LABS INTRODUCTION

Operating Systems

Operating System

CLI

GUI

Shell

Kernel

Hardware

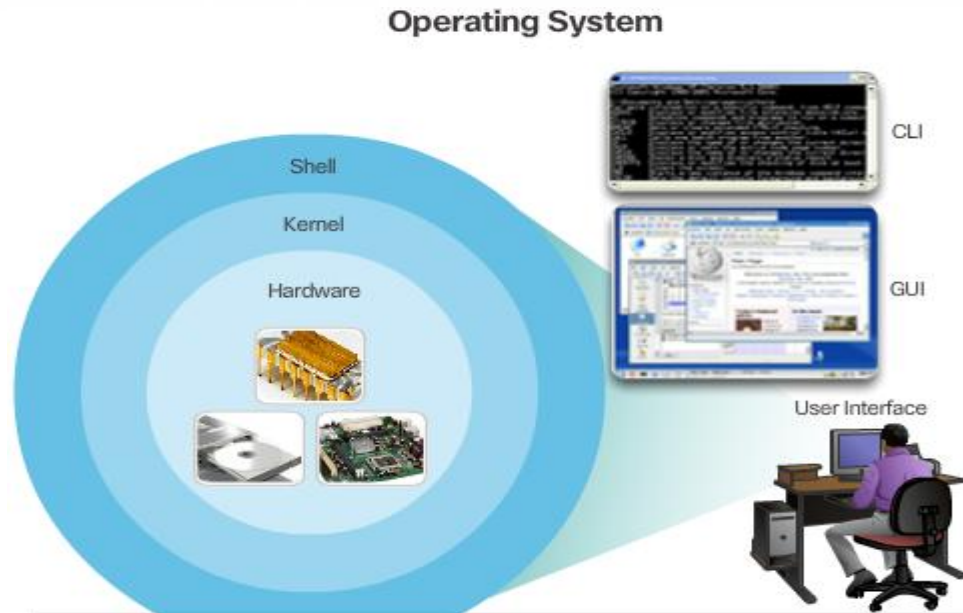User Interface

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 enable a user to:
    - Use a mouse to make selections and run programs.
    - Enter text and text-based commands.
    - View output on a monitor.

- Cisco IOS enables a network technician to:
    - Use a keyboard to run CLI-based network programs.
    - Use a keyboard to enter text and text-based commands.
    - View output on a monitor.

- All networking devices come with a default IOS.

- It is possible to upgrade the IOS version or feature set.

Access Methods

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.
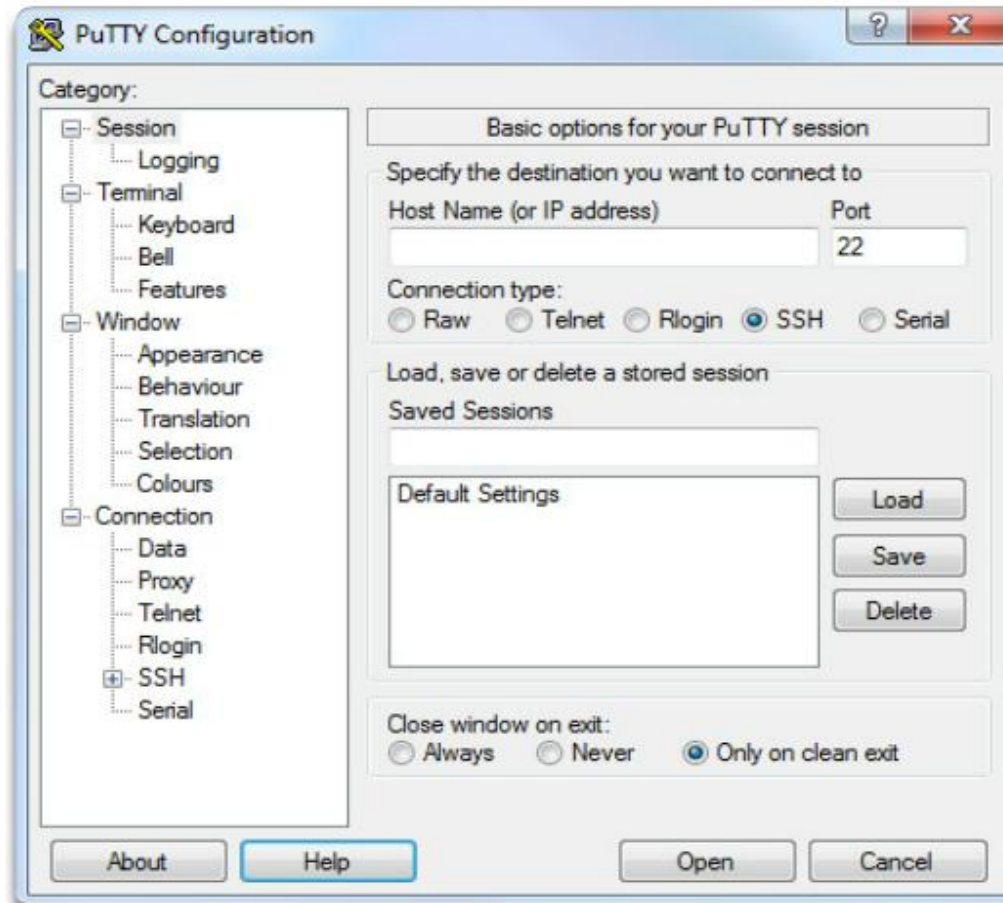
Telnet

Best practice dictates to use SSH instead of Telnet for remote management CLI connections. Cisco IOS includes a Telnet server and a Telnet client that can be used to establish Telnet sessions with other devices.

SSH

SSH is the recommended method for remote management because it provides a secure connection. SSH provides encrypted password authentication and transport of session data. This keeps the user ID, password, and the details of the management session private. Most versions of Cisco IOS include an SSH server and an SSH client that can be used to establish SSH sessions with other devices.
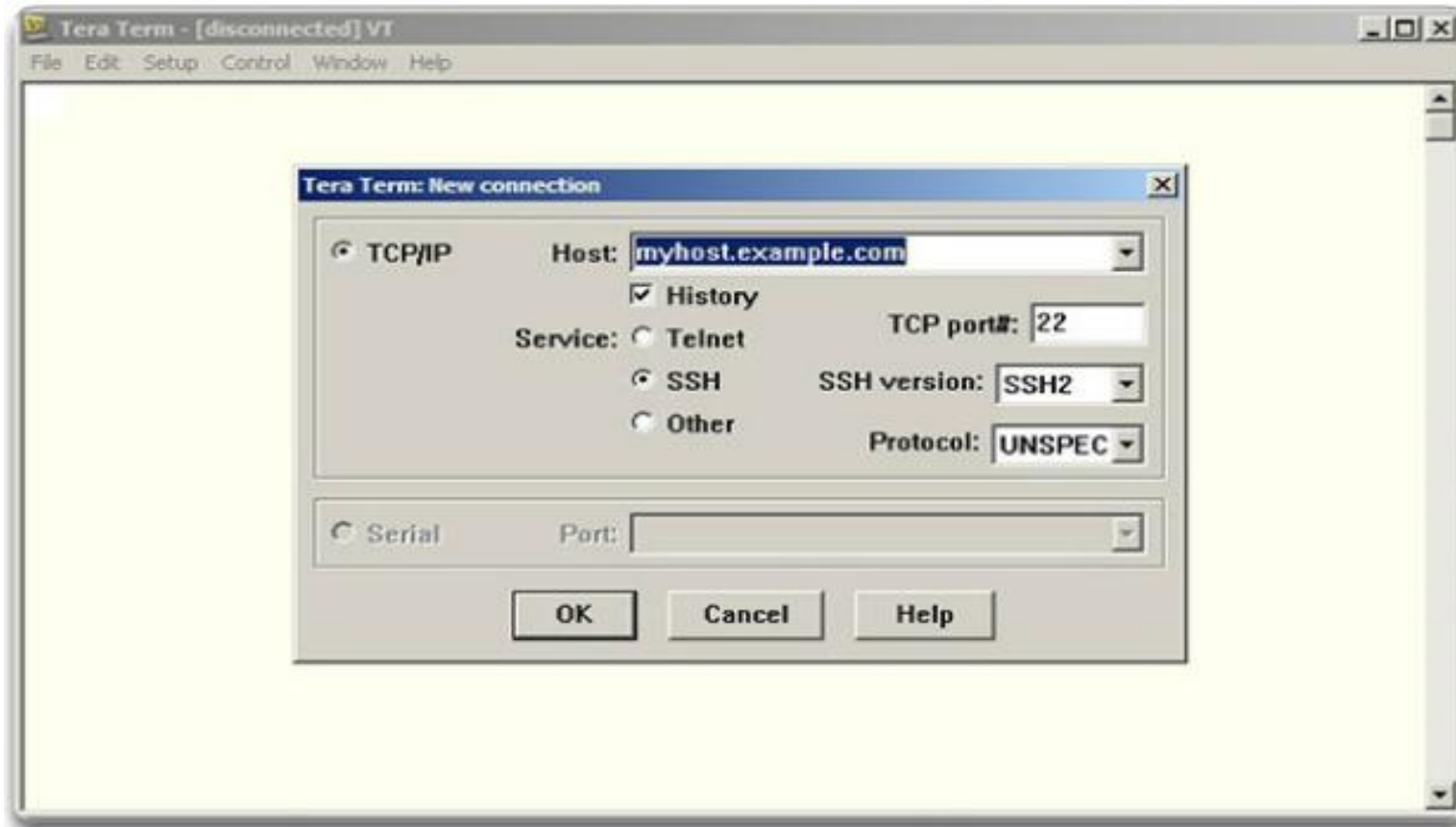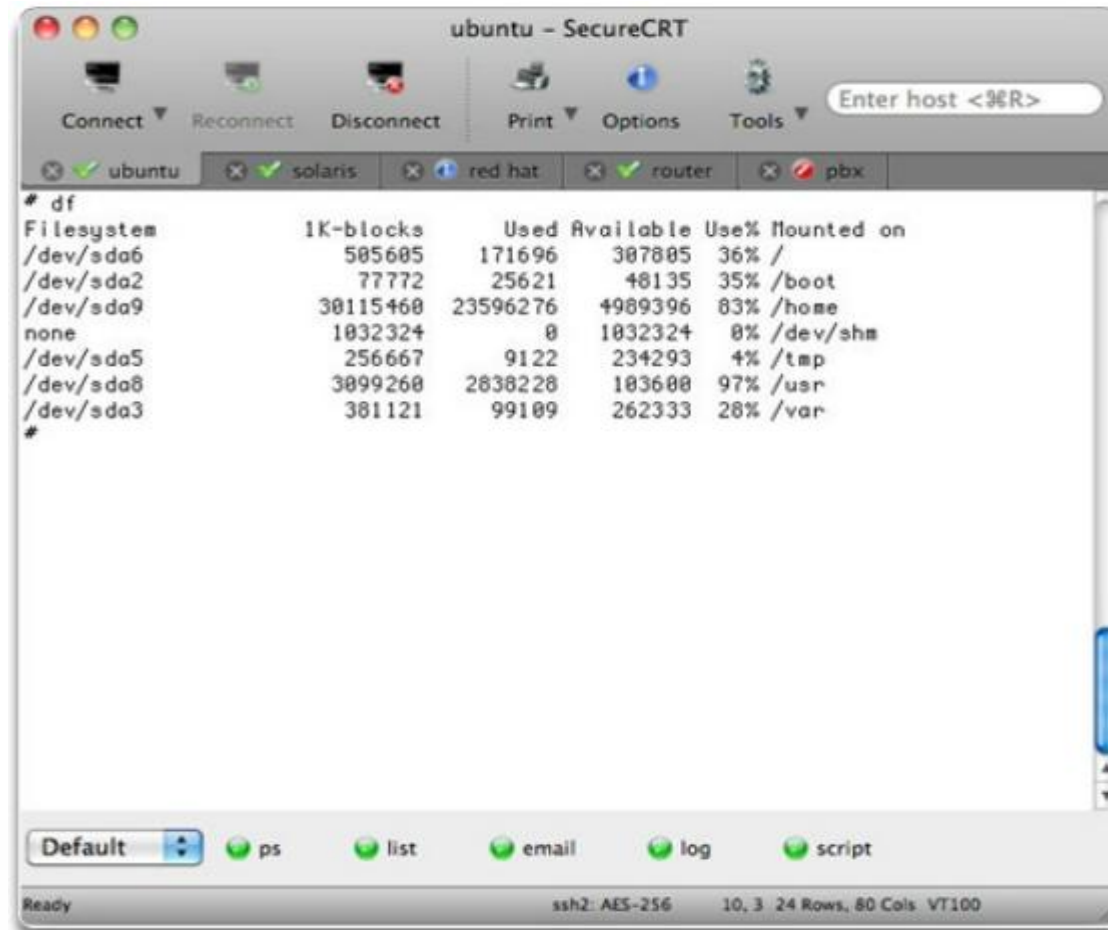
Terminal Emulation Programs

PuTTY

Terminal Emulation Programs (cont.)

Tera Term

Terminal Emulation Programs (cont.)

SecureCRT

Primary Command 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.

Configuration Command Modes

Global Configuration Mode

- To configure the device must enter this mode with **configure terminal** command
- Example: **Switch(config)#**
- CLI configuration changes are made that affect the operation of the device as a whole
- From this mode, the user can enter different sub-configuration modes

Two common sub-configuration modes include:

- **Line Configuration Mode -** Used to configure console, SSH, Telnet, or AUX access. Example: **Switch(config-line)#**
- **Interface Configuration Mode -** Used to configure a switch port or router network interface. Example: **Switch(config-if)#**

Navigate Between IOS Modes

```
Router con0 is now available.

Press RETURN to get started.

User Access Verification
Password:
Router>                           User EXEC Mode Prompt
Router> enable
Password:
Router#                           Privileged EXEC Mode Prompt
Router# disable
Router>                           User EXEC Mode Prompt
Router> exit
```
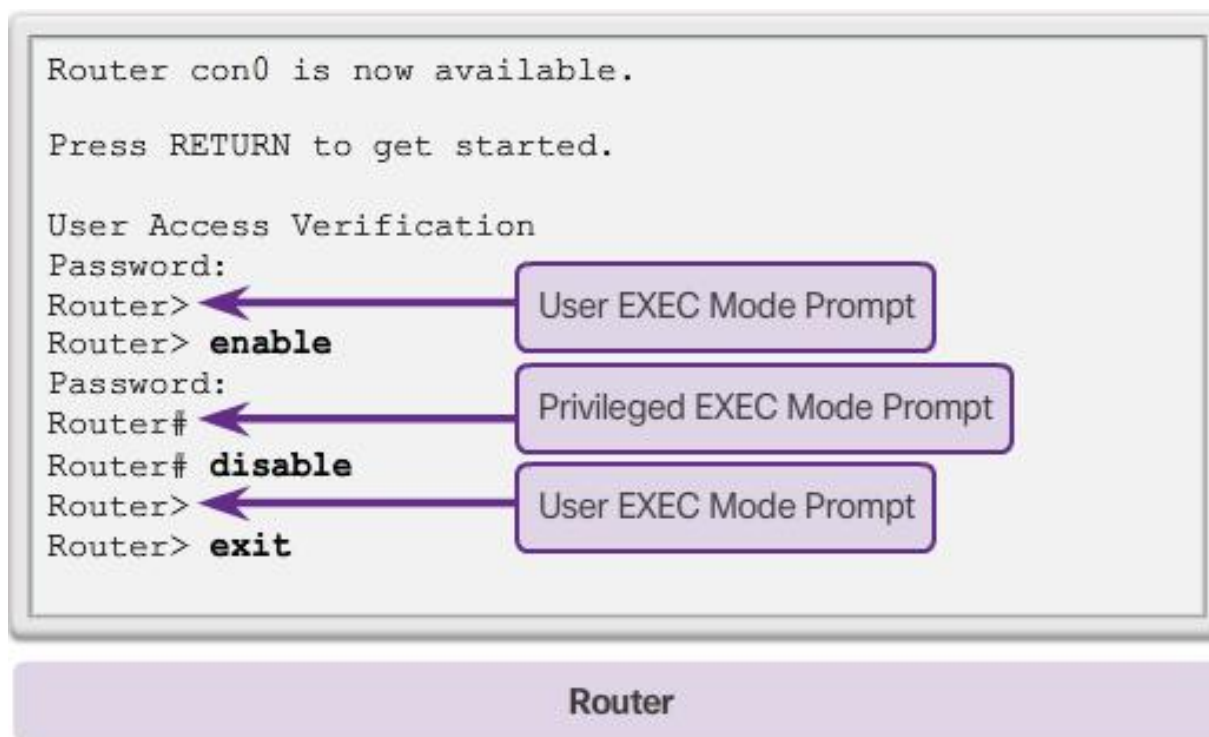
Router

Switch | Router

Navigate 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#
```

Exit
End or **Ctrl+Z**

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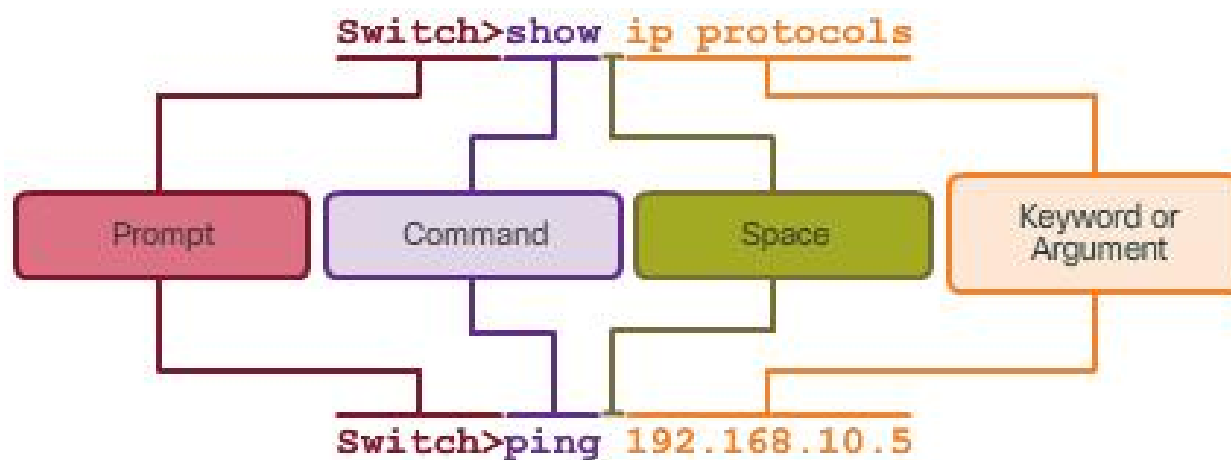
```
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# line vty 0 4
Switch(config-line)# interface fastethernet 0/1
Switch(config-if)# end
Switch#
```

Basic IOS Command Structure
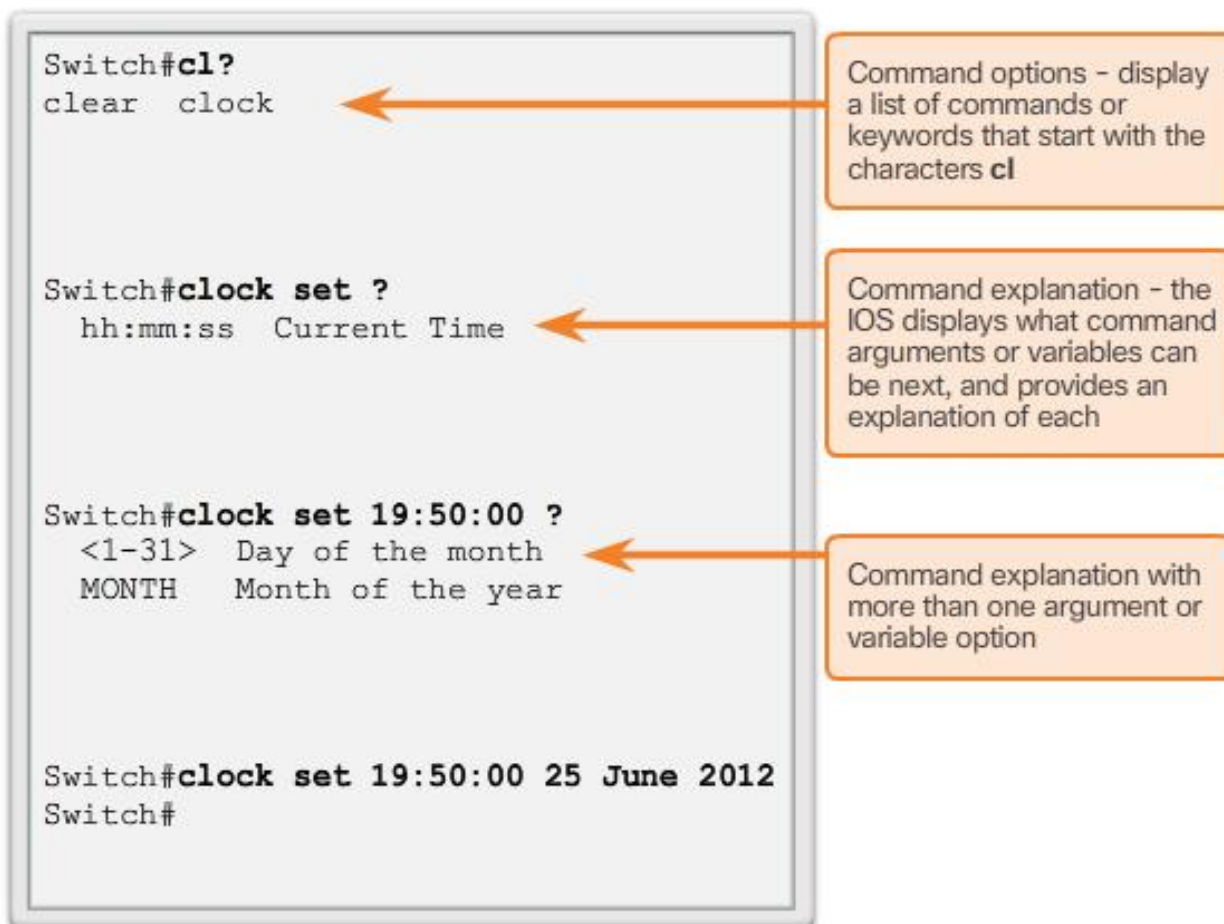
IOS Command Syntax

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

Convention	Description
boldface	Boldface text indicates commands and keywords that you enter literally as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets indicate an optional element (keyword or argument).
{x}	Braces indicate a required element (keyword or argument).
[x {y | z}]	Braces and vertical lines within square brackets indicate a required choice within an optional element.

IOS Help Features

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#
```

IOS Help Features (cont.)

```
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.

Hotkeys 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

Configure Hostnames

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

Secure Device Access

Securing Administrative Access

- Secure privileged EXEC access with a password

- Secure user EXEC access with a password

- Secure remote Telnet access with a password

Other tasks

- Encrypt all passwords

- Provide legal notification

When Choosing Passwords:

- Use passwords that are more than 8 characters in length.

- Use a combination of upper and lowercase letters, numbers, special characters, and/or numeric sequences.

- Avoid using the same password for all devices.

- Don't use common words because these are easily guessed.

Configure Passwords

```
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#
```

Class

Privileged EXEC Password Example

```
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)#
```

User EXEC Password Example

```
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)#
```

VTY Line Password Example

Configure Passwords (cont.)

```
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#
```

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

Configure Passwords (cont.)

```
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.

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

Encrypt Passwords

```
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

Switch#
You successfully encrypted the plain text passwords.
```

Reset   Show Me

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.
- After this command is applied, removing the encryption service does not reverse the encryption

Banner Messages

- These are an 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

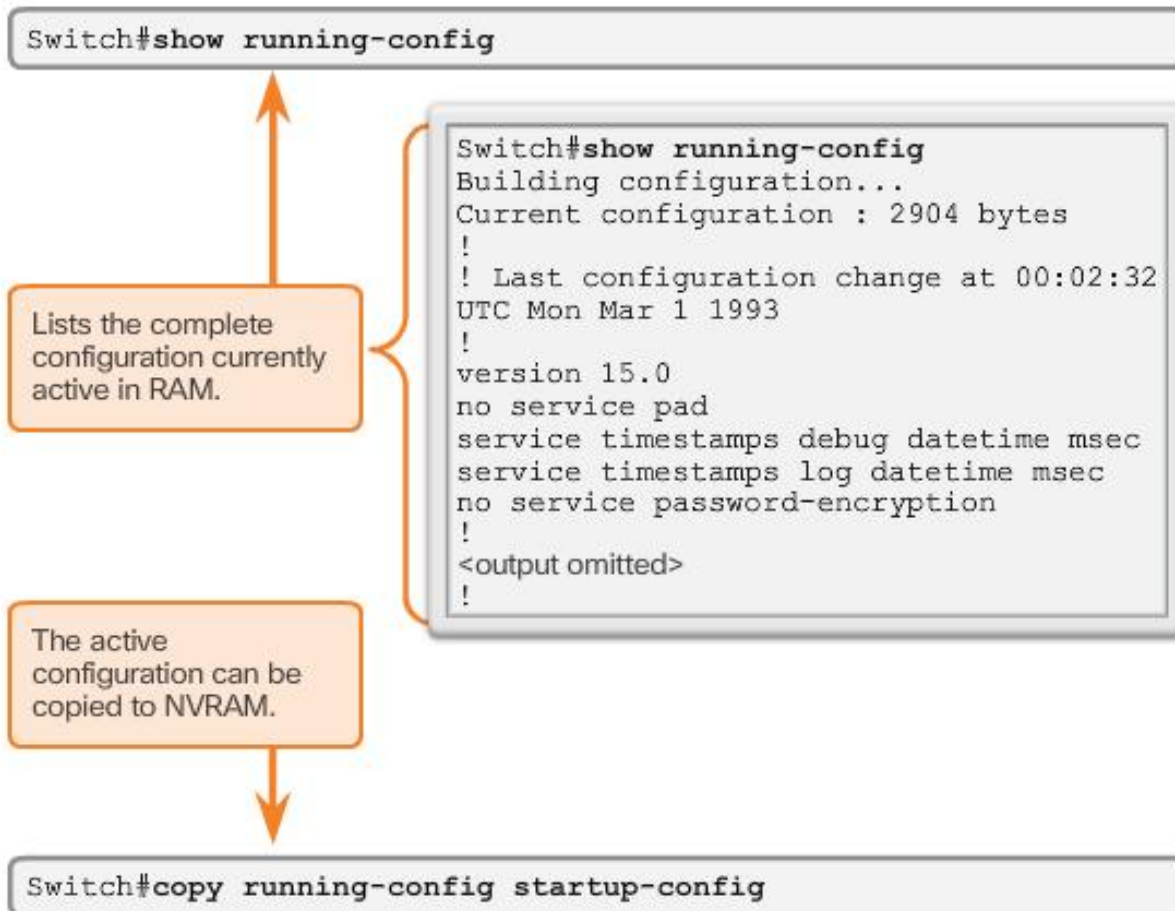`Sw1-Floor-1(config)#banner motd # This is a secure system. Authorized Access ONLY!!! #`

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#
```

Save the Running Configuration File

```
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
```

- **Startup configuration** –File stored in NVRAM that contains all of the commands that will be used upon startup or reboot. NVRAM does not lose its contents when the device is powered off.

- **Running configuration** – File stored in RAM that reflects the current configuration, modifying affects the operation of a Cisco device immediately. RAM loses all of its content when the device is powered off or restarted.

Alter the Running Configuration

- Restore the device to its previous configuration by removing the changed commands individually.
- Copy the startup configuration file to the running configuration with the **copy startup-config running-config** privileged EXEC mode command.
- Reload the device with the **reload** command from privileged EXEC mode.
- Switch# **reload**
  - System configuration has been modified. Save? [yes/no]: **n**
  - Proceed with reload? [confirm]

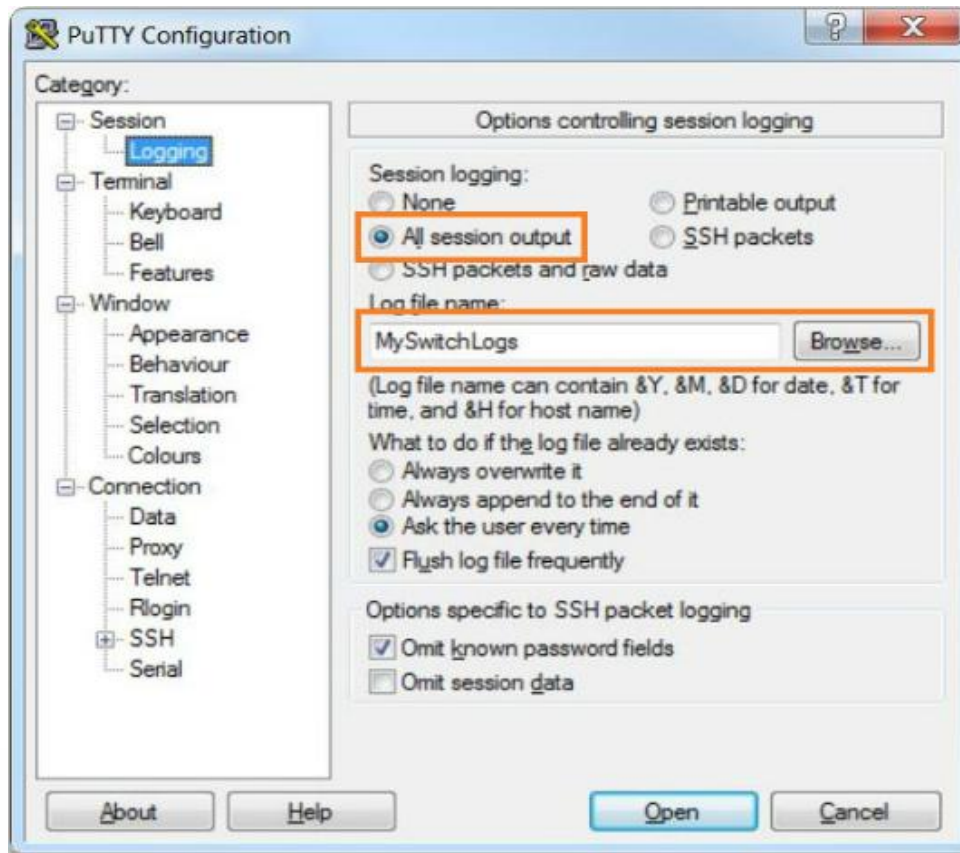# Capture Configuration to a Text File

Using PuTTY to Capture Console Session
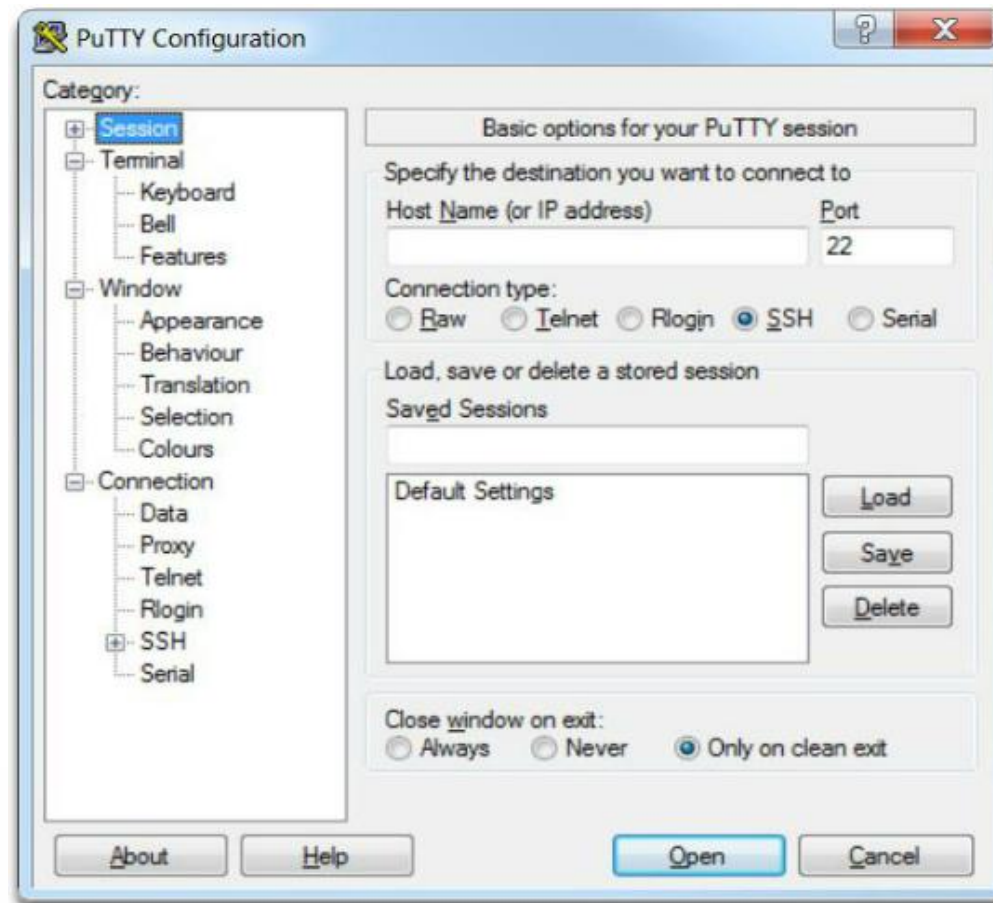
Capture Configuration to a Text File (cont.)

Enabling Session Logging in PuTTY

- All session output will be captured to the file specified, MySwitchLogs.

- Execute the show running-config or show startup-config command at the privileged EXEC prompt. Text displayed in the terminal window will be placed into the chosen file.

Capture Configuration to a Text File (cont.)
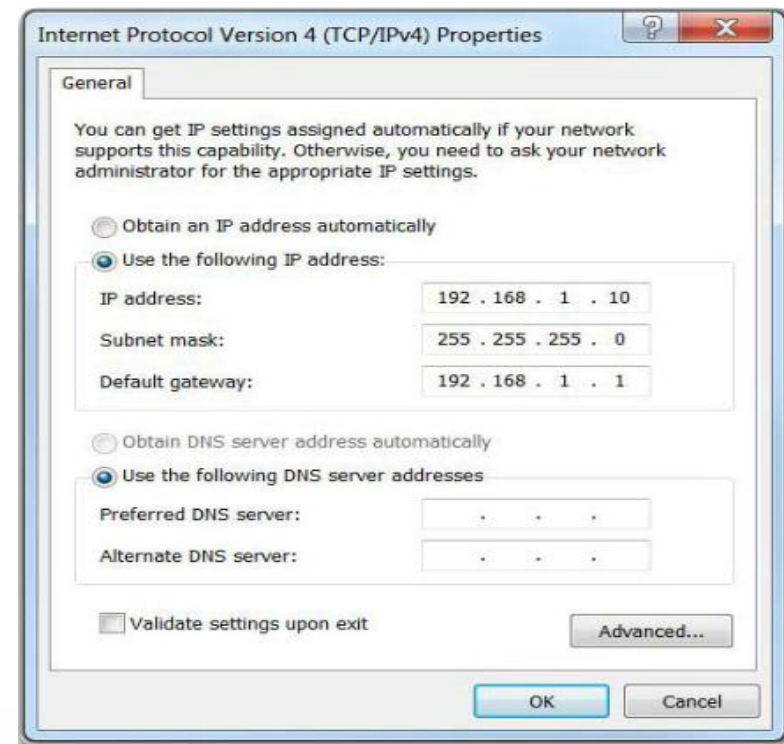
Disabling Session Logging in PuTTY

IP Addresses

Connecting End Devices

Configuring a Static IP
Address on a Host

Devices Requiring IP Addresses

- Computers (work stations, laptops, file servers, web servers)

- Network printers

- VoIP phones

- Security cameras

- Smart phones

- Mobile handheld devices (such as wireless barcode scanners)

Internet Protocol Version 4 (TCP/IPv4) 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 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses

Preferred DNS server: . . .
Alternate DNS server: . . .

☐ Validate settings upon exit   Advanced...

OK   Cancel

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 they also have one or more switch virtual interfaces (SVIs). No physical hardware on the device is associated with it. It is created in software.
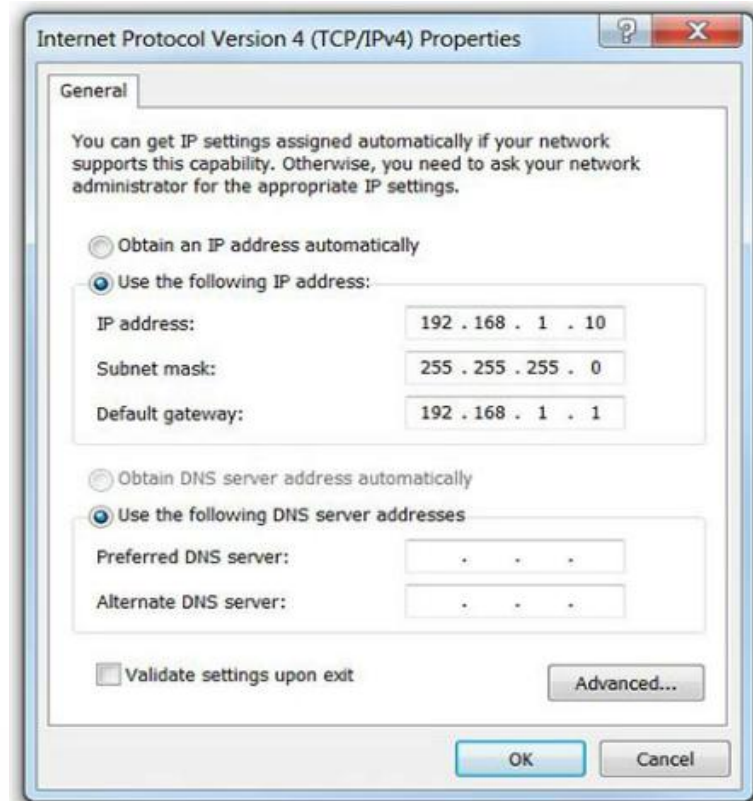- SVI provides a means to remotely manage a switch over a network.

Manual IP Address Configuration for End Devices

Strathmore
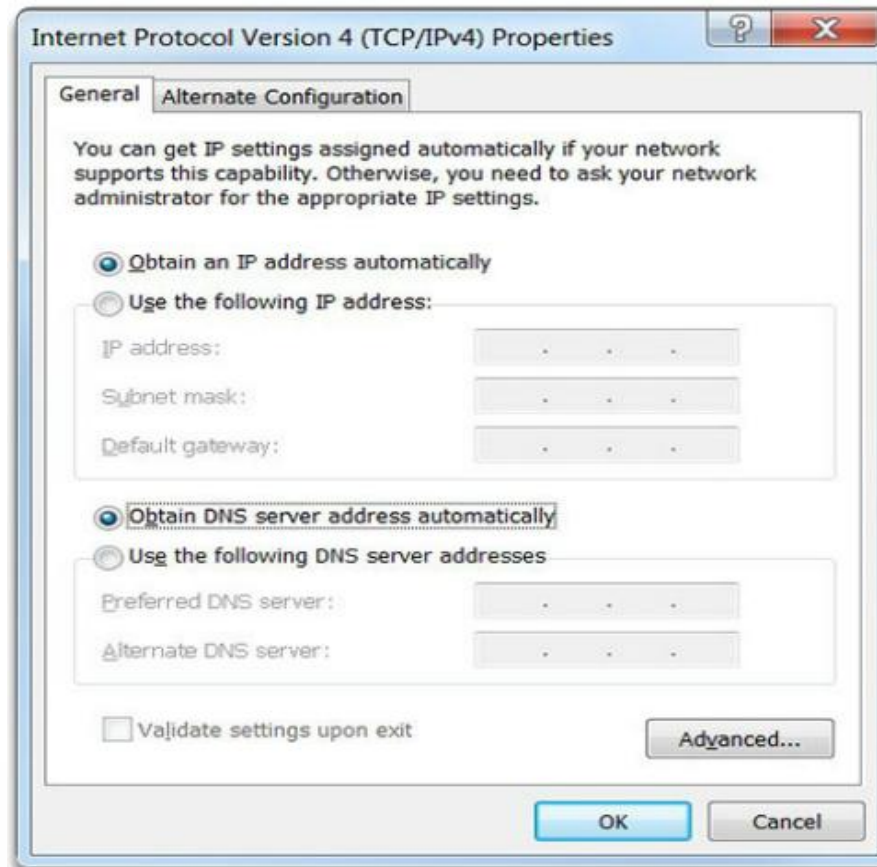UNIVERSITY

Ethernet Adapter Properties
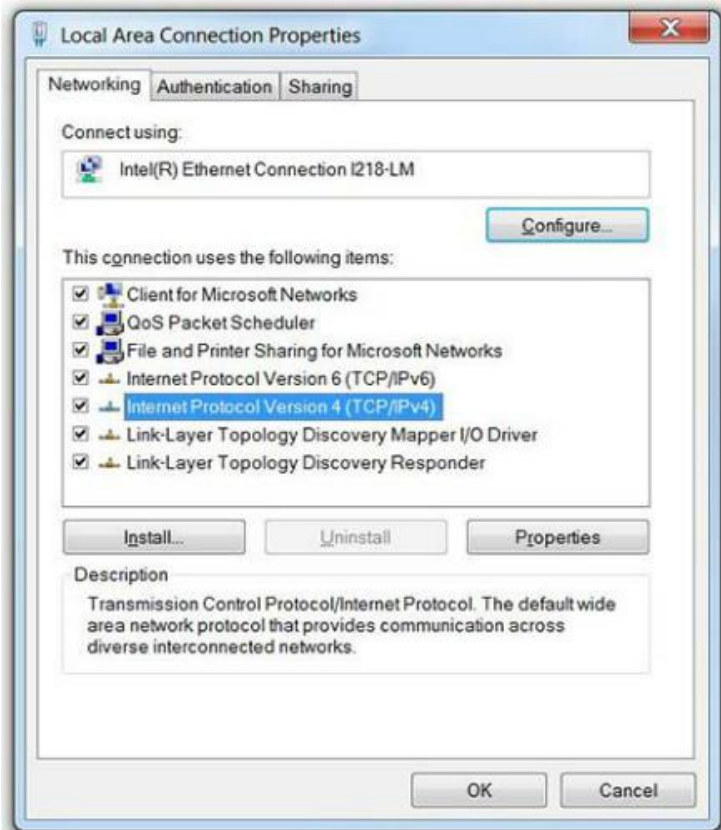
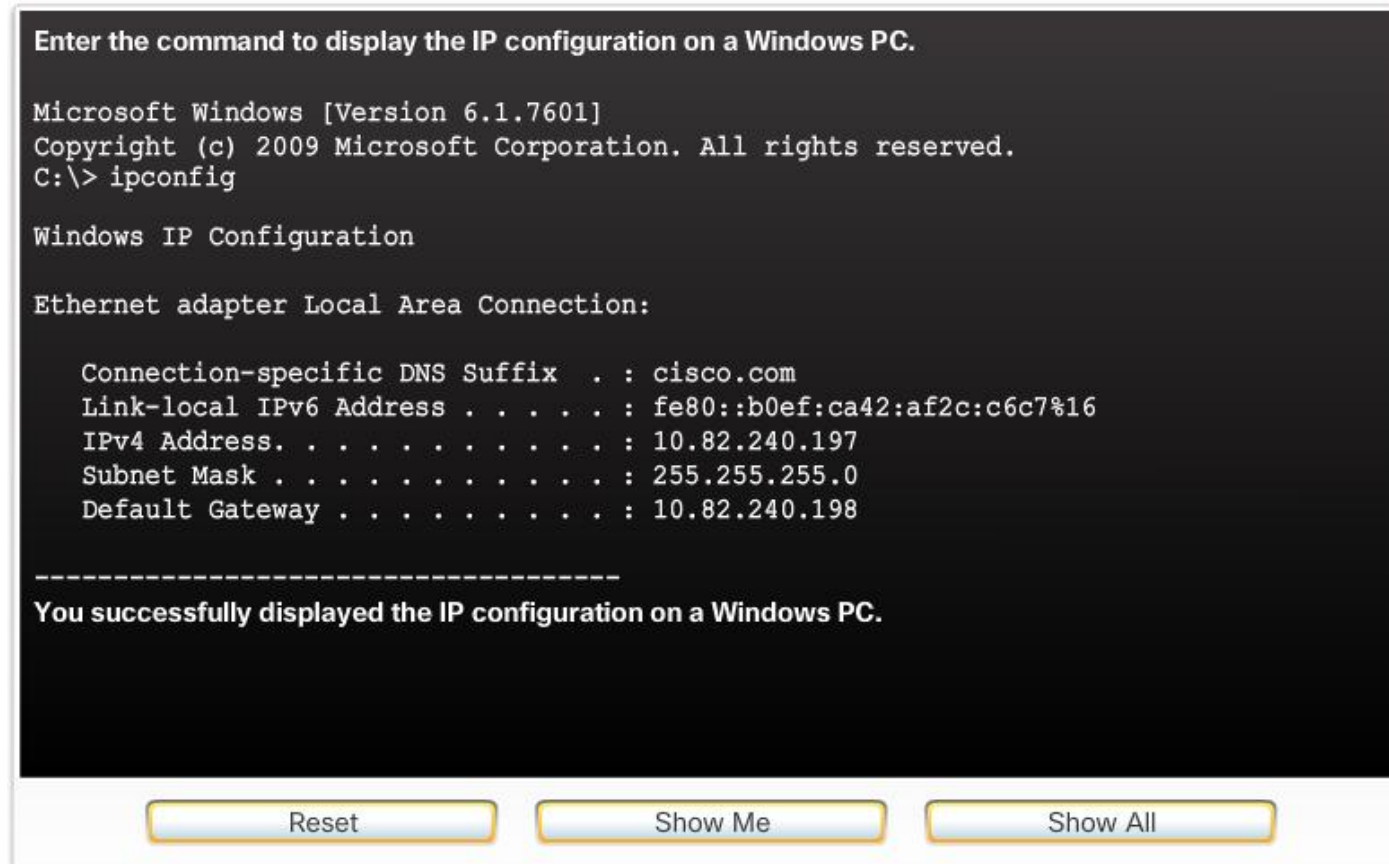## Manually Assigning IPv4 Address Information

Automatic IP Address Configuration for End Devices

Assigning Dynamic Addresses

Automatic IP Address Configuration for End Devices (cont.)

Verifying Windows PC IP Configuration

```
Enter the command to display the IP configuration on a Windows PC.

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : cisco.com
    Link-local IPv6 Address . . . . . : fe80::b0ef:ca42:af2c:c6c7%16
    IPv4 Address. . . . . . . . . . . : 10.82.240.197
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . : 10.82.240.198

--------------------------------------
You successfully displayed the IP configuration on a Windows PC.
```

| Reset | Show Me | Show All |

Switch Virtual Interface Configuration

```
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

Interface Addressing Verification

```
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
```

End-to-End Connectivity Test


```
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:\>
```

Ole Sangale Road, Madaraka Estate. PO Box 59857-00200, Nairobi, Kenya
Tel: (+254) (0)703 034000/200/300 Fax : +254 (0)20 607498
Email: info@strathmore.edu Website: www.strathmore.edu