



Chapter 2: Configuring a Network Operating System



Introduction to Networks

Cisco | Networking Academy®
Mind Wide Open™



Chapter 2 - Objectives

Upon completion of this chapter you will be able to:

- Explain the purpose of the Cisco IOS.
- Explain how to access and navigate Cisco IOS to configure network devices.
- Describe the command structure of the Cisco IOS software.
- Configure hostnames on a Cisco IOS device using the CLI.
- Use Cisco IOS commands to limit access to device configurations.
- Use Cisco IOS commands to save the running configuration.
- Explain how devices communicate across network media.
- Configure a host device with an IP address.
- Verify connectivity between two end devices.



Chapter 2

2.0 Introduction

2.1 IOS Bootcamp

2.2 Getting Basic

2.3 Addressing Schemes

2.4 Summary



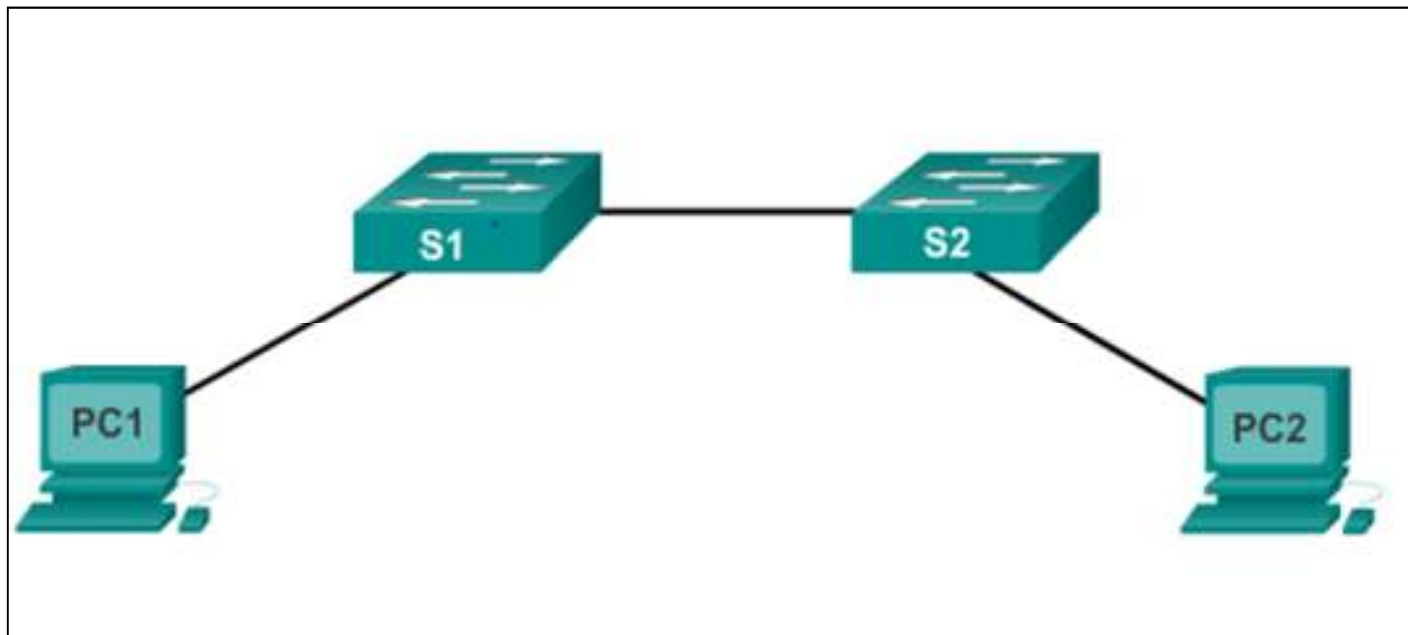
2.1 IOS Bootcamp



Cisco | Networking Academy®
Mind Wide Open™

Cisco IOS Operating Systems

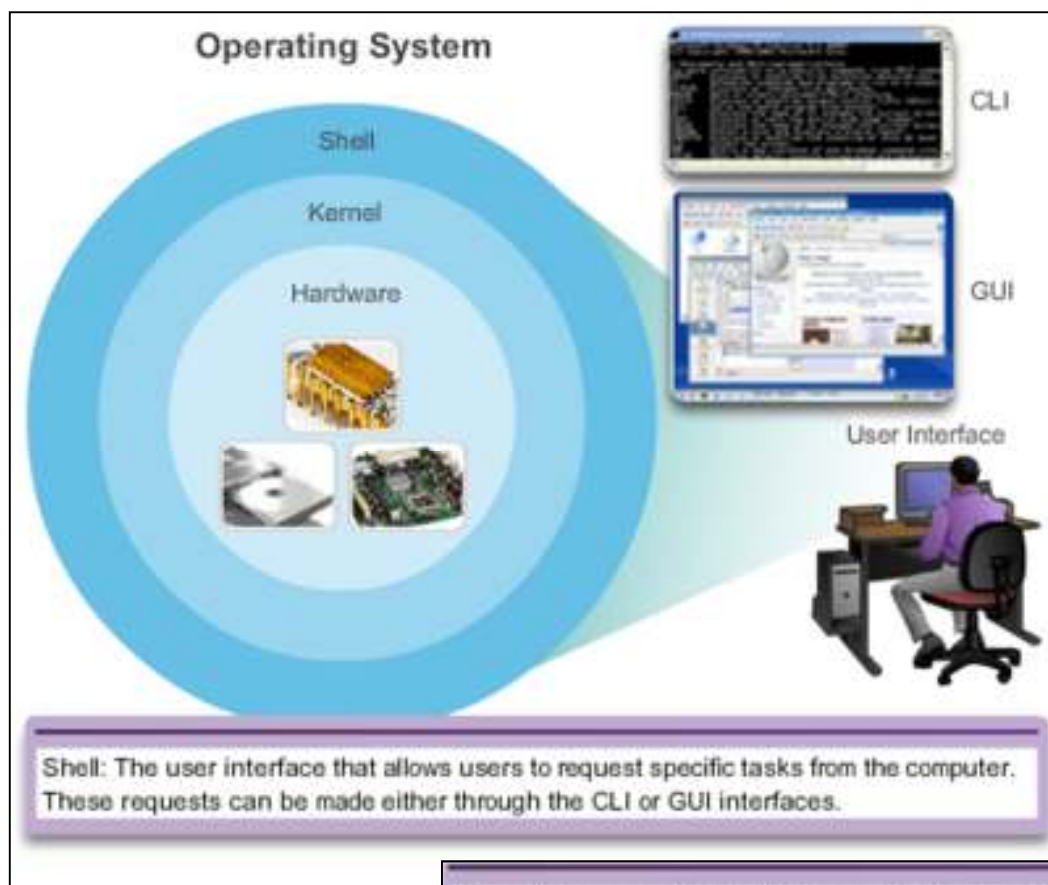
- All networking equipment dependent on operating systems
- The operating system on home routers is usually called firmware
- Cisco IOS – Collection of network operating systems used on Cisco devices





Cisco IOS

Operating Systems (cont.)



Kernel: Communicates between the hardware and software of a computer and manages how hardware resources are used to meet software requirements.

Hardware: The physical part of a computer including underlying electronics.



Cisco IOS

Purpose of OS

- PC operating systems (Windows 8 and OS X) perform technical functions that enable:
 - Use of a mouse
 - View output
 - Enter text
- Switch or router IOS provides options to:
 - Configure interfaces
 - Enable routing and switching functions
- All networking devices come with a default IOS
- Possible to upgrade the IOS version or feature set
- In this course, primary focus is Cisco IOS Release 15.x

Cisco IOS

Location of the Cisco IOS

Cisco 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



Cisco IOS

IOS Functions

These are the major functions performed or enabled by Cisco routers and switches.



Accessing a Cisco IOS Device

Console Access Method

Most common methods to access the CLI:

- Console
- Telnet or SSH
- AUX port



Accessing a Cisco IOS Device

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 cannot be easily accessed





Accessing a Cisco IOS Device

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

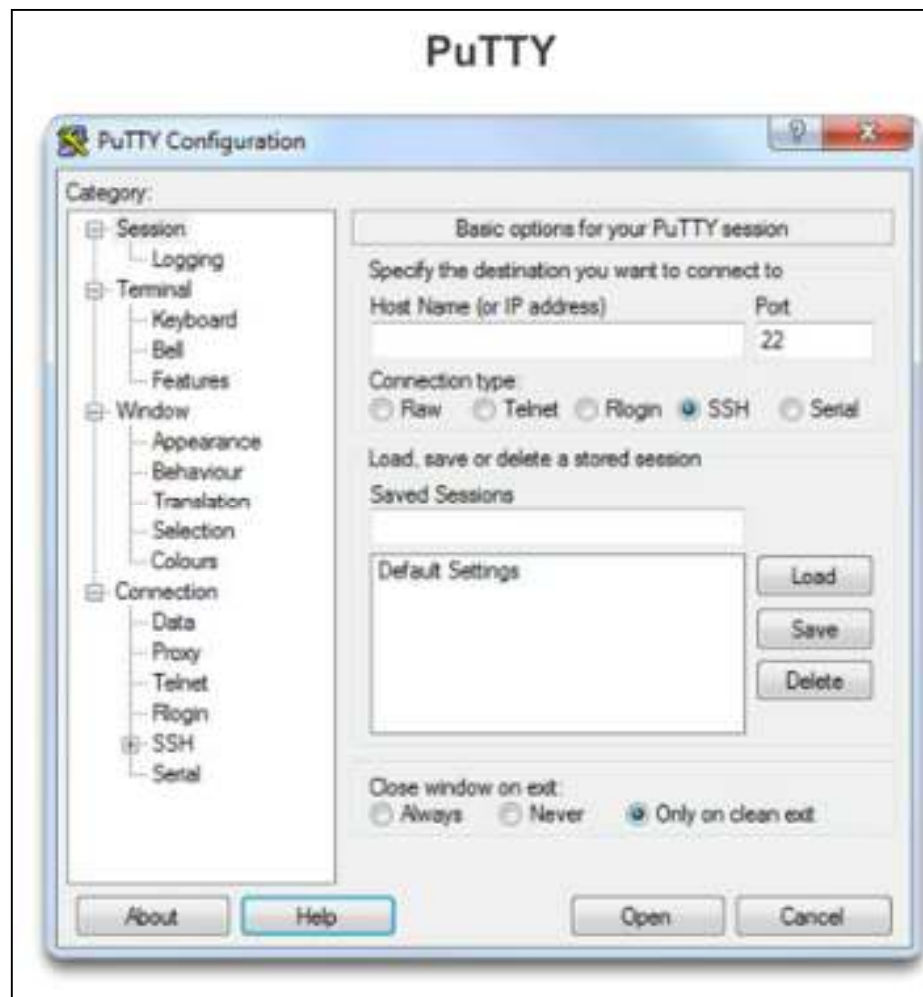


Accessing a Cisco IOS Device

Terminal Emulation Programs

Software available for connecting to a networking device:

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

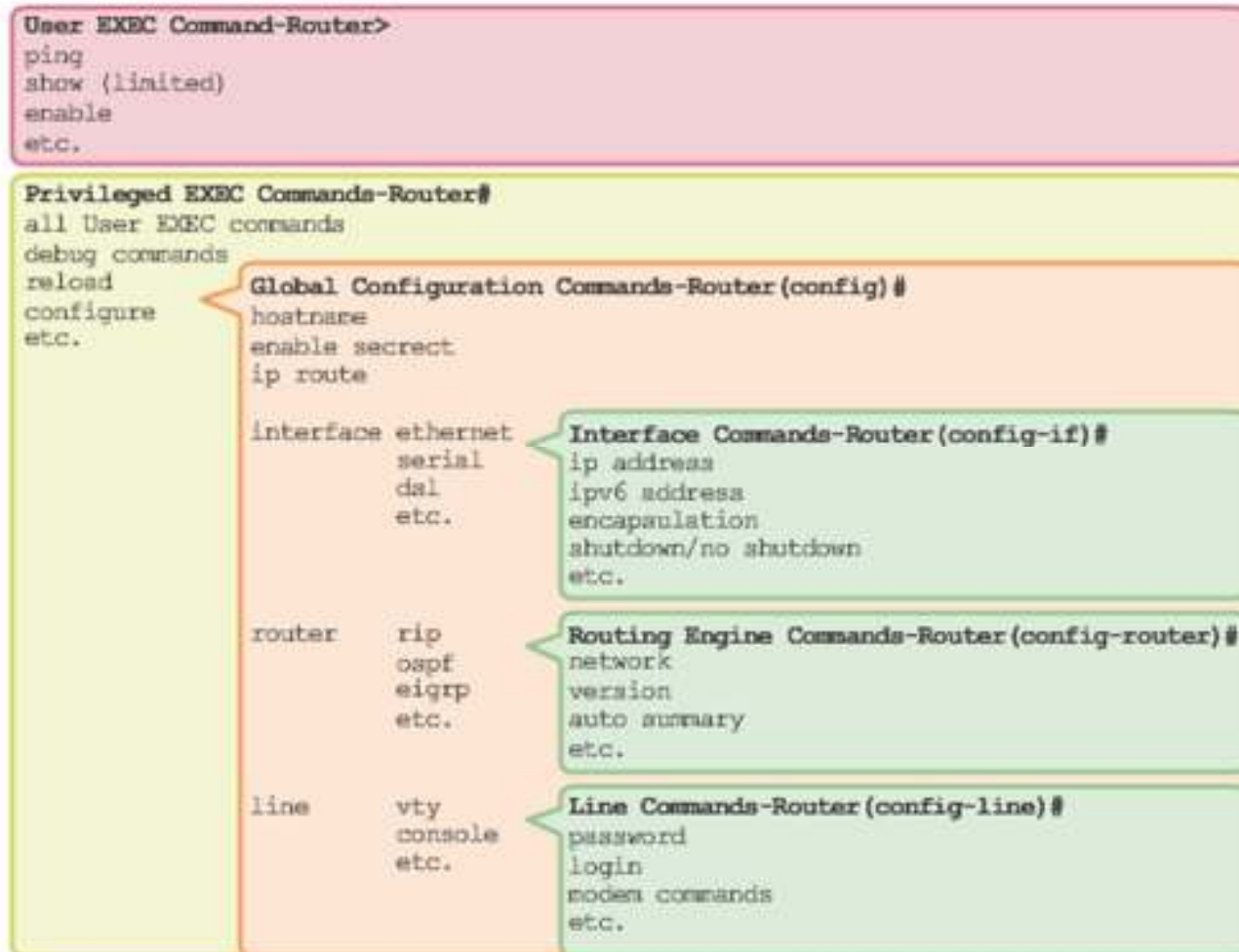




Navigating the IOS

Cisco IOS Modes of Operation

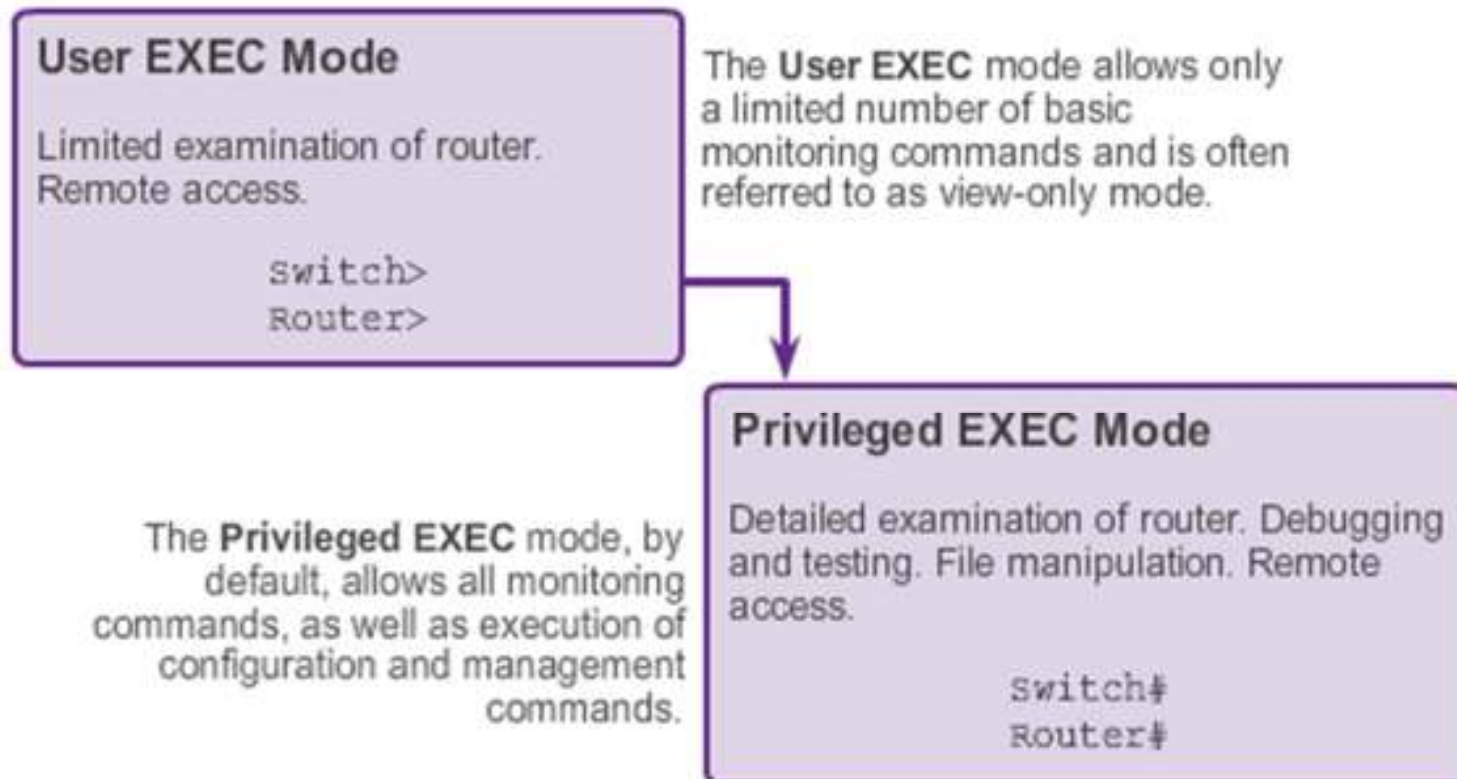
IOS Mode Hierarchical Structure





Navigating the IOS

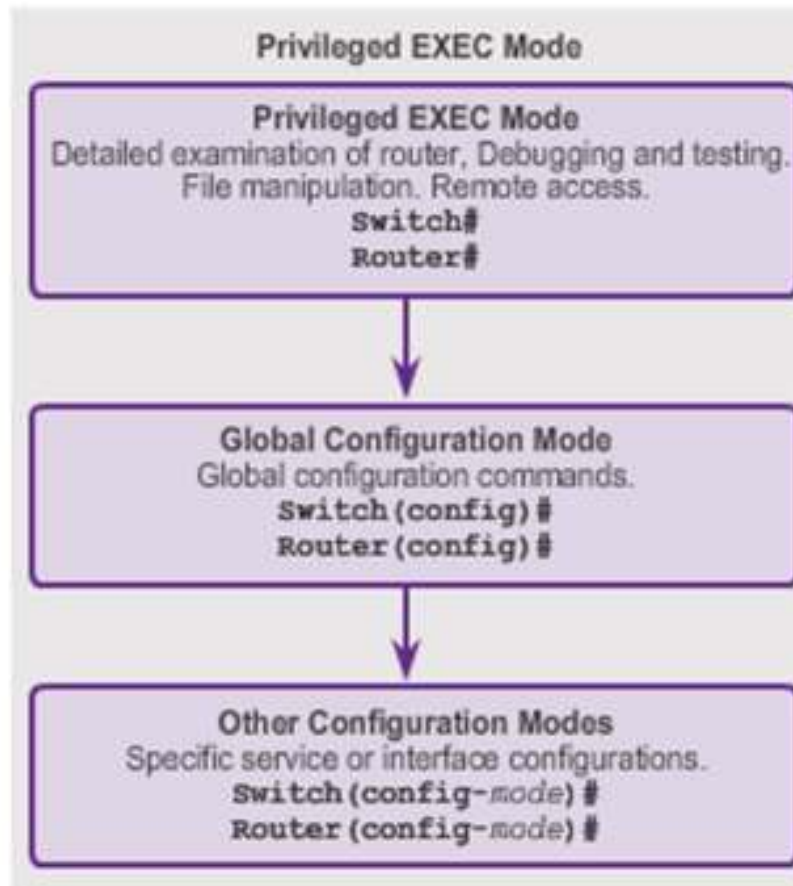
Primary Modes





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
```




Navigating the IOS

Navigating Between IOS Modes





Navigating the IOS

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#
```

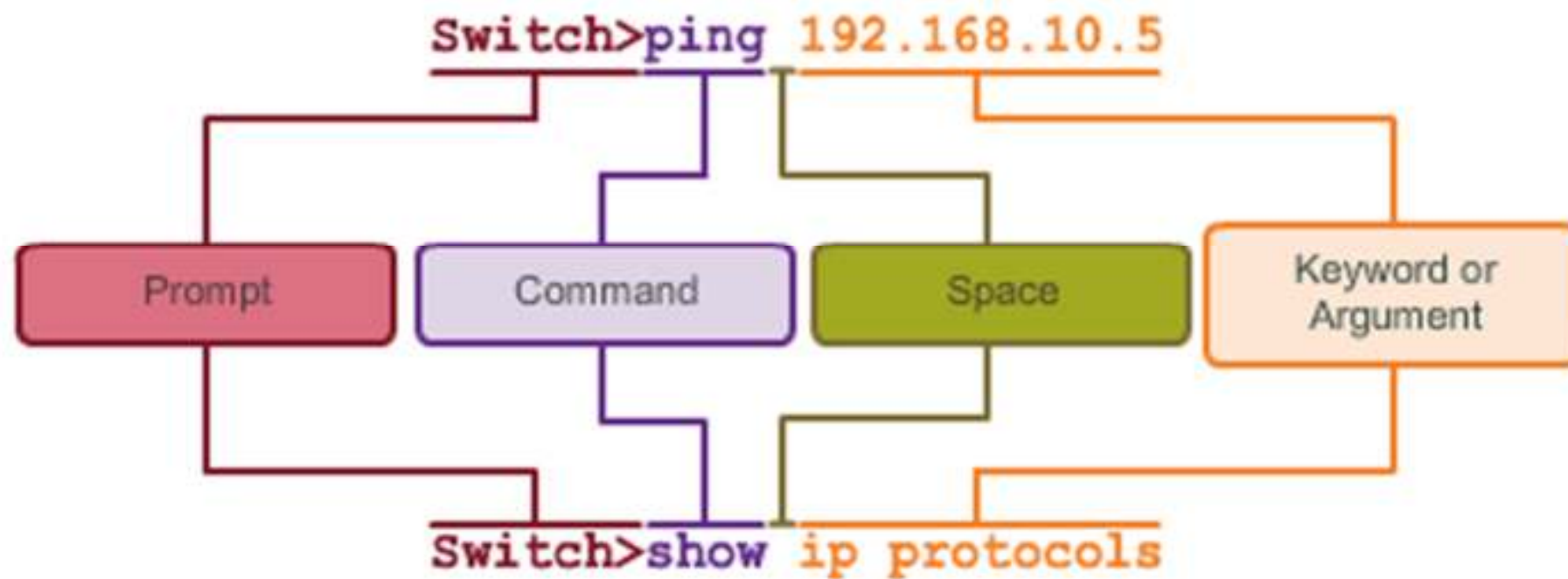
```
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# vlan 1
Switch(config-vlan)# end
Switch#
```

```
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#
```



The Command Structure

IOS Command Structure





The Command Structure

Cisco IOS Command Reference

To navigate to Cisco's *IOS Command Reference* to find a command:

1. Go to <http://www.cisco.com>.
2. Click **Support**.
3. Click **Networking Software (IOS & NX-OS)**.
4. Click **15.2M&T** (for example).
5. Click **Reference Guides**.
6. Click **Command References**.
7. Click the particular technology that encompasses the command you reference.
8. Click the link on the left that alphabetically matches the command you referencing.
9. Click the link for the command.



The Command Structure

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



The Command Structure

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.



The Command Structure

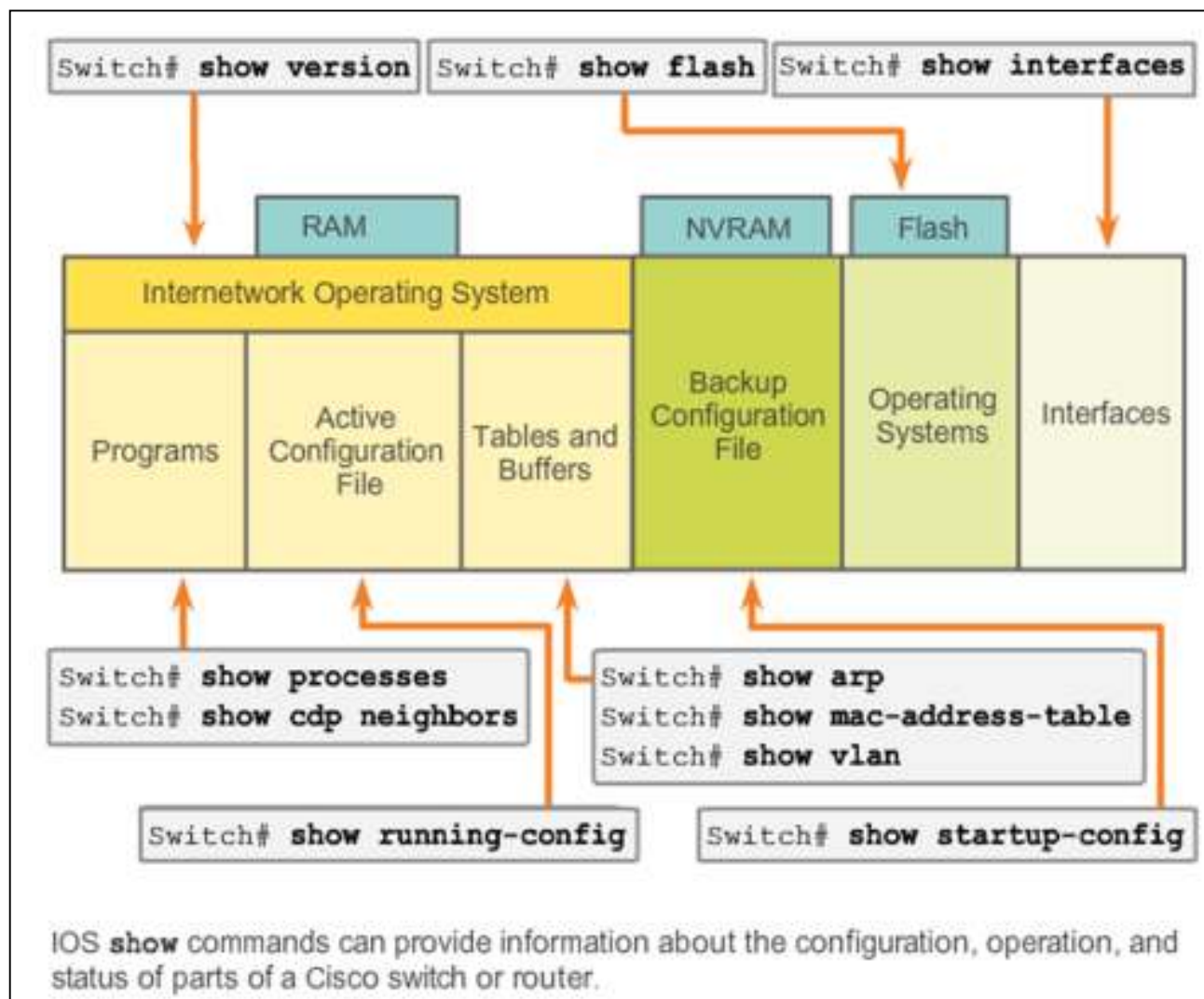
Hot Keys and Shortcuts

- **Tab** – Completes the remainder of a partially typed command or keyword.
- **Ctrl-R** – Redisplays a line.
- **Ctrl-A** – Moves to the beginning of the line.
- **Ctrl-Z** – Exits the configuration mode and returns to user EXEC.
- **Down Arrow** – Allows the user to scroll forward through former commands.
- **Up Arrow** – Allows the user to scroll backward through former commands.
- **Ctrl-shift-6** – Allows the user to interrupt an IOS process such as **ping** or **traceroute**.
- **Ctrl-C** – Exits the current configuration or aborts the current command.



The Command Structure

IOS Examination Commands





The Command Structure

The show version Command

```
Router# show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version
15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 19:34 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)

cisco1941 uptime is 41 minutes
System returned to ROM by power-on
System image file is ""flash0:c1900-universalk9-mz.SPA.152-
4.M1.bin""
Last reload type: Normal Reload
Last reload reason: power-on

This product contains cryptographic features and is subject to
United
States and local country laws governing import, export, transfer
and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use
encryption.
```

Router# show version



2.2 Getting Basic



Cisco | Networking Academy®
Mind Wide Open™

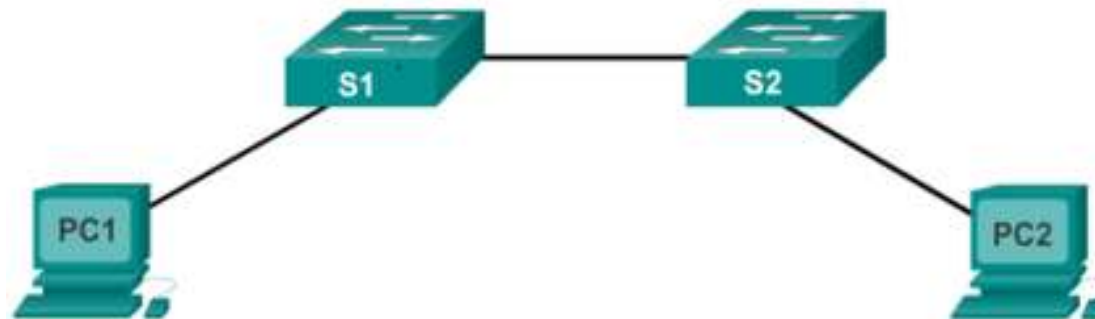


Hostnames

Why the Switch

Let's focus on:

- Creating a two PC network connected via a switch
- Setting a name for the switch
- Limiting access to the device configuration
- Configuring banner messages
- Saving the configuration





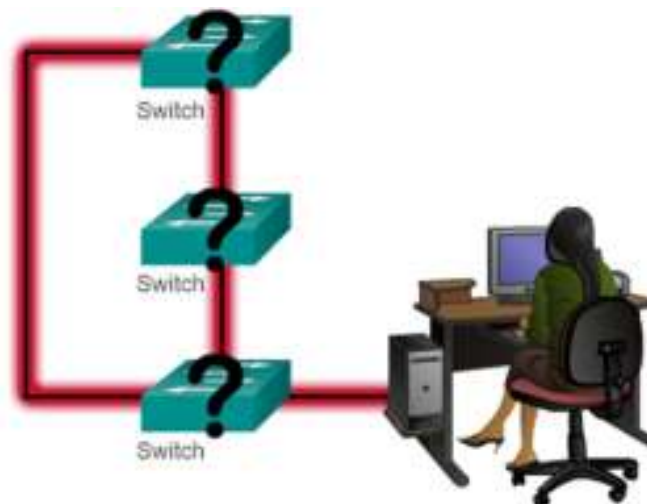
Hostnames

Device Names

Some guidelines for naming conventions:

- Start with a letter
- Contains no spaces
- Ends with a letter or digit
- Uses only letters, digits, and dashes
- Be less than 64 characters in length

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

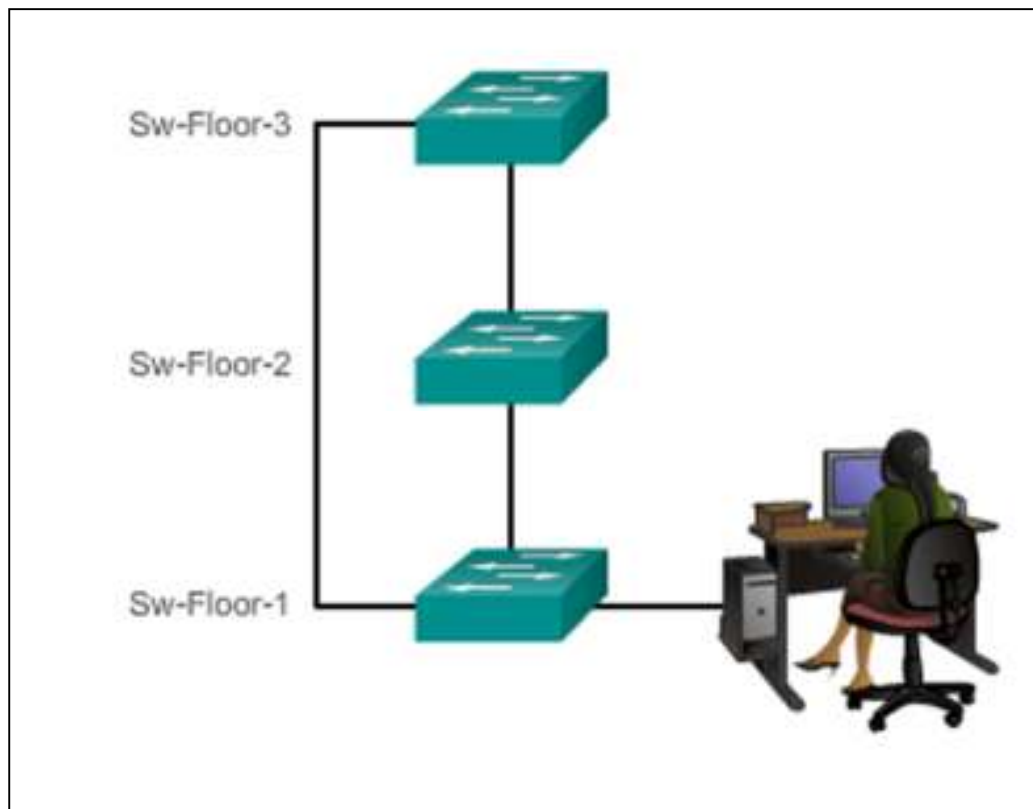




Hostnames

Configuring Device Names

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





Hostnames

Configuring Hostnames

Configure a Hostname

Configure the switch hostname to be 'Sw-Floor-1'.

```
Switch# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

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

```
Sw-Floor-1(config)#
```

You successfully configured the switch hostname.



Limiting Access to Device Configurations

Securing Device Access

These are device access passwords:

- **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

Note: In most of the labs in this course, we will be using simple passwords such as **cisco** or **class**.



Limiting Access to Device Configurations

Securing Privileged EXEC Access Mode

- Use the **enable secret** command, not the older **enable password** command.
- The **enable secret** command 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#
```




Limiting Access to Device Configurations

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; it 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. The number of VTY lines supported varies with the type of device and the IOS version.



Limiting Access to Device Configurations

Encrypting Password Display

Configuring Password Encryption

```

Enter the command to encrypt the plain text passwords.

Switch(config)# service password-encryption
Exit global configuration mode and view the running configuration.

Switch(config)# exit
Switch# show running-config
!
<output omitted>
!
line con 0
 password 7 094F471A1A0A
 login
!
line vty 0 4
 password 7 03095A0F034F38435B49150A1819
 login
!
!
end
  
```

service password-encryption

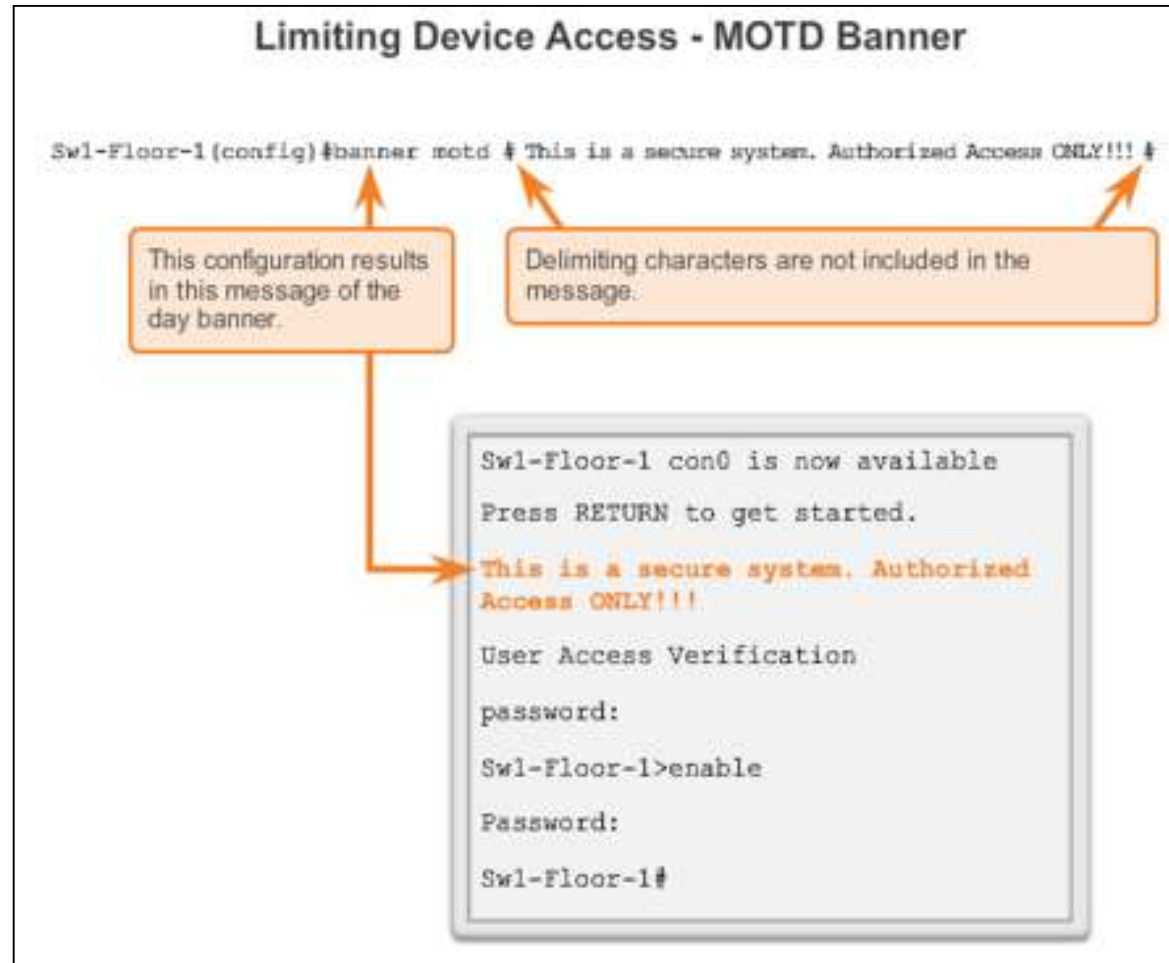
- Prevents passwords from showing up as plain text when viewing the configuration
- Keeps unauthorized individuals from viewing passwords in the configuration file
- Once applied, removing the encryption service does not reverse the encryption



Limiting Access to Device Configurations

Banner Messages

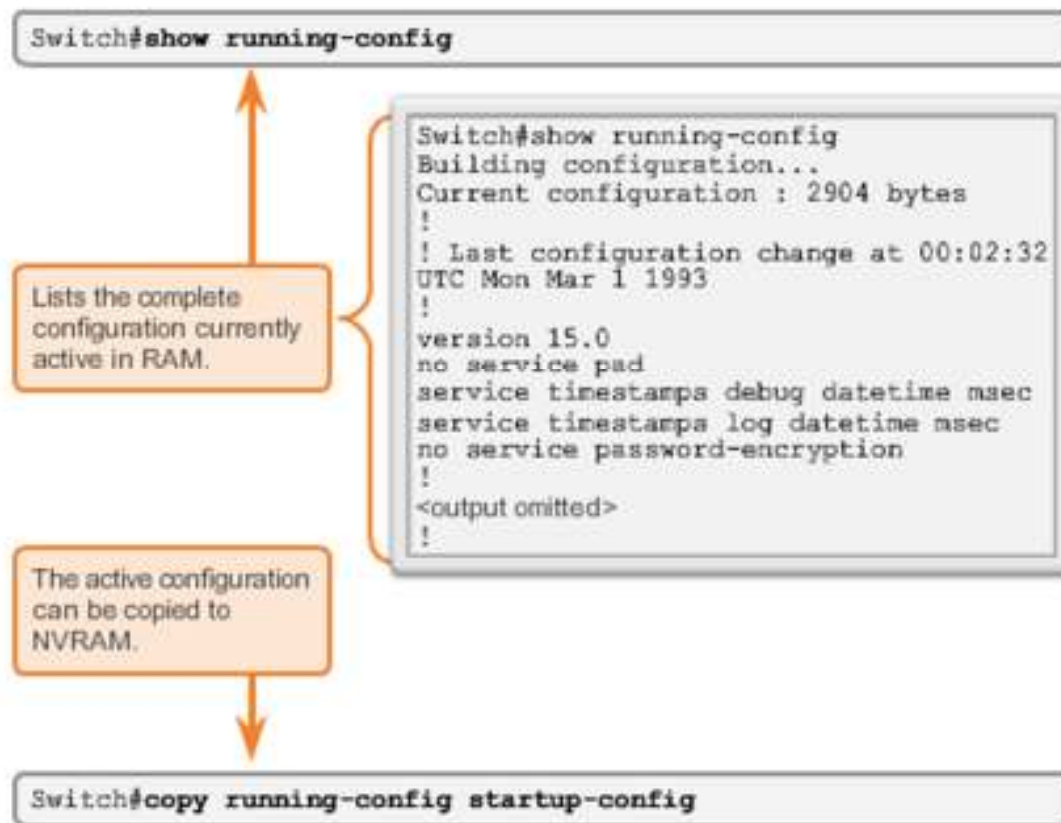
- Important part of the legal process in the event that someone is prosecuted for breaking into a device
- Wording that implies that a login is "welcome" or "invited" is not appropriate
- Often used for legal notification because it is displayed to all connected terminals





Saving Configurations Configuration Files

Saving and Erasing the Configuration



- Switch# **reload**

System configuration has been modified. Save?

[yes/no]: **n**

Proceed with reload?

[confirm]

- Startup configuration is removed by using the **erase startup-config**

Switch# **erase startup-config**

- On a switch, you must also issue the **delete vlan.dat**

Switch# **delete vlan.dat**

Delete filename
[vlan.dat]?

Delete flash:vlan.dat?
[confirm]



Saving Configurations Capturing Text

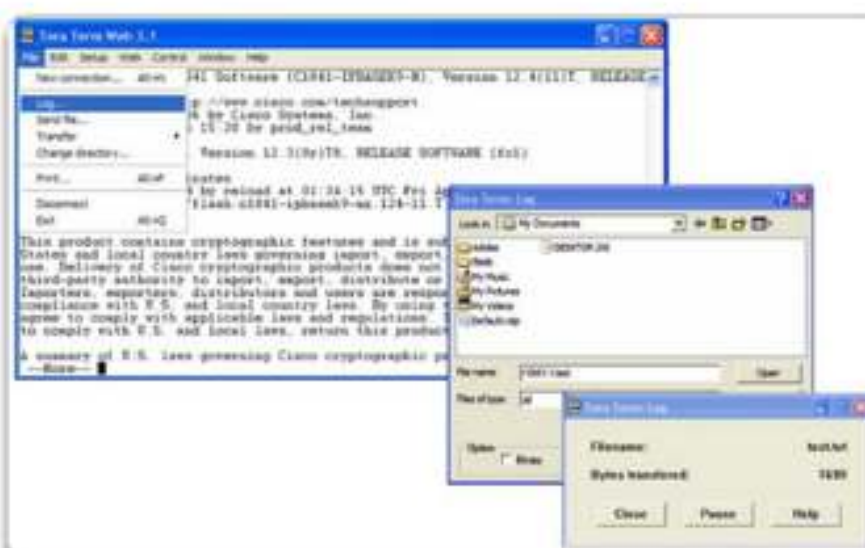
Saving to a Text File in HyperTerminal



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

Saving to a Text File in Tera Term



In the terminal session:

1. Start the log process
2. Issue a **show running-config** command
3. Close the log



2.3 Addressing Schemes



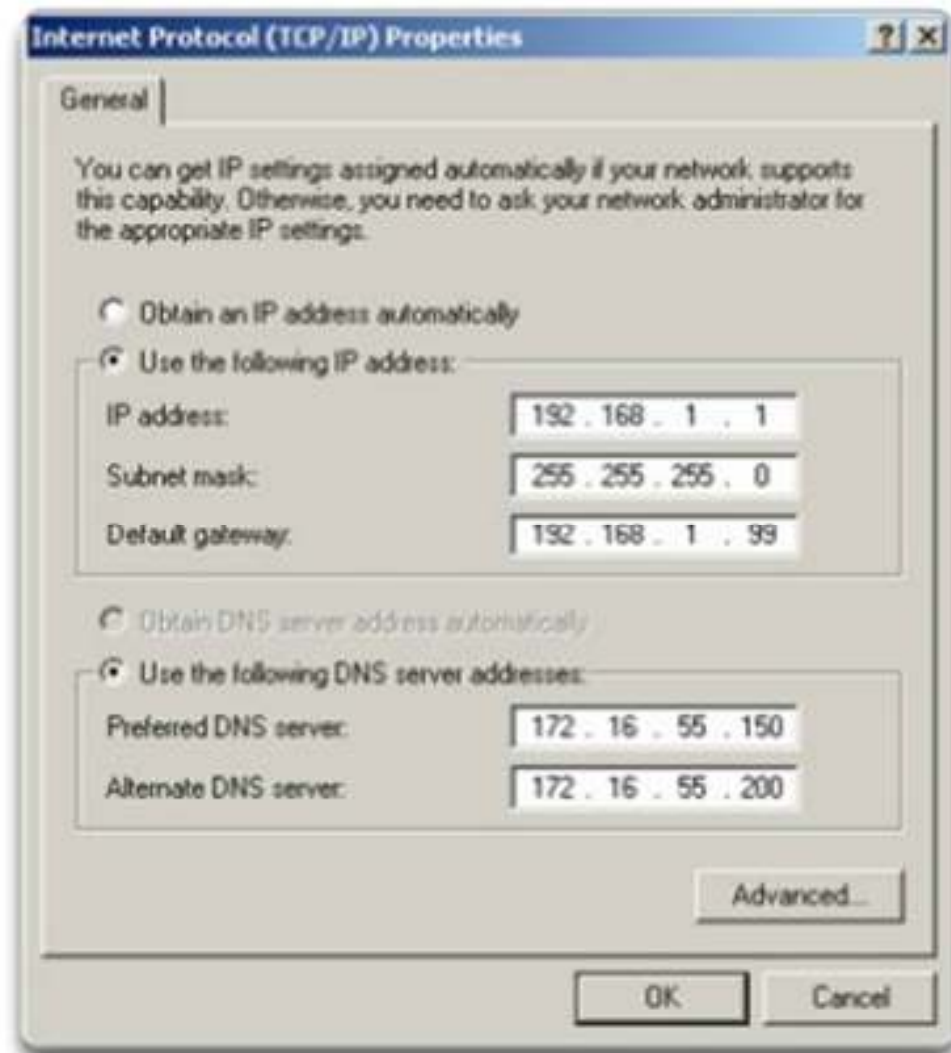
Cisco | Networking Academy®
Mind Wide Open™



Ports and Addresses

IP Addressing of Devices

- 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.





Ports and Addresses

Interfaces and Ports

- Network communications depend on end user device interfaces, networking device interfaces, and the cables that connect them.
- Types of network media include twisted-pair copper cables, fiber-optic cables, coaxial cables, or wireless.
- Different types of network media have different features and benefits.
- Ethernet is the most common local area network (LAN) technology.
- Ethernet ports are found on end user devices, switch devices, and other networking devices.
- Cisco IOS switches have physical ports for devices to connect to, but also have one or more switch virtual interfaces (SVIs; no physical hardware on the device associated with it; created in software).
- SVI provides a means to remotely manage a switch over a network.





Addressing Devices

Configuring a Switch Virtual Interface

- **IP address** – Together with subnet mask, uniquely identifies end device on internetwork.
- **Subnet mask** – Determines which part of a larger network is used by an IP address.
- **interface VLAN 1** – Available in interface configuration mode,
- **ip address 192.168.10.2 255.255.255.0** – Configures the IP address and subnet mask for the switch.
- **no shutdown** – Administratively enables the interface.
- Switch still needs to have physical ports configured and VTY lines to enable remote management.



Addressing Devices

Configuring a Switch Virtual Interface

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
```

Addressing Devices

Manual IP Address Configuration for End Devices

Addressing End Devices

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 the 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: | 192.168.1.254 |

☐ Use the following DNS server addresses:

Preferred DNS server: 172.16.55.150

Alternate DNS server: 172.16.55.200

Advanced...


OK Cancel



Addressing Devices

Automatic IP Address Configuration for End Devices

Assigning Dynamic Addresses

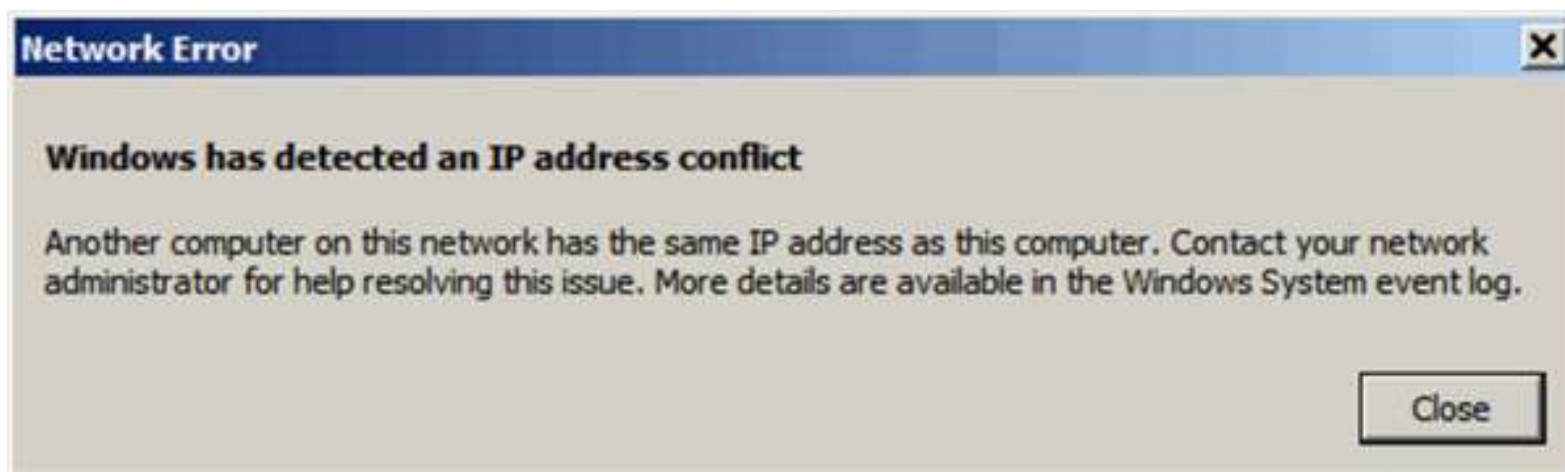


This property will set the device to obtain an IP address automatically.



Addressing Devices

IP Address Conflicts






Verifying Connectivity


Test the Loopback Address on an End Device

Testing Local TCP/IP Stack

Pinging the local host confirms that TCP/IP is installed and working on the local network adapter.



Pinging **127.0.0.1** causes a device to ping itself.





Verifying Connectivity

Testing the Interface Assignment

Verifying the VLAN Interface Assignment

Enter the command to verify the interface configuration on S1.

```
S1# show ip interface brief
```

| Interface | IP-Address | OK? | Method | Status | Protocol |
|-----------------|------------|-----|--------|--------|----------|
| FastEthernet0/1 | unassigned | YES | manual | up | up |
| FastEthernet0/2 | unassigned | YES | manual | up | up |

<output omitted>

| | | | | | |
|-------|--------------|-----|--------|----|----|
| Vlan1 | 192.168.10.2 | YES | manual | up | up |
|-------|--------------|-----|--------|----|----|

You are now on S2. Enter the command to verify the interface configuration on S2.

```
S2# show ip interface brief
```

| Interface | IP-Address | OK? | Method | Status | Protocol |
|-----------------|------------|-----|--------|--------|----------|
| FastEthernet0/1 | unassigned | YES | manual | up | up |
| FastEthernet0/2 | unassigned | YES | manual | up | up |

<output omitted>

| | | | | | |
|-------|--------------|-----|--------|----|----|
| Vlan1 | 192.168.10.3 | YES | manual | up | up |
|-------|--------------|-----|--------|----|----|

You successfully verified the interface assignment on S1 and S2.



Verifying Connectivity

Testing End-to-End Connectivity

```

Enter the command to verify connectivity to PC2 at '192.168.10.11'.
C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time=838ms TTL=35
Reply from 192.168.10.11: bytes=32 time=820ms TTL=35
Reply from 192.168.10.11: bytes=32 time=883ms TTL=36
Reply from 192.168.10.11: bytes=32 time=828ms TTL=36

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 820ms, Maximum = 883ms, Average = 842ms

C:\>
You successfully verified connectivity to S1 and PC2.

```



Configuring a Network Operating System

Chapter 2 Summary

Cisco IOS:

- The technician can enter commands to configure, or program, the device to perform various networking functions.
- Services are generally accessed using a command-line interface (CLI), which is accessed by either the console port, the AUX port, or through telnet or SSH.
- Once connected to the CLI, network technicians can make configuration changes to Cisco IOS devices.
- Cisco IOS is designed as a modal operating system, which means a network technician must navigate through various hierarchical modes of the IOS.
- Cisco IOS routers and switches support a similar modal operating system, support similar command structures, and support many of the same commands. In addition, both devices have identical initial configuration steps when implementing them in a network.



Configuring a Network Operating System

Chapter 2 Summary (cont.)

```
User EXEC Command-Router>  
ping  
show (limited)  
enable  
etc.
```



Configuring a Network Operating System

Chapter 2 Summary (cont.)

