Introduction

NETWORK SECURITY

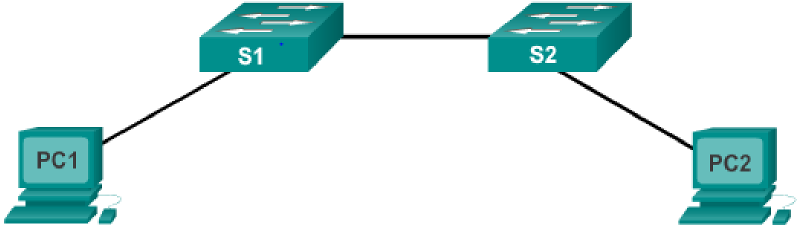
Dr. Md. Nadir Bin Ali

Lecture-2

Operating Systems

All networking equipment depend

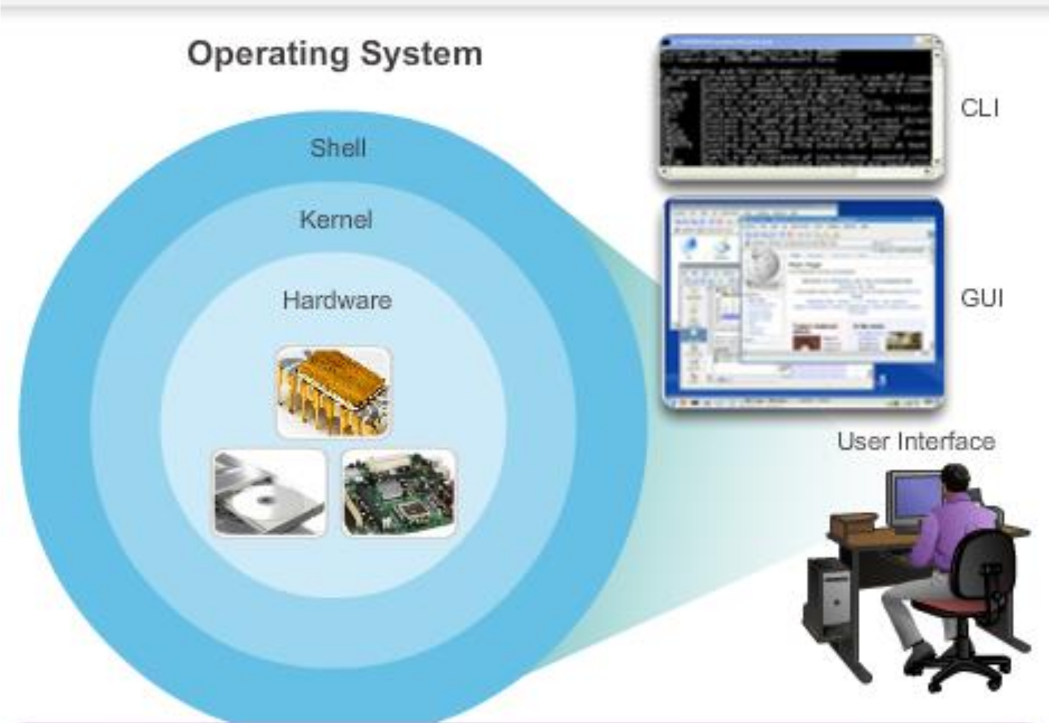
- End users (PCs, laptops, sma
- Switches
- Routers
- Wireless access points
- Firewalls



Internetwork Operating System (IOS)

- Collection of network operating systems used on devices

Operating Systems



Shell: The user interface that allows users to request specific tasks from the computer. These requests can be made either through the CLI or GUI interfaces.

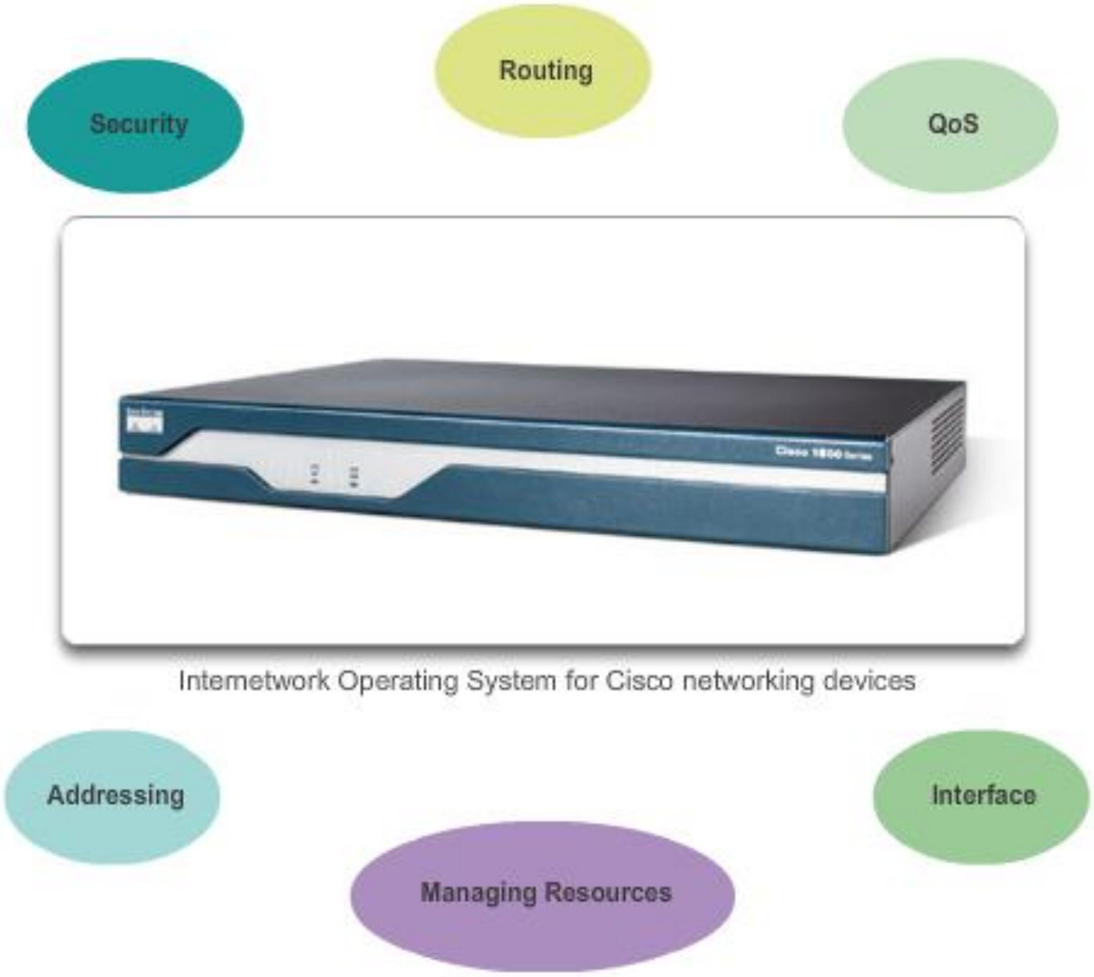
Location of the Cisco IOS

IOS stored in **Flash**

- Non-volatile storage – not lost when power is lost
- Can be changed or overwritten as needed
- Can be used to store multiple versions of IOS
- IOS copied from flash to volatile RAM
- Quantity of flash and RAM memory determines IOS that can be used

IOS Functions

Major functions performed or enabled by Cisco routers and switches include:



Security

Routing

QoS

Internetwork Operating System for Cisco networking devices

Addressing

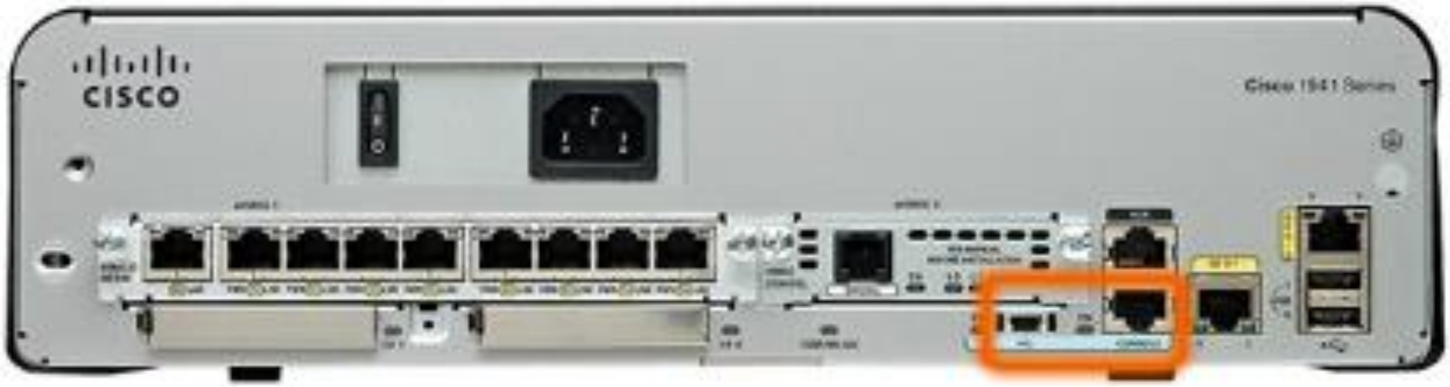
Interface

Managing Resources

Console Access Method

Most common methods to access the Command Line Interface

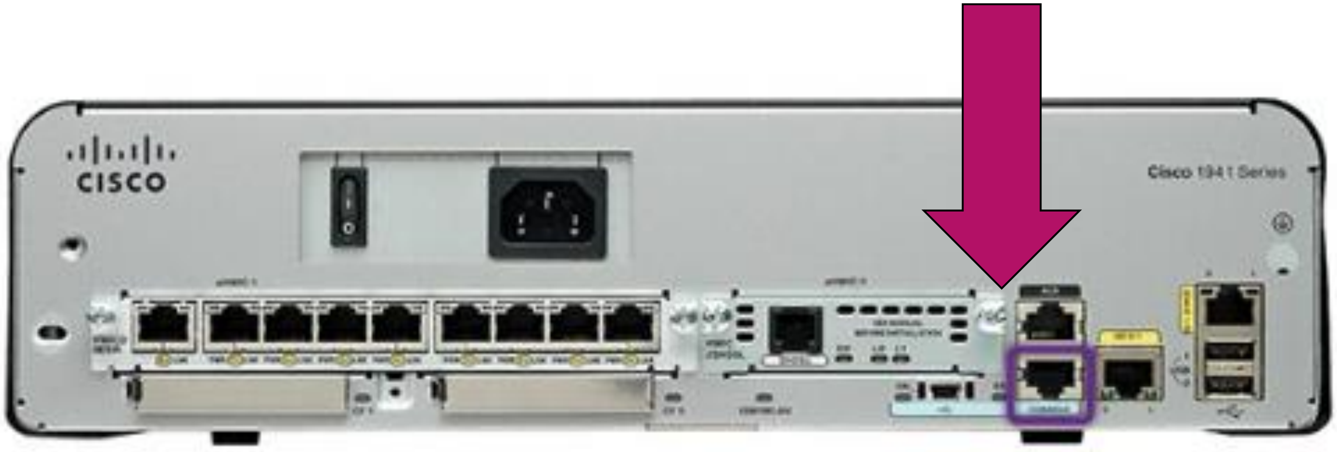
- Console
- Telnet or SSH
- AUX port



Console Access Method

Console port

- Device is accessible even if no networking services have been configured (out-of-band)
- Need a special console cable
- Allows configuration commands to be entered
- Should be configured with passwords to prevent unauthorized access
- Device should be located in a secure room so console port can not be easily accessed



Telnet, SSH, and AUX Access Methods

Telnet

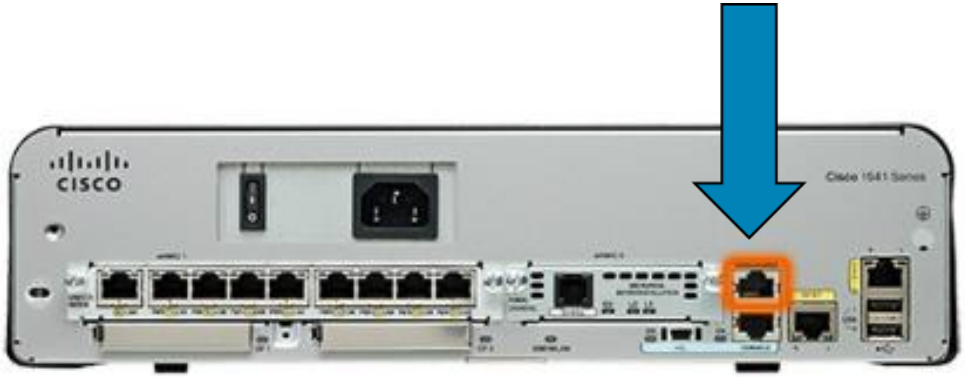
- Method for remotely accessing the CLI over a network
- Require active networking services and one active interface that is configured

Secure Shell (SSH)

- Remote login similar to Telnet but utilizes more security
- Stronger password authentication
- Uses encryption when transporting data

Aux Port

- Out-of-band connection
- Uses telephone line
- Can be used like console port

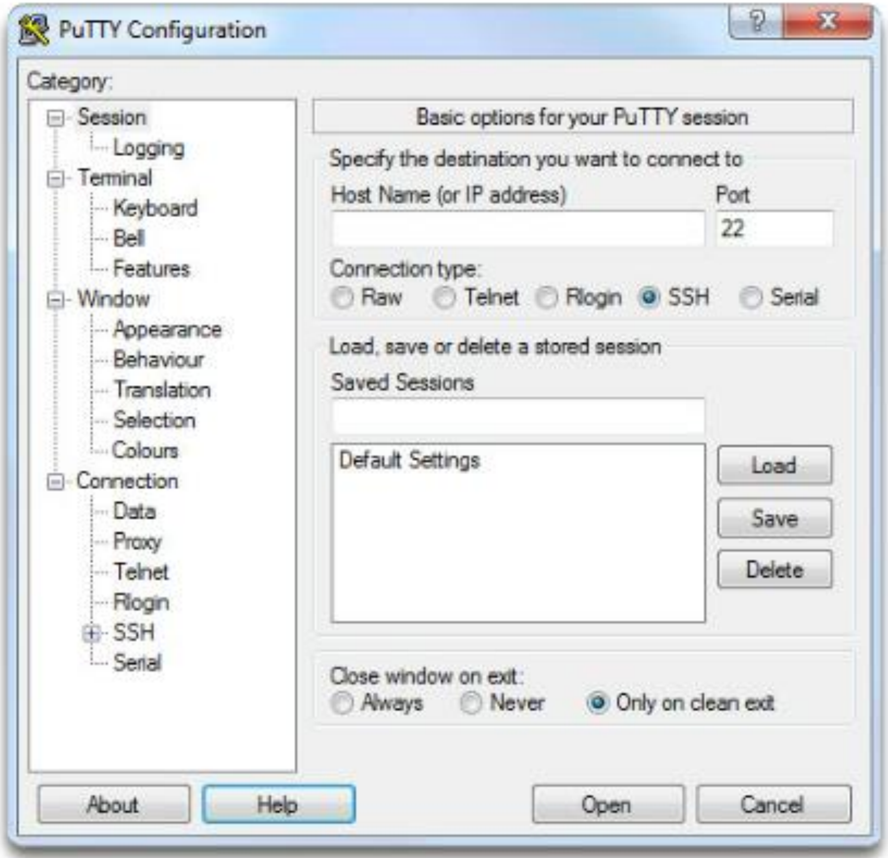


Terminal Emulation Programs

Software available for connecting to a networking device

- PuTTY
- Tera Term
- SecureCRT
- HyperTerminal
- OS X Terminal

PuTTY



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

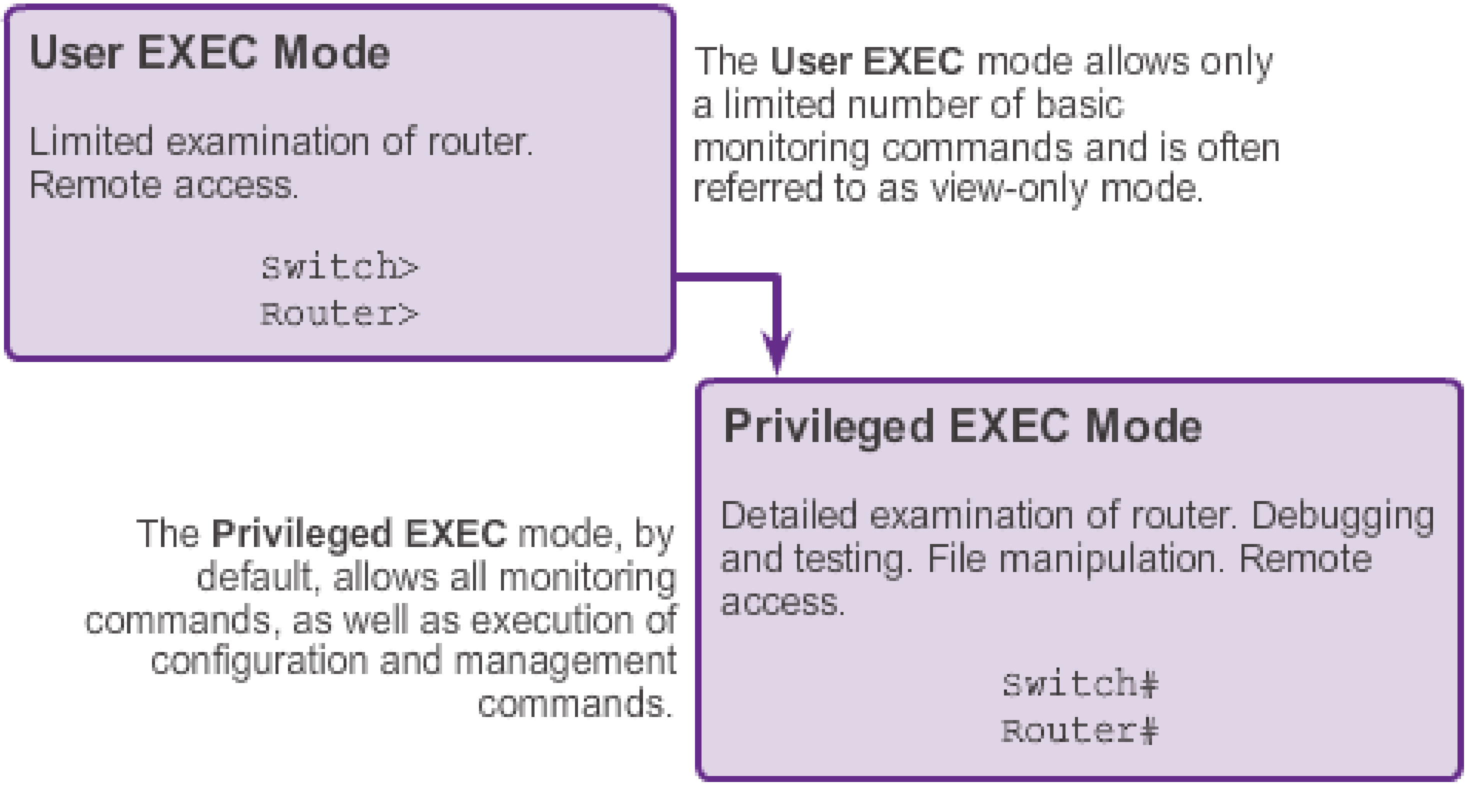
Load, save or delete a stored session

Saved Sessions

Default Settings

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

Primary Modes



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.

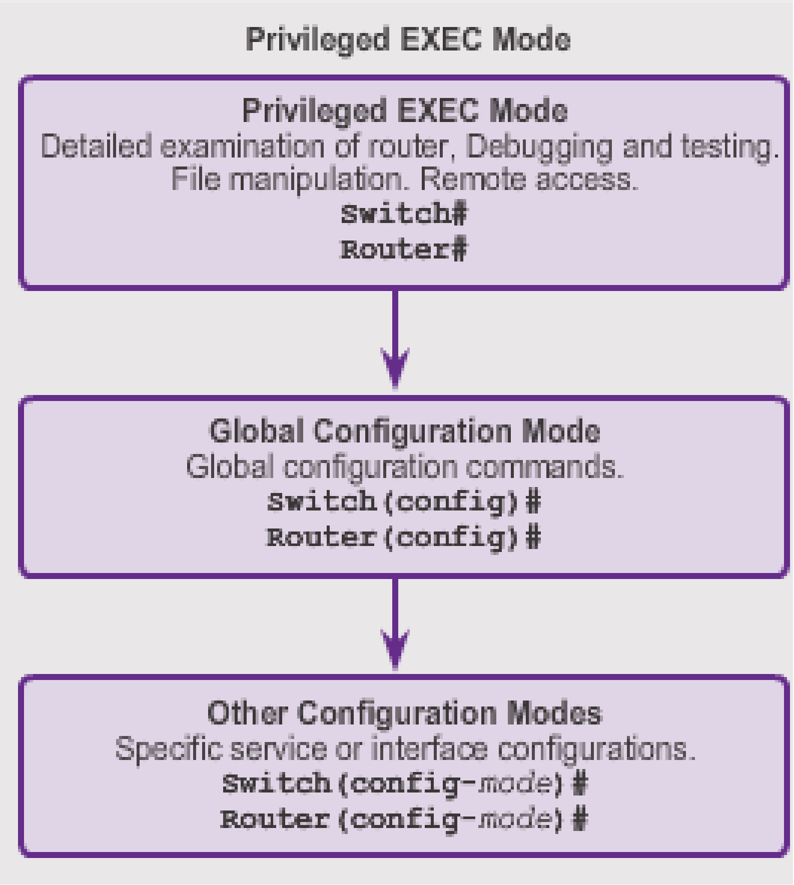
Privileged EXEC Mode

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.

Global Configuration Mode and Submodes

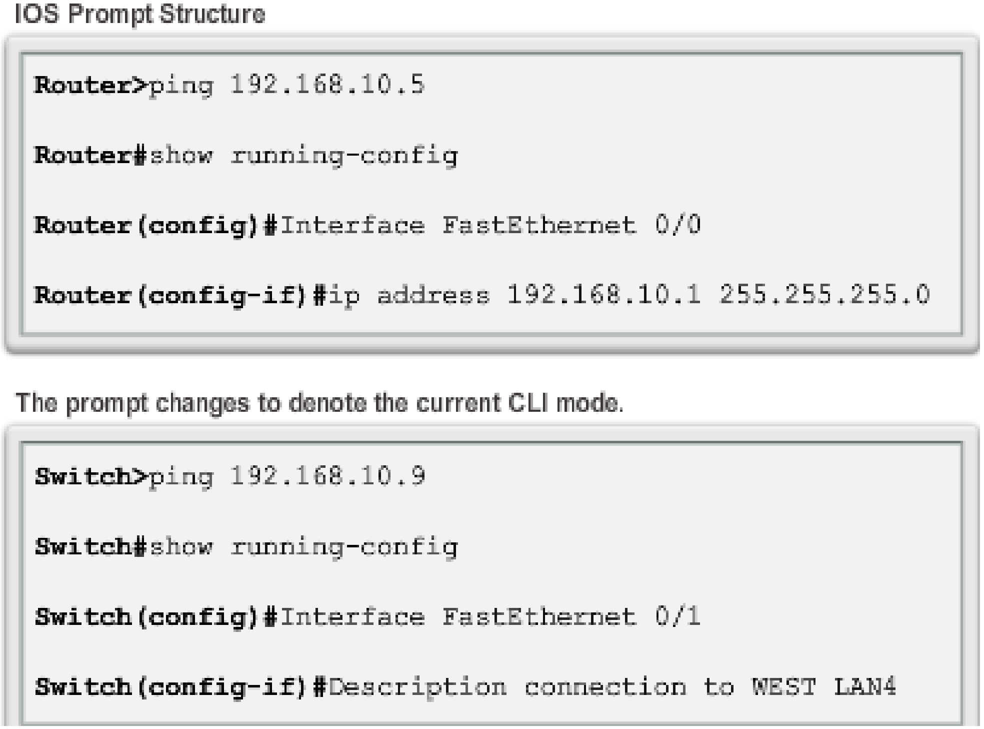


Privileged EXEC Mode

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)#`



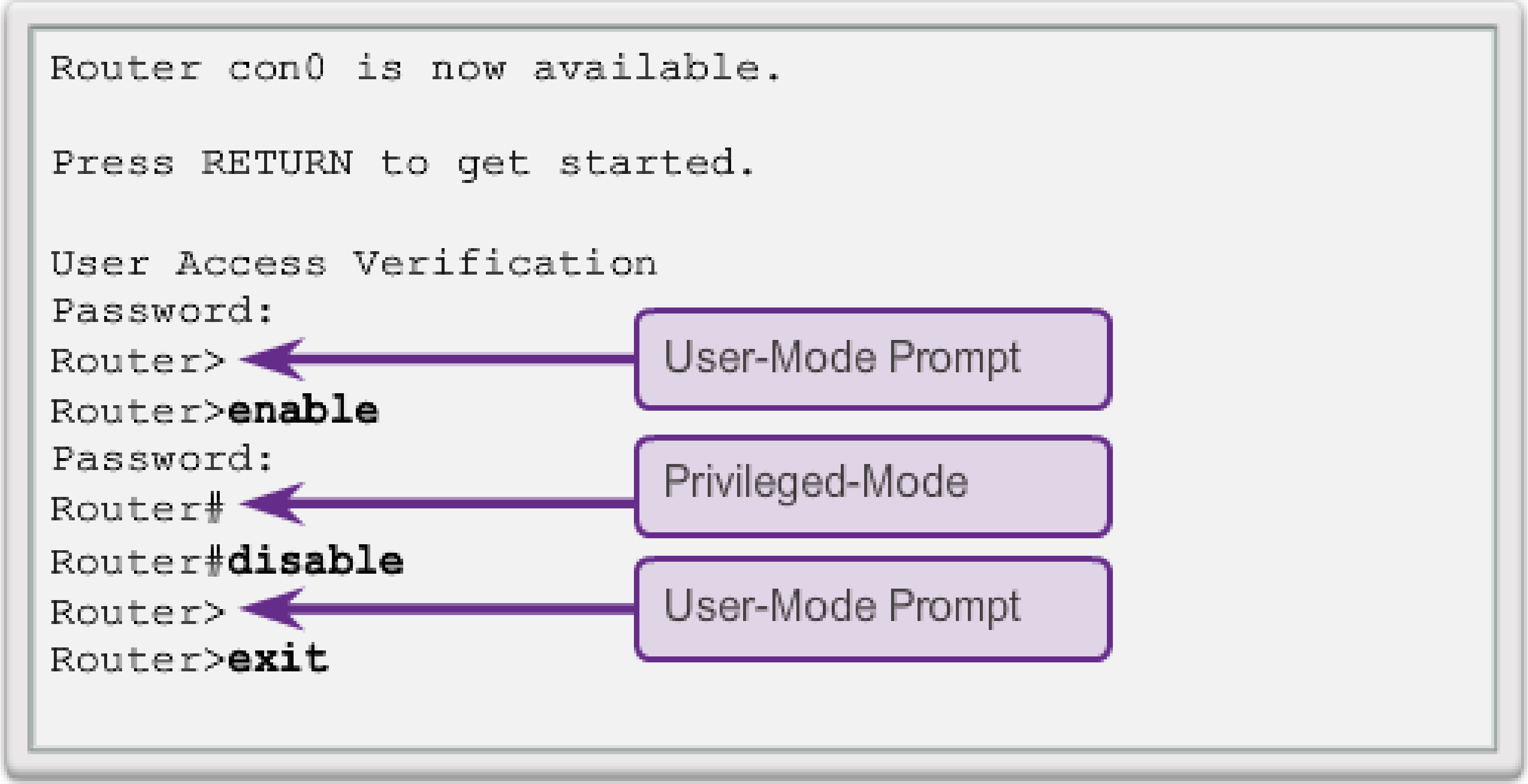
IOS Prompt Structure

```
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
```

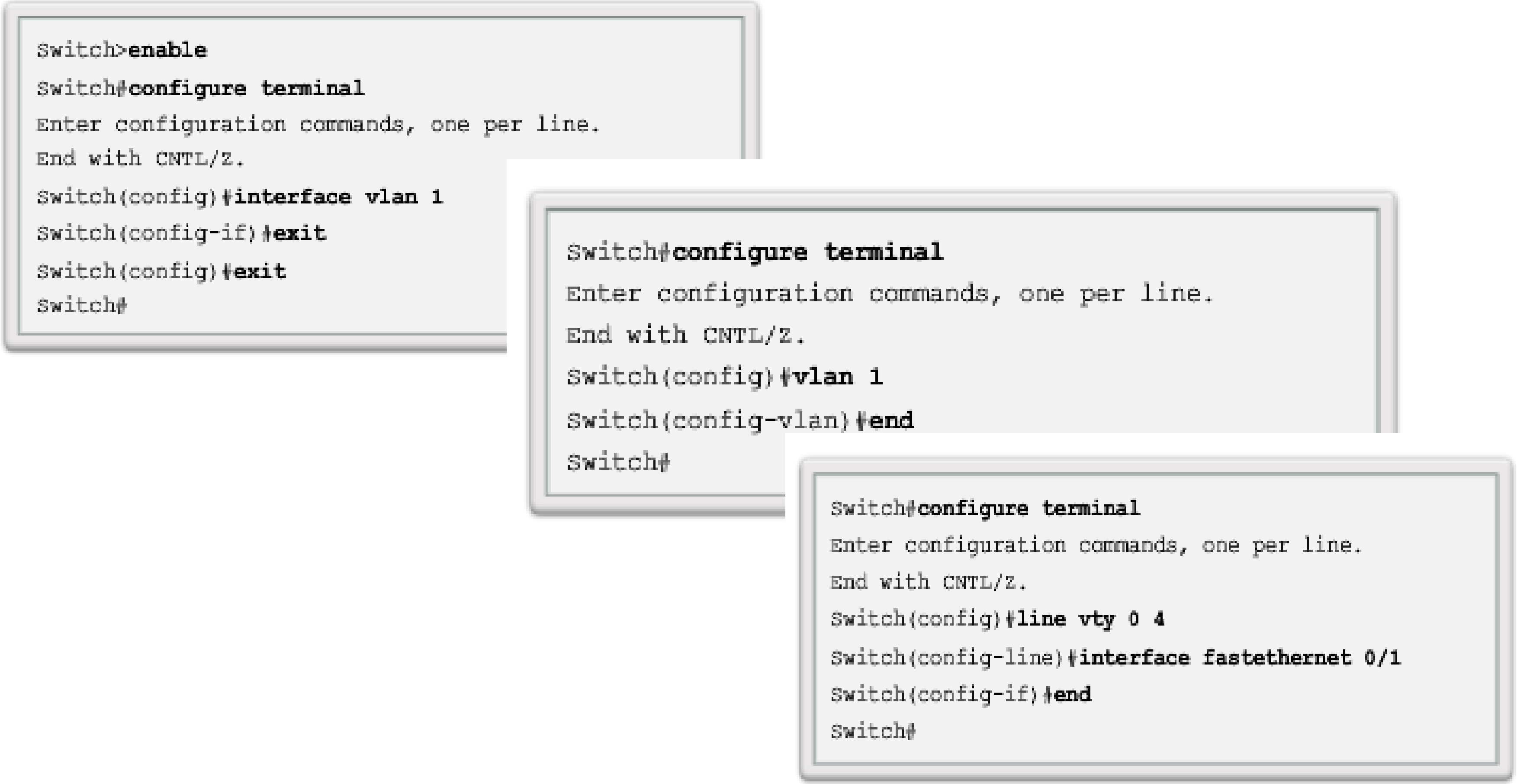
Navigating between IOS Modes



```
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 between IOS Modes (cont.)



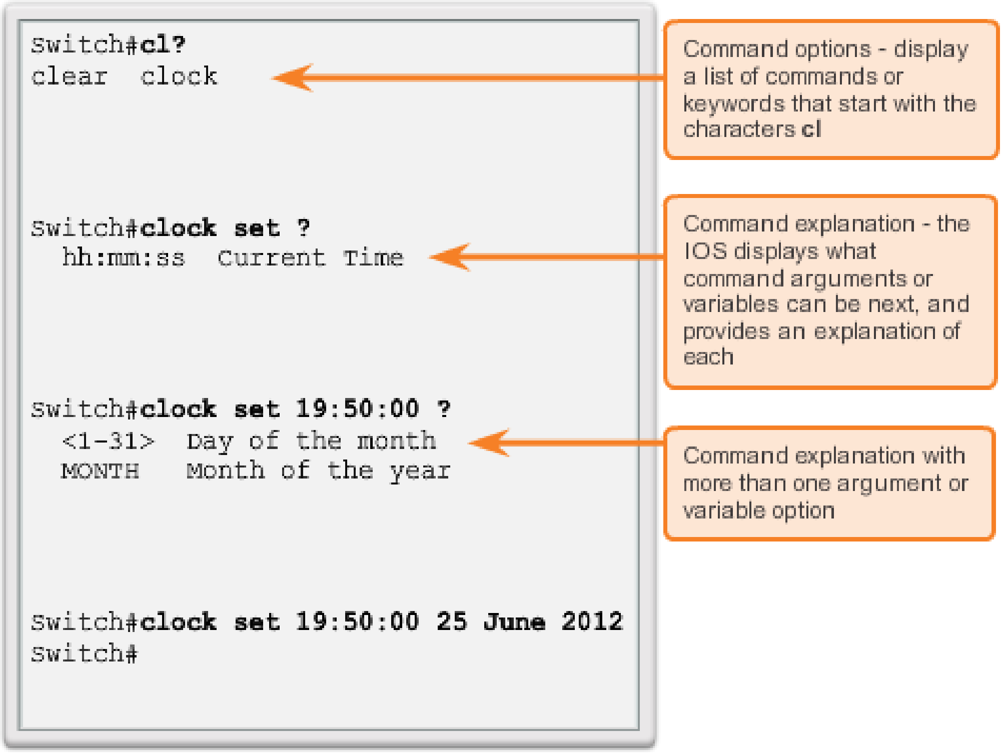
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#exit
Switch(config)#exit
Switch#
```

```
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#
```

Context Sensitive Help

Context Sensitive Help



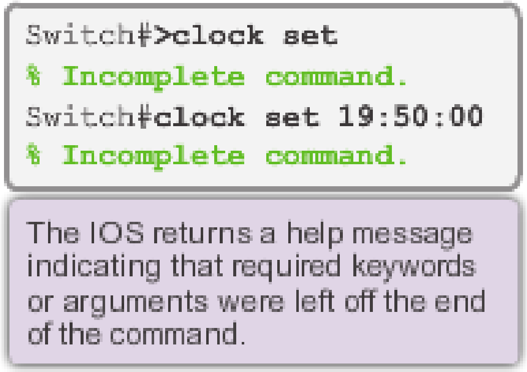
```
Switch#cl?
clear  clock



Switch#clock set ?
  hh:mm:ss  Current Time



Switch#clock set 19:50:00 ?
  <1-31>  Day of the month
  MONTH   Month of the year



Switch#clock set 19:50:00 25 June 2012
Switch#
```

Command options - display a list of commands or keywords that start with the characters **cl**

Command explanation - the IOS displays what command arguments or variables can be next, and provides an explanation of each

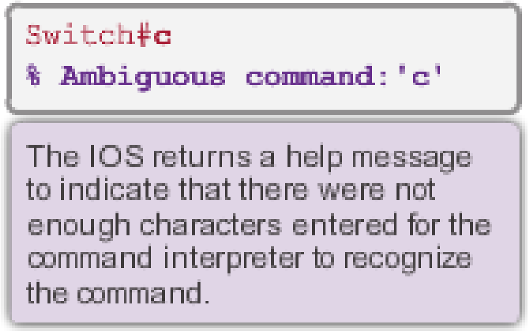
Command explanation with more than one argument or variable option

Command Syntax Check



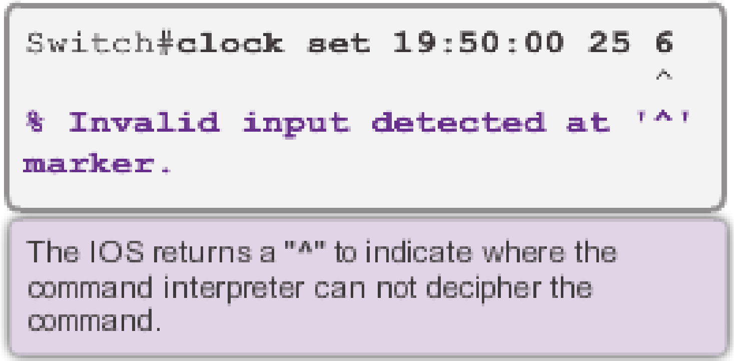
```
Switch#>clock set
% Incomplete command.
Switch#clock set 19:50:00
% Incomplete command.
```

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



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

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



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

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

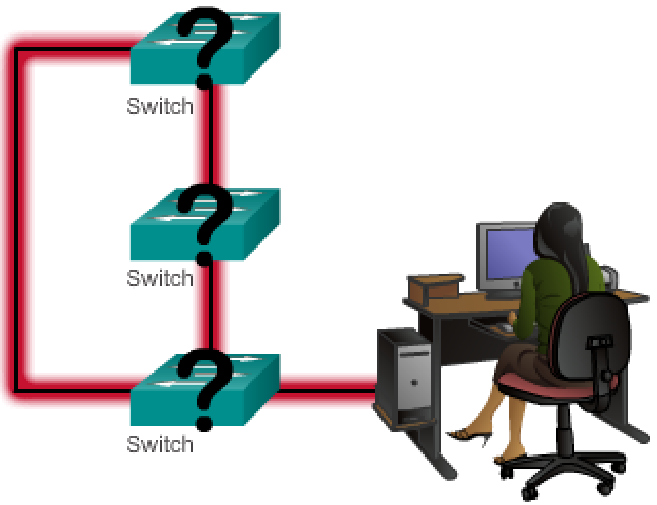
Getting Basic

Device Names

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

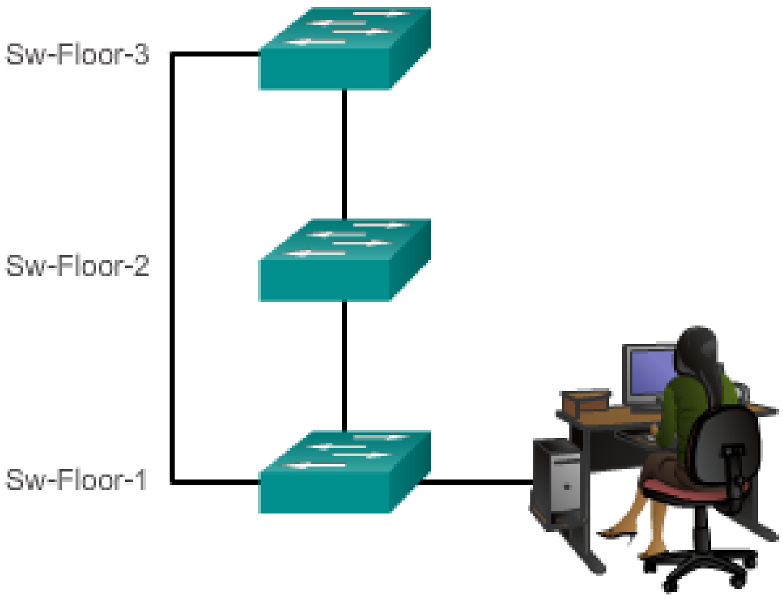
Without names, network devices are difficult to identify for configuration purposes.



Hostnames

Hostnames allow devices to be identified by network administrators over a network or the Internet.

Configuring Device Names



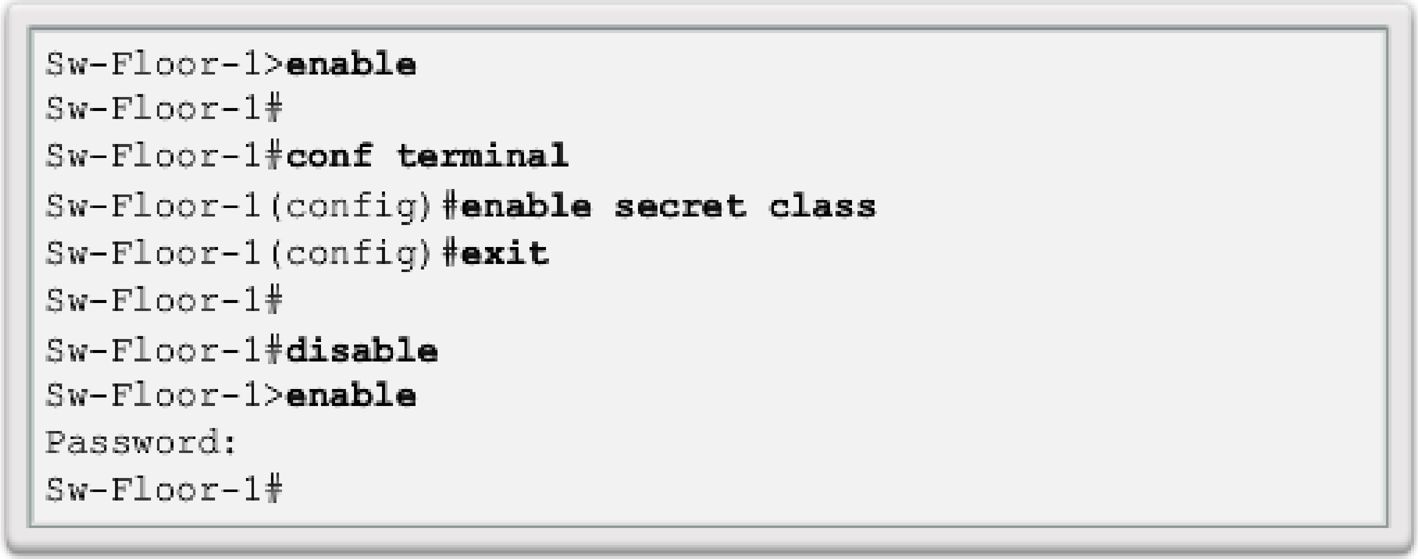
Securing Device Access

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

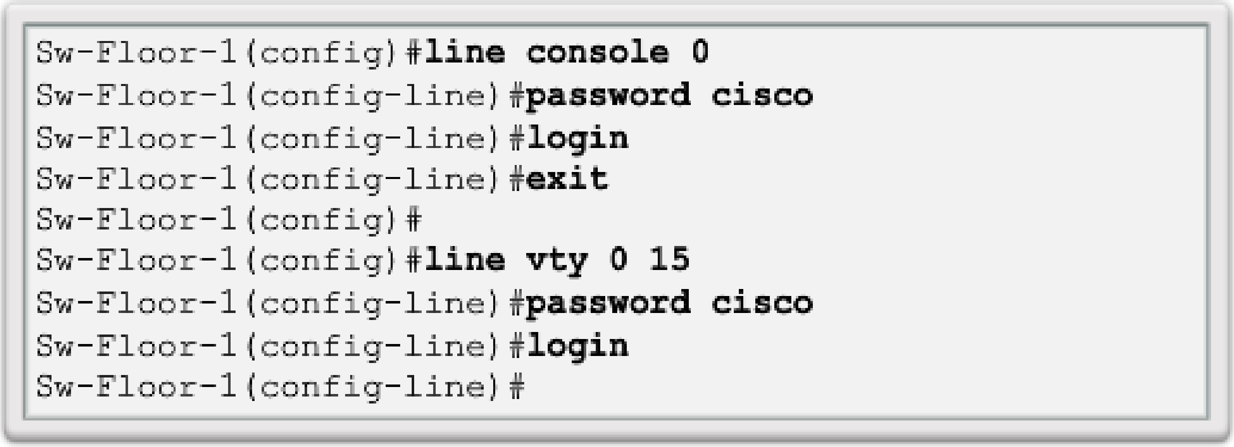
Securing Privileged EXEC Access

- use the **enable secret** command, not the older **enable** password command
- **enable secret** provides greater security because the password is encrypted



```
Sw-Floor-1>enable
Sw-Floor-1#
Sw-Floor-1#conf terminal
Sw-Floor-1(config)#enable secret class
Sw-Floor-1(config)#exit
Sw-Floor-1#
Sw-Floor-1#disable
Sw-Floor-1>enable
Password:
Sw-Floor-1#
```

Securing User EXEC Access



```
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)#
```

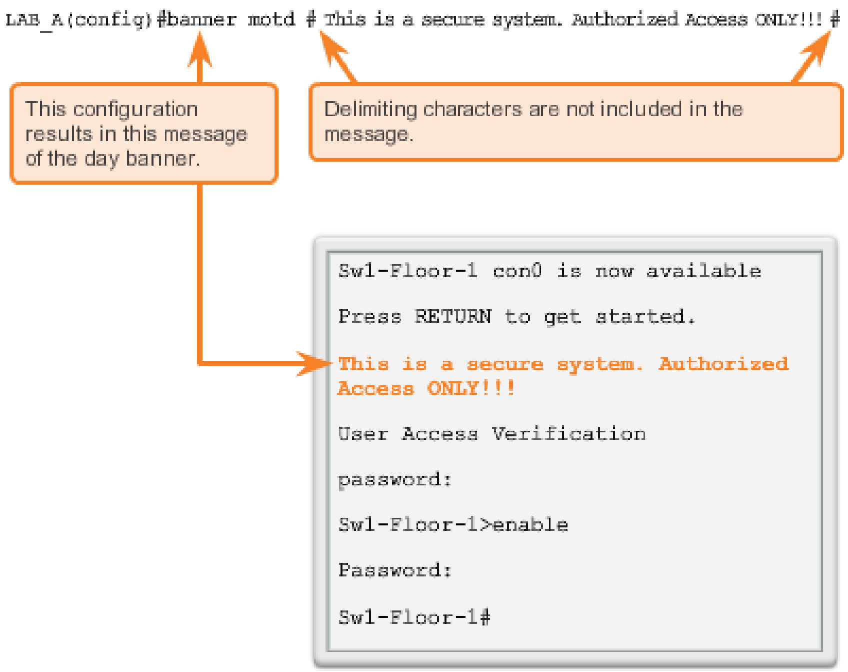
- Console port must be secured
  - reduces the chance of unauthorized personnel physically plugging a cable into the device and gaining device access

- vty lines allow access to a Cisco device via Telnet
  - number of vty lines supported varies with the type of device and the IOS version

Banner Messages

- important part of the legal process in the event that someone is prosecuted for breaking into a device
- wording that implies that a login is "welcome" or "invited" is not appropriate
- often used for legal notification because it is displayed to all connected terminals

Limiting Device Access - MOTD Banner



```
LAB_A(config)#banner motd # This is a secure system. Authorized Access ONLY!!! #
```

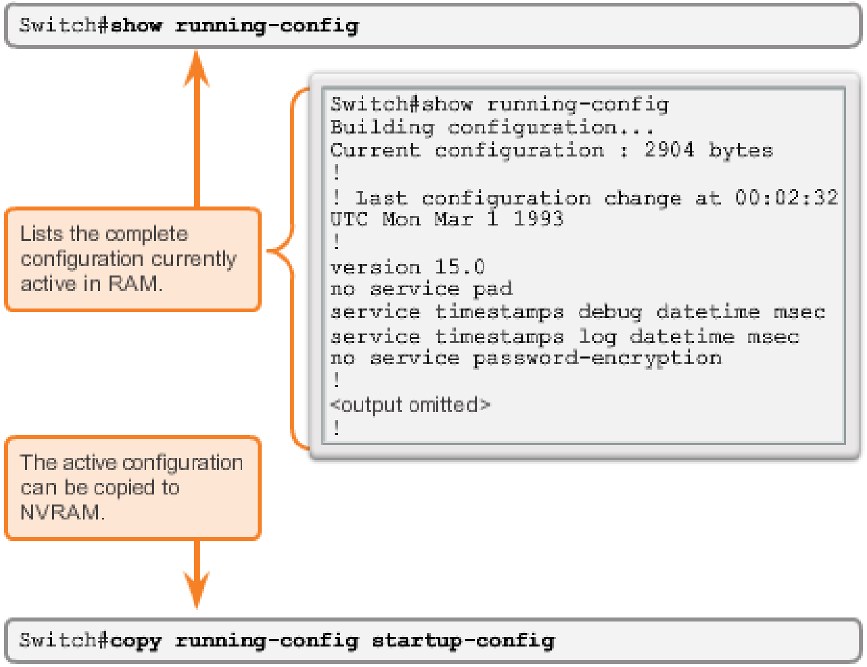
This configuration results in this message of the day banner.

Delimiting characters are not included in the message.

```
Sw1-Floor-1 con0 is now available

Press RETURN to get started.

This is a secure system. Authorized
Access ONLY!!!

User Access Verification

password:

Sw1-Floor-1>enable

Password:

Sw1-Floor-1#
```

Configuration Files

Saving and Erasing the Configuration



```
Switch#show running-config
```

```
Switch#show running-config
Building configuration...
Current configuration : 2904 bytes
!
! Last configuration change at 00:02:32
UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
<output omitted>
!
```

Lists the complete configuration currently active in RAM.

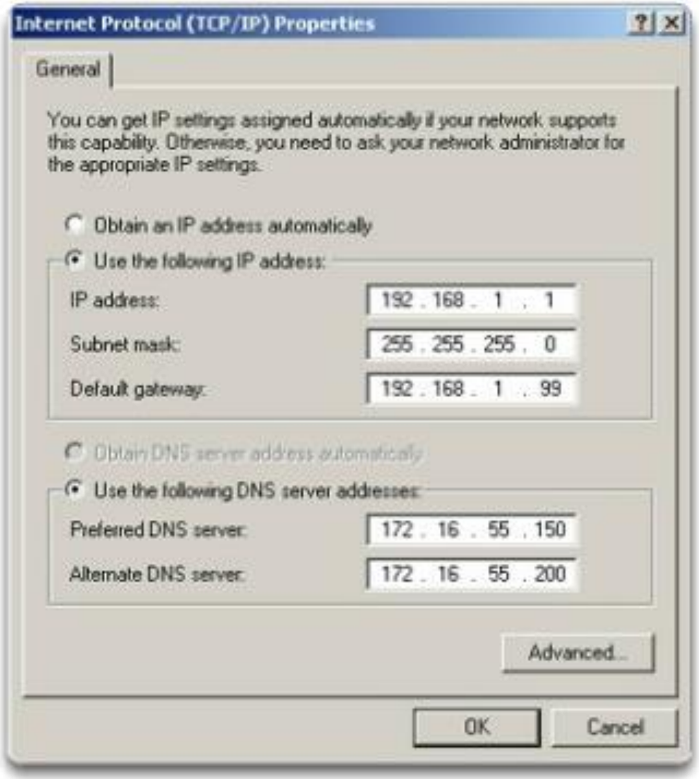
The active configuration can be copied to NVRAM.

```
Switch#copy running-config startup-config
```

Address Schemes

IP Addressing in the Large

- Each end device on a network must be configured with an IP address
- Structure of an IPv4 address is called *dotted decimal*
- IP address displayed in decimal notation, with four decimal numbers between 0 and 255
- With the IP address, a subnet mask is also necessary
- IP addresses can be assigned to both physical ports and virtual interfaces



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

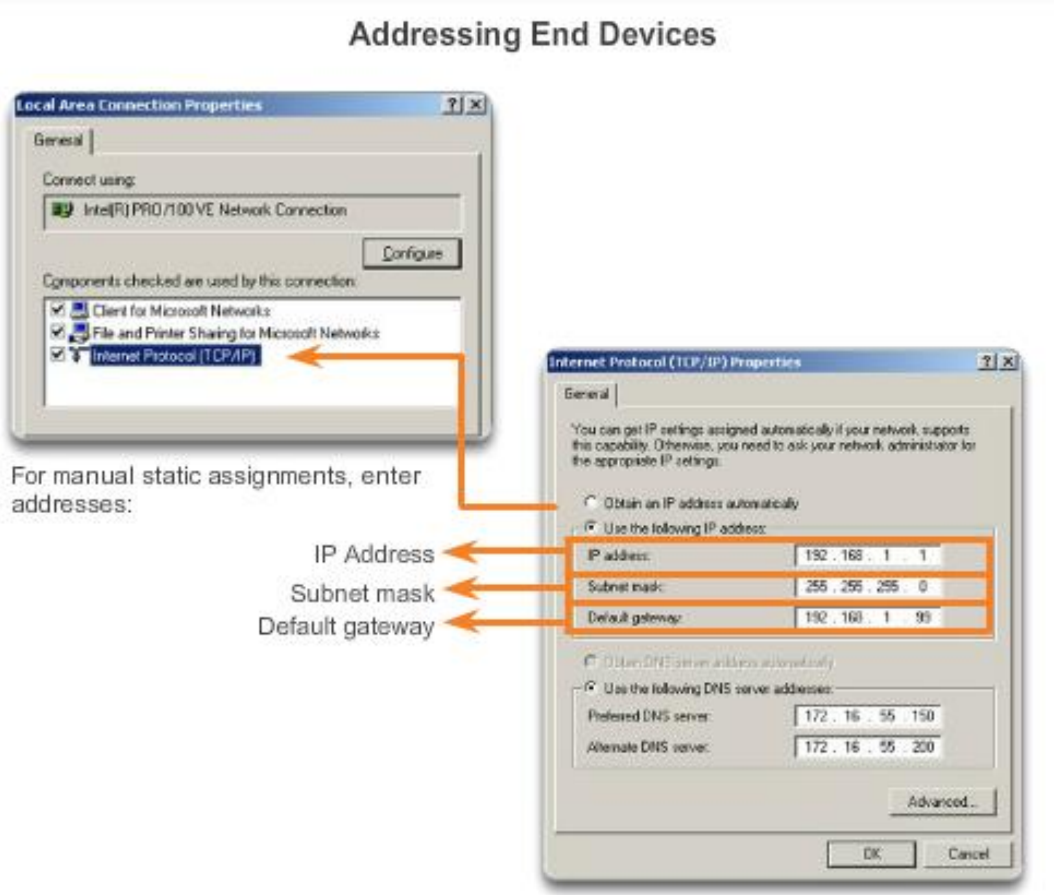
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 172 . 16 . 55 . 150

Alternate DNS server: 172 . 16 . 55 . 200

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)

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

For manual static assignments, enter addresses:

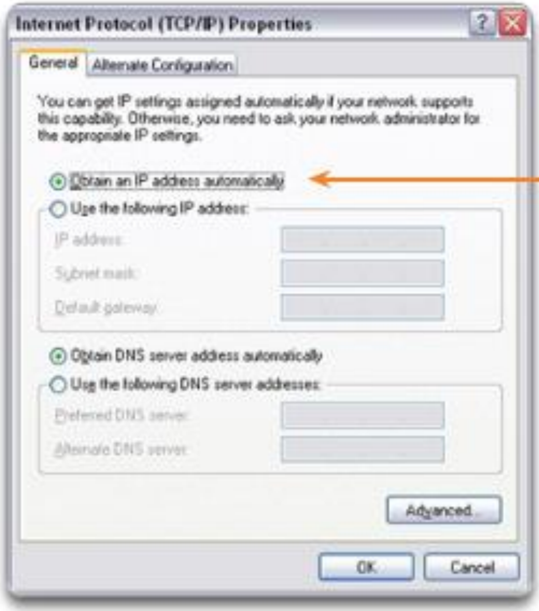
IP Address

Subnet mask

Default gateway

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

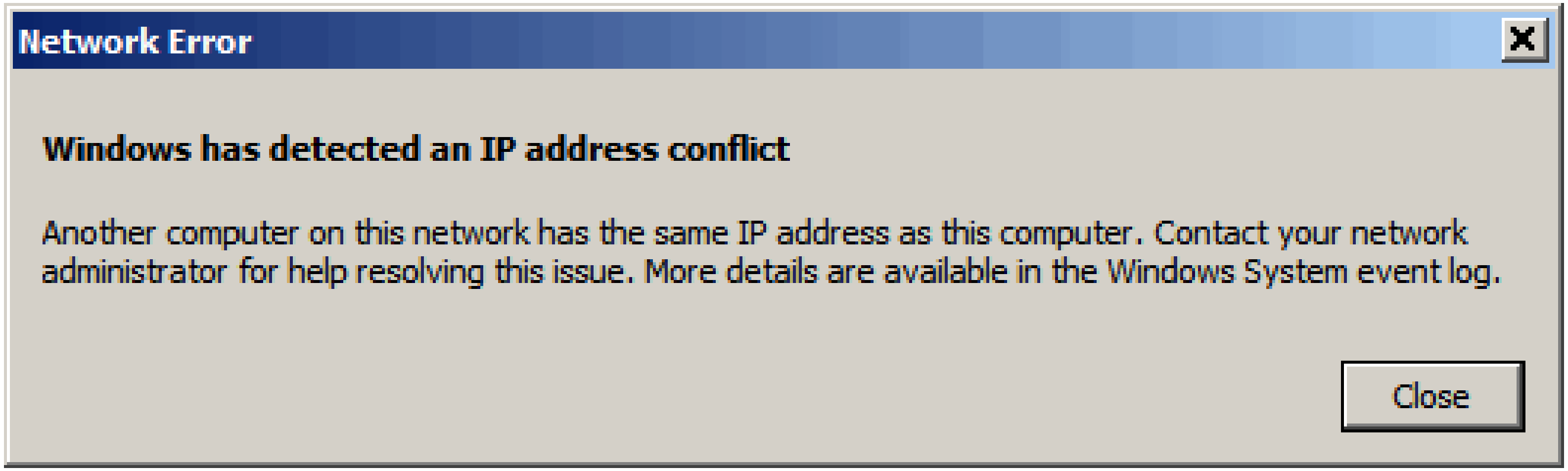
○ Use the following DNS server addresses:

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.

Thank You