of commands that allow you to determine whether the router is functionally correct or where problems have occurred. In addition, router status commands are shown below:

-show version -- displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot image

-show processes -- displays information about the active processes

-show protocols -- displays the configured protocols; shows the status of all configured Layer 3 protocols

-show mem -- shows statistics about the router's memory, including memory free pool statistics

-show stacks -- monitors the stack use of processes and interrupt routines and displays the reason for the last system reboot

-show buffers -- provides statistics for the buffer pools on the router

-show flash -- shows information about the Flash memory device

-show running-config (write term on Cisco IOS Release 10.3 or earlier) -- displays the active configuration file

-show startup-config (show config on Cisco IOS Release 10.3 or earlier) -- displays the backup configuration file

-show interfaces -- displays statistics for all interfaces configured on the router

The show running-config and show startup-config commands

Among the most used Cisco IOS software EXEC commands are show running-config and show startup-config. They allow an administrator to see the current running configuration on the router or the startup configuration commands that the router will use on the next restart. (Note: The commands, write term and show config, used with Cisco IOS Release 10.3 and earlier, have been replaced with new commands. The commands that have been replaced continue to perform their normal functions in the current release but are no longer documented. Support for these commands will cease in a future release.)

You can recognize an active configuration file by the words current configuration at the top. You can recognize a backup configuration file when you see a message at the top that tells you how much non-volatile memory you have used.

The show interfaces, show version, and show protocols commands

The show interfaces command displays configurable parameters and real-time statistics related to router interfaces. The show version command displays information about the Cisco IOS software version that is currently running on the router .

You use the show protocols command to display the protocols configured on the router. This command shows the global and interface-specific status of any configured Level 3 protocols (for example, IP, DECnet, IPX, and AppleTalk).

Router's Network Neighbors

Gaining access to other routers by using Cisco Discovery Protocol (CDP)

Cisco Discovery Protocol (CDP) provides a single proprietary command that enables network administrators to access a summary of what the configurations look like on other directly-connected routers. CDP runs over a data link layer that connects lower physical media and upper network layer protocols. Because it operates at this level, CDP devices that support different network layer protocols can learn about each other. (Remember that a data link address is the same as a MAC address.)

When a Cisco device that is running Cisco IOS (Release 10.3 or later) boots up, CDP starts up automatically, which then allows the device to detect neighboring Cisco devices that are also running CDP. Such devices extend beyond those using TCP/IP, and include directly-connected Cisco devices, regardless of which Layer 3 and 4 protocol suite they run.

Showing CDP neighbor entries

The primary use of CDP is to discover platforms and protocols on your neighboring devices. Use the show cdp neighbors command to display the CDP updates on the local router.

The Figure displays an example of how CDP delivers its collection of information to a network administrator. Each router that is running CDP exchanges information regarding any protocol entries with its neighbors. The administrator can display the results of this CDP information exchange on a console that is connected to a router configured to run CDP on its interfaces.

The network administrator uses a show command to display information about the networks directly connected to the router. CDP provides information about each CDP neighbor device. Values include the following:

-device identifiers -- e.g. the router's configured host name and domain name (if any)

-ddress list -- at least one address for SNMP, up to one address for each supported protocol

-port identifier -- e.g. Ethernet 0, Ethernet 1, and Serial 0

-apabilities list -- e.g. if the device acts as a source route bridge as well as a router

-version -- information such as that provided by the local command show version

-platform -- the device's hardware platform, e.g. Cisco 7000

Notice that the lowest router is not directly connected to the administrator's console router. To obtain CDP information about this device, the administrator would need to Telnet to a router that is directly connected to this target.

A CDP configuration example

CDP begins automatically upon a device’s system startup. The CDP function normally starts by default when a Cisco product boots up with Cisco IOS Release 10.3 or later.

Although CDP runs by default, you must explicitly enable it on the device’s interface by using the command cdp enable. For example, the Figure shows the cdp enable in use on the E0 and S0 interface on Router A. This command begins CDPs dynamic discovery function on the device’s interfaces. Only directly connected neighbors exchange CDP frames. A router caches any information it receives from its CDP neighbors. If a subsequent CDP frame indicates that any of the information about a neighbor

has changed, the router discards the older information and replaces it with the new information.

Use the command show cdp interface, as shown in Figure , to display the values of the CDP timers, the interface status, and the encapsulation used by CDP for its advertisement and discovery frame transmission. Default values for timers set the frequency for CDP updates and for aging CDP entries. These timers are set automatically at 60 seconds and 180 seconds, respectively. If the device receives a more recent update, or if this hold-time value expires, the device must discard the CDP entry.

Showing CDP entries for a device and CDP neighbors

CDP was designed and implemented as a very simple, low-overhead protocol. A CDP frame can be small yet retrieve a lot of useful information about neighboring routers. You use the command show cdp entry {device name} to display a single cached CDP entry. Notice that the output from this command includes all the Layer 3 addresses present in the neighbor router, Router B. An administrator can view the IP addresses of the targeted CDP neighbor

(Router B) with the single command entry on Router A. The hold-time value indicates the amount of elapsed time since the CDP frame arrived with this information. The command includes abbreviated version information about Router B.

You use the command show cdp neighbors, as shown in Figure , to display the CDP updates received on the local router. Notice that for each local port, the display shows the following:

- -neighbor device ID
- -local port type and number
- -decremental hold-time value, in seconds
- -neighbor device capability code
- -neighbor hardware platform
- -neighbor remote port type and number

To display this information as well as information like that from show cdp entry, you use the optional show cdp neighbors detail.

Basic Networking Testing

Testing process that uses the OSI model

Addressing problems are the most common problems that occur on IP networks. It is important to test your address configuration before continuing with further configuration steps. Basic testing of a network should proceed in sequence from one OSI reference model layer to the next. Each test presented in this section focuses on network operations at
a specific layer of the OSI model. Telnet, ping, trace, show ip route, show interfaces and debug are commands that allow you to test your network.

Testing the application layer by using telnet

Another way to learn about a remote router is to connect to it. Telnet, a virtual terminal protocol that is part of the TCP/IP protocol suite, allows connections to be made to hosts. You can set a connection between a router and a connected device. Telnet allows you to verify the application-layer software between source and destination stations.

This is the most complete test mechanism available. A router can have up to five simultaneous incoming Telnet sessions.

Let’s begin testing by initially focusing on upper-layer applications. The telnet command provides a virtual terminal so that administrators can use Telnet operations to connect with other routers running TCP/IP.

With Cisco’s implementation of TCP/IP, you do not need to enter the command connect or telnet to establish a Telnet connection. If you prefer, you can just enter the learned host name. To end a Telnet session, use the EXEC commands exit or logout.

The following list shows alternative commands for the operations :

- Initiate a session from Denver:
  Denver> connect paris
  Denver> paris
  Denver> 131.108.100.152
  -Resume a session (enter session number or name):
  Denver>1
  Paris>
  -End a session:
  Paris> exit

As you have already learned, the Telnet application provides a virtual terminal so that you can connect to other hosts that are running TCP/IP. You can use Telnet to perform a test to determine whether or not you can access a remote router. If you can successfully use Telnet to connect the York router to the Paris router, then you have performed a basic test of the network connection.

If you can remotely access another router through Telnet, then you know that at least one TCP/IP application can reach the remote router. A successful Telnet connection indicates that the upper-layer application (and the services of lower layers, as well) function properly.

If we can Telnet to one router but not to another router, it is likely that the Telnet failure is caused by specific addressing, naming, or access permission problems. These problems can exist on your router or on the router that failed as a Telnet target. The next step is to try ping, which is covered in this section. This command lets you test end-to-end at the network layer.

Testing the network layer using the ping command

As an aid to diagnosing basic network connectivity, many network protocols support an echo protocol, which is a test to determine whether protocol packets are being routed. The ping command sends a packet to the destination host and then waits for a reply packet from that host. Results from this echo protocol can help evaluate the path-to-host reliability, delays over the

path, and whether the host can be reached or is functioning.

The ping target 172.16.1.5 responded successfully to all five datagrams sent. The exclamation points (!) indicate each successful echo. If you instead receive one or more periods (.) on your display, the application on your router timed out waiting for a given packet echo from the ping target. You can use the ping user EXEC command to diagnose basic network connectivity. ping uses the ICMP (Internet Control Message Protocol).

Testing the network layer with the trace command

The trace command is the ideal tool for finding where data is being sent in your network. The trace command is similar to the ping command, except that instead of testing end-to-end connectivity, trace tests each step along the way. This operation can be performed at either the user or privileged EXEC levels.

The trace command takes advantage of the error messages generated by routers when a packet exceeds its Time To Live (TTL) value. The trace command sends several packets and displays the round-trip time for each. The benefit of the trace command is that it tells which router in the path was the last one to be reached. This is called fault isolation.

In this example, we are tracing the path from York to Rome. Along the way the path must go through London and Paris. If one of these routers had been unreachable, you would have seen three asterisks (*) instead of the name of the router. The trace command would continue attempting to reach the next step until you escaped using the Ctrl-Shift-6 escape sequence.

Testing network layer with the show ip route command

The router offers some powerful tools at this point in the search. You can actually look at the routing table - the directions that the router uses to determine how it will direct traffic across the network.

The next basic test also focuses on the network layer. Use the show ip route command to determine whether a routing table entry exists for the target network. The highlight in the graphic shows that Rome (131.108.33.0)

is reachable by Paris (131.108.16.2) via the Enternet1 interface.

Using the show interfaces serial command to test the physical and data link layers

The interface has two pieces, physical (hardware) and logical (software):

-The hardware -- such as cables, connectors, and interfaces -- must make the actual connection between the devices.

-The software is the messages -- such as keepalive messages, control information, and user information -- that are passed between adjacent devices. This information is data being passed between two connected router interfaces.

When you test the physical and data link, you ask these questions:

- Is there a Carrier Detect signal?
-Is the physical link between devices good?
-Are the keepalive messages being received?
-Can data packets be sent across the physical link?

One of the most important elements of the show interfaces serial command output is display of the line and data link protocol status.

The line status in this example is triggered by a Carrier Detect signal, and refers to the physical layer status. However, the line protocol, triggered by keepalive frames, refers to the data link framing.

The show interfaces and clear counters commands

The router tracks statistics that provide information about the interface. You use the show interfaces command to display the statistics. The statistics reflect router operation since the last time the counters were cleared, as shown in the top highlighted line in the graphic. This graphic shows that it was two weeks and four days earlier. The bottom set of highlights shows the critical counters. Use the clear counters command to reset the

counters to 0. By starting from 0, you get a better picture of the current status of the network.

Checking real-time traffic with debug

The router includes hardware and software to aid it in tracking down problems, on it, or on other hosts in the network. The debug privileged EXEC command starts the console display of the network events specified in the command parameter. Use the terminal monitor command to forward debug output to your Telnet session terminal.

In this example, data link broadcasts received by the router are displayed. Use the undebug all command (or no debug all) to turn debugging off when you no longer need it. Debugging is really intended for solving problems.

(Note: Be very careful with this tool on a live network. Substantial debugging on a busy network will slow down the network significantly. Do not leave debugging turned on; use it to diagnose a problem, and then turn it off.)

By default, the router sends system error messages and output from the debug EXEC command to the console terminal. Messages can be redirected to a UNIX host or to an internal buffer. The terminal monitor command gives you the capability to redirect these messages to a terminal.