Jaringan Komputer (CCNA-1)

#2 Configuring a Network Operating System

Susmini I. Lestariningati, M.T

Introduction (1)

- Home networks typically interconnect a wide variety of end devices including PCs, laptops, tablets, smartphones, smart TVs, Digital Living Network Alliance (DLNA) compliant network media players, such as the Xbox 360 or PlayStation 3, and more.

- All of these end devices are usually connected to a home router. Home routers are actually four devices in one:

    - Router - Forwards data packets to and receives data packets from the Internet
    - Switch - Connects end devices using network cables
    - Wireless access point - Consists of a radio transmitter capable of connecting end devices wirelessly
    - Firewall appliance - Secures outgoing traffic and restricts incoming traffic

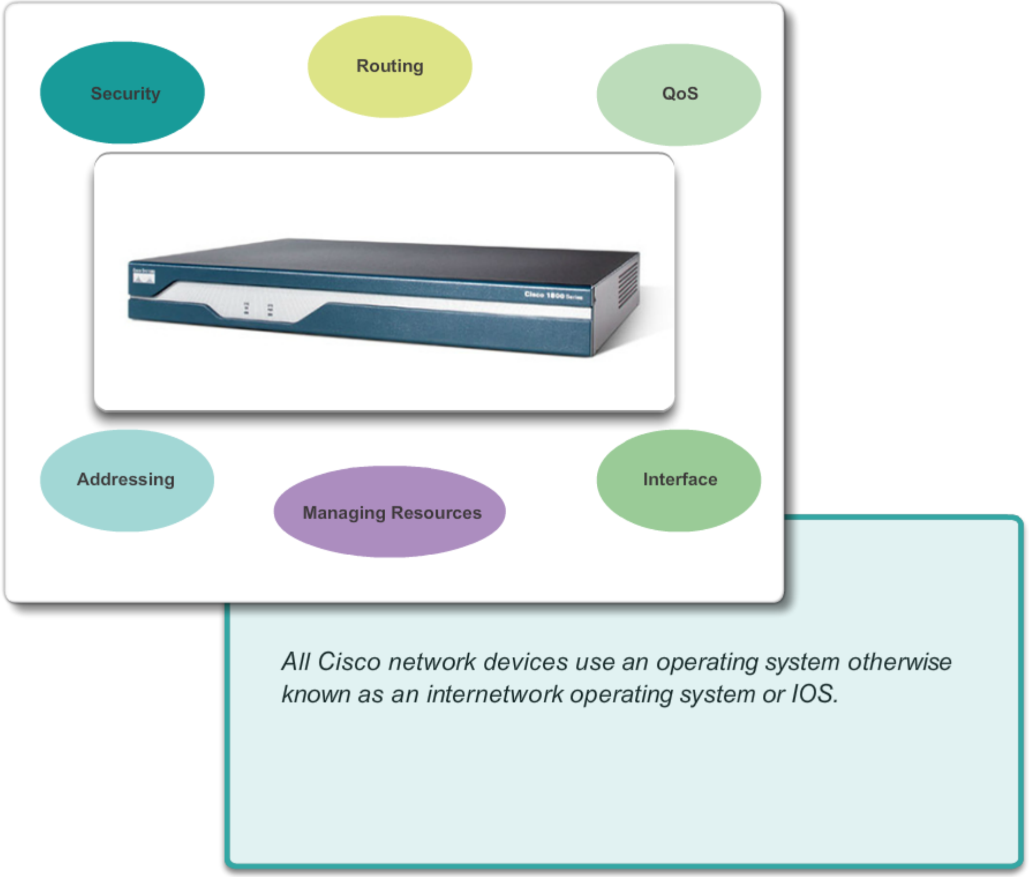
- In larger, business networks with significantly more devices and traffic, these devices are often incorporated as independent, stand-alone devices, providing dedicated service. End-devices, such as PCs and laptops, are connected to network switches using wired connections. To send packets beyond the local network, network switches connect to network routers. Other infrastructure devices on a network include wireless access points and dedicated security devices, such as firewalls.

Introduction (2)

- Each device is very different in hardware, use, and capability. But in all cases, it is the operating system that enables the hardware to function.

- Operating systems are used on virtually all end user and network devices connected to the Internet. End user devices include devices such as smart phones, tablets, PCs, and laptops. Network devices, or intermediary devices, are devices used to transport data across the network and include switches, routers, wireless access points, and firewalls. The operating system on a network device is known as a network operating system.

- The Cisco Internetwork Operating System (IOS) is a generic term for the collection of network operating systems used on Cisco networking devices. Cisco IOS is used for most Cisco devices regardless of the type or size of the device.



All Cisco network devices use an operating system otherwise known as an internetwork operating system or IOS.

Cisco IOS

- All end devices and network devices connected to the Internet require an operating system (OS) to help them perform their function.

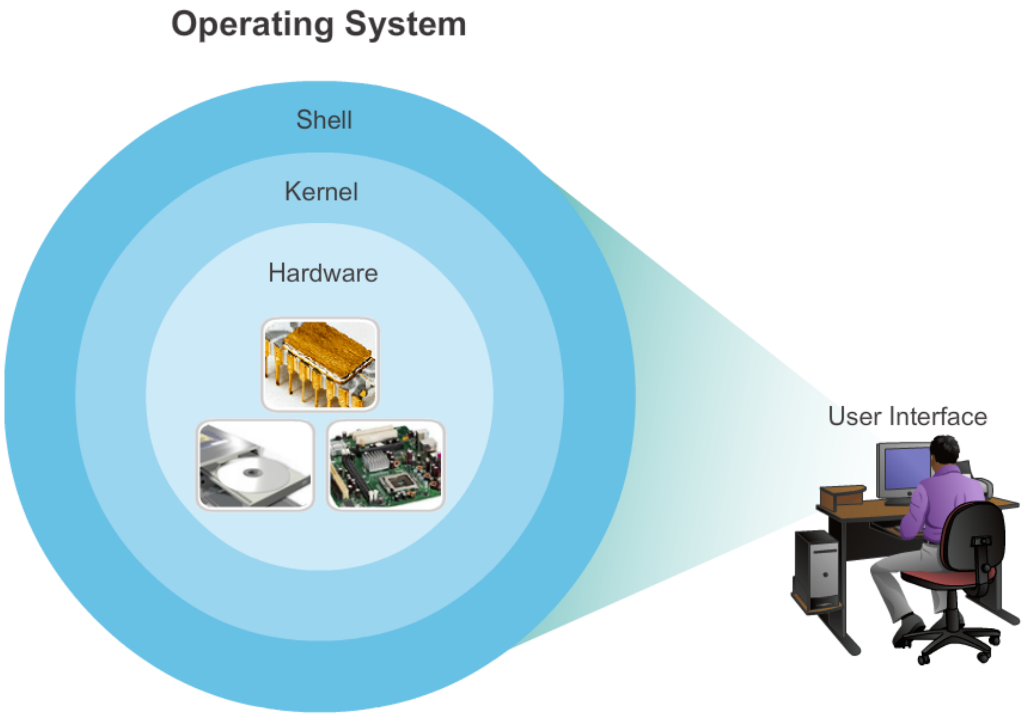
- When a computer is powered on, it loads the OS, normally from a disk drive, into RAM. The portion of the OS code that interacts directly with the computer hardware is known as the kernel. The portion that interfaces with the applications and user is known as the shell. The user can interact with the shell using either the command-line interface (CLI) or graphical user interface (GUI).

- When using the CLI, the user interacts directly with the system in a text-based environment by entering commands on the keyboard at a command prompt. The system executes the command, often providing textual output. The GUI interface allows the user to interact with the system in an environment that uses graphical images, multimedia, and text. Actions are performed by interacting with the images on screen. GUI is more user friendly and requires less knowledge of the command structure to utilize the system. For this reason, many individuals rely on the GUI environments. Many operating systems offer both GUI and CLI.

- Click on the hardware, kernel, and shell portions of the figure for more information.

Cisco IOS

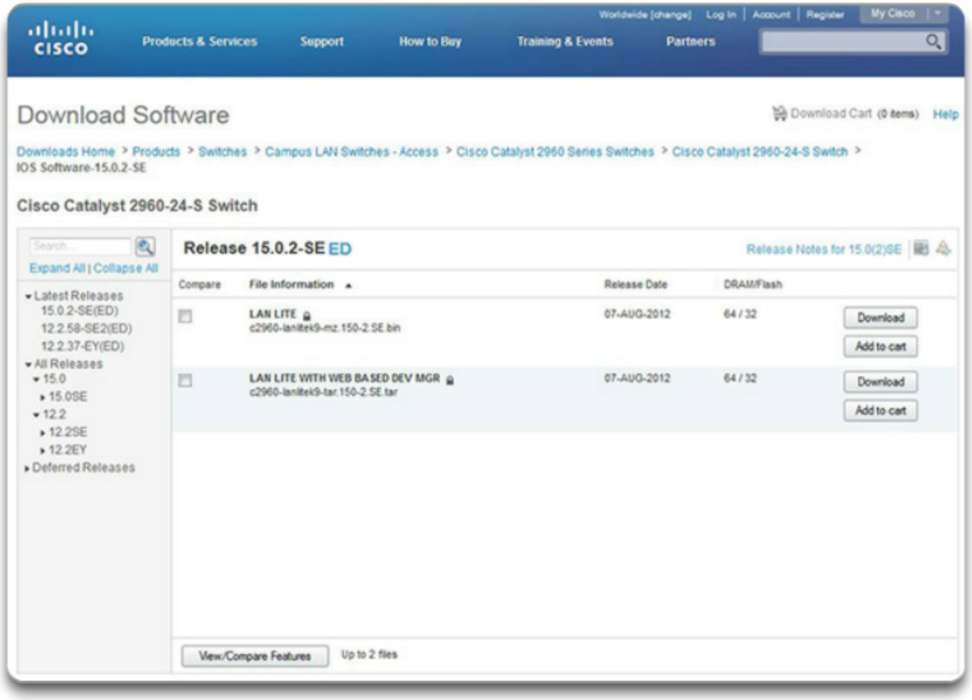
- Most end device operating systems are accessed using a GUI, including MS Windows, MAC OS X, Linux, Apple iOS, Android, and more.
- The operating system on home routers is usually called firmware. The most common method for configuring a home router is using a web browser to access an easy to use GUI. Most home routers enable the update of the firmware as new features or security vulnerabilities are discovered.
- Infrastructure network devices use a network operating system. The network operating system used on Cisco devices is called the Cisco Internetwork Operating System (IOS). Cisco IOS is a generic term for the collection of network operating systems used on Cisco networking devices. Cisco IOS is used for most Cisco devices regardless of the type or size of the device. The most common method of accessing these devices is using a CLI.
- This chapter will focus on a small business network switch topology. The topology consists of two switches and two PCs and will be used to demonstrate the use of Cisco IOS using the CLI.



Cisco IOS

- Network operating systems are in many ways similar to the operating systems of PCs. An operating system performs a number of technical functions "behind the scenes" that enable a user to:
  - Use a mouse
  - View output on a monitor
  - Enter text commands
  - Select options within a dialog box window

- The "behind the scenes" functions for switches and routers are very similar. The IOS on a switch or router provides the network technician with an interface. The technician can enter commands to configure, or program, the device to perform various networking functions. The IOS operational details vary on internetworking devices, depending on the purpose of the device and the features supported.



Download Software

Downloads Home > Products > Switches > Campus LAN Switches - Access > Cisco Catalyst 2960 Series Switches > Cisco Catalyst 2960-24-S Switch > IOS Software-15.0.2-SE

Cisco Catalyst 2960-24-S Switch

- Latest Releases
  - 15.0.2-SE(ED)
  - 12.2.58-SE2(ED)
  - 12.2.37-EY(ED)
- All Releases
  - 15.0
    - 15.0SE
  - 12.2
    - 12.2SE
    - 12.2EY
- Deferred Releases

Release 15.0.2-SE ED

Compare	File Information	Release Date	DRAM/Flash	
□	LAN LITE c2960-lanlitek9-mz.150-2.SE.bin	07-AUG-2012	64 / 32	Download Add to cart
□	LAN LITE WITH WEB BASED DEV MGR c2960-lanlitek9-tar.150-2.SE.tar	07-AUG-2012	64 / 32	Download Add to cart

Cisco IOS

- Cisco IOS is a term that encompasses a number of different operating systems that run on various networking devices. There are many distinct variations of Cisco IOS:
  - IOS for switches, routers, and other Cisco networking devices
  - IOS numbered versions for a given Cisco networking device
  - IOS feature sets providing distinct packages of features and services

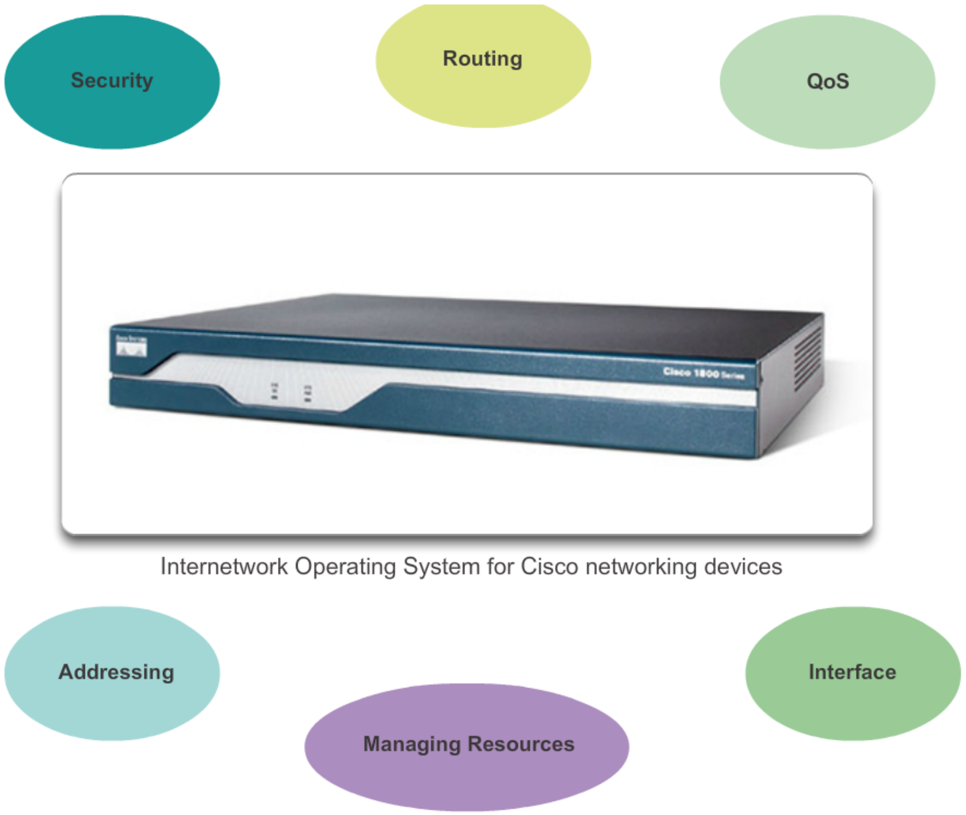
- Just as a PC may be running Microsoft Windows 8 and a MacBook may be running OS X, a Cisco networking device runs a particular version of the Cisco IOS. The version of IOS is dependent on the type of device being used and the required features. While all devices come with a default IOS and feature set, it is possible to upgrade the IOS version or feature set, in order to obtain additional capabilities.

Location of the Cisco IOS

- The IOS file itself is several megabytes in size and is stored in a semi-permanent memory area called flash.
- The figure shows a compact flash card. Flash memory provides non-volatile storage. This means that the contents of the memory are not lost when the device loses power. Although the contents of flash are not lost during a loss of power, they can be changed or overwritten if needed. This allows the IOS to be upgraded to a newer version or to have new features added without replacing hardware. Additionally, flash can be used to store multiple versions of IOS software at the same time.
- In many Cisco devices, the IOS is copied from flash into random access memory (RAM) when the device is powered on. The IOS then runs from RAM when the device is operating. RAM has many functions including storing data that is used by the device to support network operations. Running the IOS in RAM increases performance of the device, however, RAM is considered volatile memory because data is lost during a power cycle. A power cycle is when a device is purposely or accidently powered off and then powered back on.
- The quantity of flash memory and RAM memory required for a given IOS varies dramatically. For the purposes of network maintenance and planning, it is important to determine the flash and RAM requirements for each device, including the maximum flash and RAM configurations. It is possible that the requirements of the newest versions of IOS could demand more RAM and flash than can be installed on some devices.

Introduction

- Cisco IOS routers and switches perform functions that network professionals depend upon to make their networks operate as expected. Major functions performed or enabled by Cisco routers and switches include:
  - Providing network security
  - IP addressing of virtual and physical interfaces
  - Enabling interface-specific configurations to optimize connectivity of the respective media
  - Routing
  - Enabling quality of service (QoS) technologies
  - Supporting network management technologies

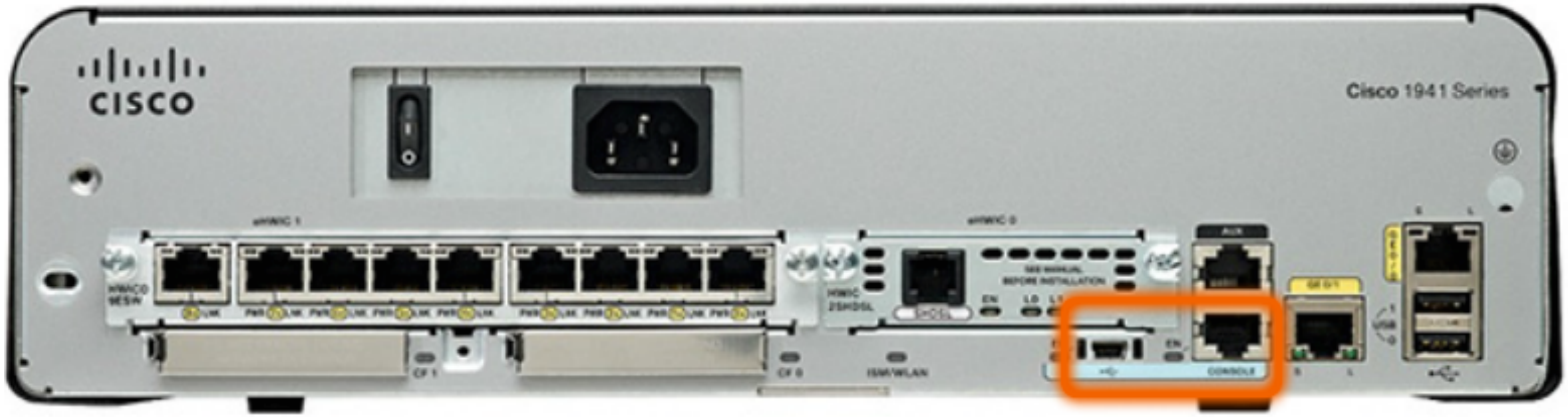


Internetwork Operating System for Cisco networking devices

- Each feature or service has an associated collection of configuration commands that allow a network technician to implement it.
- The services provided by the Cisco IOS are generally accessed using a CLI.

Accessing a Cisco IOS Device

- There are several ways to access the CLI environment. The most common methods are:
  - Console
  - Telnet or SSH
  - AUX port



Console

- The advantage of using a console port is that the device is accessible even if no networking services have been configured, such as when performing an initial configuration of the networking device. When performing an initial configuration, a computer running terminal emulation software is connected to the console port of the device using a special cable. Configuration commands for setting up the switch or router can be entered on the connected computer.

- The console port can also be used when the networking services have failed and remote access of the Cisco IOS device is not possible. If this occurs, a connection to the console can enable a computer to determine the status of the device. By default, the console conveys the device startup, debugging, and error messages. After the network technician is connected to the device, the network technician can perform any configuration commands necessary using the console session.

- For many IOS devices, console access does not require any form of security, by default. However, the console should be configured with passwords to prevent unauthorized device access. In the event that a password is lost, there is a special set of procedures for bypassing the password and accessing the device. The device should also be located in a locked room or equipment rack to prevent unauthorized physical access.

Telnet

- Telnet is a method for remotely establishing a CLI session of a device, through a virtual interface, over a network.
- 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 an Internet address, such as an IPv4 address.
- Cisco IOS devices include a Telnet server process that allows users to enter configuration commands from a Telnet client.
- In addition to supporting the Telnet server process, the Cisco IOS device also contains a Telnet client. This allows a network administrator to telnet from the Cisco device CLI to any other device that supports a Telnet server process.

SSH

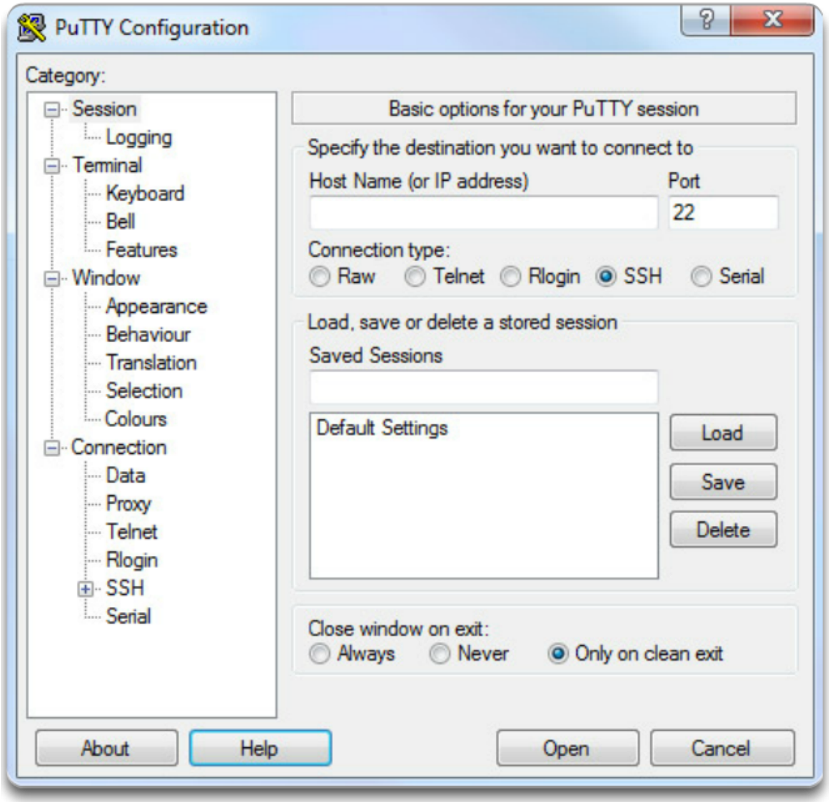
- The Secure Shell (SSH) protocol provides a remote login similar to Telnet, except that it uses more secure network services.
- SSH provides stronger password authentication than Telnet and uses encryption when transporting session data.
- This keeps the user ID, password, and the details of the management session private. As a best practice, use SSH instead of Telnet whenever possible.
- Most versions of Cisco IOS include an SSH server. In some devices, this service is enabled by default. Other devices require the SSH server to be enabled manually. IOS devices also include an SSH client that can be used to establish SSH sessions with other devices.

AUX

- An older way to establish a CLI session remotely is via a telephone dialup connection using a modem connected to the auxiliary (AUX) port of a router, which is highlighted in the figure. Similar to the console connection, the AUX method is also an out-of-band connection and does not require any networking services to be configured or available on the device. In the event that network services have failed, it may be possible for a remote administrator to access the switch or router over a telephone line.

- The AUX port can also be used locally, like the console port, with a direct connection to a computer running a terminal emulation program. However, the console port is preferred over the AUX port for troubleshooting because it displays startup, debugging, and error messages by default.

- There are a number of excellent terminal emulation programs available for connecting to a networking device either by a serial connection over a console port or by a Telnet/SSH connection. Some of these include:
  - PuTTY (Figure 1)
  - Tera Term (Figure 2)
  - SecureCRT (Figure 3)
  - HyperTerminal
  - OS X Terminal



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

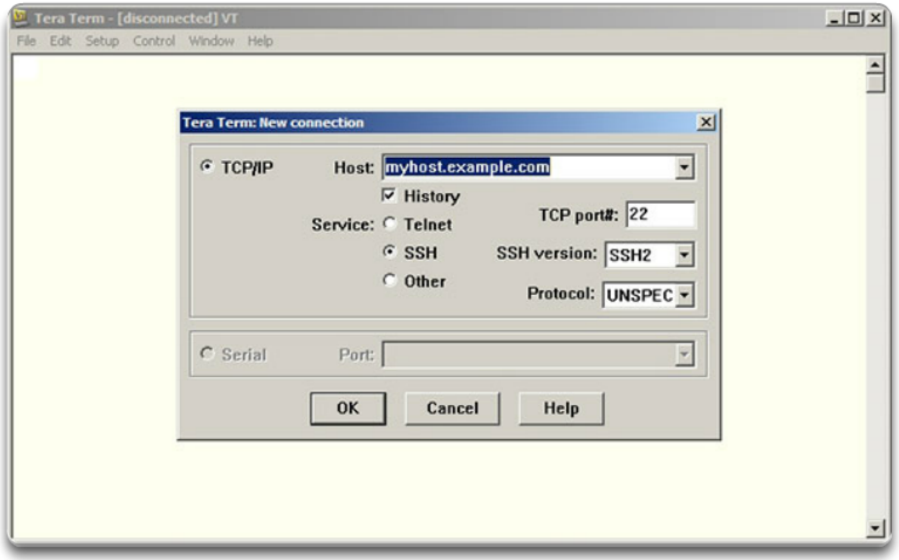
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions:

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit


Tera Term - [disconnected] VT
File Edit Setup Control Window Help
Tera Term: New connection
OK
Cancel
Help

● TCP/IP Host: myhost.example.com

☑ History

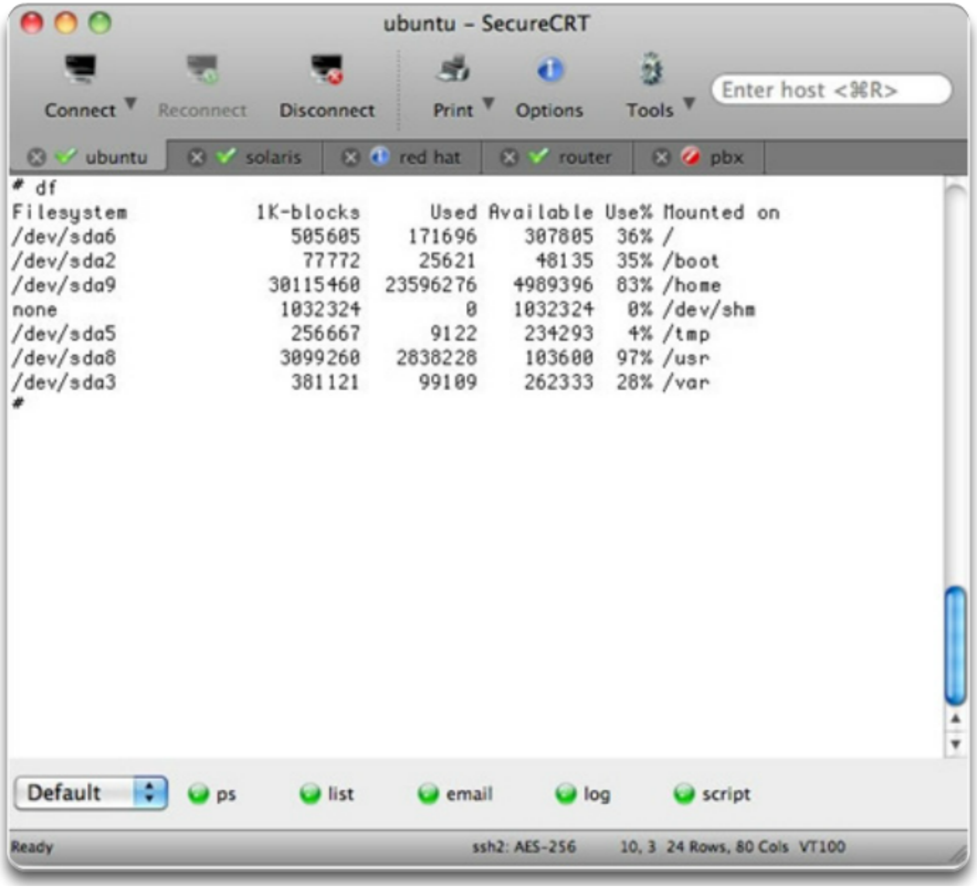
Service: ○ Telnet TCP port#: 22

● SSH SSH version: SSH2

○ Other Protocol: UNSPEC

○ Serial Port:

Tera Term



```
# df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sda6               505605    171696    307805  36% /
/dev/sda2                77772     25621     48135  35% /boot
/dev/sda9             30115460  23596276   4989396  83% /home
none                   1032324         0   1032324   0% /dev/shm
/dev/sda5               256667      9122    234293   4% /tmp
/dev/sda8              3099260   2838228    103600  97% /usr
/dev/sda3               381121     99109    262333  28% /var
#
```

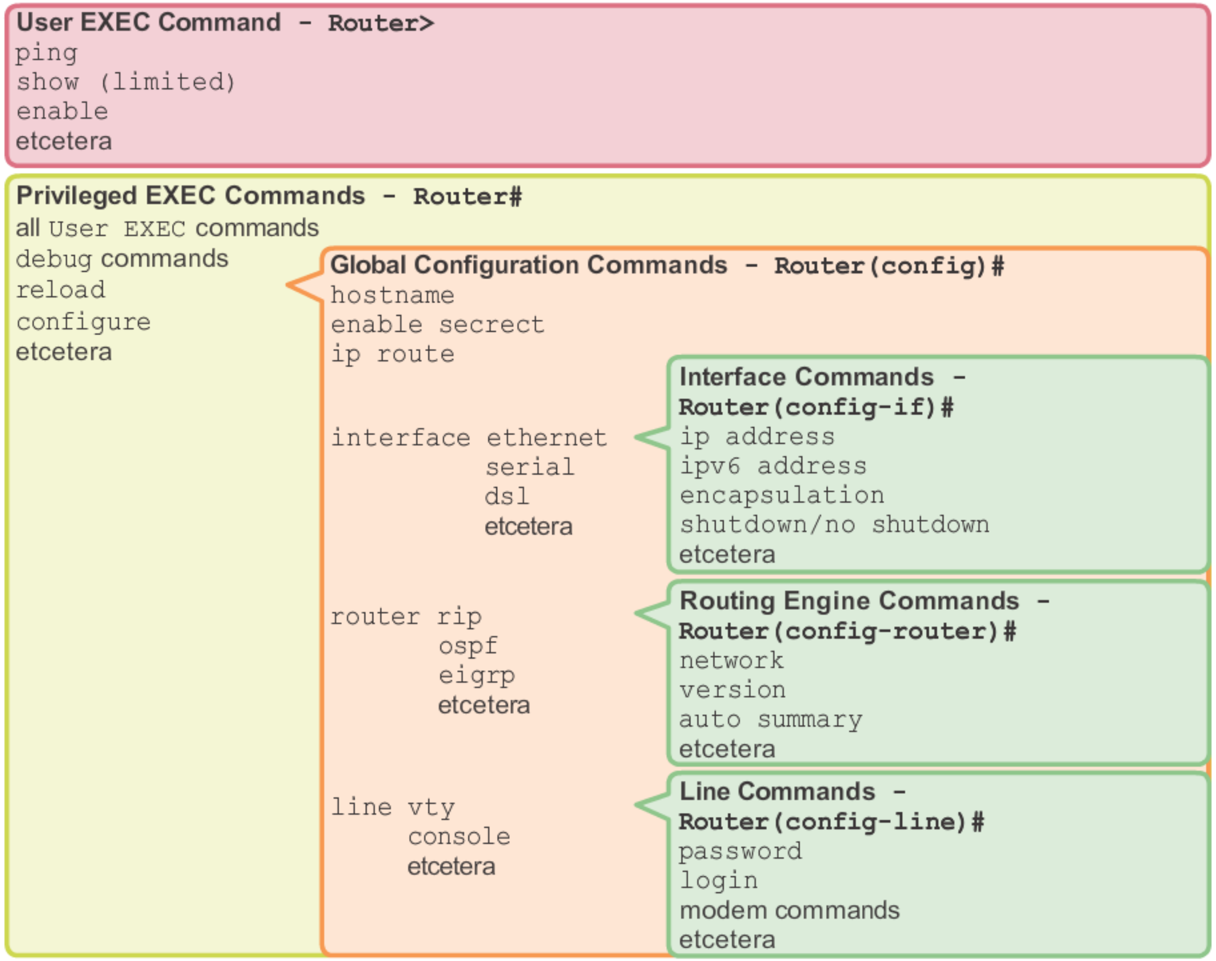
Ready ssh2: AES-256 10, 3 24 Rows, 80 Cols VT100

Secure CRT

Cisco IOS Modes of Operation

- The CLI uses a hierarchical structure for the modes.
- In hierarchical order from most basic to most specialized, the major modes are:
  - User executive (User EXEC) mode
  - Privileged executive (Privileged EXEC) mode
  - Global configuration mode
  - Other specific configuration modes, such as interface configuration mode

IOS Mode Hierarchical Structure



User EXEC Command - Router>

```
ping
show (limited)
enable
etcetera
```

Privileged EXEC Commands - Router#

```
all User EXEC commands
debug commands
reload
configure
etcetera
```

Global Configuration Commands - Router(config)#

```
hostname
enable secrect
ip route

interface ethernet
          serial
          dsl
          etcetera

router rip
       ospf
       eigrp
       etcetera

line vty
     console
     etcetera
```

Interface Commands - Router(config-if)#

```
ip address
ipv6 address
encapsulation
shutdown/no shutdown
etcetera
```

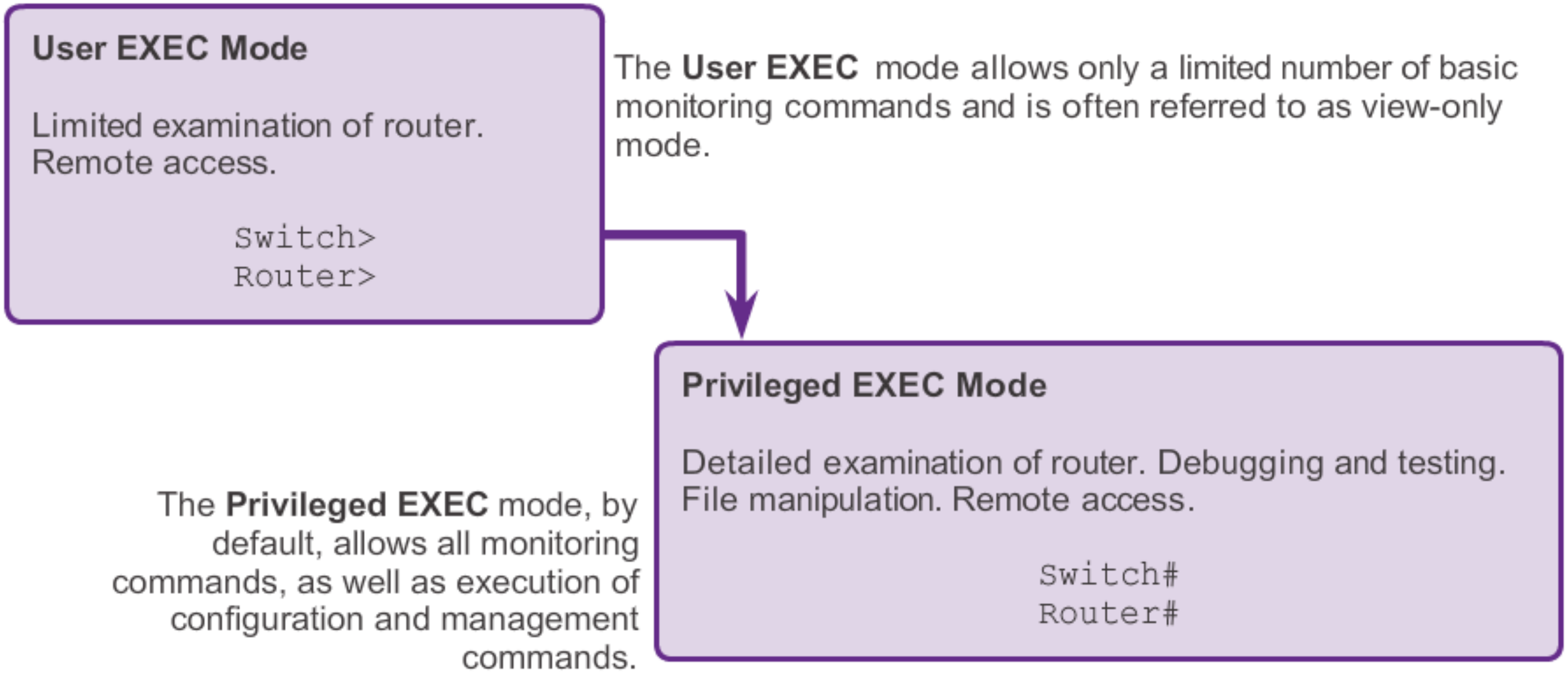
Routing Engine Commands - Router(config-router)#

```
network
version
auto summary
etcetera
```

Line Commands - Router(config-line)#

```
password
login
modem commands
etcetera
```

Navigating the IOS



User EXEC Mode

Limited examination of router. Remote access.

```
Switch>
Router>
```

The **User EXEC** mode allows only a limited number of basic monitoring commands and is often referred to as view-only mode.

Privileged EXEC Mode

Detailed examination of router. Debugging and testing. File manipulation. Remote access.

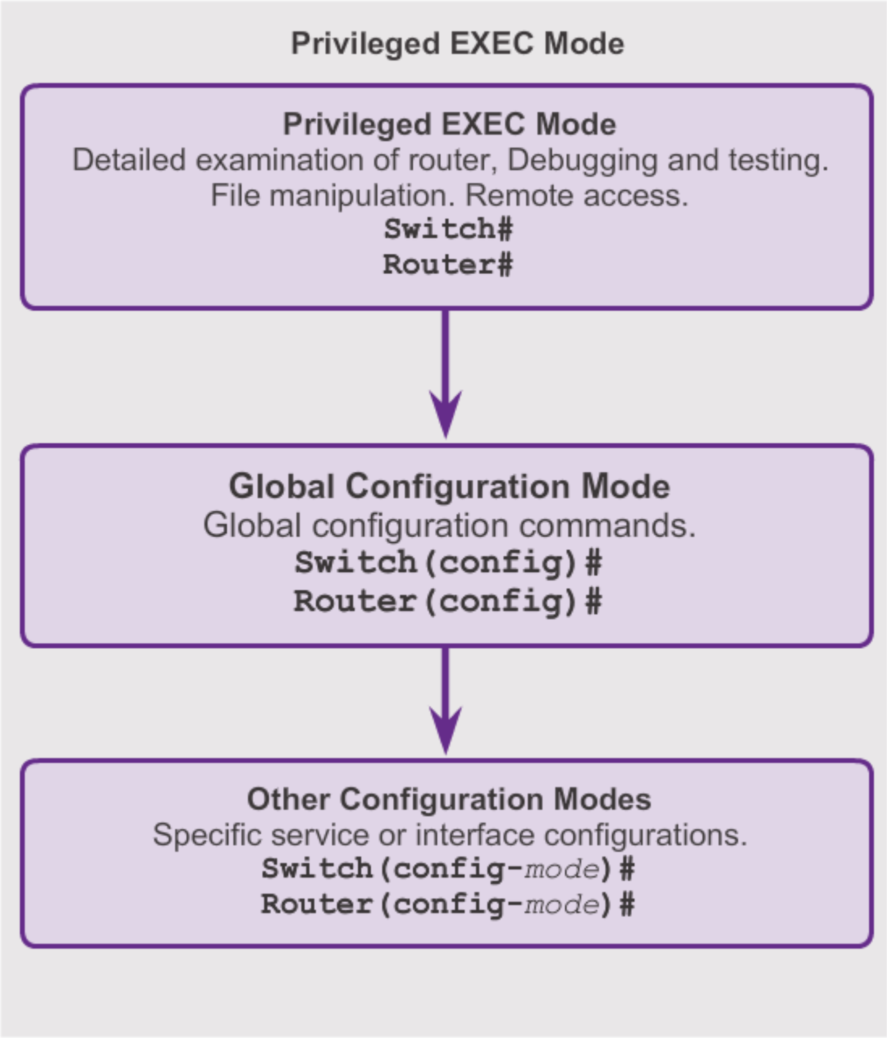
```
Switch#
Router#
```

The **Privileged EXEC** mode, by default, allows all monitoring commands, as well as execution of configuration and management commands.

- The user EXEC mode is identified by the CLI prompt that ends with the > symbol.
- The privileged EXEC mode can be identified by the prompt ending with the # symbol.

Priviledged EXEC Mode

Within Privileged EXEC mode, network administrators can access the global configuration mode and all other sub-configuration modes.



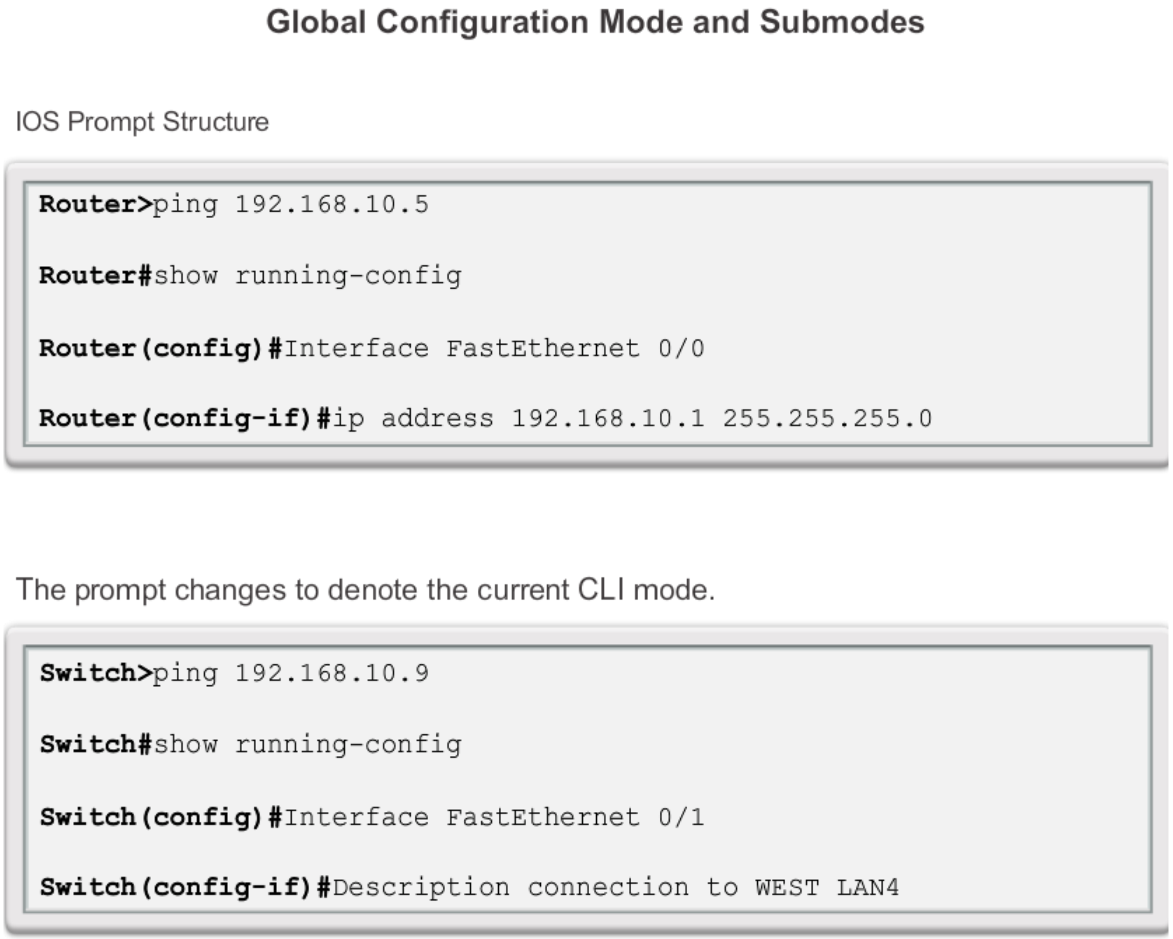
Privileged EXEC Mode

Privileged EXEC Mode
Detailed examination of router, Debugging and testing.
File manipulation. Remote access.
`Switch#`
`Router#`

Global Configuration Mode
Global configuration commands.
`Switch(config)#`
`Router(config)#`

Other Configuration Modes
Specific service or interface configurations.
`Switch(config-mode)#`
`Router(config-mode)#`

Navigating the IOS



Global Configuration Mode and Submodes

IOS Prompt Structure

```
Router>ping 192.168.10.5

Router#show running-config

Router(config)#Interface FastEthernet 0/0

Router(config-if)#ip address 192.168.10.1 255.255.255.0
```

The prompt changes to denote the current CLI mode.

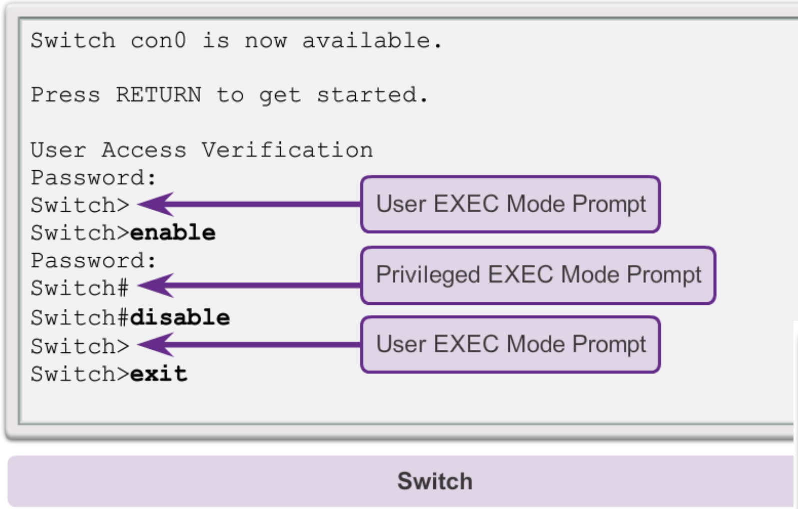
```
Switch>ping 192.168.10.9

Switch#show running-config

Switch(config)#Interface FastEthernet 0/1

Switch(config-if)#Description connection to WEST LAN4
```

- Global configuration mode and interface configuration modes can only be reached from the privileged EXEC mode.

Specific Configuration Modes

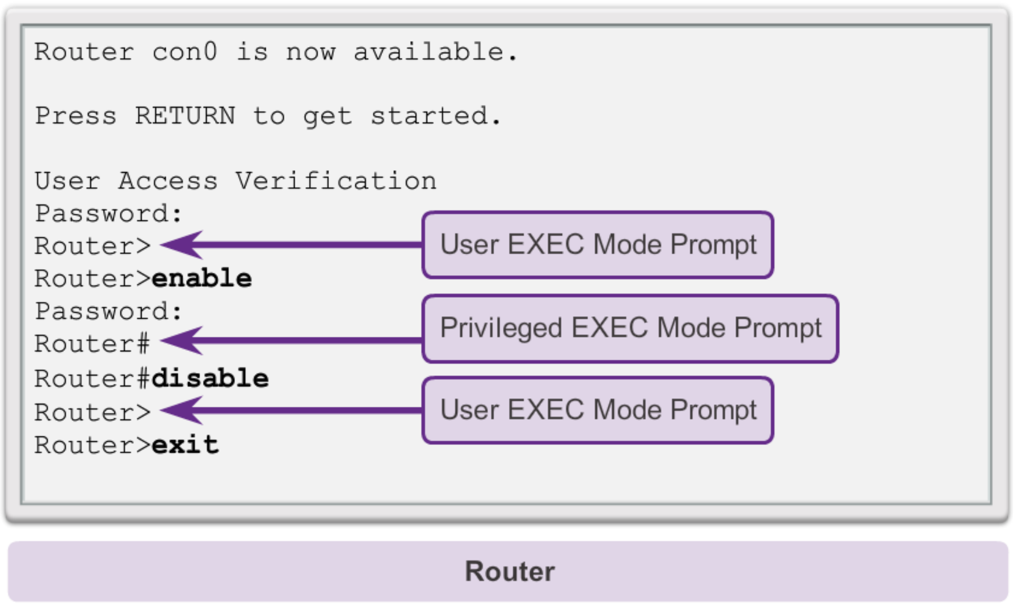
- From the global configuration mode, the user can enter different sub-configuration modes. Each of these modes allows the configuration of a particular part or function of the IOS device. The list below shows a few of them:
  - Interface mode - to configure one of the network interfaces (Fa0/0, S0/0/0)
  - Line mode - to configure one of the physical or virtual lines (console, AUX, VTY)

Navigating between IOS Mode



```
Switch con0 is now available.

Press RETURN to get started.

User Access Verification
Password:
Switch>
Switch>enable
Password:
Switch#
Switch#disable
Switch>
Switch>exit
```

Switch



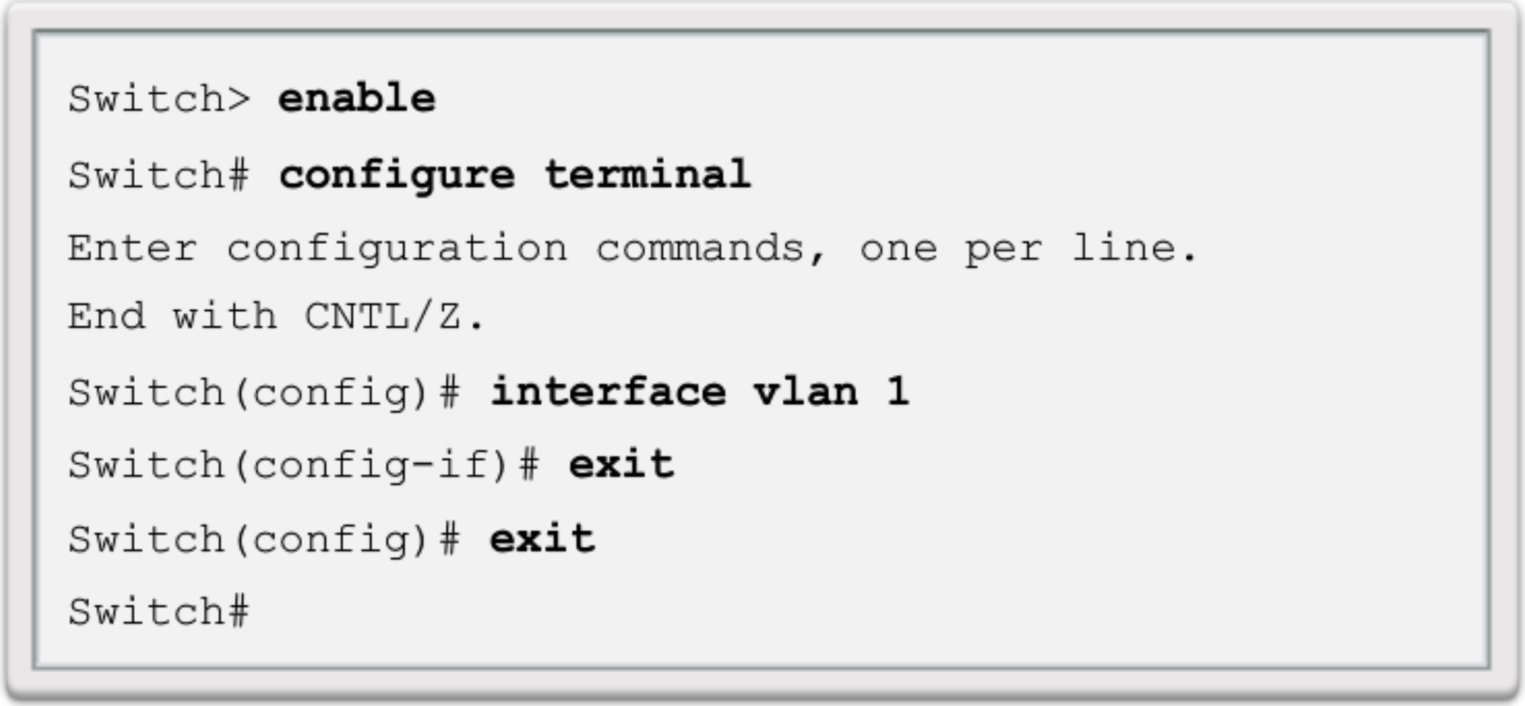
```
Router con0 is now available.

Press RETURN to get started.

User Access Verification
Password:
Router>
Router>enable
Password:
Router#
Router#disable
Router>
Router>exit
```

Router

Navigating the IOS

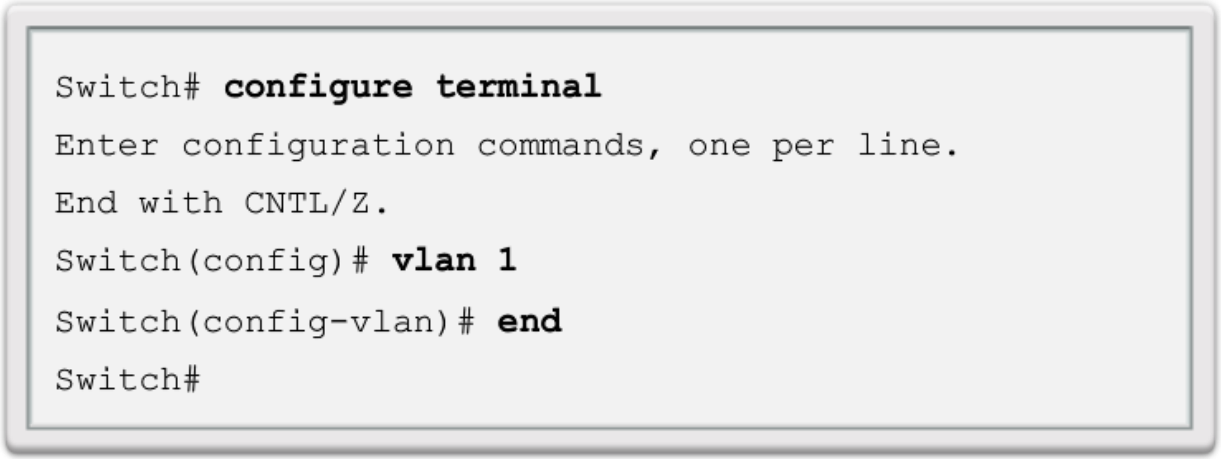
Moving from and to Global Configuration Mode and Submodes

- To quit from the global configuration mode and return to the privileged EXEC mode, enter the exit command.

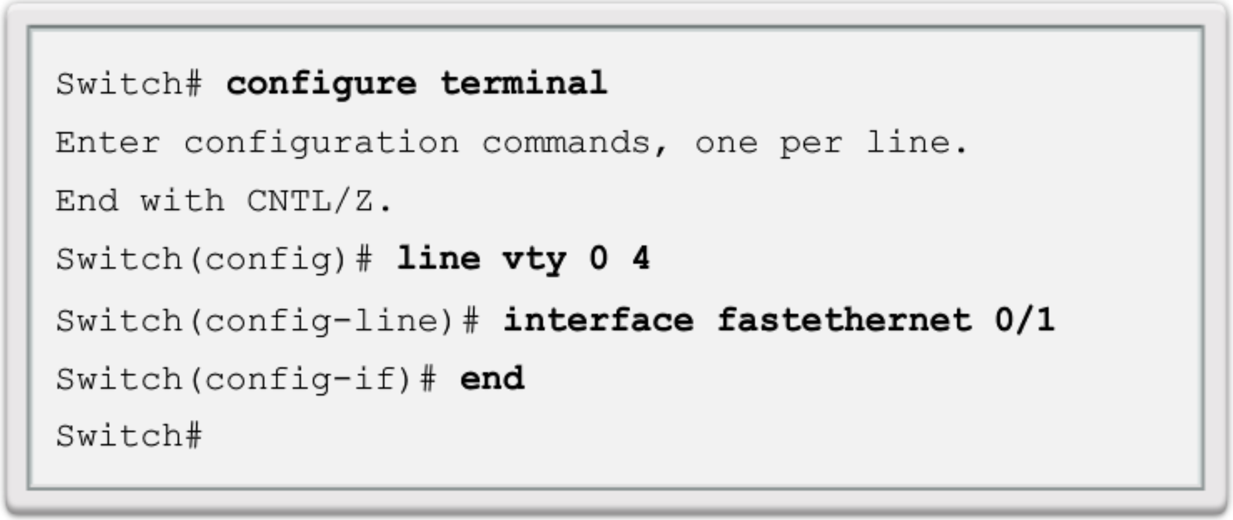


```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# interface vlan 1
Switch(config-if)# exit
Switch(config)# exit
Switch#
```

Navigating the IOS



```
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# vlan 1
Switch(config-vlan)# end
Switch#
```



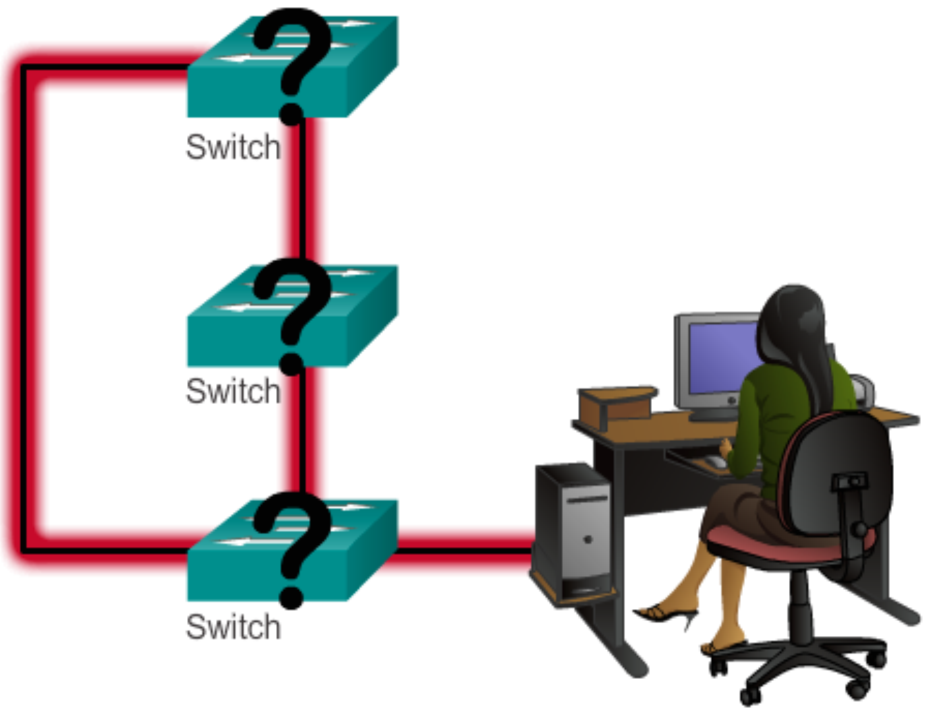
```
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# line vty 0 4
Switch(config-line)# interface fastethernet 0/1
Switch(config-if)# end
Switch#
```

Getting Basic - Hostnames

- When configuring a networking device, one of the first steps is configuring a unique device name, or hostname.
- Some guidelines for naming conventions are that names should:
  - Start with a letter
  - Contain no spaces
  - End with a letter or digit
  - Use only letters, digits, and dashes
  - Be less than 64 characters in length

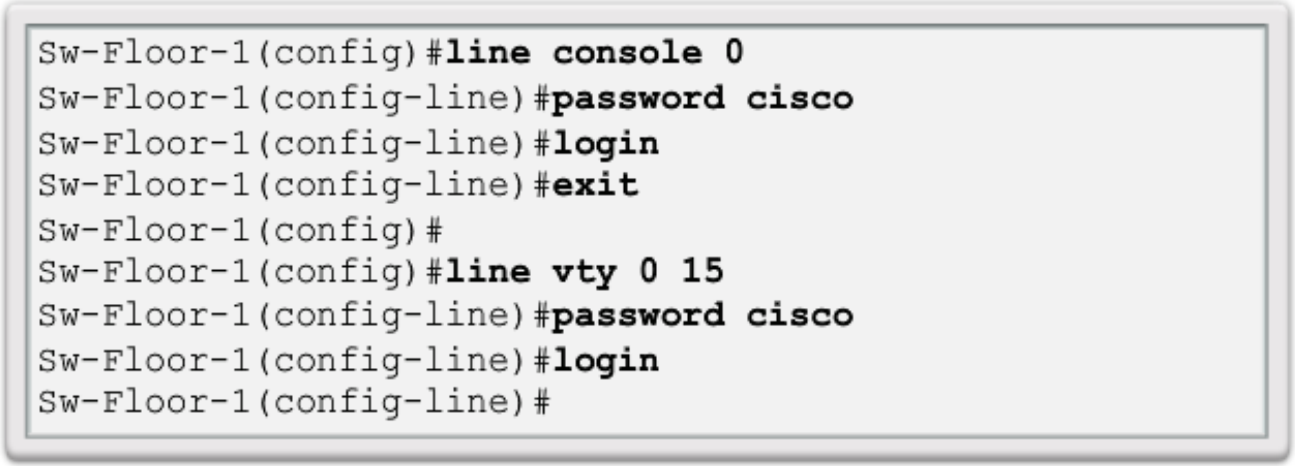
```
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

Basic Configuration Using Cisco IOS



Limiting Access to Device Configurations

- The passwords introduced here are:
  - Enable password - Limits access to the privileged EXEC mode
  - Enable secret - Encrypted, limits access to the privileged EXEC mode
  - Console password - Limits device access using the console connection
  - VTY password - Limits device access over Telnet

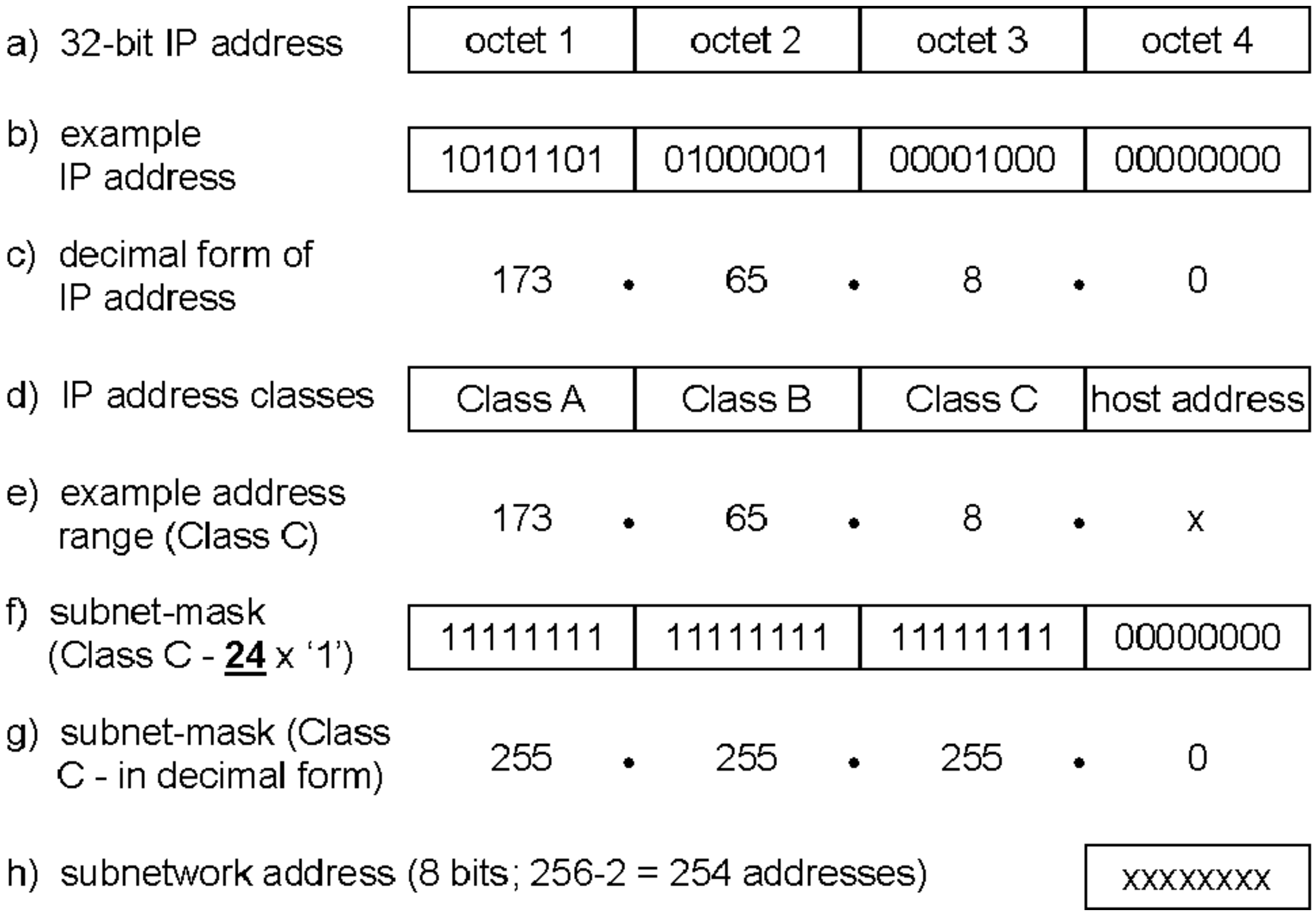


```
Sw-Floor-1(config)#line console 0
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#exit
Sw-Floor-1(config)#
Sw-Floor-1(config)#line vty 0 15
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#
```

Address Schemes - Ports and Addresses

- Each end device on a network must be configured with IP addresses. Some examples of end devices are:
  - Computers (work stations, laptops, file servers, web servers)
  - Network printers
  - VoIP phones
  - Security cameras
  - Smart phones
  - Mobile handheld devices (such as wireless barcode scanners)

IP Address v4



a) 32-bit IP address	octet 1	octet 2	octet 3	octet 4
b) example IP address	10101101	01000001	00001000	00000000
c) decimal form of IP address	173 •	65 •	8 •	0
d) IP address classes	Class A	Class B	Class C	host address
e) example address range (Class C)	173 •	65 •	8 •	x
f) subnet-mask (Class C - **<u>24</u>** x '1')	11111111	11111111	11111111	00000000
g) subnet-mask (Class C - in decimal form)	255 •	255 •	255 •	0
h) subnetwork address (8 bits; 256-2 = 254 addresses)				xxxxxxxx

Figure 5.9 Classful IP addressing scheme.

IP Addresses

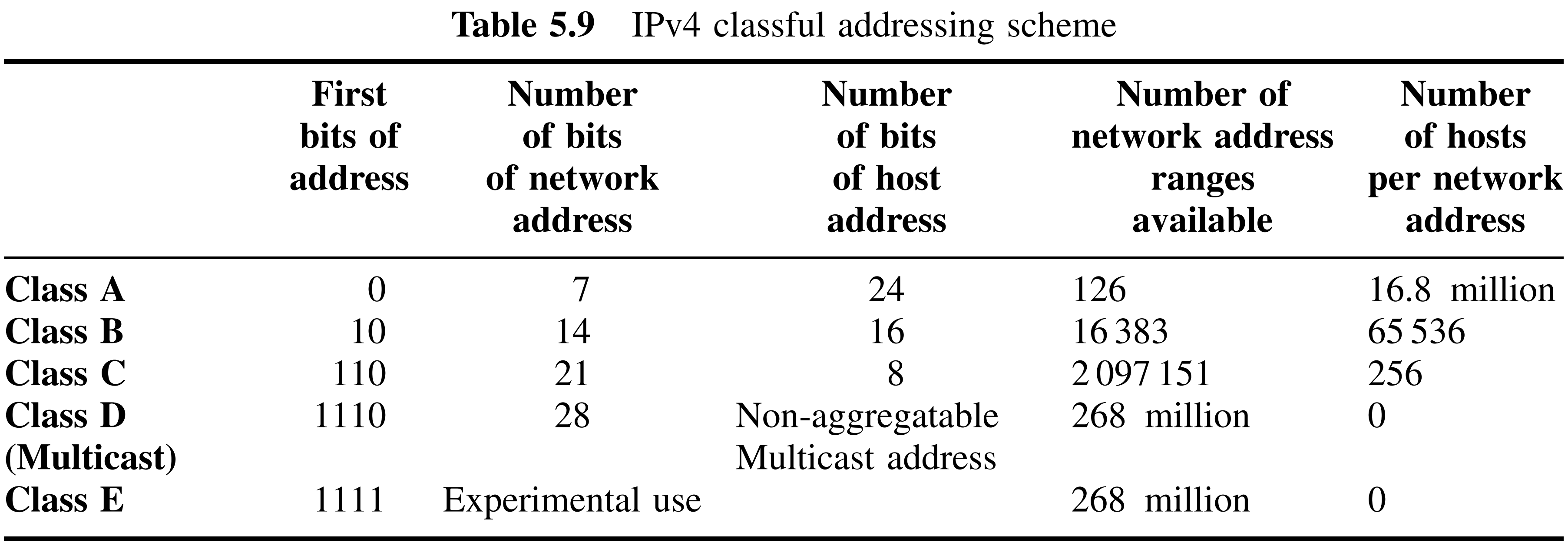
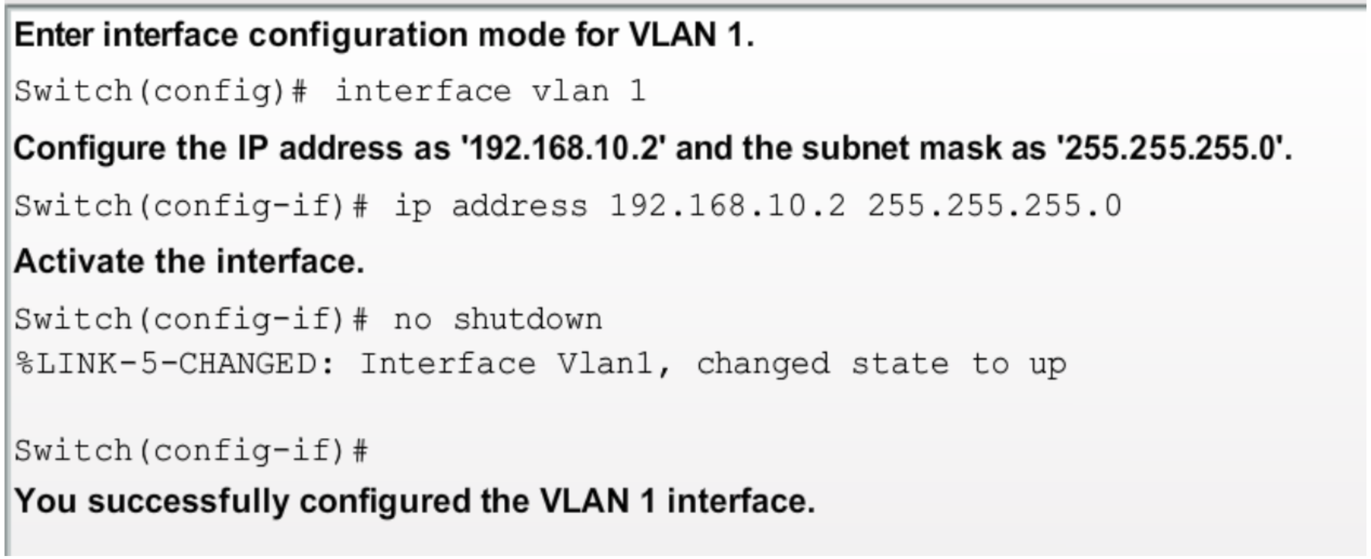


Table 5.9 IPv4 classful addressing scheme

	First bits of address	Number of bits of network address	Number of bits of host address	Number of network address ranges available	Number of hosts per network address
Class A	0	7	24	126	16.8 million
Class B	10	14	16	16 383	65 536
Class C	110	21	8	2 097 151	256
Class D (Multicast)	1110	28	Non-aggregatable Multicast address	268 million	0
Class E	1111	Experimental use		268 million	0

Addressing Scheme

- To access the switch remotely, an IP address and a subnet mask must be configured on the SVI:
  - IP address - Together with subnet mask, uniquely identifies end device on the internetwork
  - Subnet mask - Determines which part of a larger network is used by an IP address



Enter interface configuration mode for VLAN 1.

```
Switch(config)# interface vlan 1
```

Configure the IP address as '192.168.10.2' and the subnet mask as '255.255.255.0'.

```
Switch(config-if)# ip address 192.168.10.2 255.255.255.0
```

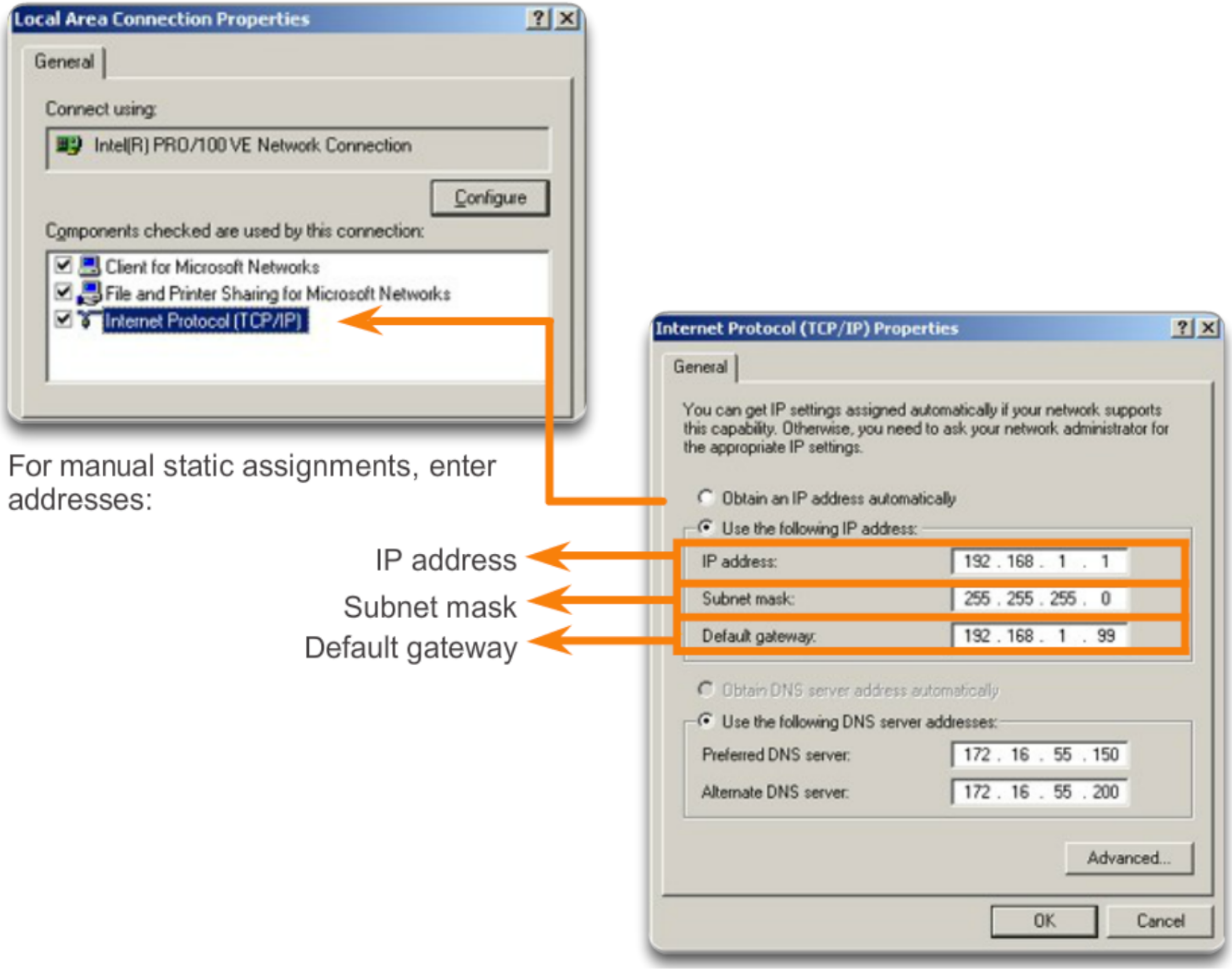
Activate the interface.

```
Switch(config-if)# no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up

Switch(config-if)#
```

You successfully configured the VLAN 1 interface.

Manual IP Address Configuration for End Devices

Addressing End Devices



Local Area Connection Properties

General

Connect using:

Intel(R) PRO/100 VE Network Connection

Components checked are used by this connection:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol (TCP/IP)

For manual static assignments, enter addresses:

IP address

Subnet mask

Default gateway

Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 1 . 1
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 99

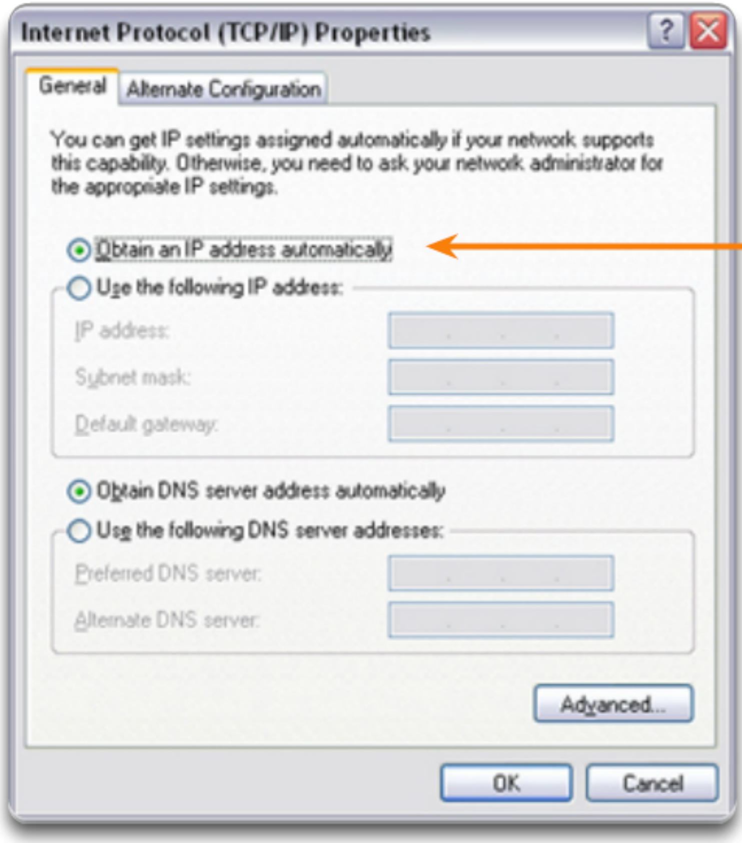
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	172 . 16 . 55 . 150
Alternate DNS server:	172 . 16 . 55 . 200

Automatic IP Address Configuration for End Devices

Assigning Dynamic Addresses



Internet Protocol (TCP/IP) Properties

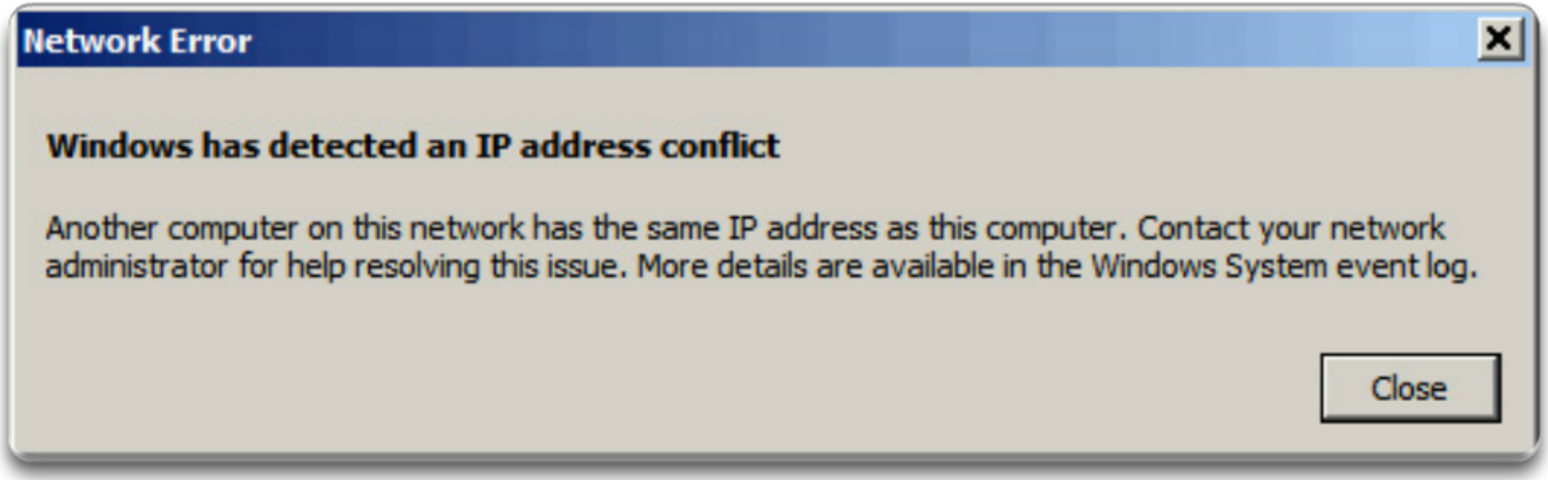
General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

- ● Obtain an IP address automatically
- ○ Use the following IP address:
  - IP address:
  - Subnet mask:
  - Default gateway:
- ● Obtain DNS server address automatically
- ○ Use the following DNS server addresses:
  - Preferred DNS server:
  - Alternate DNS server:

This property will set the device to obtain an IP address automatically.

IP Address Conflicts



Network Error

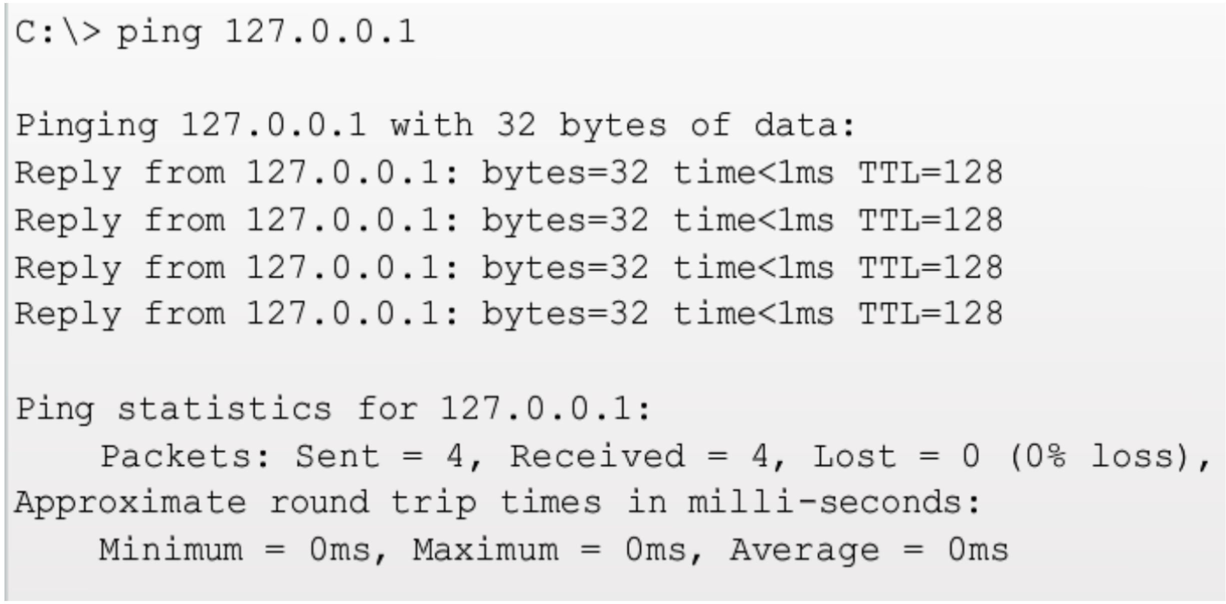
Windows has detected an IP address conflict

Another computer on this network has the same IP address as this computer. Contact your network administrator for help resolving this issue. More details are available in the Windows System event log.

- Usually static IP addresses are used with servers and printers in a small- to medium-sized business network, while employee devices use DHCP-allocated IP address information.

Verifying Connectivity

- Testing the Loopback
  - The ping command is used to verify the internal IP configuration on a local host.
  - This test is accomplished by using the ping command on a reserved address called the loopback (127.0.0.1).
  - The loopback address, 127.0.0.1, is defined by the TCP/IP protocol as a reserved address that routes packets back to the host.



```
C:\> ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```