

Advanced IOS Management

Chapter 3



CertificationKits

2014 Copyright CertificationKits LLC

In this chapter, you will learn how to manage Cisco routers on an internetwork.

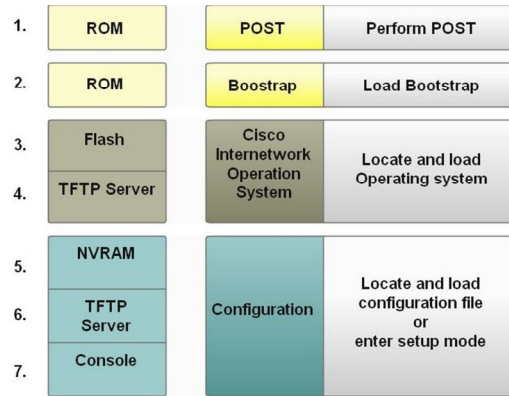
The Internetwork Operating System (IOS) and configuration files reside in different locations in a Cisco device, and it's important to understand where these files are located and how they work.

You'll also learn about the main components of a router, the router boot sequence, and the configuration register.

Router as a Computer

- Major phases to the router boot-up process

- Test router hardware
 - Power-On Self Test (POST)
 - Execute bootstrap loader
- Locate & load Cisco IOS software
 - Locate IOS
 - Load IOS
- Locate & load startup configuration file or enter setup mode
 - Bootstrap program looks for configuration file



CertificationKits

2014 Copyright CertificationKits LLC

Router components and their functions:

- CPU** - Executes operating system instructions.
- Random Access Memory (RAM)** - Contains the running copy of configuration file. Stores routing table. RAM contents lost when power is off.
- Read-Only Memory (ROM)** - Holds diagnostic software used when router is powered up. Stores the router's bootstrap program.
- Non-Volatile RAM (NVRAM)** - Stores startup configuration. This may include IP addresses (Routing protocol, Hostname of router).
- Flash memory** - Contains the operating system (Cisco IOS).
- Interfaces** - There exist multiple physical interfaces that are used to connect network. Examples of interface types:
 - Ethernet / Fast Ethernet / Gigabit Ethernet interfaces
 - Serial interfaces
 - Management interfaces
 - etc.

Router Boot Cycle

- Perform Power-On Self Test (POST) – from ROM
- Load and run bootstrap code– from ROM
- Look in NVRAM for config-register setting – default is 0x2102 (tells router where to find IOS and configuration file)
- Load the Cisco IOS software from flash – by default. Use “boot system” commands to modify
- Find the startup-config file in nvram (if none, broadcast for tftp host, if fail, go into Setup mode)
- If configuration file found, copy the file and place in RAM – file called running-config

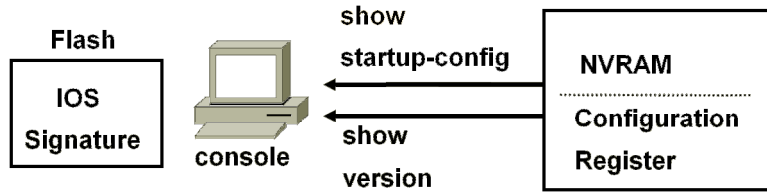


CertificationKits

2014 Copyright CertificationKits LLC

The config-register setting can be used to manipulate how the router boots. The default config-register setting is 0x2102. Changing the setting to 0x2142 will cause the router to ignore the startup configuration file stored in NVRAM. This is useful for password recovery.

Finding the Cisco IOS Image



Order of search:

- 1. Checks configuration register*
- 2. Parses configuration for boot system command*
- 3. Defaults to first file in flash memory*
- 4. Attempts to boot from network server*
- 5. Boot helper image*
- 6. ROMMON*

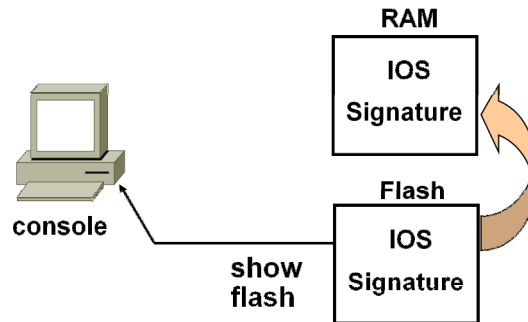


CertificationKits

2014 Copyright CertificationKits LLC

A router needs an IOS image in order to boot. In order to find an IOS image it first checks the configuration register. This will tell it whether to read the startup configuration file if it exists. If a startup file exists, it is parsed for a possible boot system command. If a boot system command does not exist, the router defaults to the first file on flash memory. If no valid IOS version exists on flash memory, the router attempts to boot over the network from a boot server. If that fails, the router will attempt to boot from a helper image. If all else fails it will enter ROMMON mode.

Loading the Cisco IOS Image from Flash Memory



The flash memory file is loaded into RAM.



CertificationKits

2014 Copyright CertificationKits LLC

When a router is booted and there is a valid IOS image store on flash memory, that IOS image is copied into RAM where it is utilized for operation of the router.

When the router is up and running you can perform a “**show flash**” command to display what IOS images are currently resident on flash.

show flash command

```
RouterX#show flash
--#-- --length-- -----date/time----- path
1      14951648 Feb 22 2007 21:38:56 -00:00 c2800nm-ipbase-mz.124-5a.bin
2         1823 Dec 14 2006 08:24:54 -00:00 sdmconfig-2811.cfg
3      4734464 Dec 14 2006 08:25:24 +00:00 sdm.tar
4      833024 Dec 14 2006 08:25:38 +00:00 es.tar
5      1052160 Dec 14 2006 08:25:54 +00:00 common.tar
6         1038 Dec 14 2006 08:26:08 +00:00 home.shtml
7      102400 Dec 14 2006 08:26:22 +00:00 home.tar
8      491213 Dec 14 2006 08:26:40 +00:00 128MB.sdf

41836544 bytes available (22179840 bytes used)
```



CertificationKits

2014 Copyright CertificationKits LLC

The “**show flash**” command displays contents of flash memory. It displays the image filename along with size and date/time created.

Prior installing a new IOS image you may need to erase an existing image in order to make room for the new image. You can determine this by looking at the last line of the “**show flash**” command as it displays how much flash memory if available along with how much is already used.

show version Command

```
Router# show version
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(12), RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 17-Nov-06 10:44 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

PIR2 uptime is 1 hour, 7 minutes
System returned to ROM by power-on
System image file is "flash:c1841-advipservicesk9-mz.124-12.bin"
...

Cisco 1841 (revision 6.0) with 115712K/15360K bytes of memory.
Processor board ID FTX1050W07X
2 FastEthernet interfaces
2 Serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
31360K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2142
```



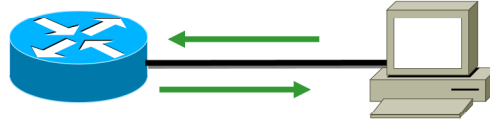
CertificationKits

2014 Copyright CertificationKits LLC

The “**show version**” command will provide basic configuration for the system hardware as well as the software version, the names and sources of configuration files, and the boot images .

The last information given from this command is the value of the configuration register. In this example, the value is 0x2142. Typical settings are 0x2102 and 0x2142. Configuration register settings will be covered in detail later in the course.

Backing up / Restoring the Cisco IOS and Configuration



IOS

`copy flash tftp`
`copy tftp flash`

Configuration

`copy run start`
`copy start run`
`copy run tftp`
`copy tftp run`

2014 Copyright CertificationKits LLC



This slide lists the various commands that can be used to both backup and restore the IOS and configuration of a device.

Each of the commands listed on the slide will be covered in more detail on subsequent slides.

Preparing to Copy IOS to TFTP server

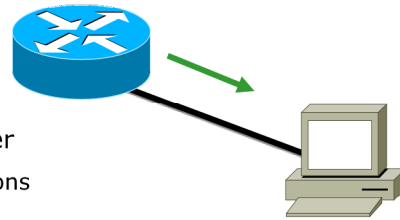
Verify the IOS file name

show version: Displays the IOS file name that the router is running

show flash: shows all files in flash memory

Verify the host

- Can be accessed (ping)
- There is space for the file
- Location of the file on the server
 - Directory and naming conventions



2014 Copyright CertificationKits LLC

CertificationKits

Before you upgrade or restore a Cisco IOS, you really should copy the existing file to a *TFTP host* as a backup just in case the new image crashes and burns.

You can use any TFTP host to accomplish this. By default, the flash memory in a router is used to store the Cisco IOS.

But before you backup an IOS image to a network server, you've got to do these three things:

- Make sure you can access the network server.
- Ensure the network server has adequate space for the code image.
- Verify the file name and path requirement.

On unix-based TFTP servers it may be necessary to create the file using the 'touch' command, and change the file security properties by doing a 'chmod' command.

Copy TFTP Flash

Copy the IOS from a TFTP host to a router (Upgrading an IOS Image from the Network)

Router# **copy tftp flash**

- **confirm router non-functionality**
- **source host name**
- **source filename**
- **destination filename**
- **confirm erase flash**



2014 Copyright CertificationKits LLC

CertificationKits

What happens if you need to restore the Cisco IOS to flash memory to replace an original file that has been damaged, or if you want to upgrade the IOS?

No worries—you just download the file from a TFTP host to flash memory by using the “**copy tftp flash**” command. This command requires the IP address of the TFTP host and the name of the file you want to download.

But before you begin, make sure that the file you want to place in flash memory is in the default TFTP directory on your host since when you issue the command, TFTP won't ask you where the file is.

In many cases, files will end in .bin, and some operating systems like Windows will truncate or hide the file extension. You will still need to specify this when prompted during the download.

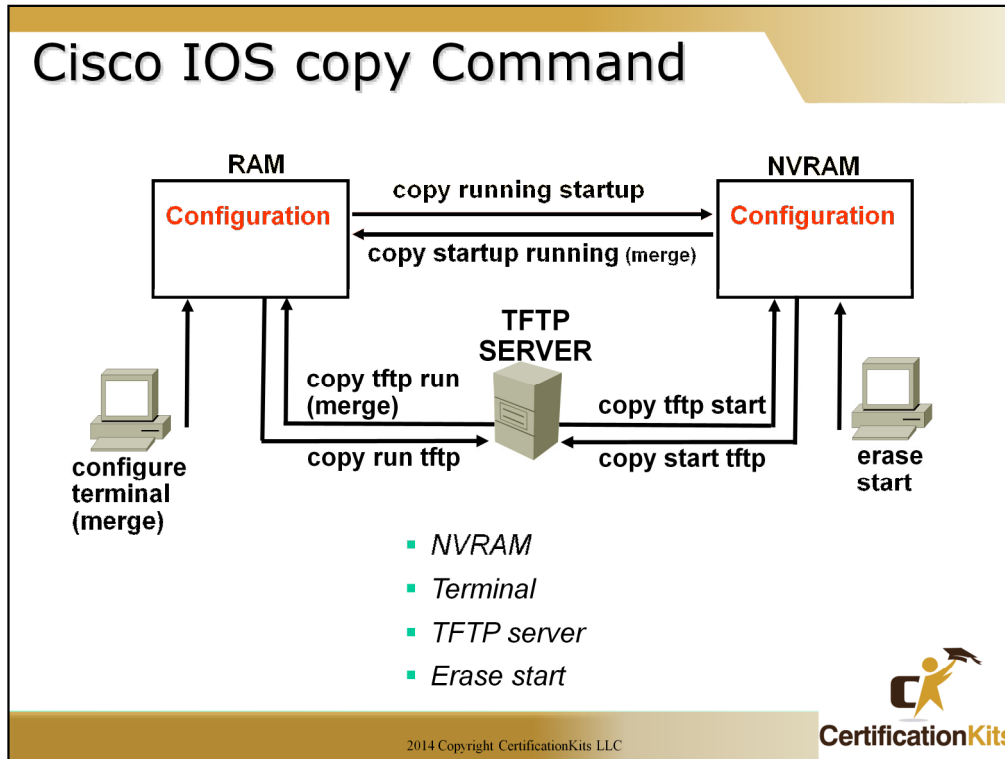
If you don't have enough room in flash memory to store both copies, or if the flash memory is new and no file has been written to flash memory before, the router will ask to erase the contents of flash memory before writing the new file into flash memory. Make sure you have a copy of the image file somewhere on your TFTP server in case restore becomes necessary.

The full syntax of the command is as follows:

```
copy tftp:[location]/directory/filename flash-filesystem:[filename]
```

You can also use **ftp** versus **tftp** using the following command:

```
copy ftp:[username[:password]@]location/directory/filename  
flash-filesystem:[filename]
```



The above commands are just some of the commands to copy router configuration files from one place to another. Note the **copy startup running** and **copy tftp running-config** commands merge the source file with the running-config it does not perform a complete replacement like the other commands.

To erase the startup-config use the **erase startup-config** or **write erase** commands.

Note: In place of **tftp**, **ftp** or **rcp** can be utilized. Parameters for the respective **ftp** and **rcp** qualifiers differ from the **tftp** parameters.

Cisco IOS copy Command Example

running-config

```
interface s0/0/0
 ip address 10.1.1.1 255.255.255.0

interface fa0/0
 ip address 10.2.2.2 255.255.255.0

interface fa0/1
 no ip address
```

TFTP Server saved.cfg

```
interface fa0/0
 ip address 172.16.1.1 255.255.255.0

interface fa0/1
 ip address 192.168.1.1 255.255.255.0
```

copy tftp run (merged)

Resulting running-config

```
interface s0/0/0
 ip address 10.1.1.1 255.255.255.0

interface fa0/0
 ip address 172.16.1.1 255.255.255.0

interface fa0/1
 ip address 192.168.1.1 255.255.255.0
```



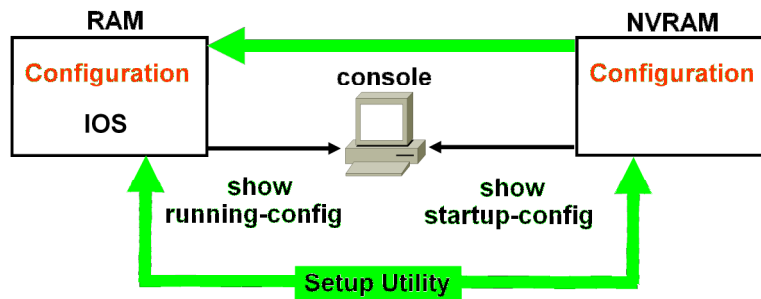
CertificationKits

2014 Copyright CertificationKits LLC

The example on the slide shows how when performing a **copy tftp running-config** or a **copy startup-config running-config** the files are merged, not replaced.

Note that s0/0/0 has an ip address configured in the running-config but not on the tftp server but still exists in the running-config after the copy command was issued. Also, the fa0/0 interface is different in the initial running-config than on the tftp server. It has been updated in the running-config after the copy. Finally, fa0/1 did not have an ip address assigned in the initial running-config but it had one on the tftp server. The running-config after the copy has the ip address configured on fa0/1.

Loading the Configuration



- Load and execute the configuration from NVRAM
- If no configuration is present in NVRAM, enter setup mode



CertificationKits

2014 Copyright CertificationKits LLC

Using the default config register value (0x2102), the router will load the config from NVRAM at startup. If no configuration is present the router will go into setup mode. If a different config register value is set (i.e. 0x2142) the startup file, if present, will be ignored and again the router will go into setup mode.

show and debug Commands

	show	debug
Processing characteristic	Static	Dynamic
Processing load	Low overhead	High overhead
Primary use	Gather facts	Observe processes



CertificationKits

2014 Copyright CertificationKits LLC

Show commands provide a snapshot of information on a router or switch. For example, interface statistics.

Debug commands are used to check the flow of protocol traffic to resolve problems.

Examples of some show commands:

show ip route – Displays the IP routing table

show running-config – Displays the running (active) configuration file

show startup-config – Displays the configuration file stored in NVRAM

show version – Displays the IOS version the router is running along with other things (i.e. config-register setting)

show ip interface – Displays the usability of interfaced configured for IP

show ip interface brief – Displays a summary of the usability status information for each interface

Examples of some debug commands:

debug ip icmp – Displays information on ICMP transactions

debug ip rip – Displays information on RIP routing transactions

debug ip routing – Displays information on Routing Information Protocol (RIP) routing table and route cache updates

debug ip ssh – Displays debug messages for Secure Shell (SSH)

debug ip ospf packet – Displays information about each Open Shortest Packet First (OSPF) packet received

Commands Related to debug

service timestamps debug datetime msec

- *Adds a time stamp to a debug or log message*

show processes

- *Displays the CPU utilization for each process*

no debug all/undebug all (un all)

- *Disables all debug commands*

terminal monitor

- *Displays debug output on your current vty session*



CertificationKits

2014 Copyright CertificationKits LLC

When debugging it is always a good idea to have time synchronized and utilize the time when displaying debug messages. This is accomplished with the following command:

service timestamps debug datetime msec

Debugging can be very CPU intensive. It is a good idea to monitor CPU utilization when debugging. This is accomplished with the following command:

show processes

In order to disable all active debugging with a single command, use the following:

no debug all or undebug all

By default debug messages go to the console. If you are remotely accessing the router via a vty line you will need to perform the following command in order to view the debug messages:

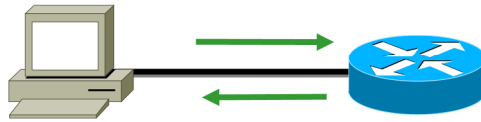
terminal monitor

Backing up the configuration

Copy the configuration to a TFTP host and back

Router# copy running-config tftp

Router# copy tftp running-config



2014 Copyright CertificationKits LLC



To copy the router's configuration from a router to a TFTP host, you can use either the “**copy running-config tftp**” or the “**copy startup-config tftp**” command.

Either one will back up the router configuration that's currently running in DRAM, or that's stored in NVRAM. Note: In order to save off the most current configuration, make sure the startup file matches the running configuration if you plan on utilizing the “**copy startup-config tftp**” command.

If you've changed your router's running-config and want to restore the configuration to the version in startup-config, the easiest way to do this is to use the “**copy startup-config running-config**” command (“**copy start run**” for short).

Note: When you copy or paste a configuration into RAM, the interfaces are shutdown by default. This is especially important if you are configuring the router for the first time, and will be shipping it out to a location where you will not have access to it unless the interface is up. To prevent this, insert “**no shutdown**” commands under each interface needed to at least obtain access to the device.

Fallback

The following commands can be utilized to have a router boot an IOS image from another source:

```
Router# config t
Router(config)# boot system flash ios_filename
Router(config)# boot system tftp ios_filename tftp_address
Router(config)# boot system rom
```

Note: Flash, TFTP server, ROM will be attempted in that order



CertificationKits

2014 Copyright CertificationKits LLC

Cisco routers, by default, load the IOS from Flash memory. However, what happens if the flash memory fails or the file in flash memory becomes corrupted?

By default, the Cisco routers will look for a TFTP server to load an IOS from, and if that fails, some routers, depending on the model, will load a mini-ios from ROM so that an IOS can be restored into flash memory.

Command syntax and parameter descriptions:

boot system flash [*flash-fs:*] [*partition-number:*] [*filename*]

flash-fs: (Optional) Flash file system containing the system image to load at startup. The colon is required.

partition-number: (Optional) Number of the flash memory partition that contains the system image to boot, specified by the optional *filename* argument. If you do not specify a filename, the router loads the first valid file in the specified partition of flash memory. This argument is only valid on routers that can be partitioned.

filename (Optional when used with the **boot system flash** command) Name of the system image to load at startup. This argument is case sensitive. If you do not specify a *filename*, the router loads the first valid file.

Command syntax is similar for **boot system tftp** and **boot system rom** commands.

ROM Monitor Mode

- **If the IOS in Flash is corrupt or missing and no network connectivity is available, and the default fallback procedure fails:**
 - The router will enter ROM monitor mode

```
System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE  
(fc1)  
Copyright (c) 1999 by cisco Systems, Inc.  
TAC:Home:SW:IOS:Specials for info  
C2600 platform with 65536 Kbytes of main memory  
rommon 1 >  
rommon 2 > confreg 0x2142  
You must reset or power cycle for new config to take effect  
rommon 3 > i
```

**Remember: when you boot your router and see “rommon” this is bad!
You’ re IOS in flash is missing or corrupt.**

2014 Copyright CertificationKits LLC

CertificationKits

In the above example, the router was rebooted and the ctrl-break key stroke was pressed, which took the router into ROM monitor mode.

You would do this to provide password recovery by changing the configuration register to 0x2142, as shown above.

When you have completed the password recovery, set the configuration register back to 0x2102 for normal operation.

The default for a router is to look in flash memory for the IOS, NVRAM for the startup-config

If this fails, the default is to look in flash, then look for a TFTP server on a network, then run a mini-ios from ROM.

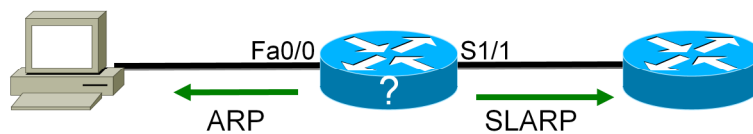
If all this fails, then the router will load ROM monitor mode.

Auto-Install

Issue the following commands to stop a router from attempting to pull a configuration from another router or from a network host:

```
Router(config)# no service config
```

```
Router(config)# no boot network
```



2014 Copyright CertificationKits LLC



The auto-install “feature” is annoying at best. If a router is powered up, has no configuration and sees Carrier Detect on an interface, it will look for an IP address by using ARP on a LAN and/or SLARP (Serial Line ARP) on a serial interface.

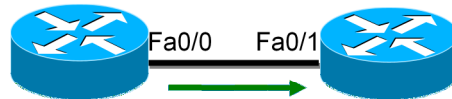
You can disable this feature with the “**no service config**” command and the “**no boot network**” command from global configuration mode.

Making Your Router a TFTP Server

Issue the following commands to make your router a TFTP server

```
Router# config t
```

```
Router(config)# tftp-server flash: [press tab or ?]
```



Connect your two routers together with a LAN connection, then copy the IOS with the **copy tftp flash** command.



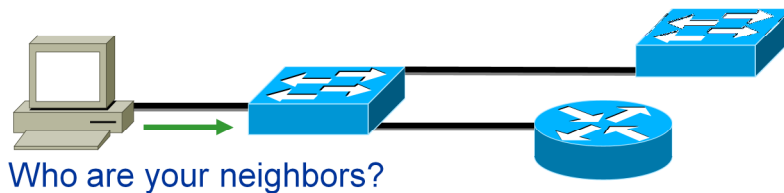
CertificationKits

2014 Copyright CertificationKits LLC

Now this is a great feature of a Cisco router! If you do not have a laptop or other host that can provide TFTP services, you can make a router a TFTP server with the global configuration command “**tftp-server flash:**”. You will then need to make sure the file (i.e. IOS image) is available on the router you configured as a tftp server. It is as simple as that, you can now copy the image from the router configured as a tftp server allowing upgrade or downgrade of your other router.

Cisco Discovery Protocol

- Cisco Proprietary
- Gathers information about other Cisco neighbor devices only
- Turned on by default on all Cisco routers and switches
- Operates at layer two



2014 Copyright CertificationKits LLC



Cisco Discovery Protocol (CDP) is a proprietary protocol designed by Cisco to help administrators collect information about both locally attached and remote devices.

By using CDP, you can gather hardware and protocol information about neighbor devices, regardless of the routed protocols enabled on the interface since it operates at layer 2. This is very useful information for troubleshooting and documenting your Cisco-based networks. CDP is turned on by default on all Cisco routers and switches.

Cisco Discovery Protocol

Show commands

```
show cdp
show cdp neighbors
show cdp neighbors detail
show cdp entry *
show cdp interface
show cdp traffic
```

Global Config

```
cdp holdtime
cdp timer
cdp run
```

Interface

```
cdp enable
```



CertificationKits

2014 Copyright CertificationKits LLC

The “**show cdp neighbor**” command (**sh cdp nei** for short) delivers information about directly connected devices.

It’s important to remember that CDP packets aren’t passed through a Cisco switch, and that you only see what’s directly attached. So this means that if your a router is connected to a switch, you won’t see any of the devices hooked up to that switch, you will need to get that information from the switch itself.

Another valuable CDP command to get more information about a neighbor is the “**show cdp neighbor detail**” command (**show cdp nei de** for short). This command can be run on both routers and switches, and it displays detailed information about each device connected to the device you’re running the command on.

The “**show cdp entry ***” command is the same as “**show cdp nei detail**”. However, on a router or switch, type “**show cdp entry * ?**” and you’ll see there are two helpful subcommands you can use.

show cdp neighbors

S1# **show cdp neighbors**

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
R2	Fas 0/1	170	R S I	Cisco 2811	Fas 0/0
R3	Fas 0/2	178	R	Cisco C804	Eth 0
S2	Fas 0/12	171	S I	WS-C3550-2	Fas 0/2
S2	Fas 0/11	171	S I	WS-C3550-2	Fas 0/1

Who are your neighbors?

CertificationKits

2014 Copyright CertificationKits LLC

Field Descriptions:

Device ID - The configured ID (name), MAC address, or serial number of the neighbor device.

Local Intrfce - (Local Interface) The protocol being used by the connectivity media.

Holdtime - (Holdtime) The remaining amount of time, in seconds, the current device will hold the CDP advertisement from a transmitting router before discarding it.

Capability – The capability code discovered on the device. This is the type of the device listed in the CDP Neighbors table.

Platform – The product number of the device.

Port ID – The protocol and port number of the device.

Command syntax:

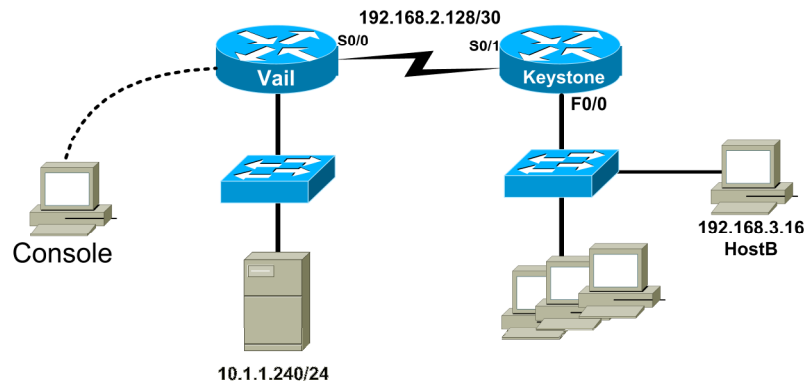
show cdp neighbors [*type number*] [**detail**]

type - (Optional) Type of the interface connected to the neighbors about which you want information.

number - (Optional) Number of the interface connected to the neighbors about which you want information.

detail - (Optional) Displays detailed information about a neighbor (or neighbors) including network address, enabled protocols, hold time, and software version.

Using CDP Example



You can only console into the Vail router and it is not configured....How can you get the Keystone 's IP address so you can configure Vail with the correct IP address? In addition, HostB needs to be able to ping the server. How will this be accomplished?



CertificationKits

2014 Copyright CertificationKits LLC

1. You first need to administratively mark up the s0/0 interface on the Vail router so you can receive CDP information

```
Vail>enable
```

```
Vail#config t
```

```
Vail(config)#int s0/0
```

```
Vail(config-if)#no shutdown
```

2. You need to find the Keystone routers IP address and set the address of the Vail s0/0 to the next address in the available pool

```
Vail(config-if)#exit
```

```
Vail(config)#exit
```

```
Vail#show cdp neighbors detail
```

3. Once you find the IP address of the Keystone router, configure the Vail interface with the correct IP address – the next available IP address in the pool.

4. Telnet from the Vail router into the Keystone router and verify the configuration. Enable the F0/0 with a **no shutdown** if needed.

5. Finally, connect to HostB and make sure you can ping the server at 10.1.1.240.

Telnet

From a host prompt:

```
> telnet ip_address
```

From a router prompt:

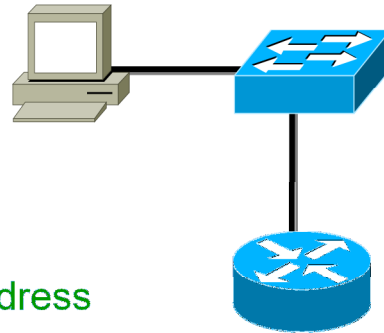
```
RouterA# telnet ip_address
```

Suspending and resuming a telnet session:

```
RouterB# [ctrl]-[shift]-6 then x
```

```
RouterA# show sessions
```

```
RouterA# resume <session#>
```



2014 Copyright CertificationKits LLC



Telnet is a virtual terminal protocol that's part of the TCP/IP protocol suite that allows you to make connections to remote devices, gather information, and run programs.

After your routers and switches are configured, you can use the Telnet program to reconfigure and/or troubleshoot your routers and switches without using a console cable.

You run the Telnet program by typing **telnet** from any command prompt (DOS or Cisco).

In order to be able to remotely telnet to your router or switch, you have to have the VTY passwords set. Otherwise, the router or switch will prompt that password is not set, and not permit the remote login.

If you telnet to a router or switch, you can end the connection by typing **exit** at any time, but what if you want to keep your connection to a remote device but still come back to your original router console?

To do that, you can press the Ctrl+Shift+6 key combination, release it, and then press X.

Another common practice is to telnet and specify a port or socket. This is useful when accessing a device hanging off of a terminal server, or when testing listener ports or firewall access rules.

```
Router# telnet 10.10.10.10 80
```

Open

The open indicates the port is listening, and access is not blocked by a firewall or ACL.

Another telnet method is to telnet to the host, and specify a source address. This can be useful when trying to verify routing to a specific subnet or host address on the router. An example would be:

```
telnet 10.10.10.10 /source-interface Ethernet0/0
```

Telnet (cont'd)

- **show sessions:** displays your open sessions
- **disconnect:** closes current session open by you
- **show users:** shows connection open by a remote device
- **clear line:** closes a session open by a remote device
- **terminal monitor:** displays console output to a telnet session



CertificationKits

2014 Copyright CertificationKits LLC

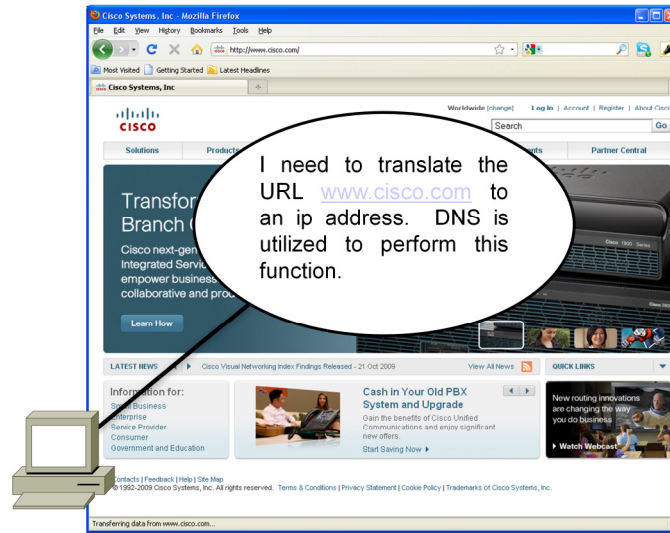
To see the connections made from your router to a remote device, use the “**show sessions command**”.

You can list all active consoles and VTY ports in use on your router with the “**show users command**”.

You can end Telnet sessions a few different ways—typing “**exit**” or “**disconnect**” is probably the easiest and quickest.

Although the console port always monitors, when accessing the router or Catalyst IOS switch using telnet/vty session, the “**terminal monitor**” command will display all console output to the telnet session.

Domain Name System (DNS)



2014 Copyright CertificationKits LLC



Domain Name System (DNS) is utilized to translate symbolic names (i.e. www.cisco.com) into IP addresses which are utilized for communication at Layer3 of the OSI reference model. DNS makes the Internet more useable as users do not have to remember IP addresses but instead can utilize names.

Resolving Host Names

Building a Hosts table

```
Router(config)# ip host hostname ip_address  
Router(config)# ip host RouterC 172.16.40.2
```

Verify the Hosts table

```
Router# show hosts
```



The **show hosts** command show temporary DNS entries and permanent IP host entries

DNS Server

```
Router(config)# ip domain-lookup  
Router(config)# ip name-server <ip address> (up to 8)  
Router(config)# ip domain-name mydomain.com
```



2014 Copyright CertificationKits LLC

CertificationKits

In order to use a hostname rather than an IP address to connect to a remote device, the device that you are using to make the connection must be able to translate the hostname to an IP address.

There are two ways to resolve hostnames to IP addresses: building a local host table on each router or building a Domain Name System (DNS) server, which is kind of like a global host table for all devices to access.

A local host table provides name resolution only on the router that it was built on. The command to build a host table on a router is:

“ip host name tcp_port_number ip_address”

The default is TCP port number 23 but you can create a session using Telnet with a different TCP port number if you want. You can also assign up to eight IP addresses to a hostname.

To view the newly built host table, use the **“show hosts”** command, which shows the temporary DNS entries and permanent IP host entries.

In lab scenarios, or when you will be performing many commands from EXEC, you may want to utilize the **“no ip domain-lookup”** command from global configuration mode. This is usually a huge timesaver; especially if you make syntax errors while typing. Without it turned off, the router will assume a mistyped command is a hostname and will query DNS. The time it takes to perform the lookup on a bogus command may seem like an eternity.

Basic Testing



Router# ping

- Uses ICMP echo request and replies. Can be used from user mode and privilege mode, but not from configuration mode. Extended mode provides multiple protocol ping support. Can be used from a router/switch as well as most servers.

Router# traceroute (Microsoft uses tracert)

- Uses TTL timeouts with ICMP error messages to find the path a packet takes through an internetwork. Can be used from a router/switch as well as most servers.



CertificationKits


2014 Copyright CertificationKits LLC

You can use the **ping** and **traceroute** commands to test connectivity to remote devices, and both of them can be used with many protocols, not just IP.

Although the router may use ICMP for traceroute, many hosts use the UDP version. This can return inconsistent results when traversing a firewall and needs to be kept in mind when obtaining traceroute information from system administrators.

Show/ping/traceroute

Router Output




Interface Testing

```
Router1#show ip interface brief
Interface      IP-Address      OK? Method Status Protocol
FastEthernet0/0 192.168.254.254 YES NVRAM  up      up
FastEthernet0/1/0 unassigned      YES unset  down    down
Serial10/0/0    172.16.0.254   YES NVRAM  up      up
Serial10/0/1    unassigned      YES unset  administratively down down

Router1#ping 192.168.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Router1#traceroute 192.168.0.1
Type escape sequence to abort.
Tracing the route to 192.168.0.1
 0 172.16.0.253 8 msec 4 msec 8 msec
 1 172.16.0.253 8 msec 4 msec 8 msec
 2 10.0.0.254 16 msec 16 msec 8 msec
 3 192.168.0.1 16 msec * 20 msec
```

2014 Copyright CertificationKits LLC


CertificationKits

The “**show ip interface brief**” command is a very useful command to quickly see the status of all interfaces. Having both status and protocol in an up state indicates the interface is active and ready to pass traffic.

You can utilize either the **ping** or **traceroute** commands to test if packets can traverse the network. In the example on the slide, the “!” in the output of the ping indicates a success. By default a ping will send out 5 packets, hence the 5 “!”. In this case all 5 packets were successful. Other potential responses are “U” for unreachable and “.” for ????????????????

As mentioned earlier, a traceroute is utilized to determine all hops along a path to a destination. It sends an ICMP packet with a Time to Live (TTL) of 1 and receives an ICMP unreachable message from the first hop when the TTL is decremented to 0. It then sends an ICMP packet with a TTL of 2 and receives an ICMP unreachable message from the second hop when the TTL is decremented to 0. This is performed again and again till the ICMP packet is initially sent with a large enough TTL to reach the ultimate destination. In the end you have a complete map of all hops along the way from source to destination.

Chapter 3 Summary

- Learned how to backup / restore router configurations and IOS images.
 - Sample commands are as follows:
 - copy tftp startup (restores configuration from tftp server)
 - copy startup tftp (saves a copy of the config to a tftp server)
 - copy tftp flash (copies an IOS image to the router)
 - copy flash tftp (copies an IOS image to a tftp server)
- Learned about telnet and console connection management.
- Learned basic testing/troubleshooting commands (ping and traceroute).
- Cisco Discovery Protocol (CDP) - Works at layer 2 to discover other Cisco devices. Works even if no layer 3 addresses are configured.

