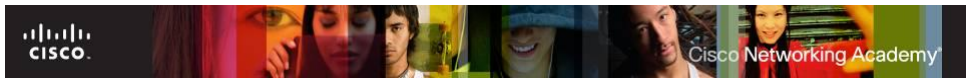
Configuring and Testing Your Network

Network Fundamentals – Chapter 11

Cisco Networking Academy®
Mind Wide Open™



Objectives

Define the role of the Internetwork Operating System (IOS)

Use Cisco CLI commands to perform basic router and switch configuration and verification

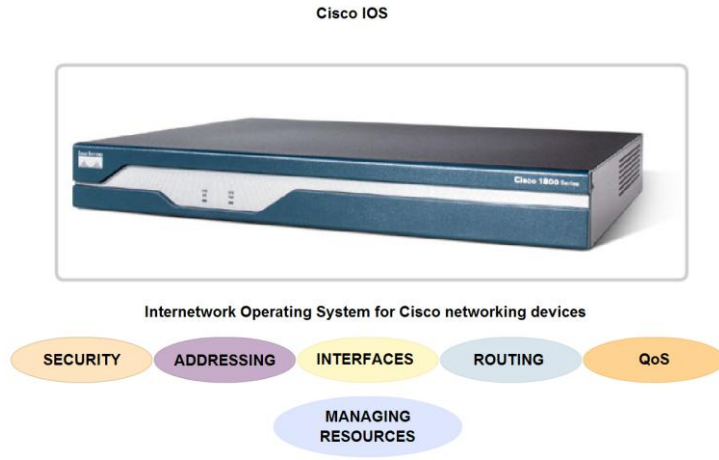
Given a network addressing scheme, select, apply, and verify appropriate addressing parameters to a host

Use common utilities to verify network connectivity between hosts

Use common utilities to establish a relative performance baseline for the network

Role of Internetwork Operating System (IOS)

Identify several classes of devices that have IOS embedded



IOS Introduction

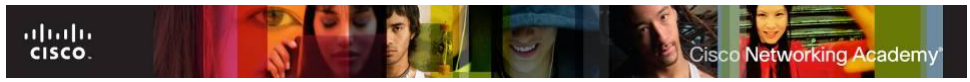
The Cisco IOS is used for most Cisco devices regardless of the size and type of the device.

It is used for routers, LAN switches, small Wireless Access Points, large routers with dozens of interfaces, and many other devices.

The Cisco IOS provides devices with the following network services:

1. Basic routing and switching functions
2. Reliable and secure access to networked resources
3. Network scalability

The IOS operational details vary on different internetworking devices, depending on the device's purpose and feature set.



IOS Introduction

The IOS file itself is several megabytes in size and is stored in a semi-permanent memory area called flash. Flash memory provides non-volatile storage.

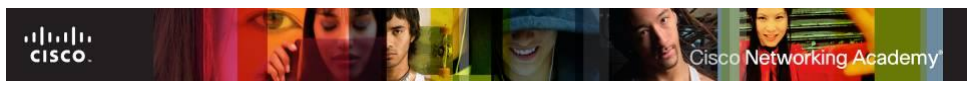
This means that the contents of the memory are not lost when the device loses power.

Even though the contents are not lost they can be changed or overwritten if needed.

Using flash memory allows the IOS to be upgraded to newer versions or to have new features added.

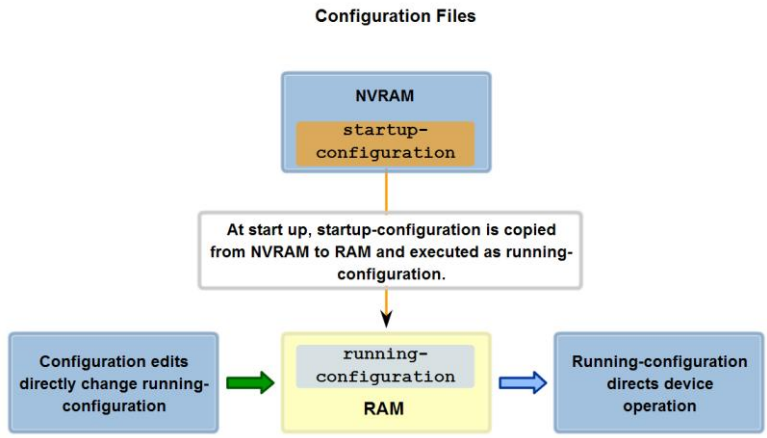
In many router architectures, the IOS is copied into RAM when the device is powered on and the IOS runs from RAM when the device is operating.

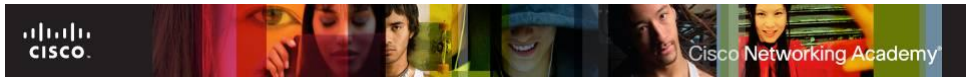
This function increases the performance of the device.



Role of Internetwork Operating System (IOS)

Define the purpose of startup config.





Start-up Configuration

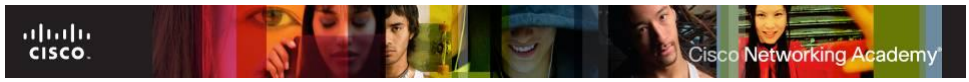
The startup configuration file (startup-config) is used during system startup to configure the device.

The startup configuration file or startup-config file is stored in non-volatile RAM (NVRAM).

Since NVRAM is non-volatile, when the Cisco device is turned off, the file remains intact.

The startup-config files are loaded into RAM each time the router is started or reloaded.

Once the configuration file is loaded into RAM, it is considered the running configuration or running-config.



Running-Config

The running configuration is modified when the network administrator performs device configuration.

Changes to the running configuration will immediately affect the operation of the Cisco device.

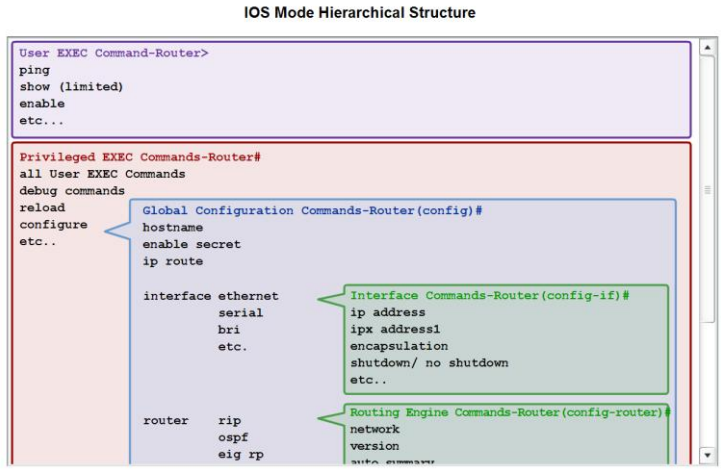
After making any changes, the administrator has the option of saving those changes back to the startup-config file so that they will be used the next time the device restarts.

Because the running configuration file is in RAM, it is lost if the power to the device is turned off or if the device is restarted.

Changes made to the running-config file will also be lost if they are not saved to the startup-config file before the device is powered down.

Role of Internetwork Operating System (IOS)

Recognize that Cisco IOS is modal and describe the implications of modes.



Router Modes

In order from top to bottom, the major modes are:

1. User executive mode
2. Privileged executive mode
3. Global configuration mode
4. Other specific configuration modes

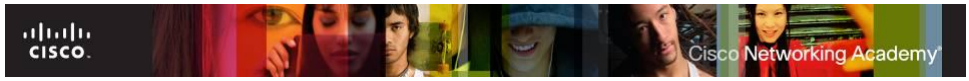
Each mode is used to accomplish particular tasks and has a specific set of commands that are available when in that mode.

For example, to configure a router interface, the user must enter interface configuration mode.

All configurations that are entered in interface configuration mode apply only to that interface.

Some commands are available to all users; others can be executed only after entering the mode in which that command is available.

Each mode is distinguished with a distinctive prompt, and only commands that are appropriate for that mode are allowed.



Role of Internetwork Operating System (IOS)

Define the different modes and identify the mode prompts in the CLI

IOS Primary Modes

User EXEC Mode
Limited examination of router.
Remote access.

```
Switch>
Router>
```

Global Configuration Mode
Simple configuration commands.

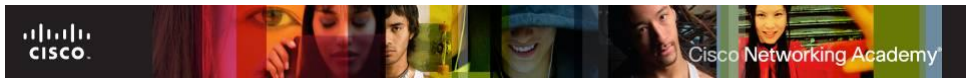
```
Switch(config)#
Router(config)#
```

Privilleged EXEC Mode
Detailed examination of router, Debugging and testing. File manipulation. Remote access.

```
Switch#
Router#
```

Other Configuration Modes
Complex and multiple-line configurations.

```
Switch(config-mode)#
Router(config-mode)#
```

Primary Modes:

The user executive mode: has limited capabilities but is useful for some basic operations. The user EXEC mode is at the top of the modal hierarchical structure. This mode is the first entrance into the CLI of an IOS router.

The user EXEC mode allows only a limited number of basic monitoring commands. This is often referred to as view-only mode. The user EXEC level does not allow the execution of any commands that might change the configuration of the device.

Privileged Exec Mode:

The execution of configuration and management commands requires that the network administrator use the privileged EXEC mode, or a specific mode further down the hierarchy.

The privileged EXEC mode can be identified by the prompt ending with the # symbol.

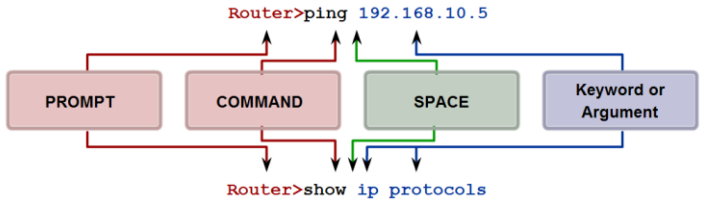
Switch#

By default, privileged EXEC does not require authentication. It is a good practice to ensure that authentication is configured.

Role of Internetwork Operating System (IOS)

Identify the basic command structure for IOS commands

Basic IOS Command Structure



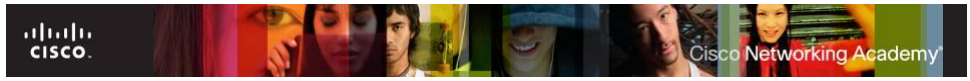
Prompt commands are followed by a space and then the keyword or arguments.

Command Conventions

IOS Command Conventions

When describing the use of commands, we generally use these conventions.

Convention	Description
boldface	Boldface text indicates commands and keywords that are entered literally as shown.
italics	Italic text indicates arguments where the user supplies values.
[X]	Square brackets enclose an optional element (keyword or argument).
|	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[X | Y]	Square brackets enclose an optional element (keyword or argument).
{X | Y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.



Role of Internetwork Operating System (IOS)

Identify the types of help and feedback available while using IOS and use these features to get help, take

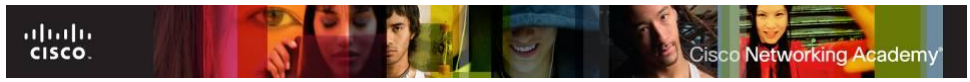
Context Sensitive Help

Example of a sequence of commands using the CLI context sensitive help

```
Cisco#cl?
clear  clock
Cisco#clock ?
  set  Set the time and date
Cisco#clock set
% Incomplete command.
Cisco#clock set ?
  hh:mm:ss  Current Time
Cisco#clock set 19:50:00
% Incomplete command.
```

```
Cisco#clock set 19:50:00 ?
  <1-31>  Day of the month
  MONTH   Month of the year
Cisco#clock set 19:50:00 25 6
                            ^
Invalid input detected at '^' marker.
Cisco#clock set 19:50:00 25 June
% Incomplete command.
Cisco#clock set 19:50:00 25 June ?
  <1993-2035>  Year
Cisco#clock set 19:50:00 25 June 2007
Cisco#
```

Command explanations
Incomplete Command messages
Invalid input messages
Variable formats



Context-Sensitive Help

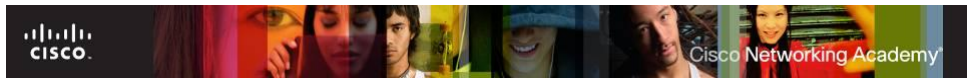
The context-sensitive help provides a list of commands and the arguments associated with those commands within the context of the current mode.

To access context-sensitive help, enter a question mark, ?, at any prompt. There is an immediate response without the need to use the <Enter> key.

One use of context-sensitive help is to get a list of available commands.

This can be used when you are unsure of the name for a command or you want to see if the IOS supports a particular command in a particular mode.

Another use of context-sensitive help is to display a list of commands or keywords that start with a specific character or characters. For example, enter sh? to get a list of commands that begin with the character sequence sh.



Command Syntax Check Help

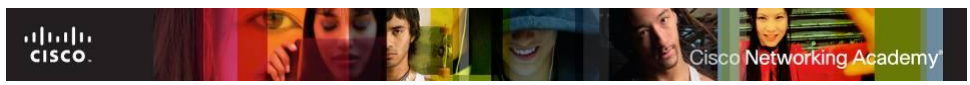
When a command is submitted by pressing the <Enter> key, the command line interpreter parses the command from left to right to determine what action is being requested.

The IOS generally only provides negative feedback. If the interpreter understands the command, the requested action is executed and the CLI returns to the appropriate prompt.

However, if the interpreter cannot understand the command being entered, it will provide feedback describing what is wrong with the command.

There are three different types of error messages:

1. Ambiguous command
2. Incomplete command
3. Incorrect command



Command Syntax Help

The IOS returns a help message indicating that required keywords or arguments were left off the end of the command:

```
Switch#>clock set
% Incomplete command.
Switch#clock set 19:50:00
% Incomplete command.
```

The IOS returns a help message to indicate that there were not enough characters entered for the command interpreter to recognize the command.

```
Switch#c
% Ambiguous command:'c'
```

The IOS returns a "^" to indicate where the command interpreter can not decipher the command:

```
Switch#clock set 19:50:00 25 6
                          ^
% Invalid input detected at '^' marker.
```

Hot Keys and Shortcuts

CLI Hot Keys and Shortcuts

CLI Line Editing	
Tab	Completes a partial command name entry.
Backspace	Erases the character to the left of the cursor.
Ctrl-D	Erases the character at the cursor.

(NOTE: **"Delete"**, the key to erase to the right of the cursor, is not recognized by terminal emulation programs.)

At the `"-----More-----"` prompt	
The Enter Key	Displays the next line.
Space Bar	Displays the next screen.
Any other alphanumeric key	Returns to the EXEC prompt.

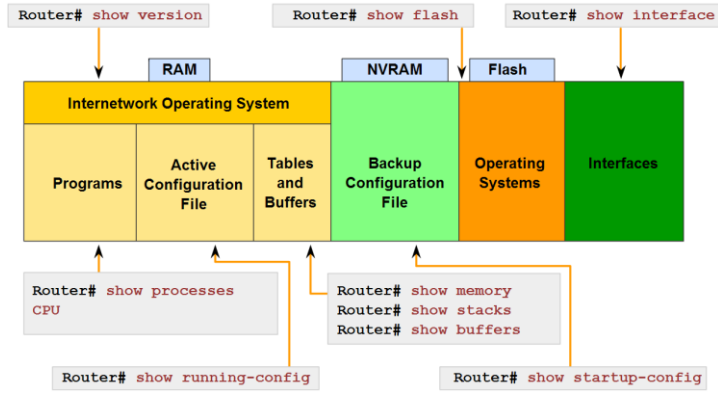
Break Keys	
Ctrl-C	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode. When in setup mode, aborts back to the command prompt.
Ctrl-Z	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode.

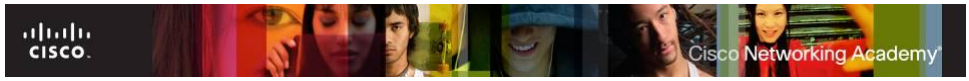
Note: Control keys - Press and hold the <Ctrl> key and then press the specified letter key .
Escape sequences - Press and release the <Esc> key, and then press the letter key.

Role of Internetwork Operating System (IOS)

Identify the purpose of the show command and several of its variations

IOS `show` commands can provide information about the configuration, operation and status of parts of a Cisco router.



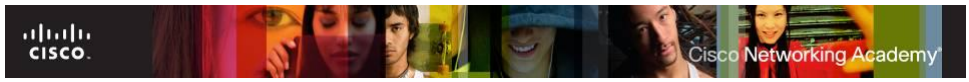


Show Version

Example of IOS Output

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-IPBASEK9-M), Version 12.4(11)T, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Sat 18-Nov-06 15:20 by prod_rel_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

Router uptime is 10 weeks, 4 days, 23 hours, 36 minutes
System returned to ROM by power-on
System restarted at 16:43:31 UTC Fri Jan 26 2007
System image file is "flash:c1841-ipbasek9-mz.124-11.T.bin"

Cisco 1841 (revision 5.0) with 115712K/15360K bytes of memory.
Processor board ID FTX0932W21Y
2 FastEthernet interfaces
2 Low-speed serial(sync/async) interfaces
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
31360K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102

Router#
```

Router#show version

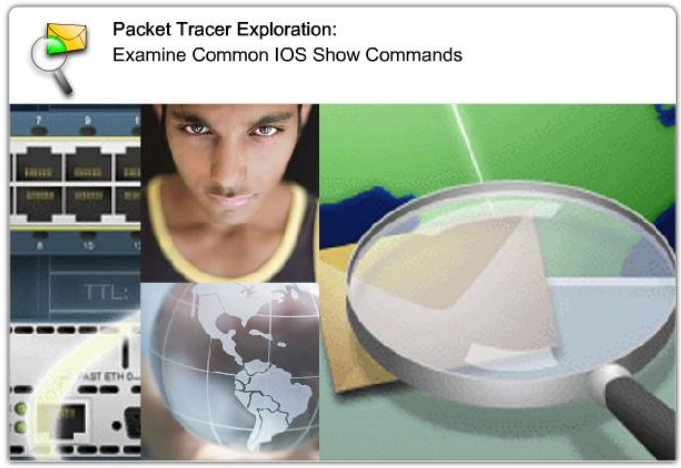


Show Version Output

Some of the information shown from this command are:

1. Software Version - IOS software version (stored in flash)
2. Bootstrap Version - Bootstrap version (stored in Boot ROM)
3. System up-time - Time since last reboot
4. System restart info - Method of restart (e.g., power cycle, crash)
5. Software image name - IOS filename stored in flash
6. Router Type and Processor type - Model number and processor type
7. Memory type and allocation (Shared/Main) - Main Processor RAM and Shared Packet I/O buffering
8. Software Features - Supported protocols / feature sets
9. Hardware Interfaces - Interfaces available on router
10. Configuration Register - Sets bootup specifications, console speed setting, and related parameters.

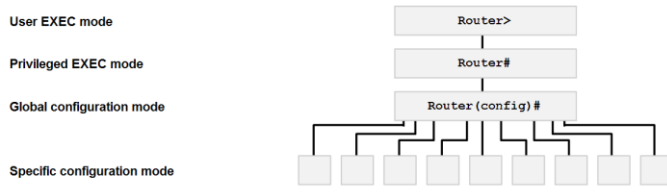
Packet Tracer Lab



Role of Internetwork Operating System (IOS)

Identify several of the configuration modes, their purpose and their associated prompt

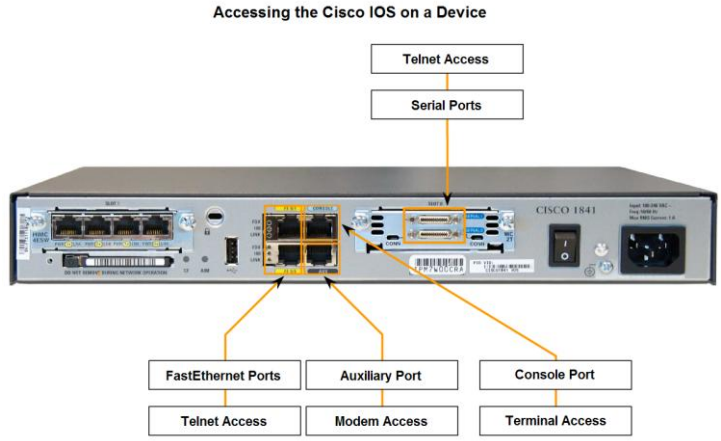
IOS Configuration Modes



Configuration Mode	Prompt
Interface	Router(config-if)#
Line	Router(config-line)#
Routers	Router(config-router)#

Role of Internetwork Operating System (IOS)

Use the CLI to access various IOS configuration modes on a device



CLI Uses

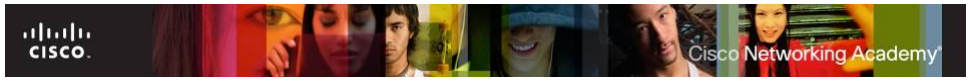
The CLI can be accessed through a console session, also known as the CTY line. A console uses a low speed serial connection to directly connect a computer or terminal to the console port on the router or switch.

The console port is a management port that provides **out-of-band** access to a router.

The console port is accessible even if no networking services have been configured on the device. The console port is often used to access a device when the networking services have not been started or have failed.

Examples of console use are:

1. The initial configuration of the network device
2. Disaster recovery procedures and troubleshooting where remote access is not possible
3. Password recovery procedures



Telnet

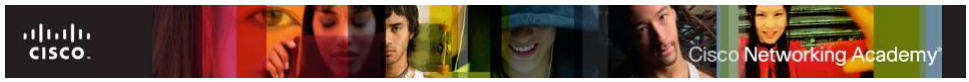
A method for remotely accessing a CLI session is to telnet to the router. Unlike the console connection, Telnet sessions require active networking services on the device.

The network device must have at least one active interface configured with a Layer 3 address, such as an IPv4 address.

Cisco IOS devices include a Telnet server process that launches when the device is started. The IOS also contains a Telnet client.

A host with a Telnet client can access the vty sessions running on the Cisco device.

For security reasons, the IOS requires that the Telnet session use a password, as a minimum authentication method. The methods for establishing logins and passwords will be discussed in a later section.



SSH

The Secure Shell (SSH) protocol is a more secure method for remote device access. This protocol provides the structure for a remote login similar to Telnet, except that it utilizes more secure network services.

SSH provides stronger password authentication than Telnet and uses encryption when transporting session data.

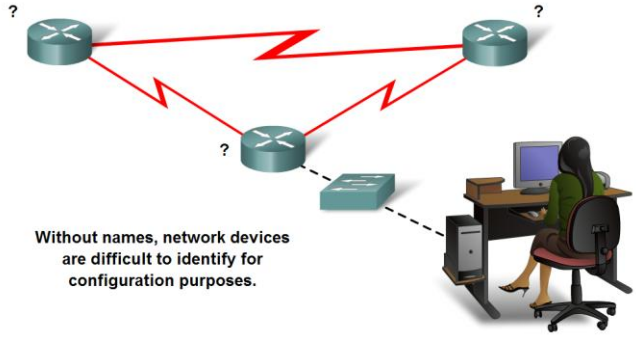
The SSH session encrypts all communications between the client and the IOS device. This keeps the user ID, password, and the details of the management session private.

As a best practice, always use SSH in place of Telnet whenever possible.

Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

Explain the reasons for naming devices.

Basic Configuration Using Cisco IOS



Naming Devices

When accessing a remote device using Telnet or SSH, it is important to have confirmation that an attachment has been made to the proper device.

If all devices were left with their default names, we could not identify that the proper device is connected.

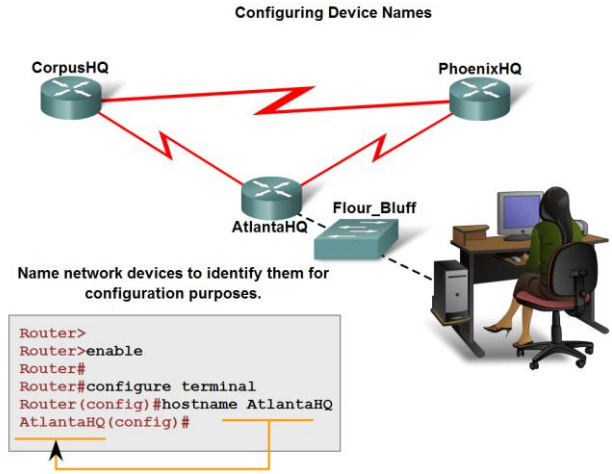
By choosing and documenting names wisely, it is easier to remember, discuss, and identify network devices.

To name devices in a consistent and useful way requires the establishment of a naming convention that spans the company or, at least, the location.

It is a good practice to create the naming convention at the same time as the addressing scheme to allow for continuity within the organization.

Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

Describe two common approaches to establishing naming conventions



Naming Conventions

To create a naming convention for routers, take into consideration the location and the purpose of the devices.

Ask yourself questions such as these: Will these routers be part of an organization's headquarters? Does each router have a different purpose?

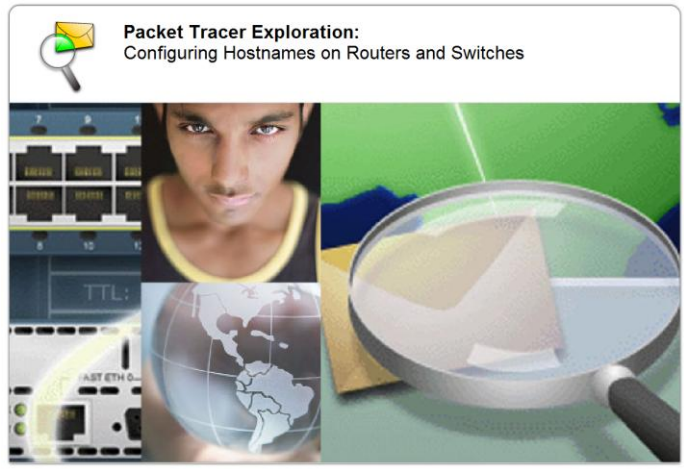
For example, is the Atlanta router a primary junction point in the network or is it one junction in a chain?

In this example, we will identify each router as a branch headquarters for each city.

The names could be AtlantaHQ, PhoenixHQ, and CorpusHQ. Had each router been a junction in a successive chain, the names could be AtlantaJunction1, PhoenixJunction2, and CorpusJunction3.

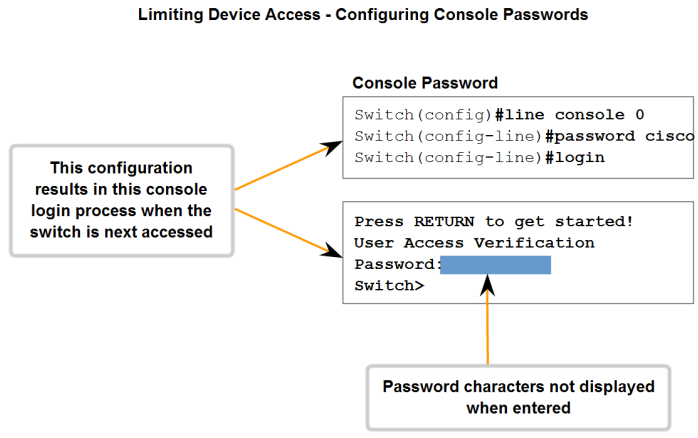
Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

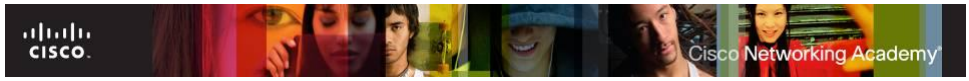
Based on a diagram, configure host names using the CLI



Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

Describe the role of passwords in limiting access to device configurations



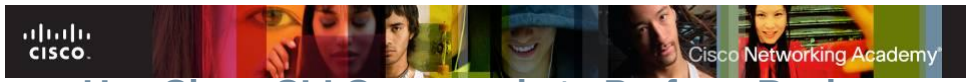


Passwords

The IOS uses hierarchical modes to help with device security. As part of this security enforcement, the IOS can accept several passwords to allow different access privileges to the device.

The passwords introduced here are:

1. Console password - limits device access using the console connection
2. Enable password - limits access to the privileged EXEC mode
3. Enable secret password - encrypted, limits access to the privileged EXEC mode
4. VTY password - limits device access using Telnet



Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

Describe several ways in which access to a device configuration can be limited

Limiting Device Access
Configuring Telnet and Password Encryption

Virtual Terminal Password

```
Router(config)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
```

Enable Password

```
Router(config)#enable password san fran
```

Enable Secret Password

```
Router(config)#enable secret cisco
```

Strongly encrypted password

Additional Security

Enable Secret:

To provide additional security, use the enable password command or the enable secret command. Either of these commands can be used to establish authentication before accessing privileged EXEC (enable) mode.

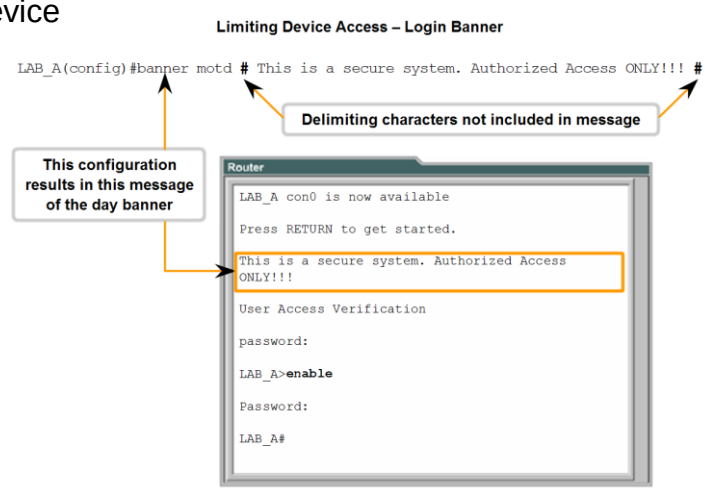
VTY:

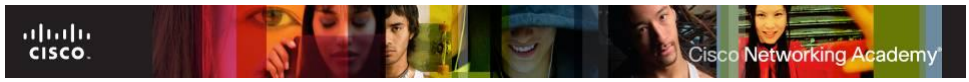
The vty lines allow access to a router via Telnet. By default, many Cisco devices support five VTY lines that are numbered 0 to 4.

A password needs to be set for all available vty lines. The same password can be set for all connections. However, it is often desirable that a unique password be set for one line to provide a fall-back for administrative entry to the device if the other connections are in use.

Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

Use the CLI to set passwords and add banners to a device



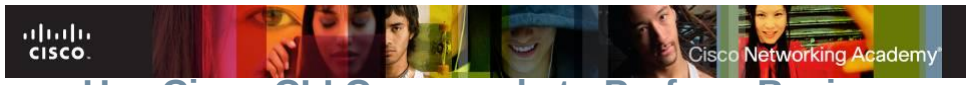


MOTD - Banners

Banners can be an important part of the legal process in the event that someone is prosecuted for breaking into a device. Some legal systems do not allow prosecution, or even the monitoring of users, unless a notification is visible.

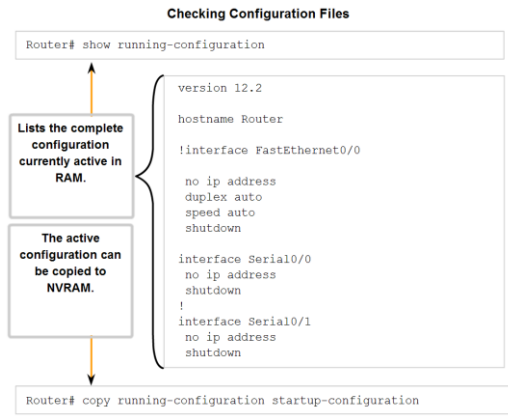
The exact content or wording of a banner depends on the local laws and corporate policies. Here are some examples of information to include in a banner:

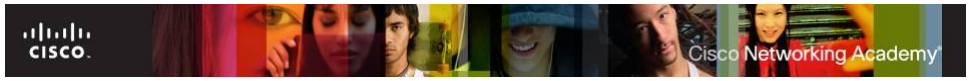
1. "Use of the device is specifically for authorized personnel."
2. "Activity may be monitored."
3. "Legal action will be pursued for any unauthorized use."



Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

Trace the steps used to examine the startup config, make changes to config, and replace the startup config with the running config





Show Run – Copy Run Start

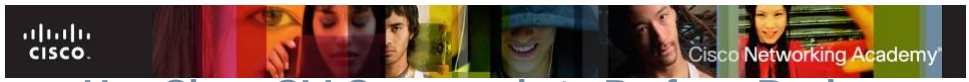
Before committing to the changes, use the appropriate show commands to verify the device's operation. As shown in the figure, the **show running-config** command can be used to see a running configuration file.

When the changes are verified to be correct, use the **copy running-config startup-config** command at the privileged EXEC mode prompt. The following example shows the command:

If the changes made to the running configuration do not have the desired effect, it may become necessary to restore the device to its previous configuration.

Assuming that we have not overwritten the startup configuration with the changes, we can replace the running configuration with the startup configuration.

This is best done by restarting the device using the reload command at the privileged EXEC mode prompt.



Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

Use basic IOS config commands to manage a device.

```
Router#copy running-config tftp
Remote host []? 131.108.2.155
Name of configuration file to write[tokyo-config]?tokyo.2
Write file tokyo.2 to 131.108.2.155? [confirm] y
Writing tokyo.2 !!!!!! [OK]
```


Backing Up Files

Configuration files should be stored as backup files in the event of a problem.

Configuration files can be stored on a Trivial File Transfer Protocol (TFTP) server, a CD, a USB memory stick, or a floppy disk stored in a safe place.

A configuration file should also be included in the network documentation.

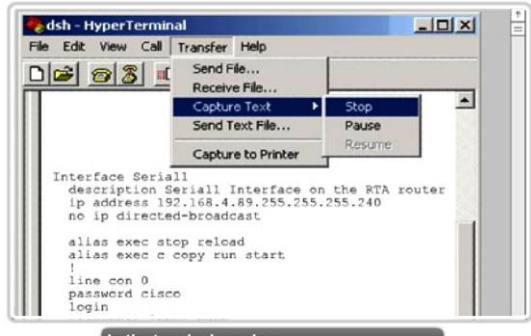
Backup Configuration on TFTP Server

As shown in the figure, one option is to save the running configuration or the startup configuration to a TFTP server. Use either the copy running-config tftp or copy startup-config tftp

Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

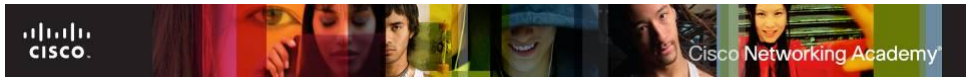
Use a text file to backup and restore config settings

Saving to a Text File in Hyperterminal



In the terminal session:

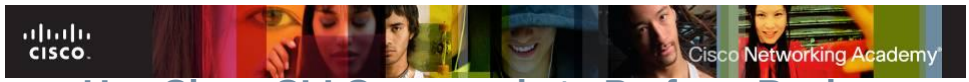
1. Start the text capture process
2. Issue a `show running-config` command
3. Stop the capture process
4. Save the text file



Capturing Text

Configuration files can be saved/archived to a text document. This sequence of steps ensures that a working copy of the configuration files is available for editing or reuse later. When using HyperTerminal, follow these steps:

1. On the Transfer menu, click Capture Text.
2. Choose the location.
3. Click Start to begin capturing text.
4. Once capture has been started, execute the show running-config or show startup-config command at the privileged EXEC prompt. Text displayed in the terminal window will be placed into the chosen file.
5. After the configurations have been displayed, Stop the capture.
6. View the output to verify that it was not corrupted.



Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

Identify the role of a router in a network.

Configuring Router Interfaces

All interfaces are accessed by issuing the `interface` command at the global configuration prompt.

In the following commands, the *type* argument includes serial, ethernet, fastethernet, and others:

```
Router(config)#interface type port
Router(config)#interface type slot/port
Router(config)#interface type slot/subslot/port
```

The following command is used to administratively turn off the interface:

```
Router(config-if)#shutdown
```

The following command is used to turn on an interface that has been shutdown:

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

The following command is used to quit the current interface configuration mode:

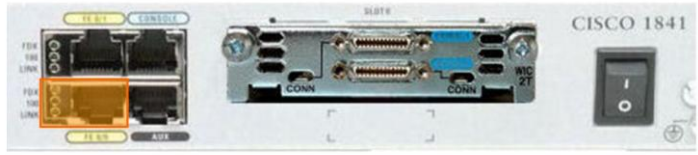
```
Router(config-if)#exit
```

When the configuration is complete, the interface is enabled and interface configuration mode is exited.

Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

Describe the purpose of having multiple interfaces in one router

Configuring Router Ethernet Interfaces




```
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

Configure Router Ethernet Interfaces

Serial Interface

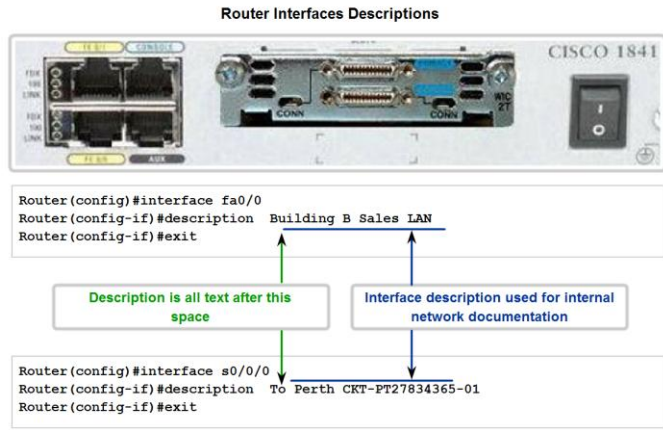
Configure Router Serial Interfaces


```
Router(config)#interface Serial 0/0/0
Router(config-if)#ip address 192.168.11.1 255.255.255.252
Router(config-if)#clock rate 56000
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

Configure Router Serial Interfaces

Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

Explain the purpose of assigning interface descriptions to a router



Interface Descriptions

As the hostname helps to identify the device on a network, an interface description indicates the purpose of the interface.

A description of what an interface does or where it is connected should be part of the configuration of each interface. This description can be useful for troubleshooting.

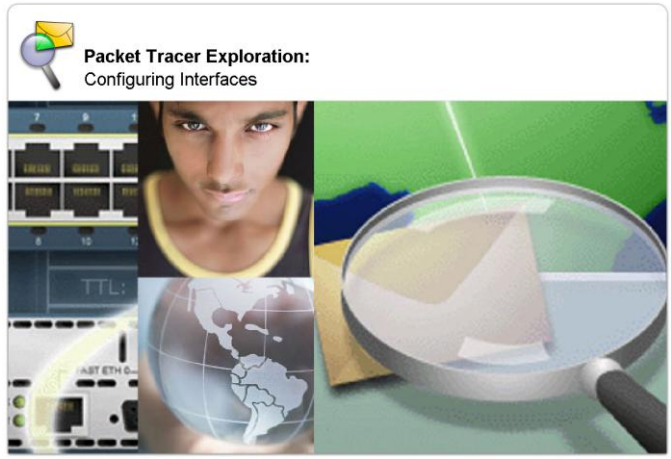
The interface description will appear in the output of these commands: show startup-config, show running-config, and show interfaces.

For example, this description provides valuable information about the purpose of the interface:

This interface is the gateway for the administration LAN. A description can assist in determining the devices or locations connected to the interface

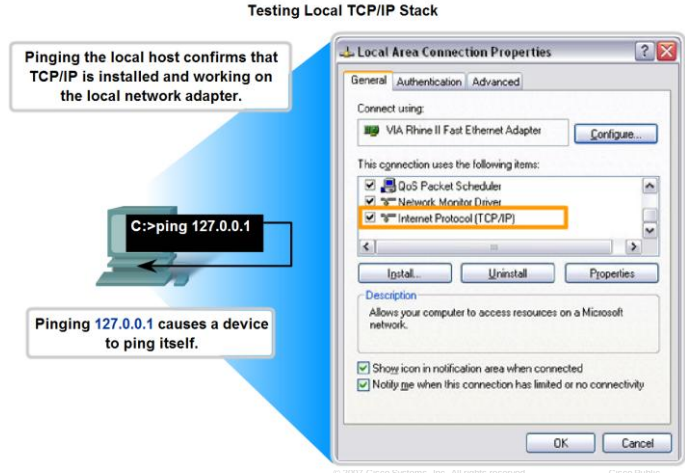
Use Cisco CLI Commands to Perform Basic Router & Switch Configuration and Verification

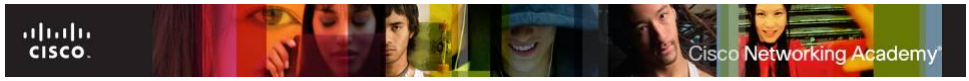
Assign a router interface, assign a meaningful interface description, and enable the interface



Select, Apply, and Verify Appropriate Addressing Parameters to a Host

Given a type of host and a master addressing scheme, trace the steps for assigning host parameters to a host





PING Command

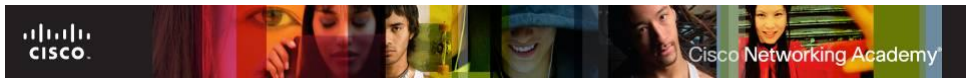
The ping command in a planned sequence of steps to establish valid connections, starting with the individual device and then extending to the LAN and, finally, to remote networks.

By using the ping command in this ordered sequence, problems can be isolated.

The ping command will not always pinpoint the nature of the problem, but it can help to identify the source of the problem, an important first step in troubleshooting a network failure.

The ping command provides a method for checking the protocol stack and IPv4 address configuration on a host.

There are additional tools that can provide more information than ping, such as Telnet or Trace, which will be discussed in more detail later.



Ping Indicators

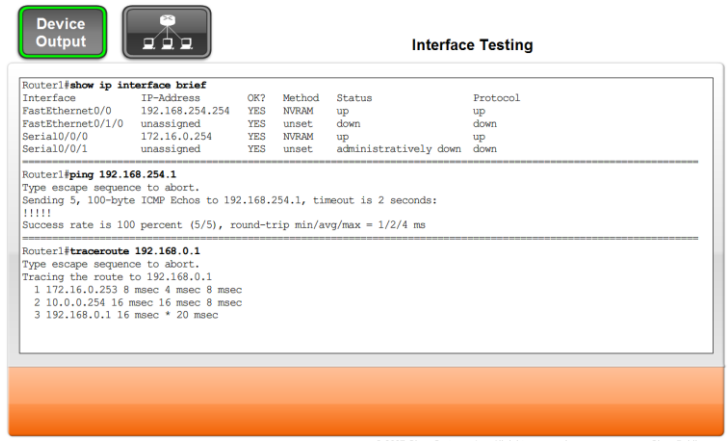
The "!" (exclamation mark) indicates that the ping completed successfully and verifies Layer 3 connectivity.

The "." (period) can indicate problems in the communication. It may indicate connectivity problem occurred somewhere along the path. It also may indicate a router along the path did not have a route to the destination and did not send an ICMP destination unreachable message. It also may indicate that ping was blocked by device security.

The "U" indicates that a router along the path did not have a route to the destination address and responded with an ICMP unreachable message.

Select, Apply, and Verify Appropriate Addressing Parameters to a Host

Trace the steps for using ipconfig/ifconfig to verify host parameter assignments and for using ping to test assignments



Show IP Interface Brief

One of the most used commands is the show ip interface brief command.

This provides a more abbreviated output than the show ip interface command. This provides a summary of the key information for all the interfaces.

Looking at the Router 1 figure, we can see that this output shows all interfaces attached on the router, the IP address, if any, assigned to each interface, and the operational status of the interface.

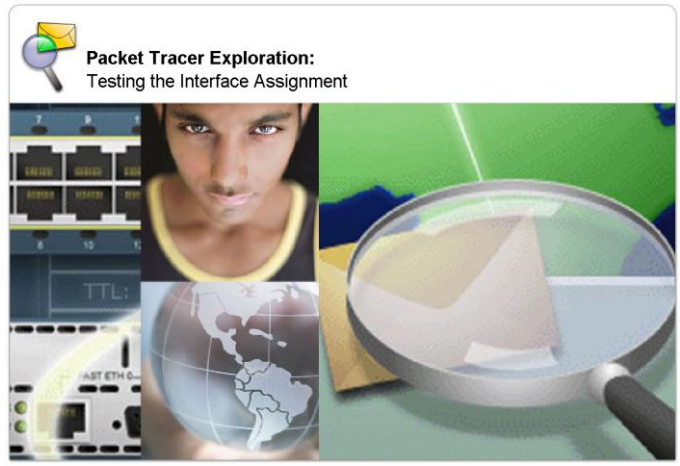
Looking at the line for the FastEthernet 0/0 interface, we see that the IP address is 192.168.254.254.

Looking at the last two columns, we can see the Layer 1 and Layer 2 status of the interface. The up in the Status column shows that this interface is operational at Layer 1.

The up in the Protocol column indicates that the Layer 2 protocol is operational.

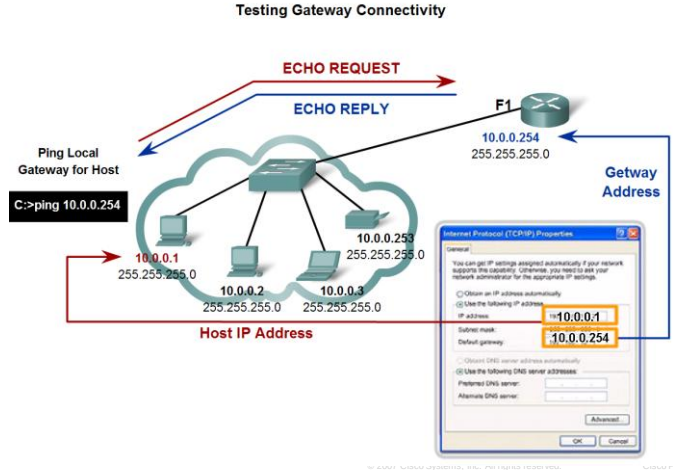
Select, Apply, and Verify Appropriate Addressing Parameters to a Host

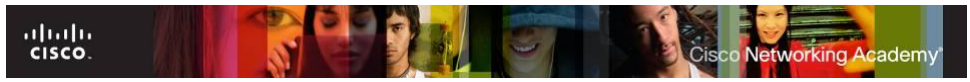
Identify two ways parameters can be assigned to hosts



Use Common Utilities to Verify Network Connectivity Between Hosts

Use the ping command in the CLI to determine if the IP protocol is operational on a local host





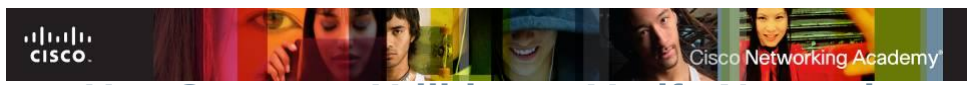
Testing the Gateway

The gateway IPv4 address should be readily available in the network documentation, but if it is not available, use the ipconfig command to discover the gateway IP address.

If the gateway test fails, back up one step in the sequence and test another host in the local LAN to verify that the problem is not the source host.

Then verify the gateway address with the network administrator to ensure that the proper address is being tested.

If all devices are configured properly, check the physical cabling to ensure that it is secure and properly connected. Keep an accurate record of what attempts have been made to verify connectivity. This will assist in solving this problem and, perhaps, future problems.

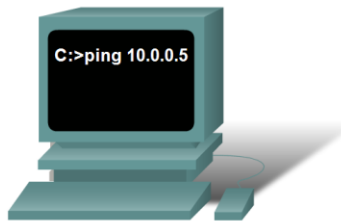


Use Common Utilities to Verify Network Connectivity Between Hosts

Use the ping command to determine if the IP protocol is properly bound to an NIC

Testing the Local NIC Assignment

```
IP Address. . . . . . . . . . . : 10.0.0.5
Subnet Mask . . . . . . . . . . :
255.255.255.0
```



Verify the host NIC address is bound and ready for transmitting signals across the media by pinging its own IP address

Testing the NIC

The next step in the testing sequence is to verify that the NIC address is bound to the IPv4 address and that the NIC is ready to transmit signals across the media.

In this example, also shown in the figure, assume that the IPv4 address assigned to a NIC is 10.0.0.5.

To verify the IPv4 address, use the following steps:

At the command line, enter the following:

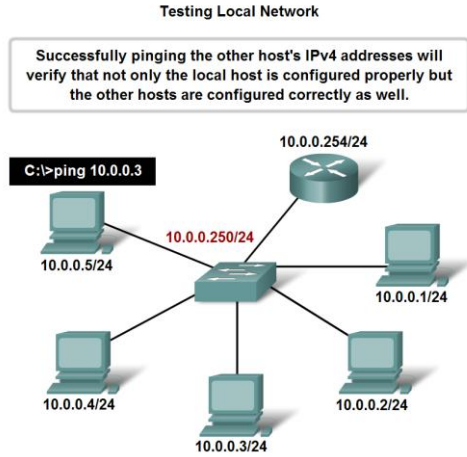
C:\>ping 10.0.0.5

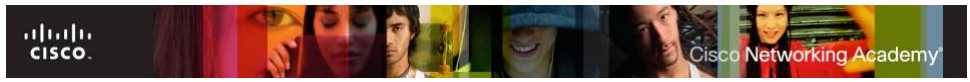
This test verifies that the NIC driver and most of the NIC hardware are working properly. It also verifies that the IP address is properly bound to the NIC, without actually putting a signal on the media.

If this test fails, it is likely that there are issues with the NIC hardware and software driver that may require reinstallation of either or both.

Use Common Utilities to Verify Network Connectivity Between Hosts

Use the ping command to determine if a host can actively communicate across the local network





Testing the Local LAN

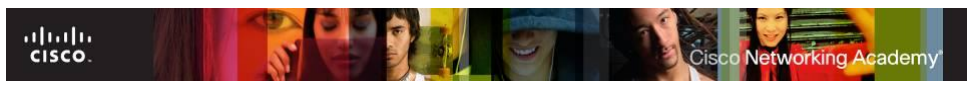
The next test in the sequence is to test hosts on the local LAN.

Successfully pinging remote hosts verifies that both the local host (the router in this case) and the remote host are configured correctly. This test is conducted by pinging each host one by one on the LAN.

See the figure for an example.

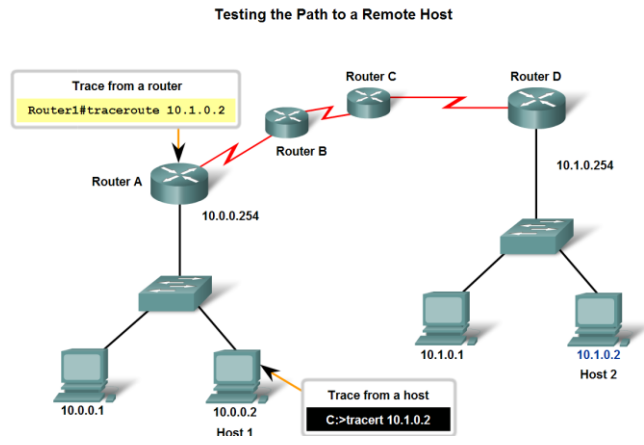
Extended Ping:

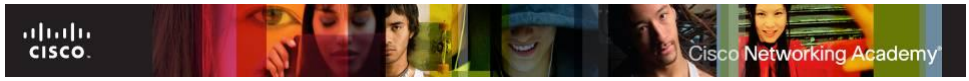
To examine this the IOS offers an "extended" mode of the ping command. This mode is entered by typing ping in privileged EXEC mode, at the CLI prompt without a destination IP address. A series of prompts are then presented as shown in this example. Pressing Enter accepts the indicated default values.



Use Common Utilities to Verify Network Connectivity Between Hosts

Use the ping command to verify that the local host can communicate across the internetwork to a given remote host.





Tracert and Ping

The next step in the testing sequence is to perform a trace.

A trace returns a list of hops as a packet is routed through a network. The form of the command depends on where the command is issued.

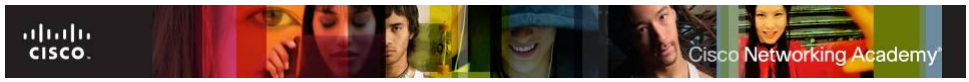
When performing the trace from a Windows computer, use tracert. When performing the trace from a router CLI, use traceroute.

Ping and trace can be used together to diagnose a problem.

Let's assume that a successful connection has been established between Host 1 and Router A, as shown in the figure.

Next, let's assume that Host 1 pings Host 2 using this command.

C:\>ping 10.1.0.2



Ping Results

The ping command returns this result:

Pinging 10.1.0.2 with 32 bytes of data:

Request timed out.

Ping statistics for 10.1.0.2:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

The ping test failed.

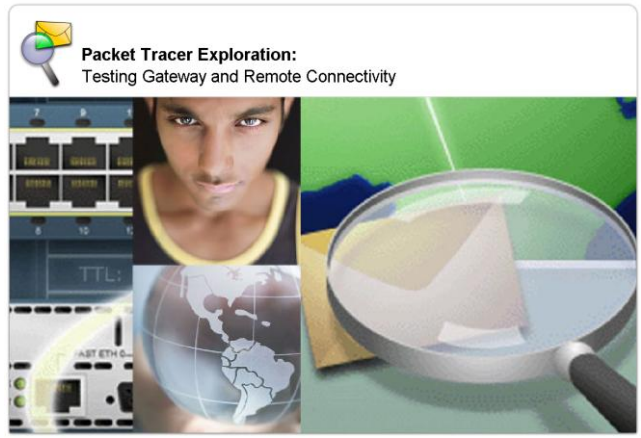
This is a test of communication beyond the local network to a remote device.

Because the local gateway responded but the host beyond did not, the problem appears to be somewhere beyond the local network.

A next step is to isolate the problem to a particular network beyond the local network. The trace commands can show the path of the last successful communication.

Use Common Utilities to Verify Network Connectivity Between Hosts

Use trace commands to identify network connectivity problem



Use Common Utilities to Establish a Relative Performance Baseline for the Network

Use the output of the ping command, saved into logs, and repeated over time, to establish relative network performance

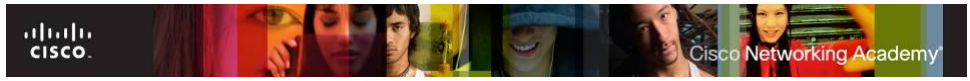
Baseline with ping

FEB 2, 2007 08:14:43

```
C:\host1>ping 10.66.254.159

Pinging 10.66.254.159 with 32 bytes of data:

Reply from 10.66.254.159: bytes=32 time<1ms TTL=128
Reply from 10.66.254.159: bytes=32 time<1ms TTL=128
Reply from 10.66.254.159: bytes=32 time<1ms TTL=128
Reply from 10.66.254.159: bytes=32 time<1ms TTL=128
```

MAR 17, 2007 14:41:06

```
C:\host1>ping 10.66.254.159

Pinging 10.66.254.159 with 32 bytes of data:

Reply from 10.66.254.159: bytes=32 time<6ms TTL=128
Reply from 10.66.254.159: bytes=32 time<6ms TTL=128
Reply from 10.66.254.159: bytes=32 time<6ms TTL=128
Reply from 10.66.254.159: bytes=32 time<6ms TTL=128
```



Baseline Performance

One of the most effective tools for monitoring and troubleshooting network performance is to establish a network baseline.

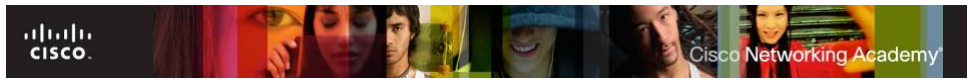
A baseline is a process for studying the network at regular intervals to ensure that the network is working as designed.

It is more than a single report detailing the health of the network at a certain point in time.

Creating an effective network performance baseline is accomplished over a period of time.

Measuring performance at varying times and loads will assist in creating a better picture of overall network performance.

The output derived from network commands can contribute data to the network baseline.



Baseline Using Ping

One method for starting a baseline is to copy and paste the results from an executed ping, trace, or other relevant command into a text file.

These text files can be time stamped with the date and saved into an archive for later retrieval.

An effective use of the stored information is to compare the results over time.

Among items to consider are error messages and the response times from host to host. If there is a considerable increase in response times, there may be a latency issue to address.

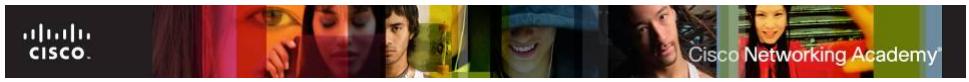
Use Common Utilities to Establish a Relative Performance Baseline for the Network

Use the output of the traceroute command, saved into logs, and repeated over time, to establish relative network performance

Capturing Trace Route

```
C:\>tracert www.cisco.com

Tracing route to www.cisco.com [198.133.219.25]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  192.168.0.1
  2    20 ms    20 ms    20 ms  nexthop.wa.ii.net [203.59.14.16]
  3    20 ms    19 ms    20 ms  gi2-4.per-qv1-bdr1.ii.net [203.215.4.32]
  4    79 ms    78 ms    78 ms  gi0-14-0-0.syd-ult-core1.ii.net [203.215.20.2]
  5    79 ms    81 ms    79 ms  202.139.19.33
  6   227 ms   228 ms   227 ms  203.208.148.17
  7   227 ms   227 ms   227 ms  203.208.149.34
  8   225 ms   225 ms   226 ms  208.30.205.145
  9   236 ms   249 ms   233 ms  sl-bb23-ana-8-0-0.sprintlink.net [144.232.9.23]

 10   241 ms   244 ms   240 ms  sl-bb25-sj-9-0.sprintlink.net [144.232.20.159]
 11   238 ms   238 ms   239 ms  sl-gw8-sj-10-0.sprintlink.net [144.232.3.114]
 12   238 ms   239 ms   240 ms  144.228.44.14
 13   240 ms   242 ms   248 ms  sjce-dmzbb-gw1.cisco.com [128.107.239.89]
```

Sample trace output



Tracert Data

The data from a trace can be added to the data from the ping commands to provide a combined picture of network performance.

For example, if the speed of a ping command decreases over time, compare the trace output for the same time period.

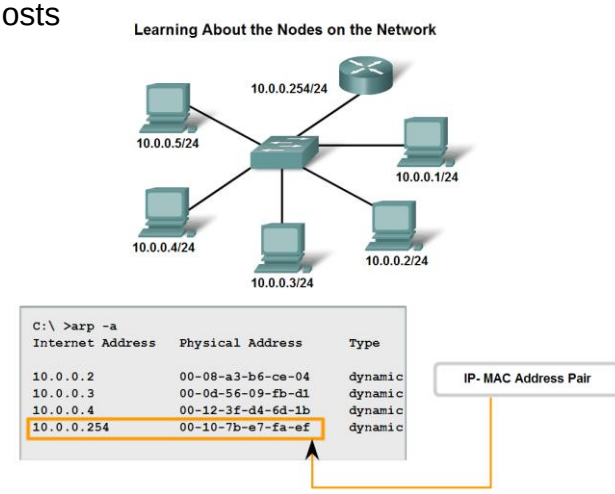
Examining the response times on a hop-by-hop comparison may reveal a particular point of longer response time. This delay may be due to congestion at that hop creating a bottleneck in the network.

Another case might show that the hop pathway to the destination may vary over time as the routers select different best paths for the trace packets.

These variations may show patterns that could be useful in scheduling large transfers between sites.

Use Common Utilities to Establish a Relative Performance Baseline for the Network

Trace the steps for verifying the physical addresses of the hosts



ARP Command

The arp command provides for the mapping of physical addresses to known IPv4 addresses.

A common method for executing the arp command is to execute it from the command prompt.

This method involves sending out an ARP request.

The device that needs the information sends out a broadcast ARP request to the network, and only the local device that matches the IP address of the request sends back an ARP reply containing its IP-MAC pair.

To execute an arp command, at the command prompt of a host, enter:

C:\host1>arp –a

As shown in the figure the arp command lists all devices currently in the ARP cache, which includes the IPv4 address, physical address, and the type of addressing (static/dynamic), for each device.

Labs

Summary

In this chapter, you learned to:

- Define the role of the Internetwork Operating System (IOS).
- Define the purpose of a configuration file.
- Identify several classes of devices that have the IOS embedded.
- Identify the factors contributing to the set of IOS commands available to a device.
- Identify the IOS modes of operation.
- Identify the basic IOS commands.
- Compare and contrast the basic show commands.