Cisco IOS
Week 4

Module : Computer Networks

Lecturer: Lucy White lbwhite@wit.ie

Office : 324

Chapter 2 - Objectives

- Explain the purpose of Cisco IOS.

- Explain how to access and navigate Cisco IOS to configure network devices.

- Describe the command structure of 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.

Operating Systems

All networking equipment dependent on operating systems

- End users (PCs, laptops, smart phones, tablets)
- Switches
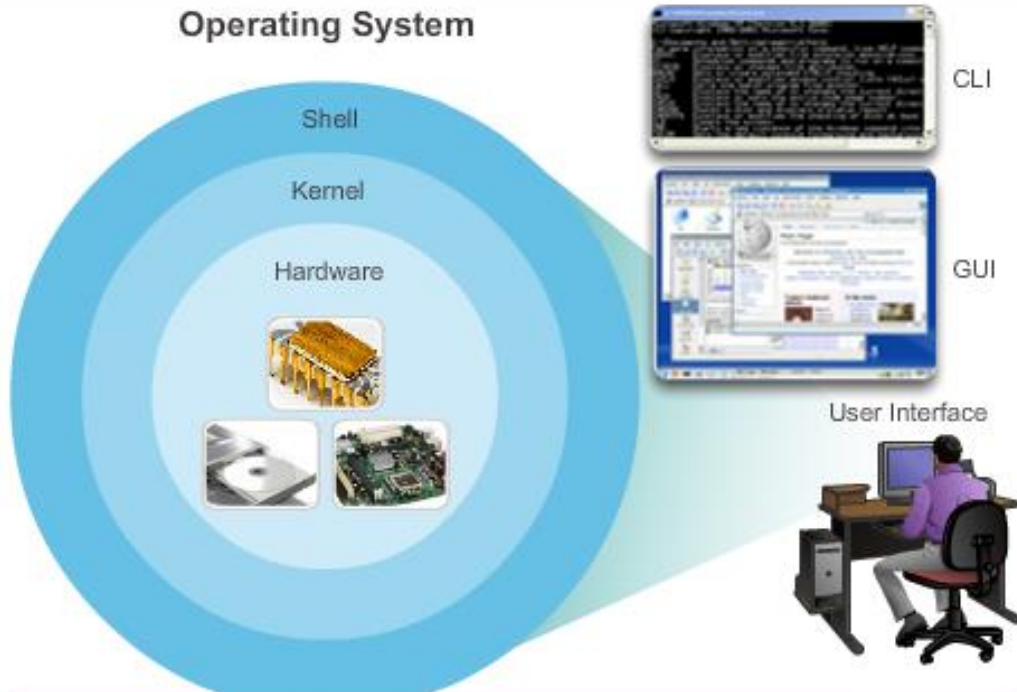- Routers
- Wireless access points
- Firewalls
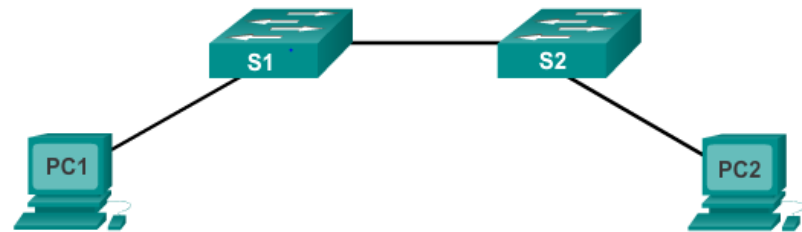
Cisco Internetwork Operating System (IOS)

- Collection of network operating systems used on Cisco devices

Operating Systems

Operating System

Shell
Kernel
Hardware

CLI
GUI
User Interface

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.

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.

Purpose of OS

- PC operating systems (Windows 8 & 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

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
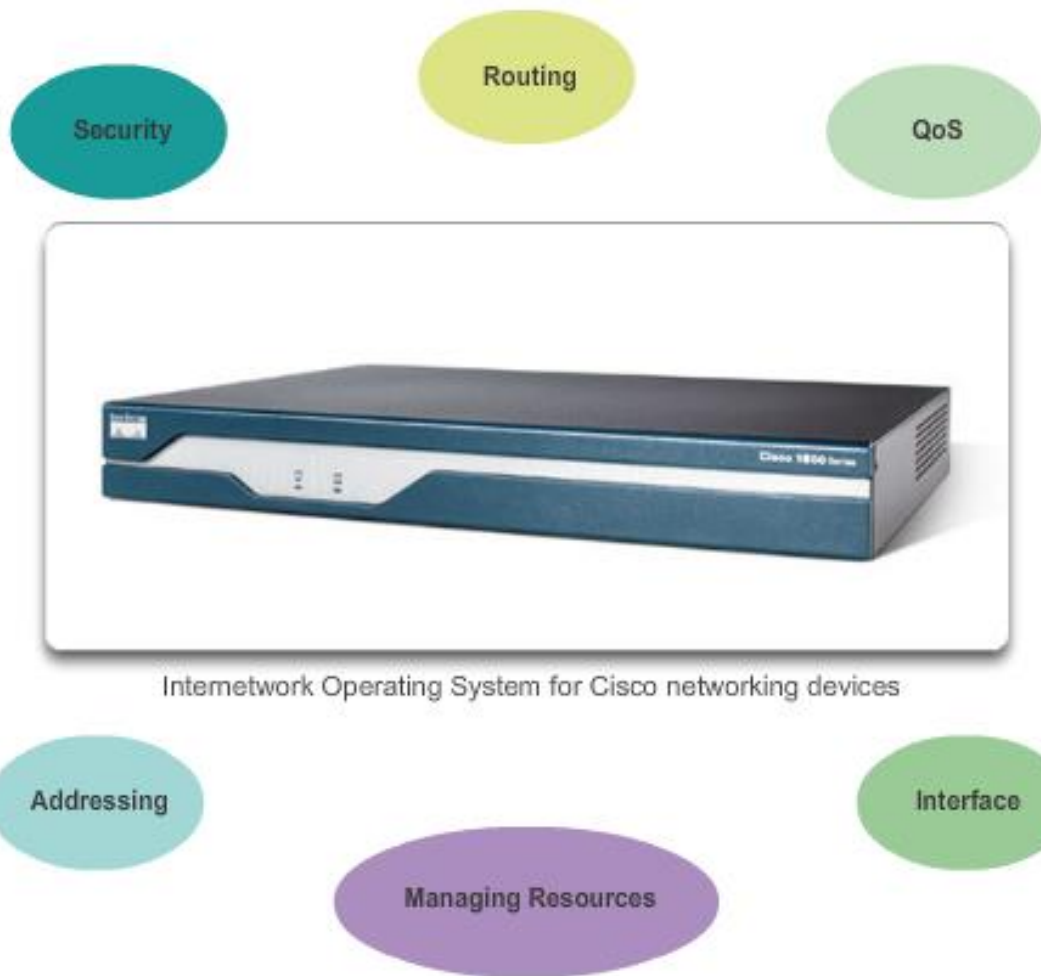- Quantity of flash and RAM memory determines IOS that can be used

IOS Functions

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

Routing

Security

QoS

Internetwork Operating System for Cisco networking devices

Addressing

Managing Resources

Interface

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
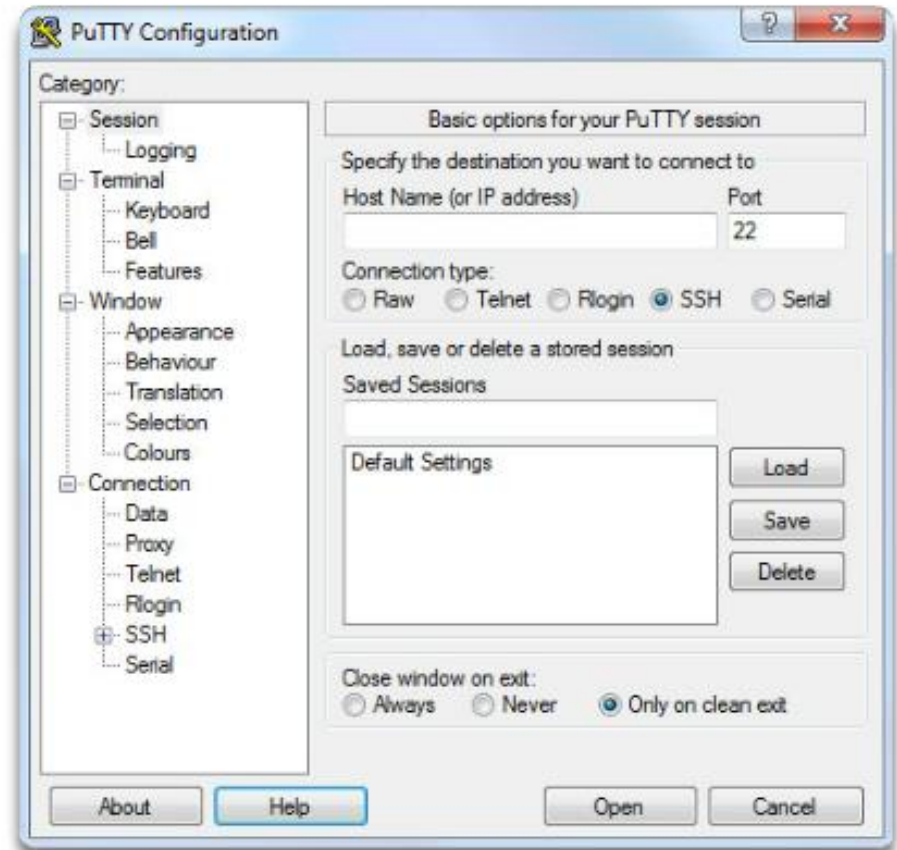- Can be used like console port

Terminal Emulation Programs

Software available for connecting to a networking device

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

PuTTY

Cisco IOS Modes of Operation

IOS Mode Hierarchical Structure

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

Privileged EXEC Commands-Router#
all User EXEC commands
debug commands
reload
configure
etc.

Global Configuration Commands-Router(config)#
hostname
enable secrect
ip route

interface   ethernet
            serial
            dsl
            etc.

Interface Commands-Router(config-if)#
ip address
ipv6 address
encapsulation
shutdown/ no shutdown
etc.

router   rip
            ospf
            eigrp
            etc.

Routing Engine Commands-Router(config-router)#
network
version
auto summary
etc.

line   vty
            console
            etc.

Line Commands-Router(config-line)#
password
login
modem commands
etc.

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.
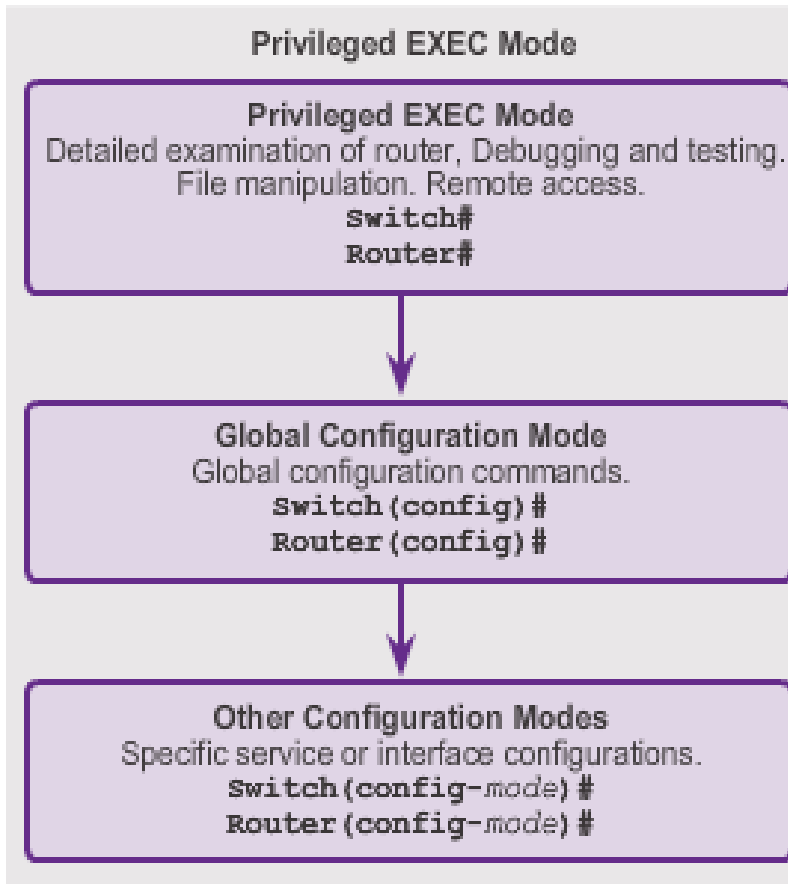
Global Configuration Mode and Submodes

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>                      User-Mode Prompt
Router>enable
Password:
Router#                      Privileged-Mode
Router#disable
Router>                      User-Mode Prompt
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#
```
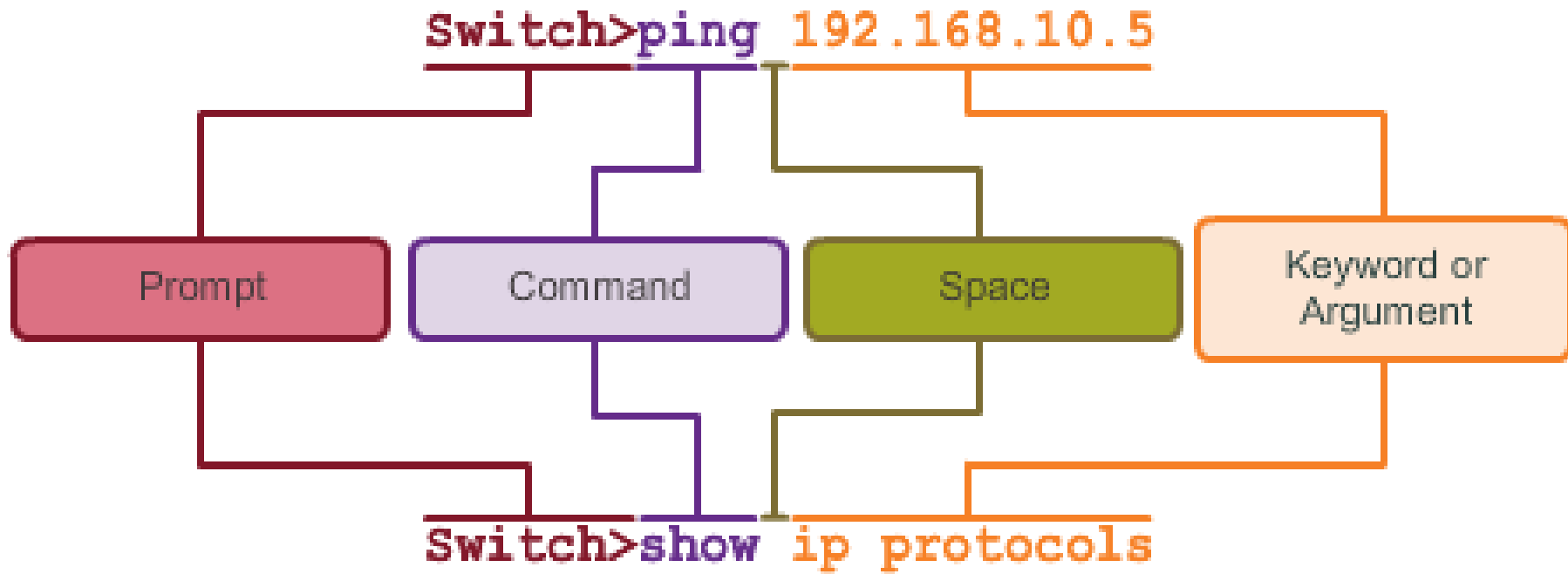
```
Switch#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)#vlan 1
Switch(config-vlan)#end
Switch#
```

```
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#
```

IOS Command Structure

Cisco IOS Command Reference

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

1. Go to 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 are referencing.

8. Click the link on the left that alphabetically matches the command you are referencing.

9. Click the link for the command.

Context Sensitive Help

Context Sensitive Help

```
Switch#cl?
clear   clock
```

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

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

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

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

Command explanation with more than one argument or variable option

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

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.

Hot Keys and Shortcuts

- **Tab** - Completes the remainder of a partially typed command or keyword

- **Ctrl-R** - Redisplays a line

- **Ctrl-A –** Moves cursor to the beginning of the line

- **Ctrl-Z** - Exits 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** - Aborts the current command and exits the configuration mode

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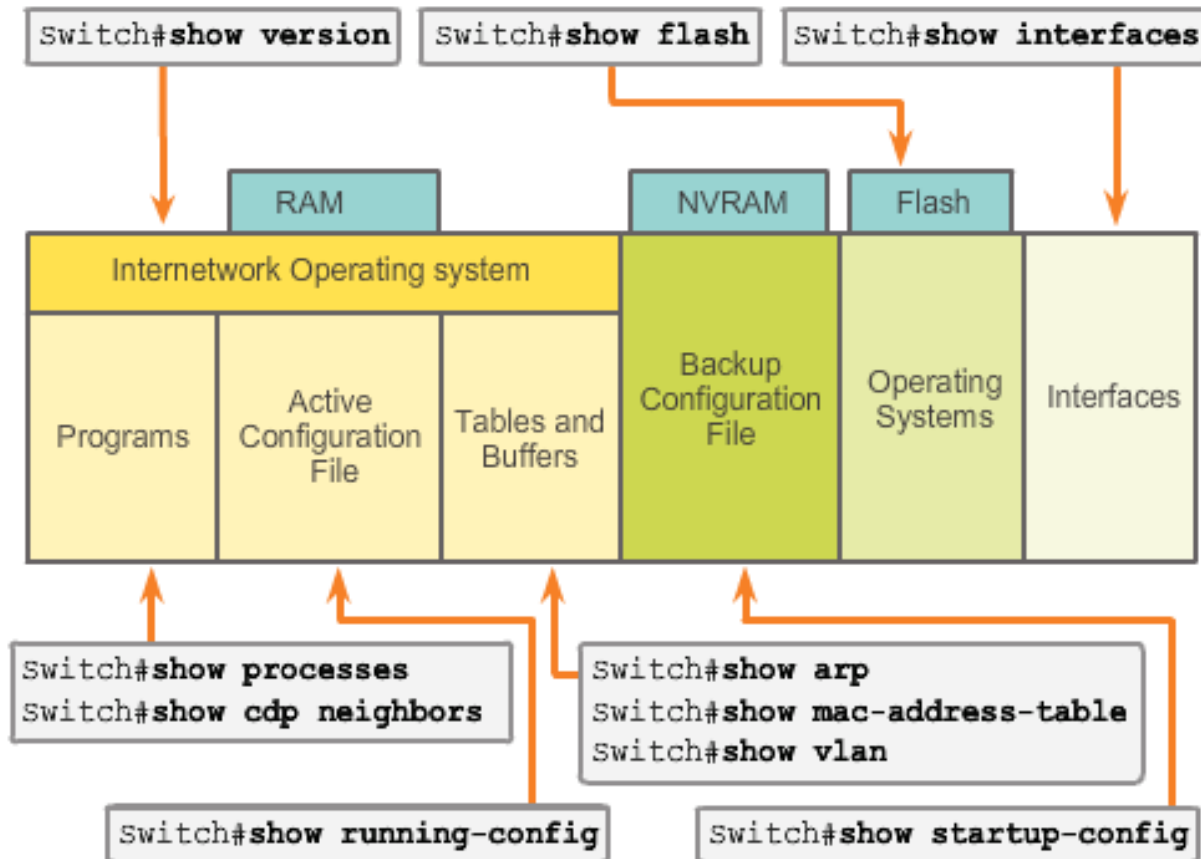
IOS **show** commands can provide information about the configuration, operation and status of parts of a Cisco router.

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.
```
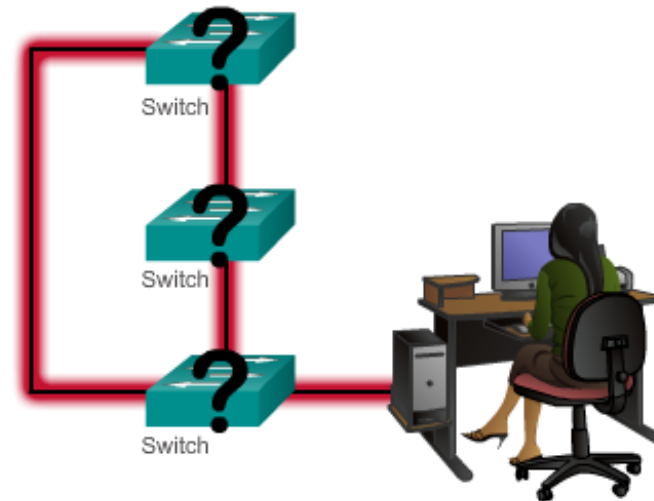
```
Router#show version
```

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.
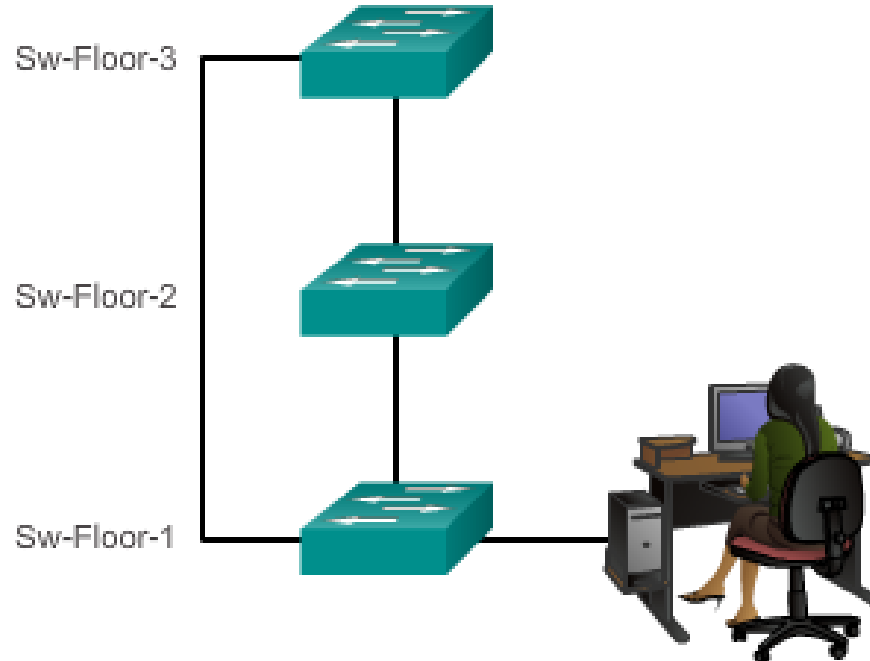
Hostnames

Configuring Device Names

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

Sw-Floor-3

Sw-Floor-2

Sw-Floor-1

Configuring Hostnames

Configure a Hostname

Configure the switch hostname to be 'AtlantaHQSw1'.

Switch# configure terminal

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

Switch(config)# hostname AtlantaHQSw1

AtlantaHQSw1(config)#

You successfully configured the switch hostname.

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

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

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

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

- purpose of this command is to keep unauthorized individuals from viewing passwords in the configuration file

- once applied, removing the encryption service does not reverse the encryption

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!!! #

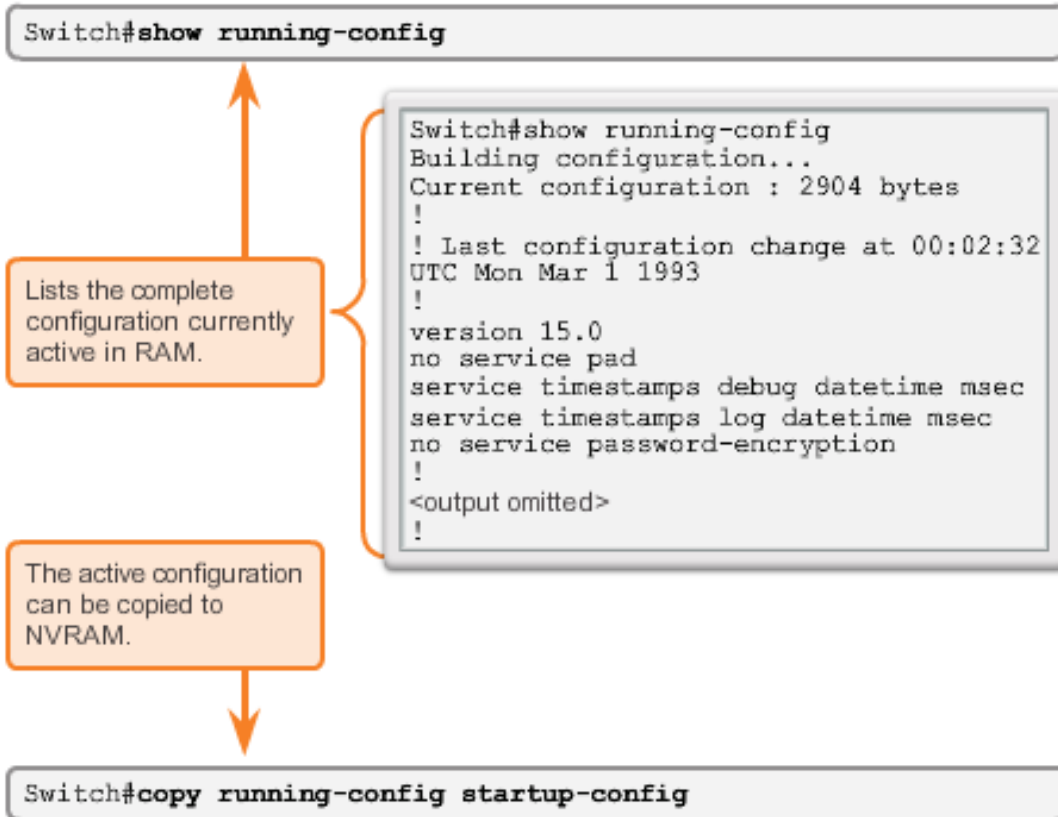This configuration results in this message of the day banner.

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#
```

Saving Configurations
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
```

- 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**
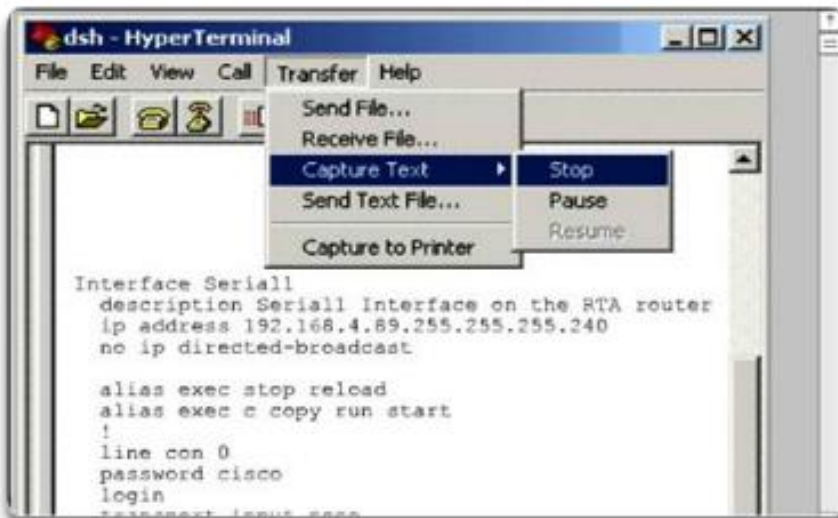
  Switch# **delete vlan.dat**

  Delete filename [vlan.dat]?

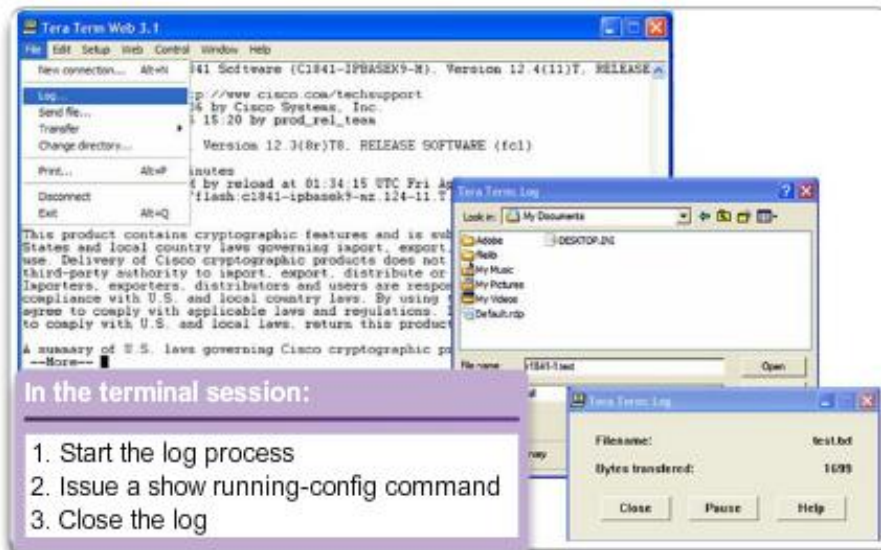 Delete flash:vlan.dat? [confirm]

Capturing Text

Saving to a Text File in Hyper Terminal

In the terminal session:

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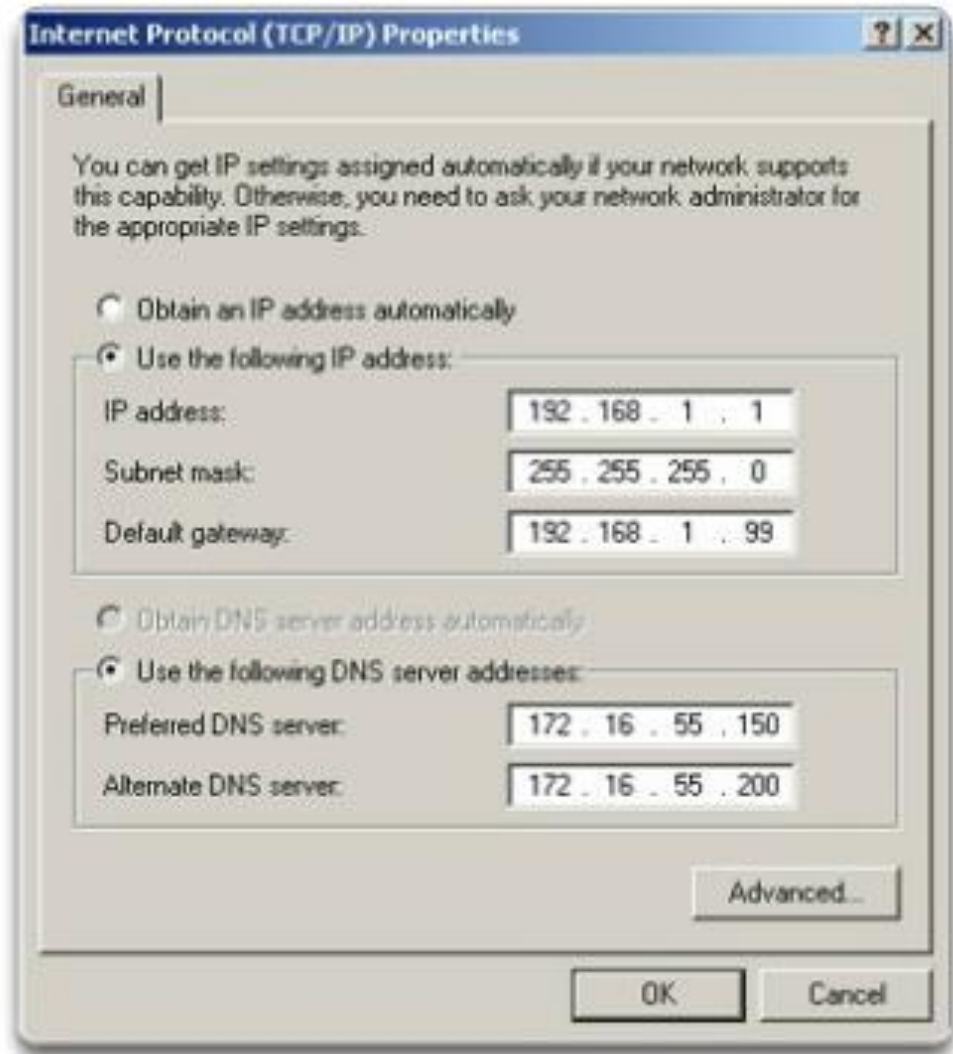4. Save the text file

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

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

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

Configuring a Switch Virtual Interface

```
Switch#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#interface VLAN 1
Switch(config-if)#ip address 192.168.10.2 255.255.255.0
Switch(config-if)#no shutdown
```

- **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** - 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

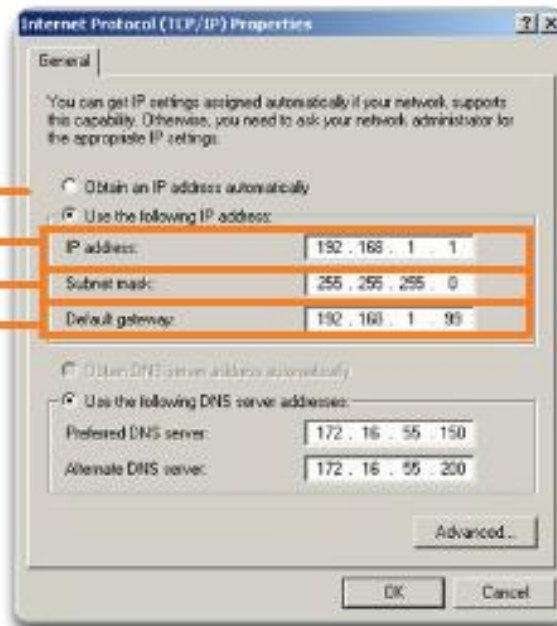# Manual IP Address Configuration for End Devices

Addressing End Devices

Automatic IP Address Configuration for End Devices

IP Address Conflicts
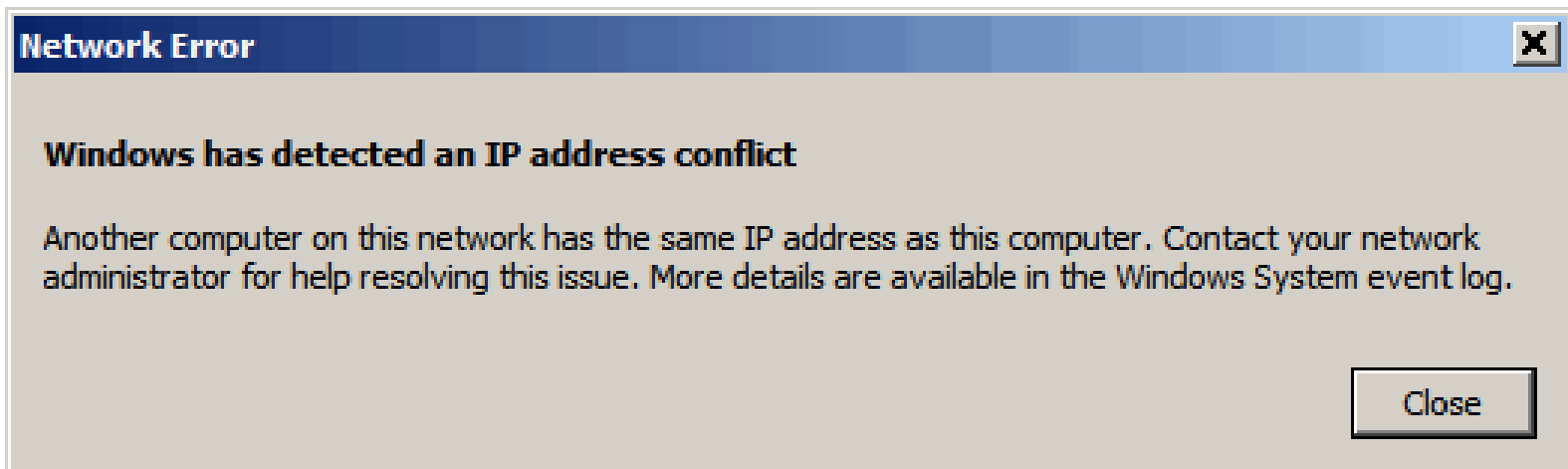
Test the Loopback Address on an End Device

Testing Local TCP/IP Stack

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

C:\>ping 127.0.0.1

Pinging 127.0.0.1 causes a device to ping itself.

Testing the Interface Assignment

```
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
```

```
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
```

Testing End-to-End Connectivity

```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=838ms TTL=35
Reply from 192.168.10.2: bytes=32 time=820ms TTL=35
Reply from 192.168.10.2: bytes=32 time=883ms TTL=36
Reply from 192.168.10.2: bytes=32 time=828ms TTL=36

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 820ms, Maximum = 883ms, Average = 842ms

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:\>
```

Chapter 2 Summary

- Services provided by the Cisco IOS accessed using a command-line interface (CLI)

  - accessed by either the console port, the AUX port, or through telnet or SSH

  - can make configuration changes to Cisco IOS devices

  - a network technician must navigate through various hierarchical modes of the IOS

- Cisco IOS routers and switches support a similar operating system

- Introduced the initial settings of a Cisco IOS switch device

  - setting a name

  - limiting access to the device configuration

  - configuring banner messages

  - saving the configuration

Chapter 2 Summary

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

 Cisco Confidential

Chapter 2 Summary

© 2008 Cisco Systems, Inc. All rights reserved.   Cisco Confidential