



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Computer Architecture & Networks
Lab Manual
ACCD4001

Applied Computing Portfolio
Wales Institute of Science and Art
University of Wales Trinity Saint David
Swansea.

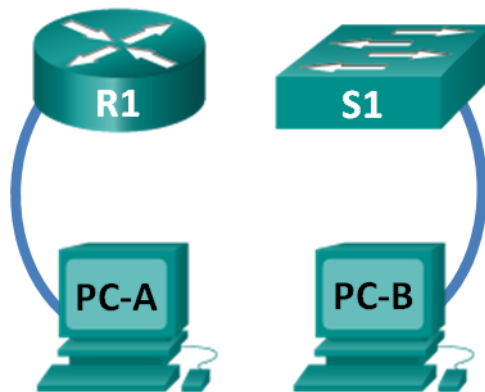
Module Leader
Dr Kapilan Radhakrishnan

Table of Contents

Lab 1 – Initializing and Reloading a Router and Switch.....	2
Lab 2 – Establishing a Console Session with Tera Term	6
Lab 3 – Building a Simple Network.....	16
Lab 4 – Configuring a Switch Management Address	28
Lab 5 – Using Wireshark to View Network Traffic.....	35
Lab 6 – Using Wireshark to Examine Ethernet Frames	47
Lab 7 – Viewing Network Device MAC Addresses	54
Lab 8 – Viewing the Switch MAC Address Table.....	59
Lab 9 – Building a Switch and Router Network.....	63
Lab 10 – Converting IPv4 Addresses to Binary	68
Lab 11 – Identifying IPv4 Addresses	72
Lab 12 – Calculating IPv4 Subnets.....	75
Lab 13 – Designing and Implementing a Sub netted IPv4 Addressing Scheme	82
Lab 14 – Designing and Implementing a VLSM Addressing Scheme.....	89
Lab 15 – Identifying IPv6 Addresses	95
Lab 16 – Configuring IPv6 Addresses on Network Devices.....	101
Lab 17 – Testing Network Connectivity with Ping and Traceroute.....	109
Lab 18 – Mapping the Internet.....	123
Lab 19 – Accessing Network Devices with SSH.....	130
Lab 20 – Examining Telnet and SSH in Wireshark.....	135
Lab 21 – Securing Network Devices.....	142
Lab 22 – Troubleshooting Connectivity Issues	149
Lab 23 – Building an Ethernet Crossover Cable	159

Lab 1 – Initializing and Reloading a Router and Switch

Topology



Objectives

Part 1: Set Up Devices in the Network as Shown in the Topology

Part 2: Initialize the Router and Reload

Part 3: Initialize the Switch and Reload

Background / Scenario

Before starting a CCNA hands-on lab that makes use of either a Cisco router or switch, ensure that the devices in use have been erased and have no startup configurations present. Otherwise, the results of your lab may be unpredictable. This lab provides a detail procedure for initializing and reloading a Cisco router and a Cisco switch.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS software, Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports

Part 1 – Set Up Devices in the Network as Shown in the Topology

Cable the network as shown in the topology.

Attach console cables to the devices shown in the topology diagram.

Power on all the devices in the topology.

Wait for all devices to finish the software load process before moving to Part 2.

Part 2 – Initialize the Router and Reload

Connect to the router.

Console into the router and enter privileged EXEC mode using the **enable** command.

```
Router> enable
Router#
```

Erase the startup configuration file from NVRAM.

Type the **erase startup-config** command to remove the startup configuration from nonvolatile random-access memory (NVRAM).

```
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
```

Reload the router.

Issue the **reload** command to remove an old configuration from memory. When prompted to Proceed with reload, press Enter to confirm the reload. Pressing any other key will abort the reload.

```
Router# reload
Proceed with reload? [confirm]

*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.

Note: You may receive a prompt to save the running configuration prior to reloading the router. Respond
by typing no and press Enter.

System configuration has been modified. Save? [yes/no]: no
```

Bypass the initial configuration dialog.

After the router reloads, you are prompted to enter the initial configuration dialog. Enter **no** and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

Terminate the autoinstall program.

You will be prompted to terminate the autoinstall program. Respond **yes** and then press Enter.

```
Would you like to terminate autoinstall? [yes]: yes
Router>
```

Initialize the Switch and Reload

Connect to the switch.

Console into the switch and enter privileged EXEC mode.

```
Switch> enable
Switch#
```

Determine if there have been any virtual local-area networks (VLANs) created.

Use the **show flash** command to determine if any VLANs have been created on the switch.

```
Switch# show flash
```

Directory of flash:/

2	-rwx	1919	Mar 1 1993 00:06:33 +00:00	private-config.text
3	-rwx	1632	Mar 1 1993 00:06:33 +00:00	config.text
4	-rwx	13336	Mar 1 1993 00:06:33 +00:00	multiple-fs
5	-rwx	11607161	Mar 1 1993 02:37:06 +00:00	c2960-lanbasek9-mz.150-2.SE.bin
6	-rwx	616	Mar 1 1993 00:07:13 +00:00	vlan.dat

32514048 bytes total (20886528 bytes free)

Switch#

Delete the VLAN file.

If the **vlan.dat** file was found in flash, then delete this file.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

You will be prompted to verify the file name. At this point, you can change the file name or just press Enter if you have entered the name correctly.

When you are prompted to delete this file, press Enter to confirm the deletion. (Pressing any other key will abort the deletion.)

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

Erase the startup configuration file.

Use the **erase startup-config** command to erase the startup configuration file from NVRAM. When you are prompted to remove the configuration file, press Enter to confirm the erase. (Pressing any other key will abort the operation.)

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

Reload the switch.

Reload the switch to remove any old configuration information from memory. When you are prompted to reload the switch, press Enter to proceed with the reload. (Pressing any other key will abort the reload.)

```
Switch# reload
Proceed with reload? [confirm]
```

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Type **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

Bypass the initial configuration dialog.

After the switch reloads, you should see a prompt to enter the initial configuration dialog. Type **no** at the prompt and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
```

Reflection

Why is it necessary to erase the startup configuration before reloading the router?

You find a couple configurations issues after saving the running configuration to the startup configuration, so you make the necessary changes to fix those issues. If you were to reload the device now, what configuration would be restored to the device after the reload?

Lab 2 – Establishing a Console Session with Tera Term

Topology



Objectives

Part 1: Access a Cisco Switch through the Serial Console Port

Part 2: Display and Configure Basic Device Settings

Part 3: (Optional) Access a Cisco Router Using a Mini-USB Console Cable

Note: Netlab users or other remote access equipment should complete only Part 2.

Background / Scenario

Various models of Cisco routers and switches are used in all types of networks. These devices are managed using a local console connection or a remote connection. Nearly all Cisco devices have a serial console port to which you can connect. Some newer models, such as the 1941 Integrated Services Router (ISR) G2 used in this lab, also have a USB console port.

In this lab, you will learn how to access a Cisco device via a direct local connection to the console port, using the terminal emulation program called Tera Term. You will also learn how to configure the serial port settings for the Tera Term console connection. After you have established a console connection with the Cisco device, you can display or configure device settings. You will only display settings and configure the clock in this lab.

Note: The routers used with CCNA hands-on labs are Cisco 1941 ISRs with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the switch and router have been erased and have no startup configuration. If you are unsure, contact your instructor.

Required Resources

1 Router (Cisco 1941 with Cisco IOS software, release 15.2(4)M3 universal image or comparable)

1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)

1 PC (Windows 7 or 8 with a terminal emulation program, such as Tera Term)

Rollover (DB-9 to RJ-45) console cable to configure the switch or router via the RJ-45 console port

Mini-USB cable to configure the router via the USB console port

You will connect a PC to a Cisco switch using a rollover console cable. This connection will allow you to access the CLI and display settings or configure the switch.

Connect a Cisco switch and computer using a rollover console cable.

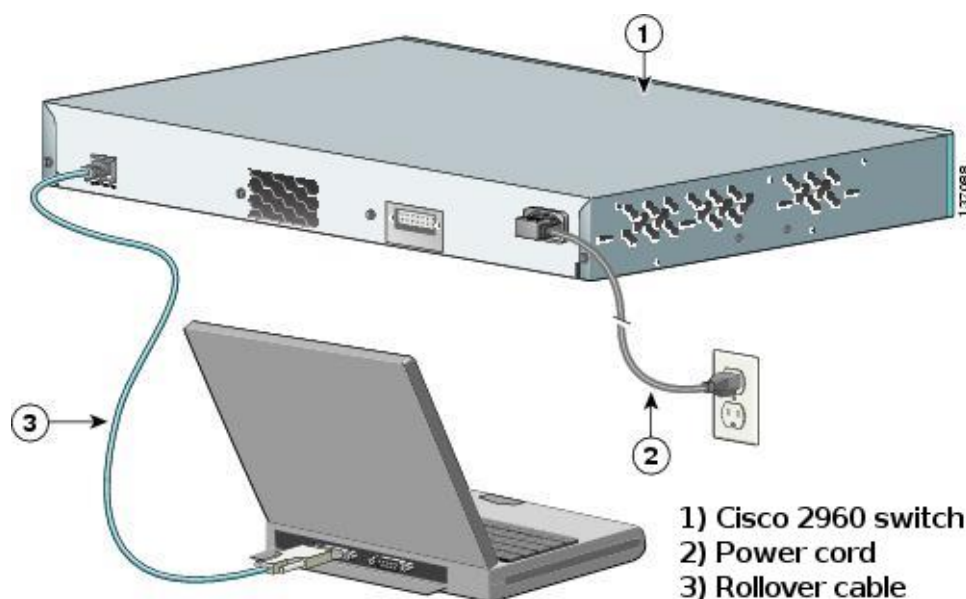
Connect the rollover console cable to the RJ-45 console port of the switch.

Connect the other cable end to the serial COM port on the computer.

Note: Serial COM ports are no longer available on most computers. A USB-to-DB9 adapter can be used with the rollover console cable for console connection between the computer and a Cisco device. USB-to-DB9 adapters can be purchased at any computer electronics store.

Note: If using a USB-to-DB9 adapter to connect to the COM port, you may be required to install a driver for the adapter provided by the manufacturer of your computer. To determine the COM port used by the adapter, please see Part 3 Step 4. The correct COM port number is required to connect to the Cisco IOS device using a terminal emulator in Step 2.

Turn on the Cisco switch and computer.



Configure Tera Term to establish a console session with the switch.

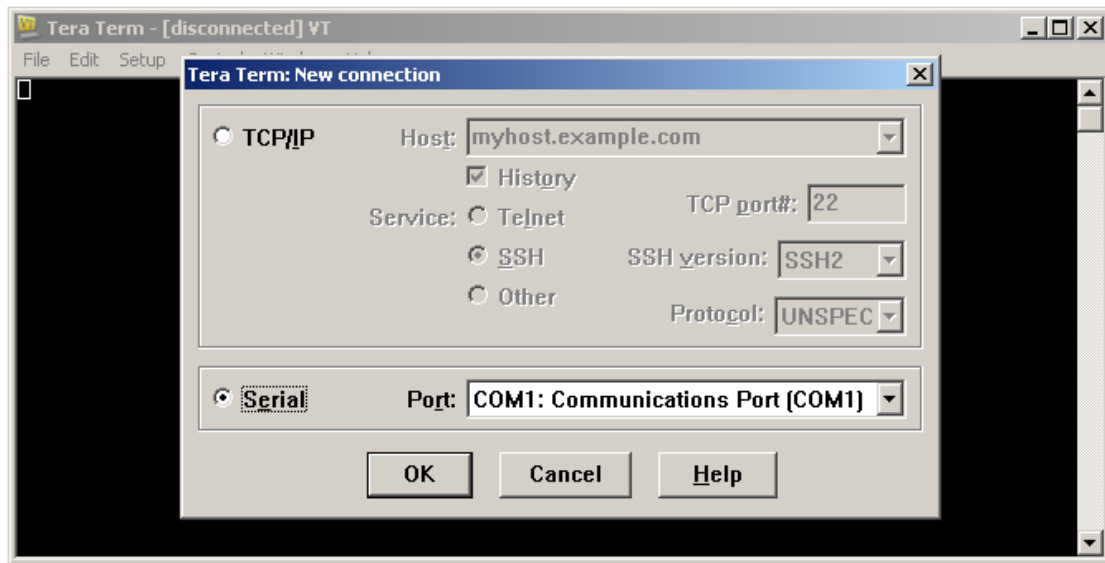
Tera Term is a terminal emulation program. This program allows you to access the terminal output of the switch. It also allows you to configure the switch.

Start Tera Term by clicking the **Windows Start** button located in the task bar. Locate **Tera Term** under **All Programs**.

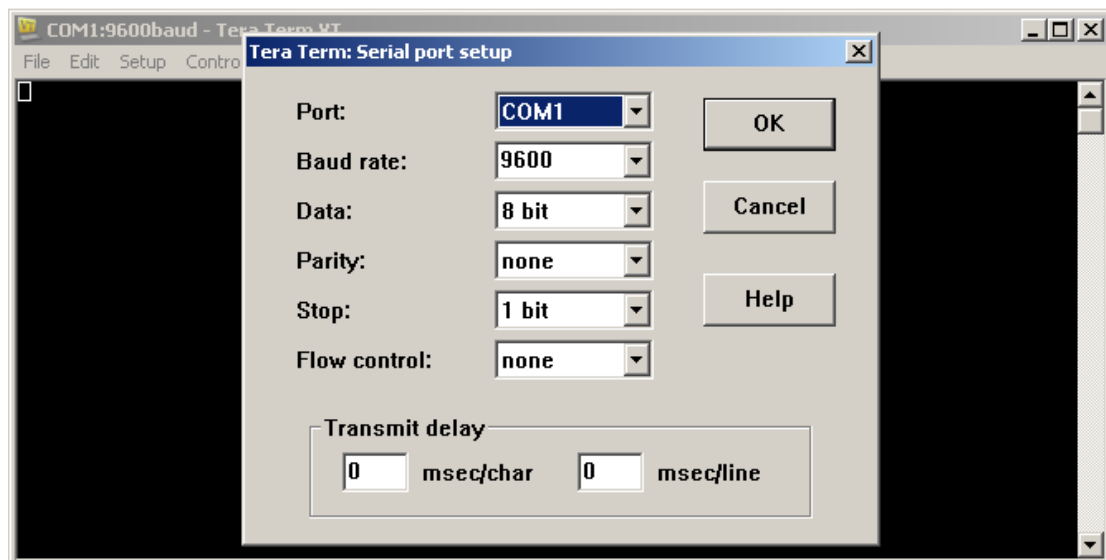
Note: If the program is not installed on the system, Tera Term can be downloaded from the following link by selecting **Tera Term**:

<http://logmett.com/index.php?/download/free-downloads.html>

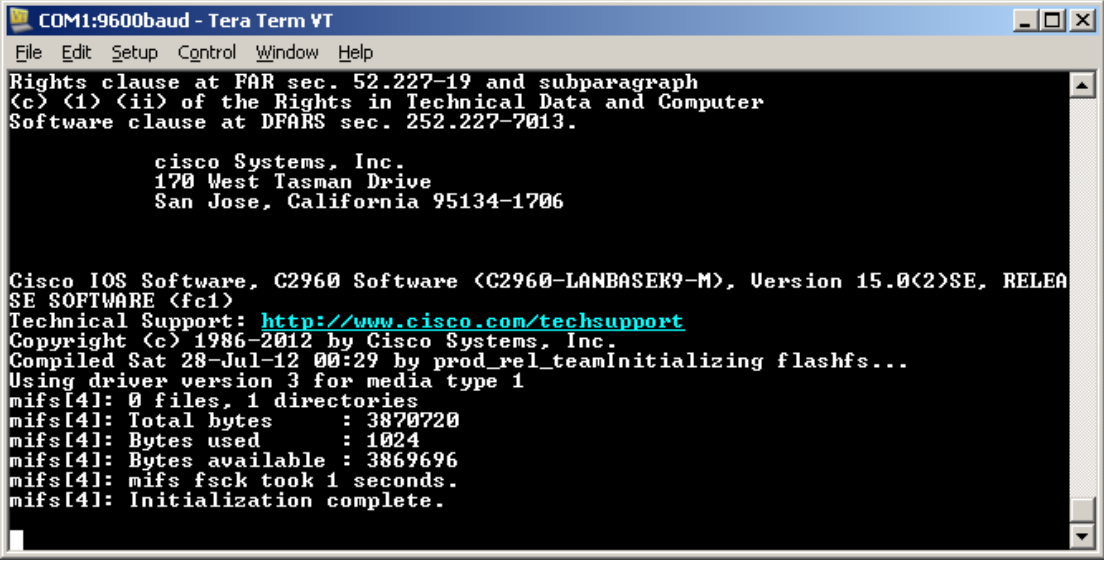
In the New Connection dialog box, click the **Serial** radio button. Verify that the correct COM port is selected and click **OK** to continue.



From the Tera Term **Setup** menu, choose the **Serial port...** to verify the serial settings. The default parameters for the console port are 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control. The Tera Term default settings match the console port settings for communications with the Cisco IOS switch.



When you can see the terminal output, you are ready to configure a Cisco switch. The following console example displays the terminal output of the switch while it is loading.



```
COM1:9600baud - Tera Term VT
File Edit Setup Control Window Help
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

    cisco Systems, Inc.
    170 West Tasman Drive
    San Jose, California 95134-1706

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEA
SE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sat 28-Jul-12 00:29 by prod_rel_teamInitializing flashfs...
Using driver version 3 for media type 1
mifs[4]: 0 files, 1 directories
mifs[4]: Total bytes      : 3870720
mifs[4]: Bytes used      : 1024
mifs[4]: Bytes available : 3869696
mifs[4]: mifs fsck took 1 seconds.
mifs[4]: Initialization complete.
```

Display and Configure Basic Device Settings

In this section, you are introduced to the user and privileged executive modes. You will determine the IOS version, display the clock settings, and configure the clock on the switch.

Display the switch IOS image version.

After the switch has completed its startup process, the following message is displayed. Enter **n** to continue.

```
Would you like to enter the initial configuration dialog? [yes/no]: n
```

Note: If you do not see the above message, please contact your instructor to reset your switch to the initial configuration.

While you are in the user EXEC mode, display the IOS version for your switch.

```
Switch> show version

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sat 28-Jul-12 00:29 by prod_rel_team

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE
(fc1)

Switch uptime is 2 minutes
System returned to ROM by power-on
System image file is "flash://c2960-lanbasek9-mz.150-2.SE.bin"
<output omitted>
```

Which IOS image version is currently in use by your switch?

Configure the clock.

As you learn more about networking, you will see that configuring the correct time on a Cisco switch can be helpful when you are troubleshooting problems. The following steps manually configure the internal clock of the switch.

Display the current clock settings.

```
Switch> show clock
*00:30:05.261 UTC Mon Mar 1 1993
```

The clock setting is changed from within the privileged EXEC mode. Enter the privileged EXEC mode by typing **enable** at the user EXEC mode prompt.

```
Switch> enable
```

Configure the clock setting. The question mark (?) provides help and allows you to determine the expected input for configuring the current time, date, and year. Press Enter to complete the clock configuration.

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

```
Switch# clock set 15:08:00 ?
<1-31> Day of the month
MONTH Month of the year
```

```
Switch# clock set 15:08:00 Oct 26 ?
<1993-2035> Year
```

```
Switch# clock set 15:08:00 Oct 26 2012
Switch#
```

```
*Oct 26 15:08:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 00:31:43
UTC Mon Mar 1 1993 to 15:08:00 UTC Fri Oct 26 2012, configured from console by
console.
```

Enter the **show clock** command to verify that the clock setting has updated.

```
Switch# show clock
15:08:07.205 UTC Fri Oct 26 2012
```

(Optional) Access a Cisco Router Using a Mini-USB Console Cable

If you are using a Cisco 1941 router, or other Cisco IOS devices with a mini-USB console port, you can access the device console port using a mini-USB cable connected to the USB port on your computer.

Note: The mini-USB console cable is the same type of mini-USB cables that are used with other electronics devices, such as USB hard drives, USB printers, or USB hubs. These mini-USB cables can be purchased from Cisco Systems, Inc. or other third-party vendors. Please verify that you are using a mini-USB cable, not a micro-USB cable, to connect to the mini-USB console port on a Cisco IOS device.



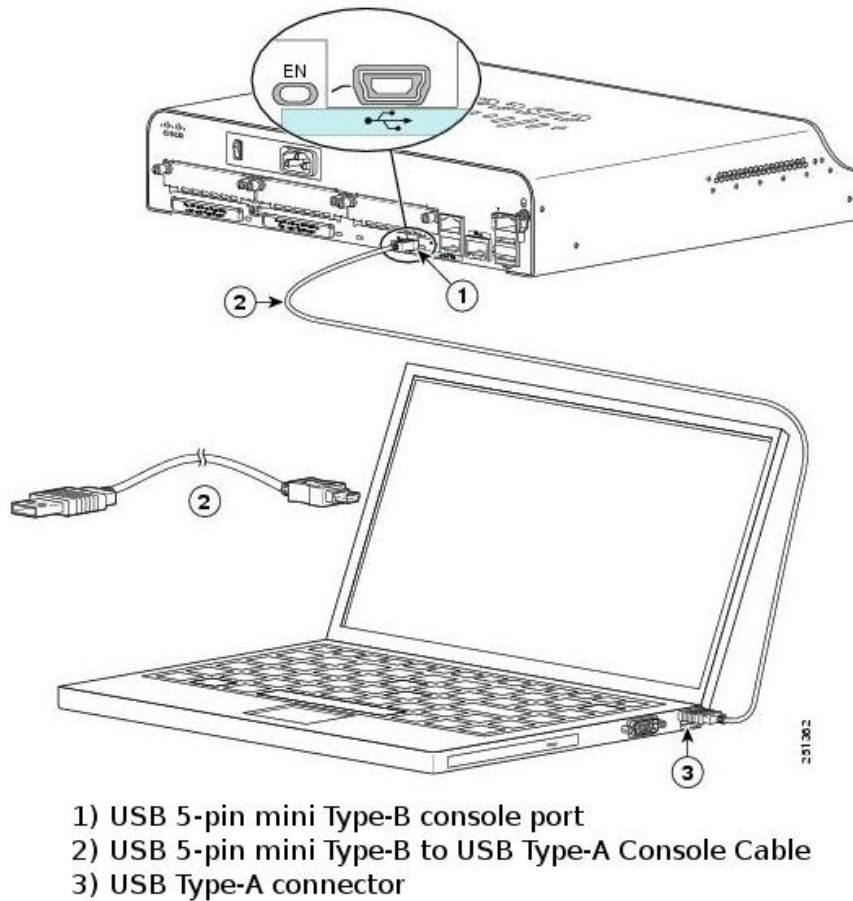
Note: You must use either the USB port or the RJ-45 port. Do not use both ports simultaneously. When the USB port is used, it takes priority over the RJ-45 console port.

Set up the physical connection with a mini-USB cable.

Connect the mini-USB cable to the mini-USB console port of the router.

Connect the other cable end to a USB port on the computer.

Turn on the Cisco router and computer.



Verify that the USB console is ready.

If you are using a Microsoft Windows-based PC and the USB console port LED indicator (labeled EN) does not turn green, please install the Cisco USB console driver.

A USB driver must be installed prior to connecting a Microsoft Windows-based PC to a Cisco IOS device with a USB cable. The driver can be found on www.cisco.com with the related Cisco IOS device. The USB driver can be downloaded from the following link:

<http://www.cisco.com/cisco/software/release.html?mdfid=282774238&flowid=714&softwareid=282855122&release=3.1&relind=AVAILABLE&rellifecycle=&reltype=latest>

Note: You must have a valid Cisco Connection Online (CCO) account to download this file.

Note: This link is related to the Cisco 1941 router. However, the USB console driver is not Cisco IOS device-model specific. This USB console driver only works with Cisco routers and switches. The computer requires a reboot after finishing the installation of the USB driver.

Note: After the files are extracted, the folder contains instructions for installation, removal, and the necessary drivers for different operating systems and architectures. Please choose the appropriate version for your system.

When the LED indicator for the USB console port has turned green, the USB console port is ready for access.

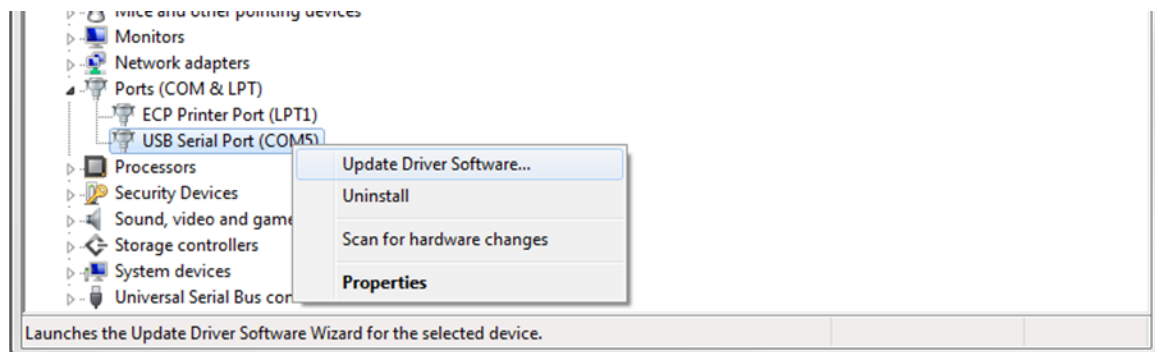
(Optional) Enable the COM port for the Windows 7 PC.

If you are using a Microsoft Windows 7 PC, you may need to perform the following steps to enable the COM port:

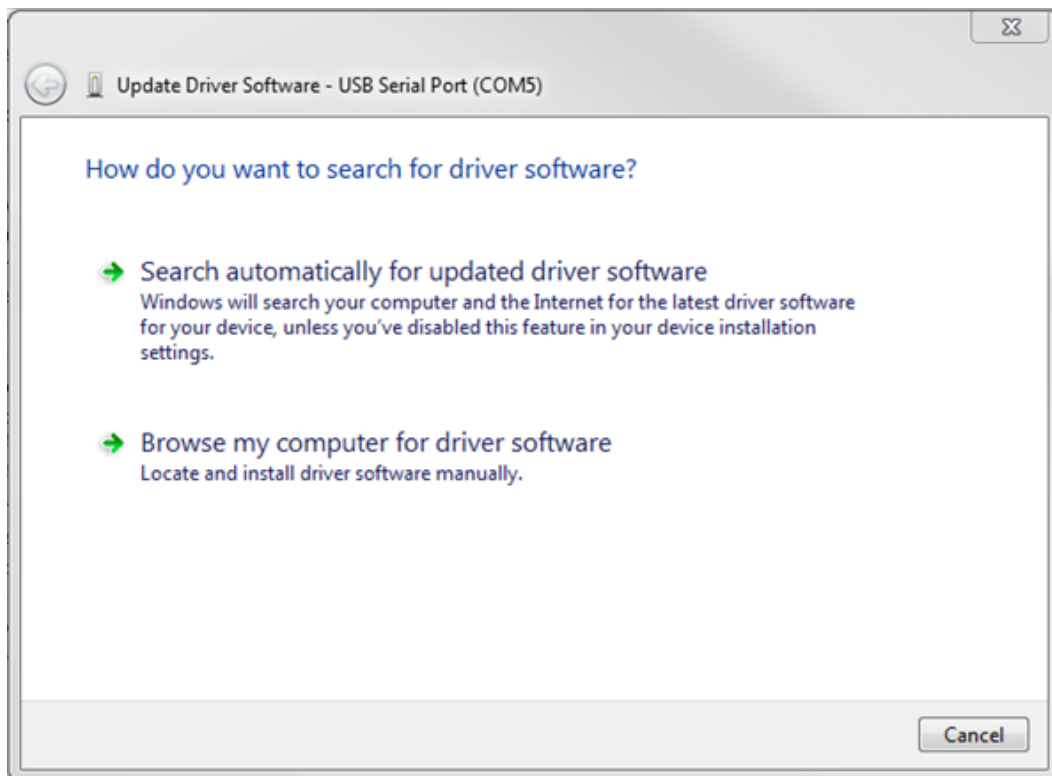
Click the **Windows Start** icon to access the **Control Panel**.

Open the **Device Manager**.

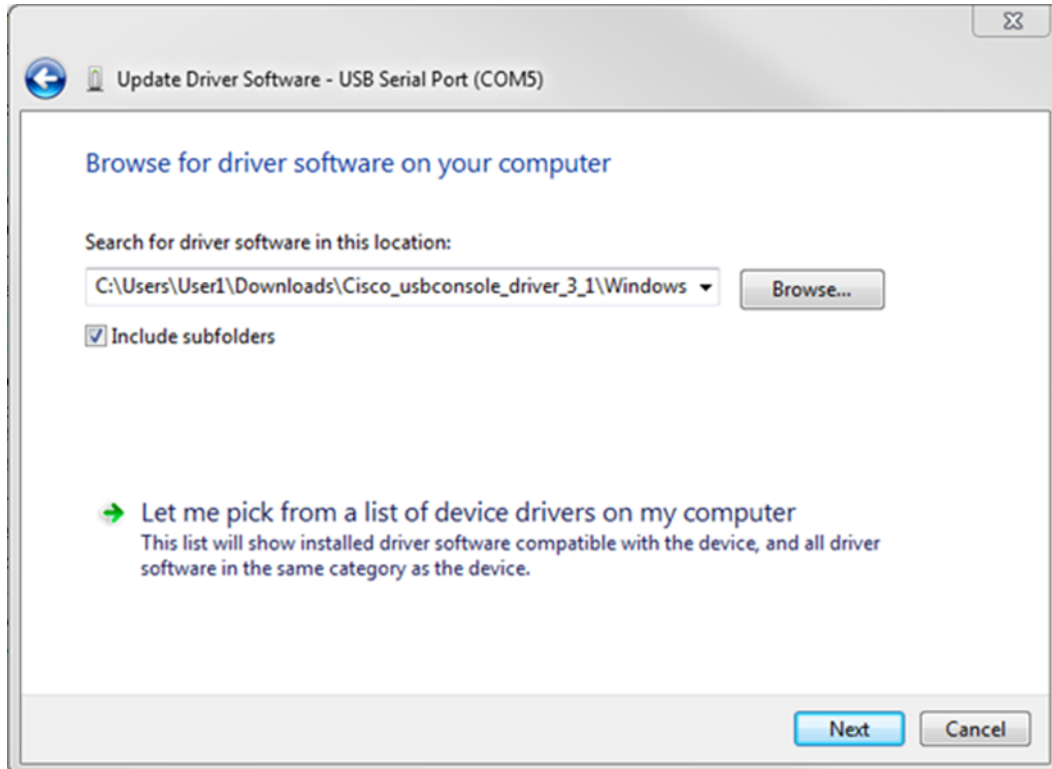
Click the **Ports (COM & LPT)** tree link to expand it. Right-click the **USB Serial Port (COM5)** icon and choose **Update Driver Software**.



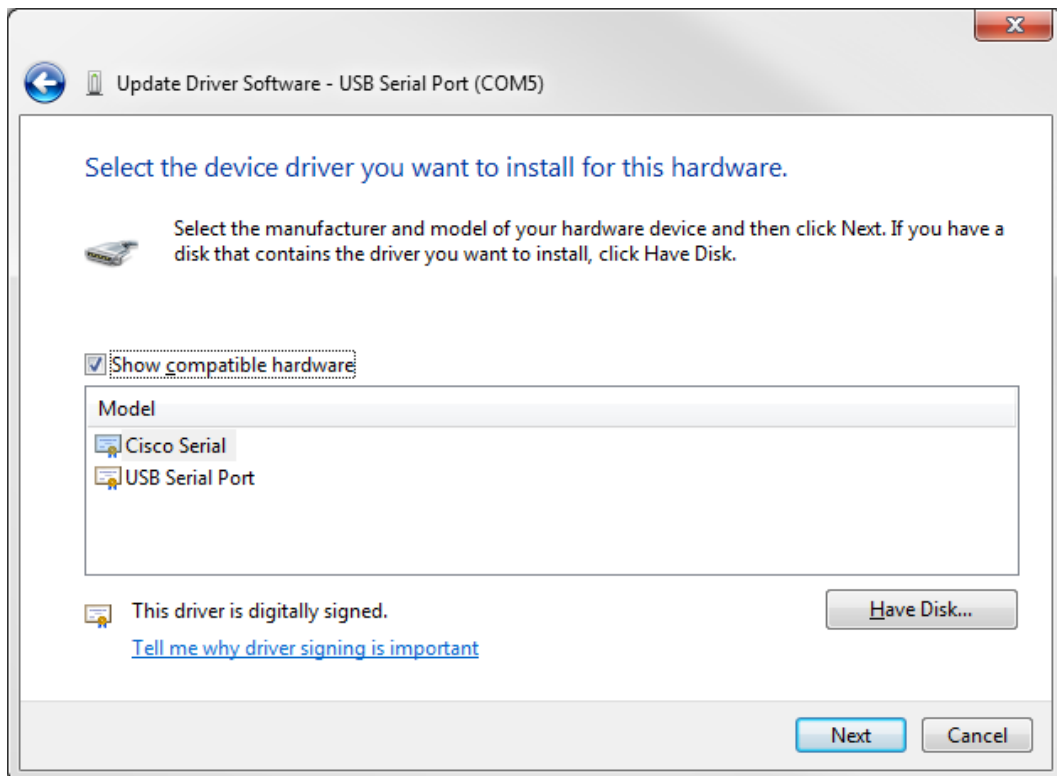
Choose **Browse my computer for driver software**.



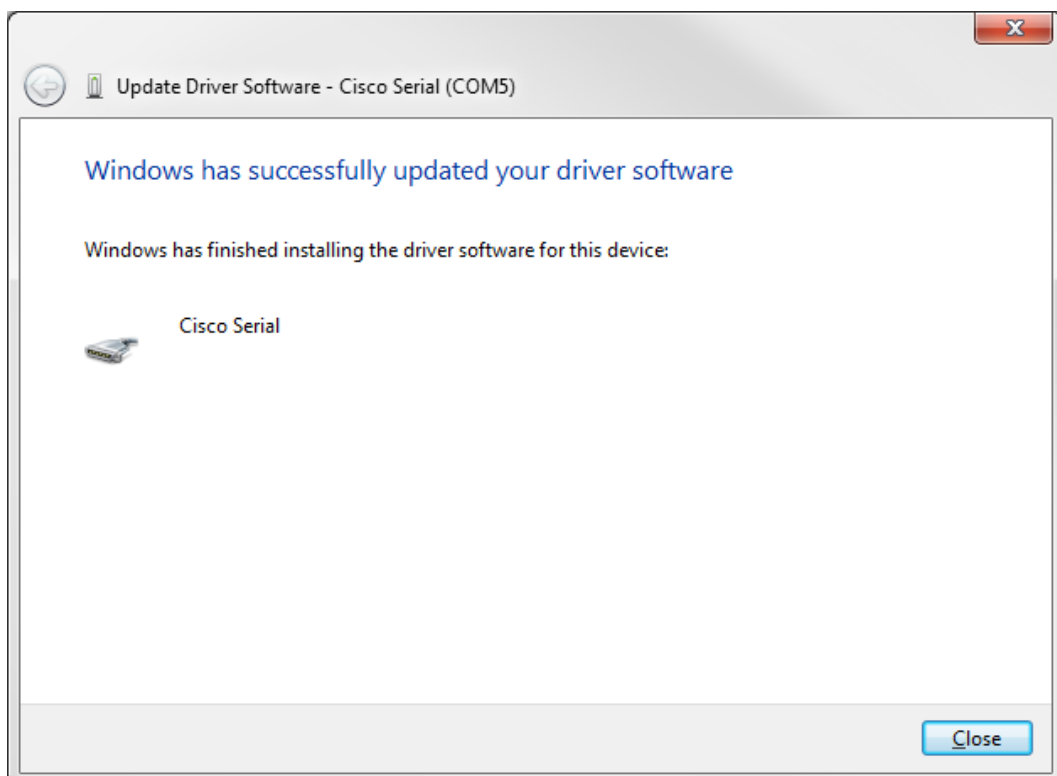
Choose **Let me pick from a list of device drivers on my computer** and click **Next**.



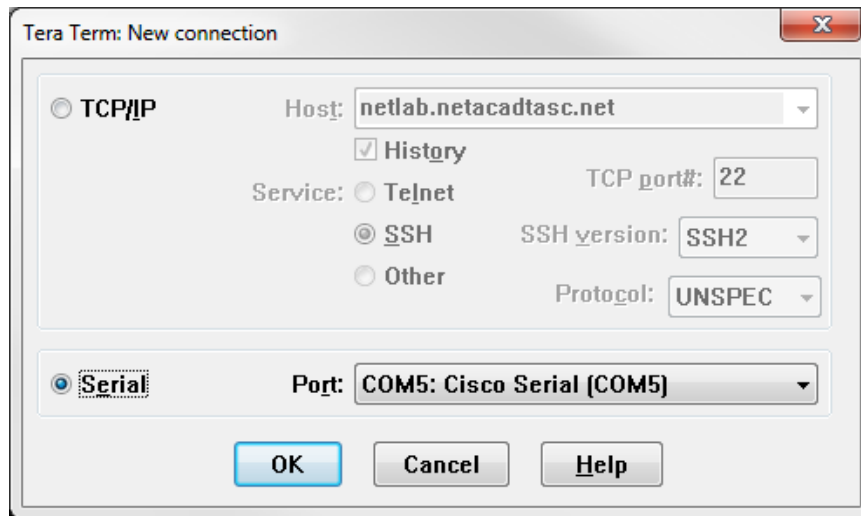
Choose the **Cisco Serial** driver and click **Next**.



Note the port number assigned at the top of the window. In this sample, COM 5 is used for communication with the router. Click **Close**.



Open Tera Term. Click the **Serial** radio button and choose the appropriate serial port, which is **Port COM5: Cisco Serial (COM 5)** in this example. This port should now be available for communication with the router. Click **OK**.



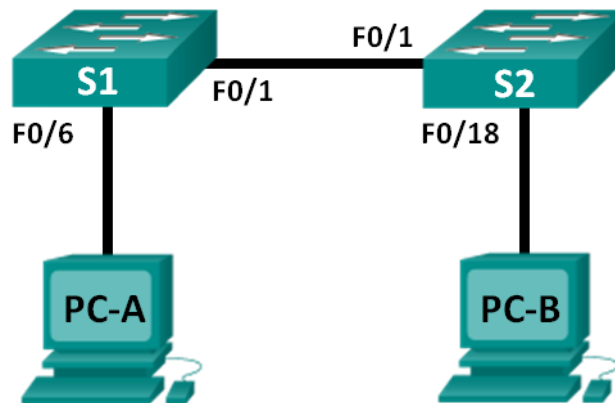
Reflection

How do you prevent unauthorized personnel from accessing your Cisco device through the console port?

What are the advantages and disadvantages of using the serial console connection compared to the USB console connection to a Cisco router or switch?

Lab 3 – Building a Simple Network

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
PC-A	NIC	192.168.1.10	255.255.255.0
PC-B	NIC	192.168.1.11	255.255.255.0

Objectives

Part 1: Set Up the Network Topology (Ethernet only)

Part 2: Configure PC Hosts

Part 3: Configure and Verify Basic Switch Settings

Background / Scenario

Networks are constructed of three major components: hosts, switches, and routers. In this lab, you will build a simple network with two hosts and two switches. You will also configure basic settings including hostname, local passwords, and login banner. Use **show** commands to display the running configuration, IOS version, and interface status. Use the **copy** command to save device configurations.

You will apply IP addressing for this lab to the PCs to enable communication between these two devices. Use the **ping** utility to verify connectivity.

Note: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Note: Make sure that the switches have been erased and have no startup configurations. Refer to Appendix A for the procedure to initialize and reload a switch.

Required Resources

2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)

2 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)

Console cables to configure the Cisco IOS devices via the console ports

Ethernet cables as shown in the topology

Set Up the Network Topology (Ethernet only)

In Part 1, you will cable the devices together according to the network topology.

Power on the devices.

Power on all devices in the topology. The switches do not have a power switch; they will power on as soon as you plug in the power cord.

Connect the two switches.

Connect one end of an Ethernet cable to F0/1 on S1 and the other end of the cable to F0/1 on S2. You should see the lights for F0/1 on both switches turn amber and then green. This indicates that the switches have been connected correctly.

Connect the PCs to their respective switches.

Connect one end of the second Ethernet cable to the NIC port on PC-A. Connect the other end of the cable to F0/6 on S1. After connecting the PC to the switch, you should see the light for F0/6 turn amber and then green, indicating that PC-A has been connected correctly.

Connect one end of the last Ethernet cable to the NIC port on PC-B. Connect the other end of the cable to F0/18 on S2. After connecting the PC to the switch, you should see the light for F0/18 turn amber and then green, indicating that the PC-B has been connected correctly.

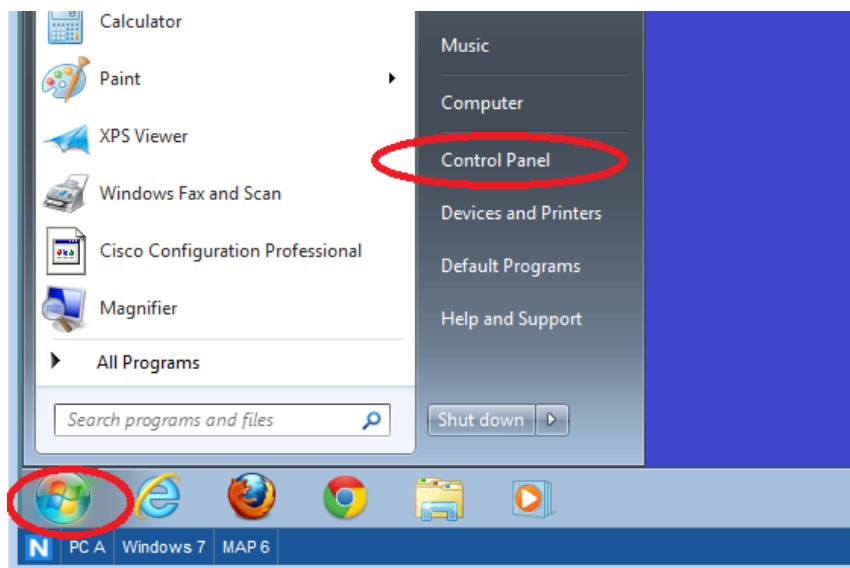
Visually inspect network connections.

After cabling the network devices, take a moment to carefully verify the connections to minimize the time required to troubleshoot network connectivity issues later.

Configure PC Hosts

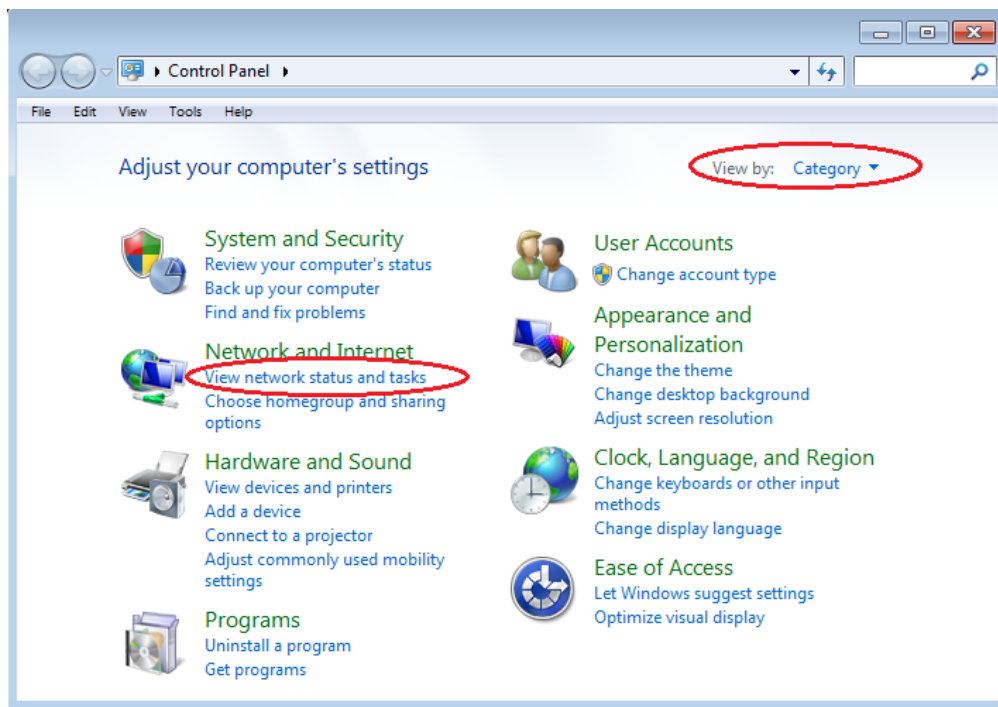
Configure static IP address information on the PCs.

Click the **Windows Start** icon and then select **Control Panel**.

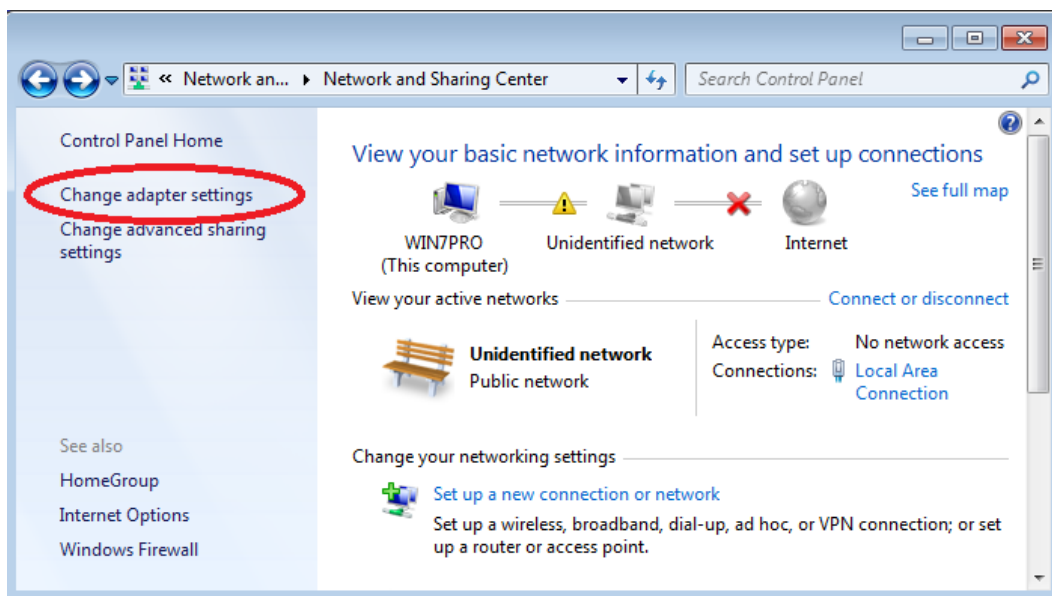


In the Network and Internet section, click the **View network status and tasks** link.

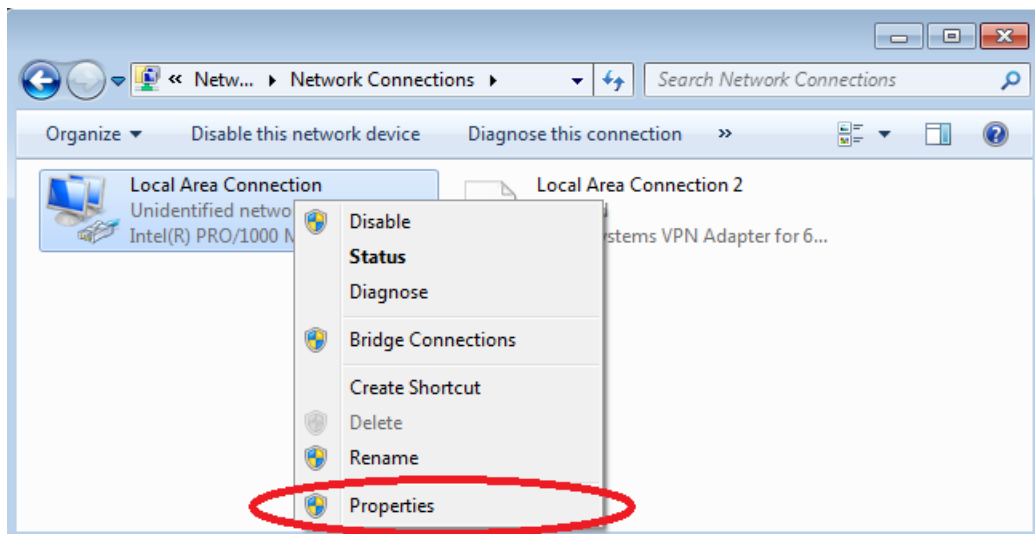
Note: If the Control Panel displays a list of icons, click the drop-down option next to the **View by:** and change this option to display by **Category**.



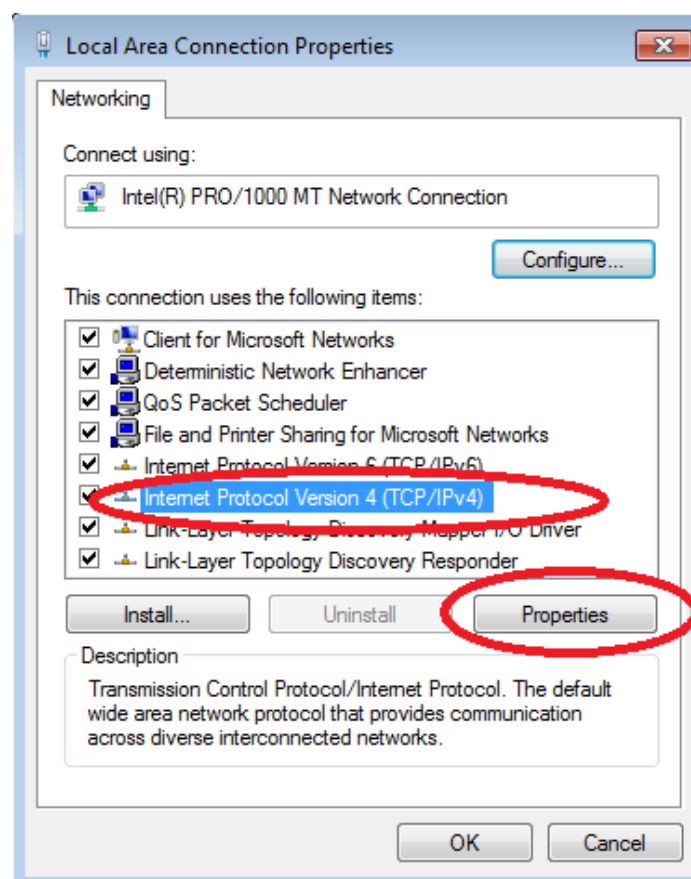
In the left pane of the Network and Sharing Center window, click the **Change adapter settings** link.



The Network Connections window displays the available interfaces on the PC. Right-click the **Local Area Connection** interface and select **Properties**.

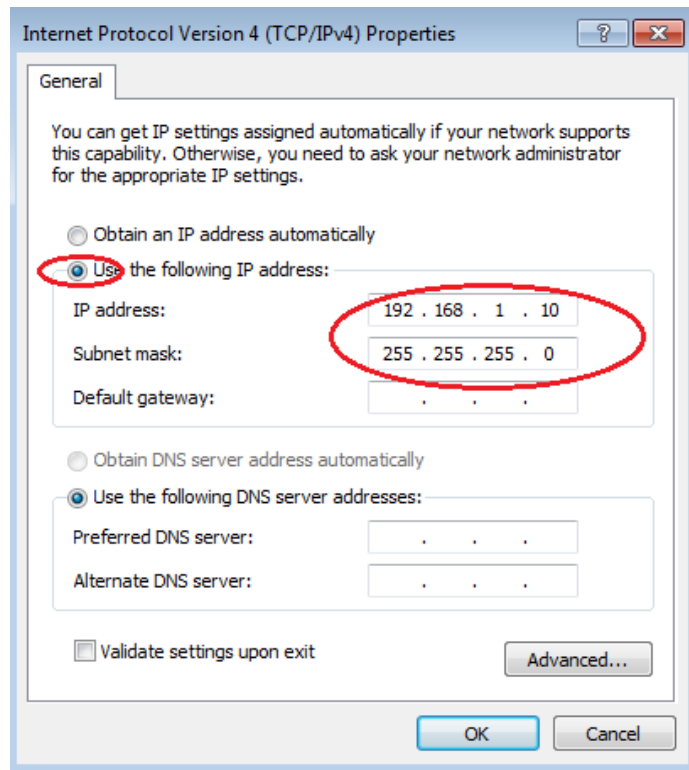


Select the **Internet Protocol Version 4 (TCP/IPv4)** option and then click **Properties**.



Note: You can also double-click **Internet Protocol Version 4 (TCP/IPv4)** to display the Properties window.

Click the **Use the following IP address** radio button to manually enter an IP address, subnet mask, and default gateway.



Note: In the above example, the IP address and subnet mask have been entered for PC-A. The default gateway has not been entered, because there is no router attached to the network. Refer to the Addressing Table on page 1 for PC-B's IP address information.

After all the IP information has been entered, click **OK**. Click **OK** on the Local Area Connection Properties window to assign the IP address to the LAN adapter.

Repeat the previous steps to enter the IP address information for PC-B.

Verify PC settings and connectivity.

Use the command prompt (**cmd.exe**) window to verify the PC settings and connectivity.

From PC-A, click the **Windows Start** icon, type **cmd** in the **Search programs and files** box, and then press Enter.



The cmd.exe window is where you can enter commands directly to the PC and view the results of those commands. Verify your PC settings by using the **ipconfig /all** command. This command displays the PC hostname and the IPv4 address information.

```
C:\Windows\system32\cmd.exe

C:\Users\NetAcad>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : PC-A
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . :
    Description . . . . . : Intel(R) PRO/1000 MT Network Connection
    Physical Address. . . . . : 00-50-56-BE-6C-89
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::d428:7de2:997c:b85a%11(Preferred)
    IPv4 Address. . . . . : 192.168.1.10(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
    DHCPv6 IAID . . . . . : 234884137
    DHCPv6 Client DUID. . . . . : 00-01-00-01-17-F6-72-3D-00-0C-29-8D-54-44
```

Type **ping 192.168.1.11** and press Enter.

```
C:\Windows\system32\cmd.exe

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\NetAcad>
```

Were the ping results successful? _____

If not, troubleshoot as necessary.

Note: If you did not get a reply from PC-B, try to ping PC-B again. If you still do not get a reply from PC-B, try to ping PC-A from PC-B. If you are unable to get a reply from the remote PC, then have your instructor help you troubleshoot the problem.

Configure and Verify Basic Switch Settings

Console into the switch.

Using Tera Term, establish a console connection to the switch from PC-A.

Enter privileged EXEC mode.

You can access all switch commands in privileged EXEC mode. The privileged EXEC command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes are gained. Enter privileged EXEC mode by entering the **enable** command.

```
Switch> enable
Switch#
```

The prompt changed from **Switch>** to **Switch#** which indicates privileged EXEC mode.

Enter configuration mode.

Use the **configuration terminal** command to enter configuration mode.

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

The prompt changed to reflect global configuration mode.

Give the switch a name.

Use the **hostname** command to change the switch name to **S1**.

```
Switch(config)# hostname S1
S1(config)#
```

Prevent unwanted DNS lookups.

To prevent the switch from attempting to translate incorrectly entered commands as though they were hostnames, disable the Domain Name System (DNS) lookup.

```
S1(config)# no ip domain-lookup
S1(config)#
```

Enter local passwords.

To prevent unauthorized access to the switch, passwords must be configured.

```
S1(config)# enable secret class
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)#
```

Enter a login MOTD banner.

A login banner, known as the message of the day (MOTD) banner, should be configured to warn anyone accessing the switch that unauthorized access will not be tolerated.

The **banner motd** command requires the use of delimiters to identify the content of the banner message. The delimiting character can be any character as long as it does not occur in the message. For this reason, symbols, such as the #, are often used.

```

S1(config)# banner motd #
Enter TEXT message. End with the character '#'.
Unauthorized access is strictly prohibited and prosecuted to the full
extent of the law. #
S1(config)# exit
S1#

```

Save the configuration.

Use the **copy** command to save the running configuration to the startup file on non-volatile random access memory (NVRAM).

```

S1# copy running-config startup-config
Destination filename [startup-config]? [Enter]
Building configuration...
[OK]
S1#

```

Display the current configuration.

The **show running-config** command displays the entire running configuration, one page at a time. Use the spacebar to advance paging. The commands configured in Steps 1 – 8 are highlighted below.

```

S1# show running-config
Building configuration...

Current configuration : 1409 bytes
!
! Last configuration change at 03:49:17 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
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!

<output omitted>

!
banner motd ^C

```

Unauthorized access is strictly prohibited and prosecuted to the full extent of the law. ^C

```
!  
line con 0  
password cisco  
login  
line vty 0 4  
login  
line vty 5 15  
login  
!  
end  
  
S1#
```

Display the IOS version and other useful switch information.

Use the **show version** command to display the IOS version that the switch is running, along with other useful information. Again, you will need to use the spacebar to advance through the displayed information.

```
S1# show version  
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE  
SOFTWARE (fc1)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2012 by Cisco Systems, Inc.  
Compiled Sat 28-Jul-12 00:29 by prod_rel_team  
  
ROM: Bootstrap program is C2960 boot loader  
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE  
(fc1)  
  
S1 uptime is 1 hour, 38 minutes  
System returned to ROM by power-on  
System image file is "flash:/c2960-lanbasek9-mz.150-2.SE.bin"
```

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. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

```
cisco WS-C2960-24TT-L (PowerPC405) processor (revision R0) with 65536K bytes of  
memory.  
Processor board ID FCQ1628Y5LE  
Last reset from power-on
```

```

1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

```

64K bytes of flash-simulated non-volatile configuration memory.

```

Base ethernet MAC Address      : 0C:D9:96:E2:3D:00
Motherboard assembly number    : 73-12600-06
Power supply part number       : 341-0097-03
Motherboard serial number      : FCQ16270N5G
Power supply serial number     : DCA1616884D
Model revision number          : R0
Motherboard revision number    : A0
Model number                   : WS-C2960-24TT-L
System serial number           : FCQ1628Y5LE
Top Assembly Part Number       : 800-32797-02
Top Assembly Revision Number   : A0
Version ID                     : V11
CLEI Code Number               : COM3L00BRF
Hardware Board Revision Number : 0x0A

```

Switch	Ports	Model	SW Version	SW Image
-----	-----	-----	-----	-----
*	1 26	WS-C2960-24TT-L	15.0(2)SE	C2960-LANBASEK9-M

```

Configuration register is 0xF
S1#

```

Display the status of the connected interfaces on the switch.

To check the status of the connected interfaces, use the **show ip interface brief** command. Press the spacebar to advance to the end of the list.

```

S1# show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	YES	unset	up	up
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	down	down
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down

```

FastEthernet0/17      unassigned      YES unset    down
FastEthernet0/18      unassigned      YES unset    down
FastEthernet0/19      unassigned      YES unset    down
FastEthernet0/20      unassigned      YES unset    down
FastEthernet0/21      unassigned      YES unset    down
FastEthernet0/22      unassigned      YES unset    down
FastEthernet0/23      unassigned      YES unset    down
FastEthernet0/24      unassigned      YES unset    down
GigabitEthernet0/1    unassigned      YES unset    down
GigabitEthernet0/2    unassigned      YES unset    down
S1#

```

Repeat Steps to configure switch S2.

The only difference for this step is to change the hostname to S2.

Record the interface status for the following interfaces.

Interface	S1		S2	
	Status	Protocol	Status	Protocol
F0/1				
F0/6				
F0/18				
VLAN 1				

Why is it that Fast Ethernet ports on the switches are up and others are down?

Reflection

What could prevent a ping from being sent between the PCs?

Note: It may be necessary to disable the PC firewall to ping between PCs.

Appendix A: Initializing and Reloading a Switch

Connect to the switch.

Console into the switch and enter privileged EXEC mode.

```

Switch> enable
Switch#

```

Determine if there have been any virtual local-area networks (VLANs) created.

Use the **show flash** command to determine if any VLANs have been created on the switch.

```

Switch# show flash

```

```

Directory of flash:/

   2  -rwx           1919   Mar 1 1993 00:06:33 +00:00  private-config.text
   3  -rwx           1632   Mar 1 1993 00:06:33 +00:00  config.text
   4  -rwx          13336   Mar 1 1993 00:06:33 +00:00  multiple-fs
   5  -rwx         11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-
2.SE.bin
   6  -rwx           616    Mar 1 1993 00:07:13 +00:00  vlan.dat

32514048 bytes total (20886528 bytes free)
Switch#

```

Delete the VLAN file.

- a. If the **vlan.dat** file was found in flash, then delete this file.

```

Switch# delete vlan.dat
Delete filename [vlan.dat]?

```

You will be prompted to verify the file name. At this point, you can change the file name or just press Enter if you have entered the name correctly.

When you are prompted to delete this file, press Enter to confirm the deletion. (Pressing any other key will abort the deletion.)

```

Delete flash:/vlan.dat? [confirm]
Switch#

```

Erase the startup configuration file.

Use the **erase startup-config** command to erase the startup configuration file from NVRAM. When you are prompted to remove the configuration file, press Enter to confirm the erase. (Pressing any other key will abort the operation.)

```

Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
Switch#

```

Reload the switch.

Reload the switch to remove any old configuration information from memory. When you are prompted to reload the switch, press Enter to proceed with the reload. (Pressing any other key will abort the reload.)

```

Switch# reload
Proceed with reload? [confirm]

```

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Type **no** and press Enter.

```

System configuration has been modified. Save? [yes/no]: no

```

Bypass the initial configuration dialog.

After the switch reloads, you should see a prompt to enter the initial configuration dialog. Type **no** at the prompt and press Enter.

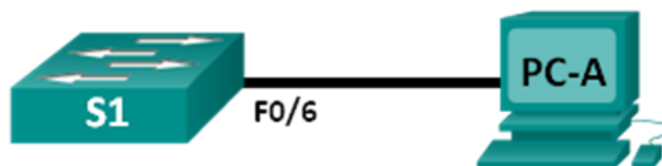
```

Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>

```

Lab 4 – Configuring a Switch Management Address

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.2	255.255.255.0
PC-A	NIC	192.168.1.10	255.255.255.0

Objectives

Part 1: Configure a Basic Network Device

Part 2: Verify and Test Network Connectivity

Background / Scenario

Cisco switches have a special interface, known as a switch virtual interface (SVI). The SVI can be configured with an IP address, commonly referred to as the management address. The management address is used for remote access to the switch to display or configure settings.

In this lab, you will build a simple network using Ethernet LAN cabling and access a Cisco switch using the console and remote access methods. You will configure basic switch settings, IP addressing, and demonstrate the use of a management IP address for remote switch management. The topology consists of one switch and one host using only Ethernet and console ports.

Note: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the available commands and output produced might vary from what is shown in the labs.

Note: Make sure that the switch has been erased and has no startup configuration. If you are unsure, contact your instructor.

Required Resources

1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)

1 PC (Windows 7 or 8 with terminal emulation program, such as Tera Term)

Console cables to configure the Cisco IOS devices via the console ports

Ethernet cables as shown in the topology

Part 1 – Configure a Basic Network Device

In Part 1, you will set up the network and configure basic settings, such as hostnames, interface IP addresses, and passwords.

Cable the network.

Cable the network as shown in the topology.

Establish a console connection to the switch from PC-A.

Configure basic switch settings.

In this step, you will configure basic switch settings, such as hostname, and configure an IP address for the SVI. Assigning an IP address on the switch is only the first step. As the network administrator, you must specify how the switch will be managed. Telnet and SSH are two of the most common management methods. However, Telnet is a very insecure protocol. All information flowing between the two devices is sent in plaintext. Passwords and other sensitive information can be easily viewed if captured by a packet sniffer.

Assuming the switch did not have a configuration file stored in NVRAM, you will be at the user EXEC mode prompt on the switch. The prompt will be `Switch>`. Enter privileged EXEC mode.

```
Switch> enable
Switch#
```

Use the privileged EXEC **show running-config** command to verify a clean configuration file. If a configuration file was previously saved, it will have to be removed. Depending on the switch model and IOS version, your configuration may look slightly different. However, there should not be any configured passwords or IP address set. If your switch does not have a default configuration, ask your instructor for help.

Enter global configuration mode and assign the switch hostname.

```
Switch# configure terminal
Switch(config)# hostname S1
S1(config)#
```

Configure the switch password access.

```
S1(config)# enable secret class
S1(config)#
```

Prevent unwanted DNS lookups.

```
S1(config)# no ip domain-lookup
S1(config)#
```

Configure a login MOTD banner.

```
S1(config)# banner motd #
Enter Text message. End with the character '#'.
Unauthorized access is strictly prohibited. #
```

Verify your access setting by moving between modes.

```
S1(config)# exit
S1#
S1# exit
Unauthorized access is strictly prohibited.
S1>
```

What shortcut keys are used to go directly from global configuration mode to privileged EXEC mode?

Return to privileged EXEC mode from user EXEC mode.

```
S1> enable
Password: class
S1#
```

Note: The password will not show up on the screen when entering.

Enter global configuration mode to set the SVI IP address to allow remote switch management.

```
S1# config t
S1#(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)#
```

Restrict console port access. The default configuration is to allow all console connections with no password needed.

```
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)#
```

Configure the VTY line for the switch to allow Telnet access. If you do not configure a VTY password, you will not be able to telnet to the switch.

```
S1(config)# line vty 0 4
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end
S1#
*Mar  1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console
```

Configure an IP address on PC-A.

Assign the IP address and subnet mask to the PC, as shown in the Addressing Table. The procedure for assigning an IP address on a PC running Windows 7 is described below:

- 1) Click the **Windows Start** icon > **Control Panel**.
- 2) Click **View By:** > **Category**.
- 3) Choose **View network status and tasks** > **Change adapter settings**.
- 4) Right-click **Local Area Network Connection** and select **Properties**.
- 5) Choose **Internet Protocol Version 4 (TCP/IPv4)**, click **Properties** > **OK**.
- 6) Click the **Use the following IP address** radio button and enter the IP address and subnet mask.

Verify and Test Network Connectivity

You will now verify and document the switch configuration, test end-to-end connectivity between PC-A and S1, and test the remote management capability of the switch.

Display the S1 device configuration.

Return to your console connection using Tera Term on PC-A. Issue the **show run** command to display and verify your switch configuration. A sample configuration is shown below. The settings you configured are highlighted in yellow. The other configuration settings are IOS defaults.

```

S1# show run
Building configuration...

Current configuration : 1508 bytes
!
! Last configuration change at 00:06:11 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
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2

<output omitted>

interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 192.168.1.2 255.255.255.0
!
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!

```

```

line con 0
password cisco
login
line vty 0 4
password cisco
login
line vty 5 15
login
!
end

```

Verify the status of your SVI management interface. Your VLAN 1 interface should be up/up and have an IP address assigned. Notice that switch port F0/6 is also up because PC-A is connected to it. Because all switch ports are initially in VLAN 1, by default, you can communicate with the switch using the IP address you configured for VLAN 1.

S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.2	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	down	down
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	down	down
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	down
FastEthernet0/20	unassigned	YES	unset	down	down
FastEthernet0/21	unassigned	YES	unset	down	down
FastEthernet0/22	unassigned	YES	unset	down	down
FastEthernet0/23	unassigned	YES	unset	down	down
FastEthernet0/24	unassigned	YES	unset	down	down
GigabitEthernet0/1	unassigned	YES	unset	down	down
GigabitEthernet0/2	unassigned	YES	unset	down	down

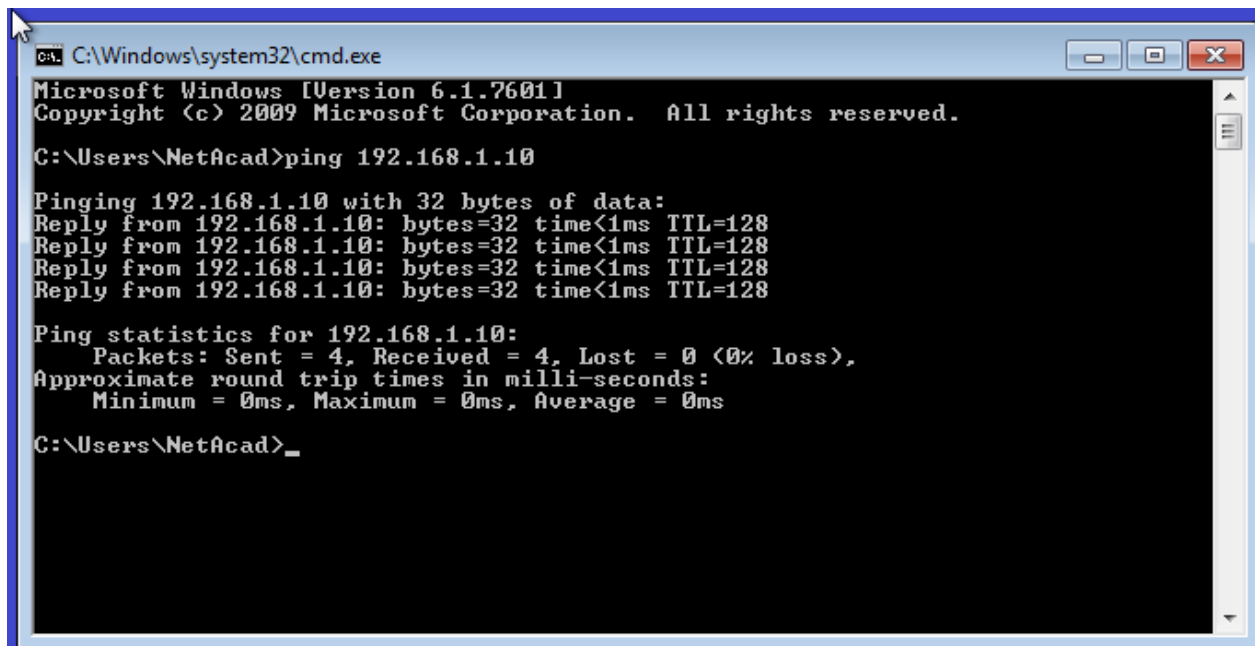
Test end-to-end connectivity.

Open a command prompt window (cmd.exe) on PC-A by clicking the **Windows Start** icon and entering **cmd** into the **Search for programs and files** field. Verify the IP address of PC-A by using the **ipconfig /all** command. This command displays the PC hostname and the IPv4 address information. Ping PC-A's address and the management address of S1.

Ping the PC-A address first.

```
C:\Users\NetAcad> ping 192.168.1.10
```

Your output should be similar to the following screen:



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128

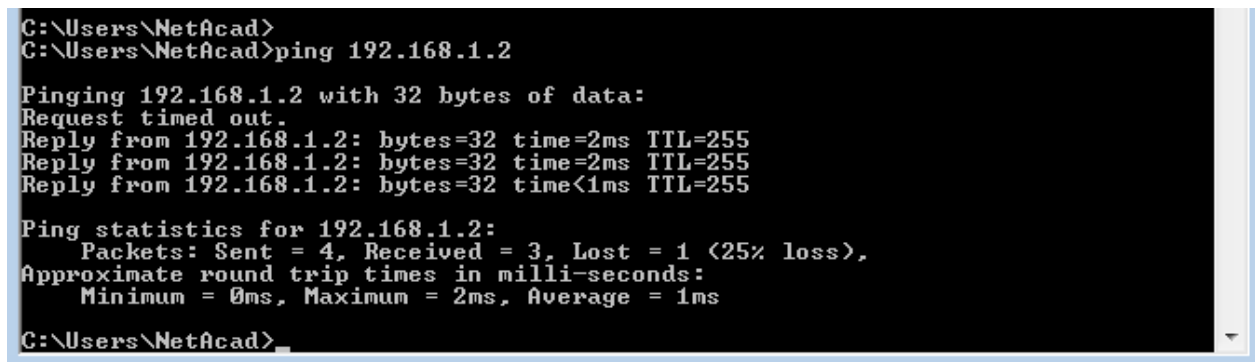
Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\NetAcad>
```

Ping the SVI management address of S1.

```
C:\Users\NetAcad> ping 192.168.1.2
```

Your output should be similar to the following screen. If ping results are not successful, troubleshoot the basic device configurations. You should check both the physical cabling and IP addressing if necessary.



```
C:\Users\NetAcad>
C:\Users\NetAcad>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.2: bytes=32 time=2ms TTL=255
Reply from 192.168.1.2: bytes=32 time=2ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\Users\NetAcad>
```

Test and verify the remote management of S1.

You will now use Telnet to remotely access the switch S1 using the SVI management address. In this lab, PC-A and S1 reside side by side. In a production network, the switch could be in a wiring closet on the top floor while your management PC is located on the ground floor. Telnet is not a secure protocol. However, you will use it in this lab to test remote access. All information sent by Telnet, including passwords and commands, is sent across the session in plaintext. In subsequent labs, you will use SSH to remotely access network devices.

Note: Windows 7 does not natively support Telnet. The administrator must enable this protocol. To install the Telnet client, open a command prompt window and type `pkgmgr /iu:"TelnetClient"`.

```
C:\Users\NetAcad> pkgmgr /iu:"TelnetClient"
```

With the command prompt window still open on PC-A, issue a Telnet command to connect to S1 via the SVI management address. The password is **cisco**.

```
C:\Users\NetAcad> telnet 192.168.1.2
```

Your output should be similar to the following screen:



After entering the **cisco** password, you will be at the user EXEC mode prompt. Type **enable** at the prompt. Enter the **class** password to enter privileged EXEC mode and issue a **show run** command.

Save the configuration file.

From your Telnet session, issue the **copy run start** command at the prompt.

```
S1# copy run start
Destination filename [startup-config]? [Enter]
Building configuration ..
S1#
```

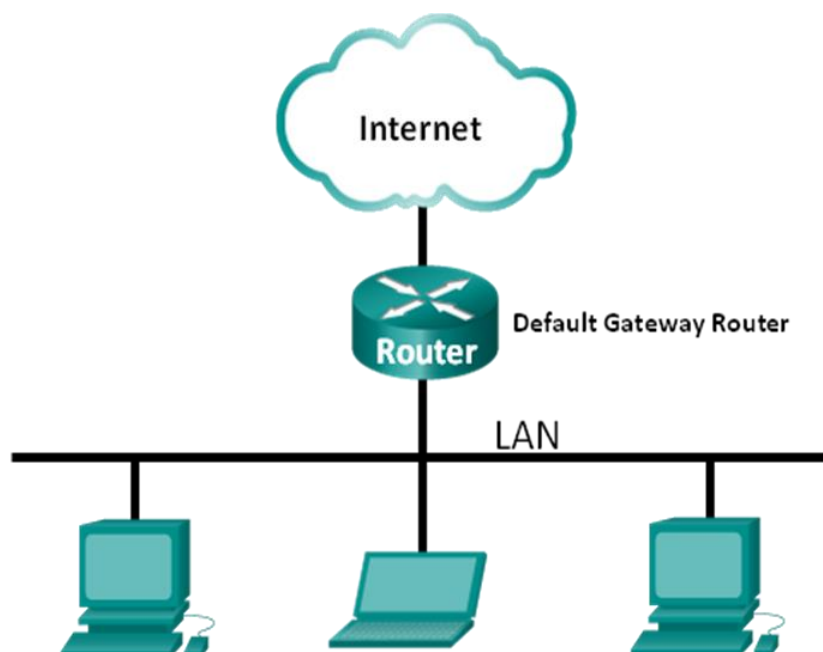
Exit the Telnet session by typing **quit**. You will be returned to the Windows 7 command prompt.

Reflection

Why must you use a console connection to initially configure the switch? Why not connect to the switch via Telnet or SSH?

Lab 5 – Using Wireshark to View Network Traffic

Topology



Objectives

Part 1: Capture and Analyze Local ICMP Data in Wireshark

Part 2: Capture and Analyze Remote ICMP Data in Wireshark

Background / Scenario

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. As data streams travel back and forth over the network, the sniffer "captures" each protocol data unit (PDU) and can decode and analyze its content according to the appropriate RFC or other specifications.

Wireshark is a useful tool for anyone working with networks and can be used with most labs in the CCNA courses for data analysis and troubleshooting. In this lab, you will use Wireshark to capture ICMP data packet IP addresses and Ethernet frame MAC addresses.

Required Resources

1 PC (Windows 7 or 8 with Internet access)

Additional PC(s) on a local-area network (LAN) will be used to reply to ping requests.

Part 1 – Capture and Analyze Local ICMP Data in Wireshark

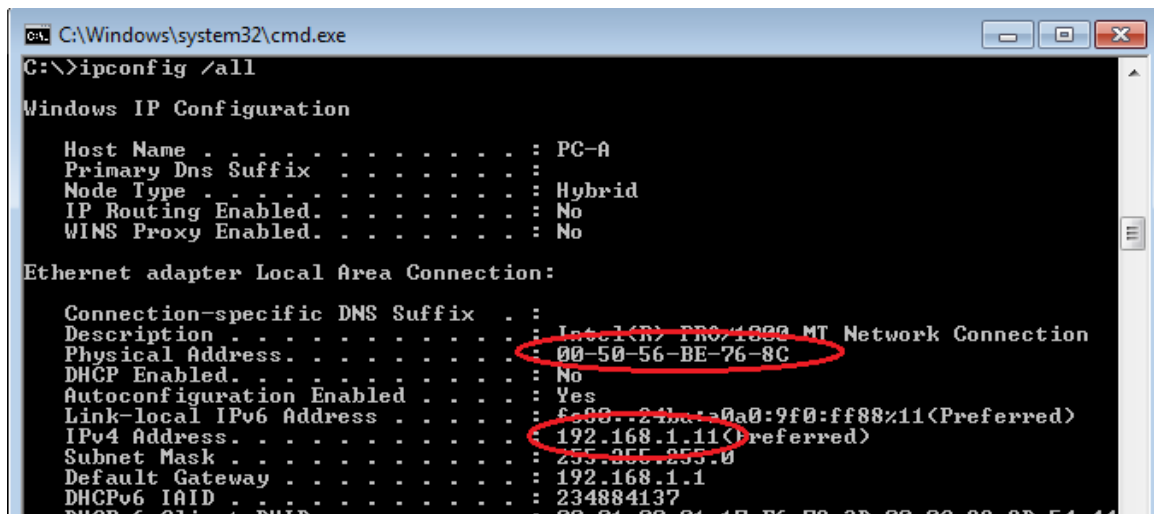
In Part 1 of this lab, you will ping another PC on the LAN and capture ICMP requests and replies in Wireshark. You will also look inside the frames captured for specific information. This analysis should help to clarify how packet headers are used to transport data to their destination.

Retrieve your PC's interface addresses.

For this lab, you will need to retrieve your PC's IP address and its network interface card (NIC) physical address, also called the MAC address.

b. Open a command window, type **ipconfig /all**, and then press Enter.

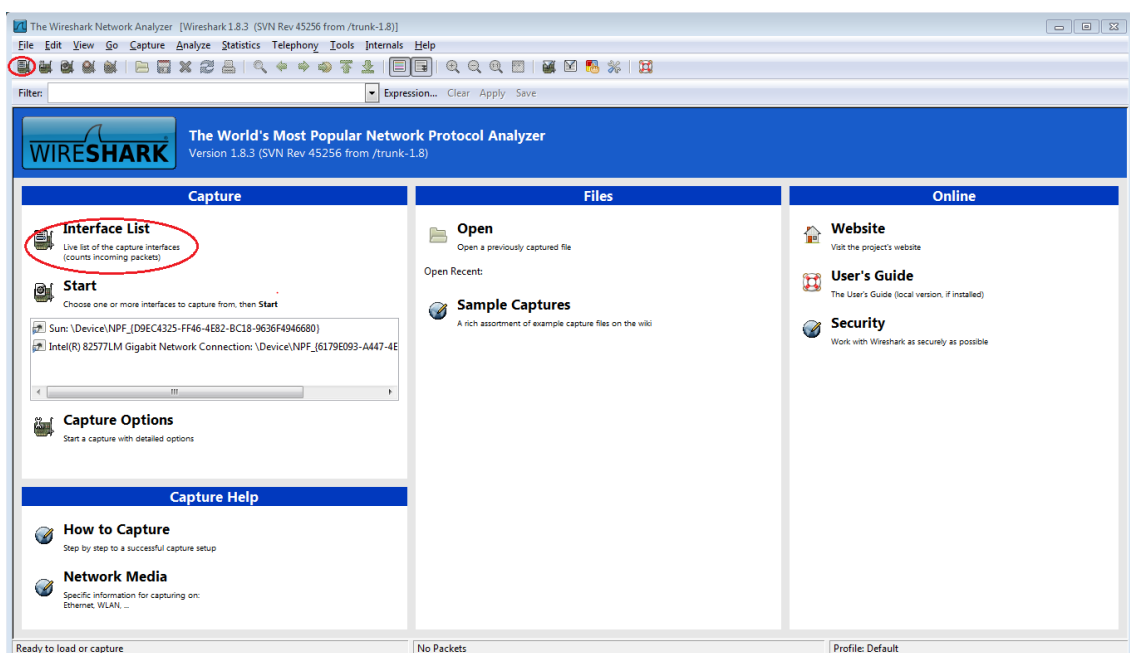
- c. Note your PC interface's IP address and MAC (physical) address.



- d. Ask a team member for their PC's IP address and provide your PC's IP address to them. Do not provide them with your MAC address at this time.

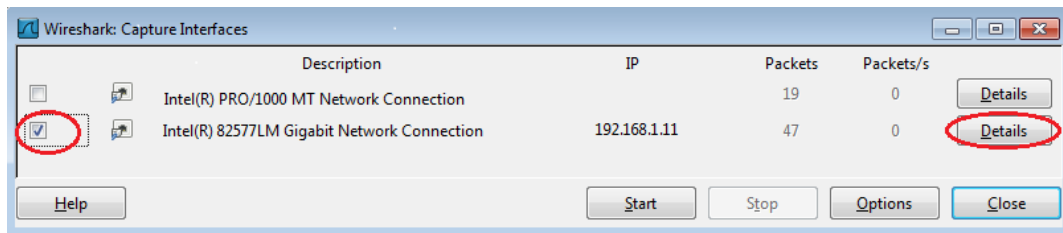
Start Wireshark and begin capturing data.

- On your PC, click the Windows **Start** button to see Wireshark listed as one of the programs on the pop-up menu. Double-click **Wireshark**.
- After Wireshark starts, click **Interface List**.

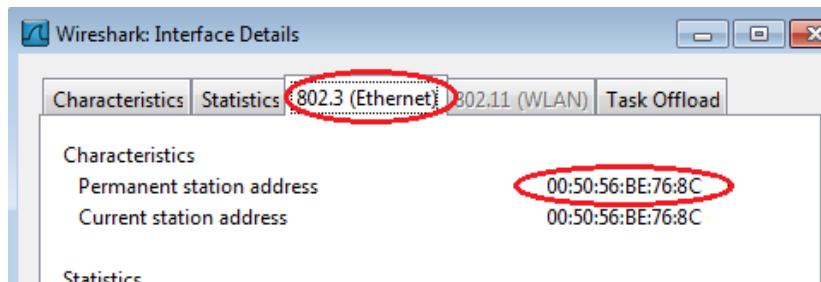


Note: Clicking the first interface icon in the row of icons also opens the Interface List.

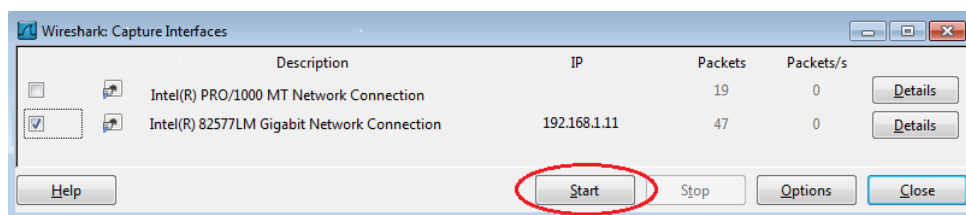
- g. On the Wireshark: Capture Interfaces window, click the check box next to the interface connected to your LAN.



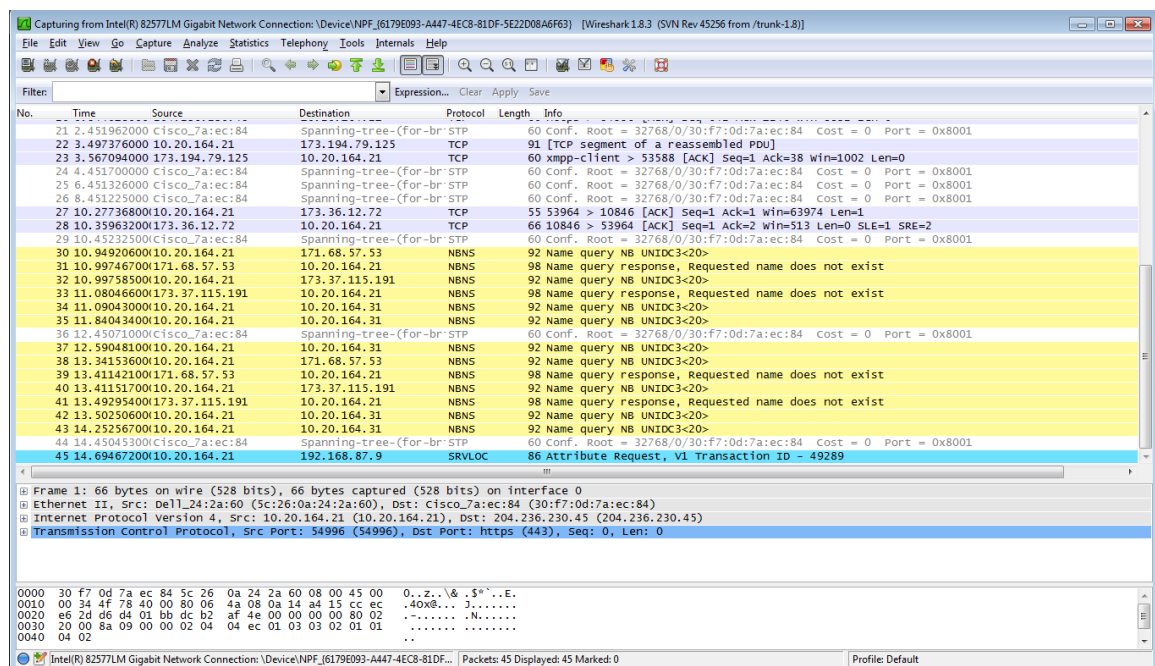
Note: If multiple interfaces are listed and you are unsure which interface to check, click the **Details** button, and then click the **802.3 (Ethernet)** tab. Verify that the MAC address matches what you noted in Step 1b. Close the Interface Details window after verifying the correct interface.



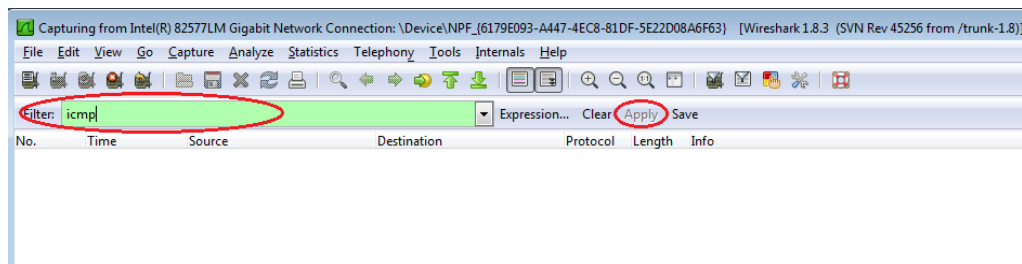
h. After you have checked the correct interface, click **Start** to start the data capture.



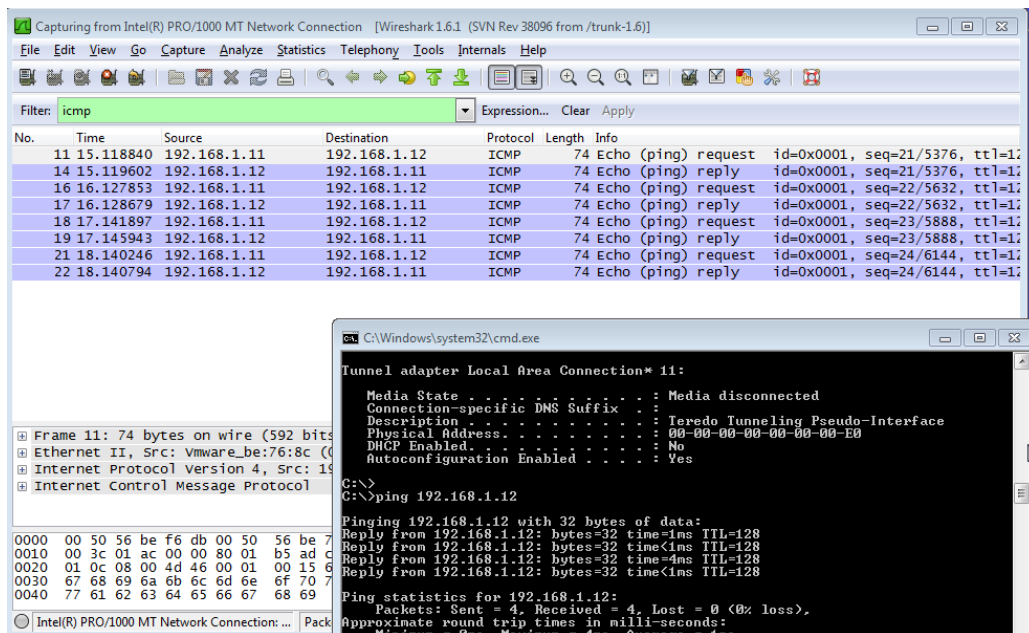
Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol.



- i. This information can scroll by very quickly depending on what communication is taking place between your PC and the LAN. We can apply a filter to make it easier to view and work with the data that is being captured by Wireshark. For this lab, we are only interested in displaying ICMP (ping) PDUs. Type **icmp** in the Filter box at the top of Wireshark and press Enter or click on the **Apply** button to view only ICMP (ping) PDUs.

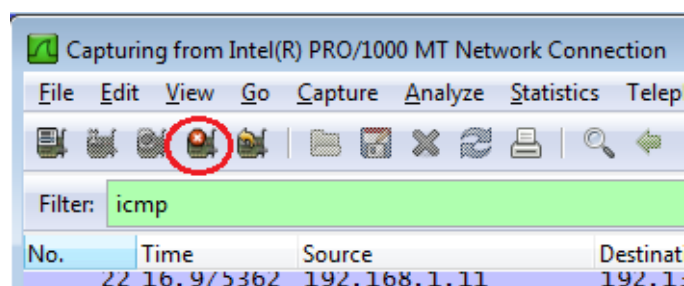


- j. This filter causes all data in the top window to disappear, but you are still capturing the traffic on the interface. Bring up the command prompt window that you opened earlier and ping the IP address that you received from your team member. Notice that you start seeing data appear in the top window of Wireshark again.



Note: If your team member's PC does not reply to your pings, this may be because their PC firewall is blocking these requests. Please see Appendix A: Allowing ICMP Traffic through a Firewall for information on how to allow ICMP traffic through the firewall using Windows 7.

- k. Stop capturing data by clicking the **Stop Capture** icon.



Examine the captured data.

In Step 3, examine the data that was generated by the ping requests of your team member's PC. Wireshark data is displayed in three sections: 1) The top section displays the list of PDU frames captured with a summary of the IP packet information listed, 2) the middle section lists PDU information for the frame selected in the top part of the screen and separates a captured PDU frame by its protocol layers, and 3) the bottom section displays the raw data of each layer. The raw data is displayed in both hexadecimal and decimal form.

Wireshark 1.6.1 (SVN Rev 38096 from /trunk-1.6) interface showing captured data from Intel(R) PRO/1000 MT Network Connection. The filter is set to **icmp**.

Top Section: List of captured frames.

No.	Time	Source	Destination	Protocol	Length	Info
11	15.118840	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=12
14	15.119602	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=12
16	16.127853	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=12
17	16.128679	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=12
18	17.141897	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=12
19	17.145943	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=12
21	18.140246	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=12
22	18.140794	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=12

Middle Section: Details of Frame 11.

- Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
- Ethernet II, Src: IntelCor_34:92:1c (58:94:6b:34:92:1c), Dst: Intel_Of:91:48 (00:11:11:0f:91:48)
- Internet Protocol Version 4, Src: 192.168.1.11 (192.168.1.11), Dst: 192.168.1.12 (192.168.1.12)
- Internet Control Message Protocol

Bottom Section: Raw data in hexadecimal and decimal form.

```

0000  00 50 56 be f6 db 00 50 56 be 76 8c 08 00 45 00  .PV...P V.v...E.
0010  00 3c 01 ac 00 00 80 01 b5 ad c0 a8 01 0b c0 a8  .<.....
0020  01 0c 08 00 4d 46 00 01 00 15 61 62 63 64 65 66  ....MF...abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcedefg hi
  
```

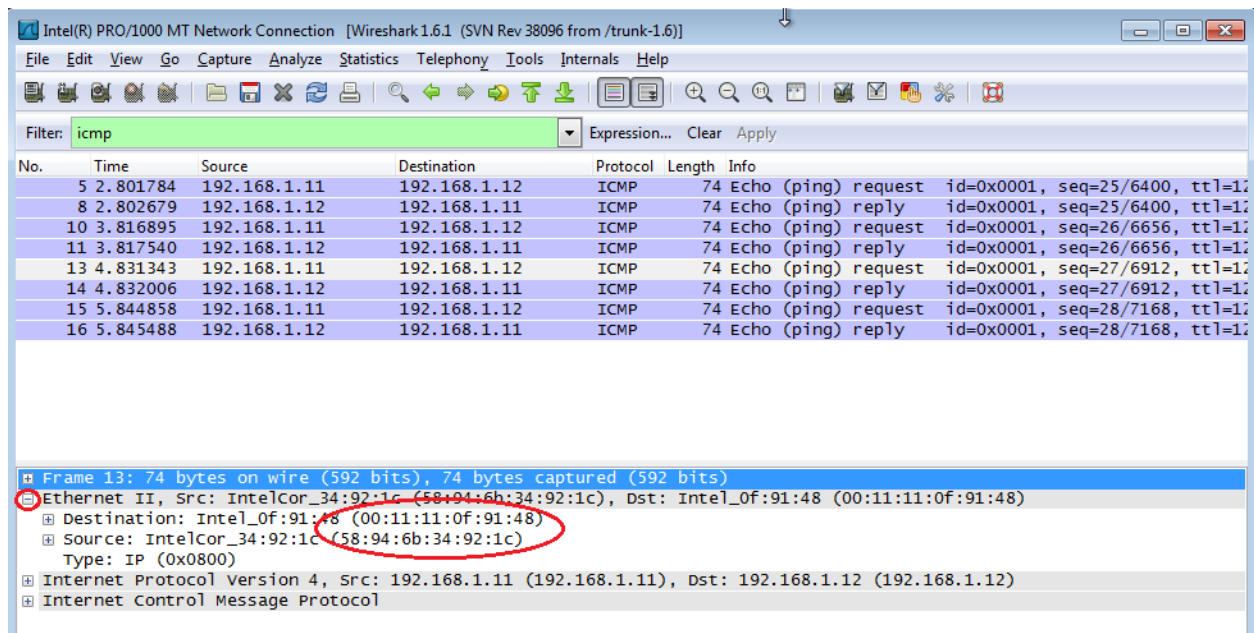
- Click the first ICMP request PDU frames in the top section of Wireshark. Notice that the Source column has your PC's IP address, and the Destination contains the IP address of the teammate's PC you pinged.

Wireshark 1.6.1 (SVN Rev 38096 from /trunk-1.6) interface showing captured data from Intel(R) PRO/1000 MT Network Connection. The filter is set to **icmp**.

Top Section: List of captured frames.

No.	Time	Source	Destination	Protocol	Length	Info
5	2.801784	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=12
8	2.802679	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=12
10	3.816895	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=12
11	3.817540	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=12
13	4.831343	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=12
14	4.832006	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=12
15	5.844858	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=12
16	5.845488	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168, ttl=12

- m. With this PDU frame still selected in the top section, navigate to the middle section. Click the plus sign to the left of the Ethernet II row to view the Destination and Source MAC addresses.



Does the Source MAC address match your PC's interface? _____

Does the Destination MAC address in Wireshark match your team member's MAC address?

How is the MAC address of the pinged PC obtained by your PC?

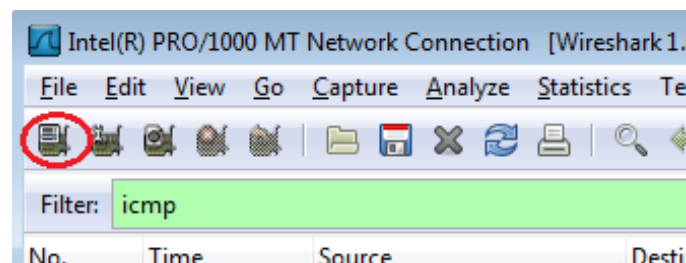
Note: In the preceding example of a captured ICMP request, ICMP data is encapsulated inside an IPv4 packet PDU (IPv4 header) which is then encapsulated in an Ethernet II frame PDU (Ethernet II header) for transmission on the LAN.

Part 2 – Capture and Analyze Remote ICMP Data in Wireshark

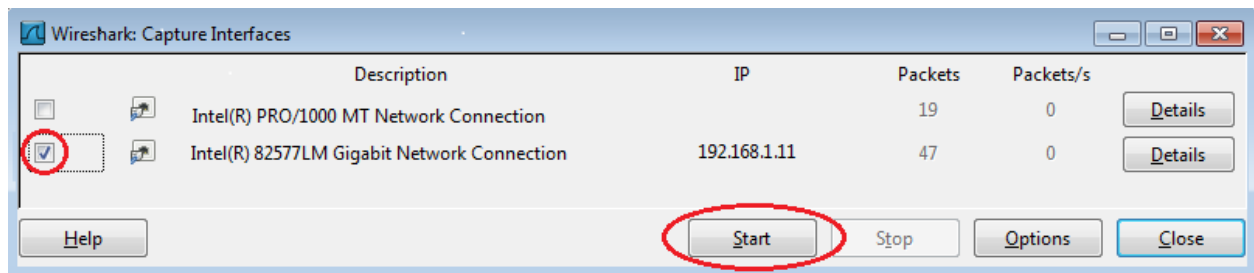
In Part 2, you will ping remote hosts (hosts not on the LAN) and examine the generated data from those pings. You will then determine what is different about this data from the data examined in Part 1.

Start capturing data on the interface.

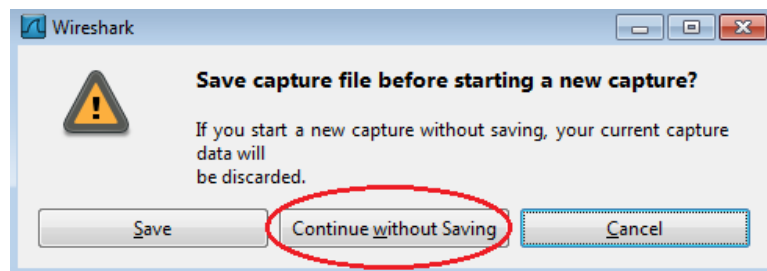
- n. Click the **Interface List** icon to bring up the list PC interfaces again.



- o. Make sure the check box next to the LAN interface is checked, and click **Start**.



- p. A window prompts to save the previously captured data before starting another capture. It is not necessary to save this data. Click **Continue without Saving**.



- q. With the capture active, ping the following three website URLs:
- 1) www.yahoo.com
 - 2) www.cisco.com
 - 3) www.google.com

```
C:\Windows\system32\cmd.exe

C:\>ping www.yahoo.com

Pinging www.yahoo.com [72.30.38.140] with 32 bytes of data:
Reply from 72.30.38.140: bytes=32 time=1ms TTL=255
Reply from 72.30.38.140: bytes=32 time<1ms TTL=255
Reply from 72.30.38.140: bytes=32 time<1ms TTL=255
Reply from 72.30.38.140: bytes=32 time<1ms TTL=255

Ping statistics for 72.30.38.140:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping www.cisco.com

Pinging www.cisco.com [198.133.219.25] with 32 bytes of data:
Reply from 198.133.219.25: bytes=32 time<1ms TTL=255
Reply from 198.133.219.25: bytes=32 time<1ms TTL=255
Reply from 198.133.219.25: bytes=32 time<1ms TTL=255
Reply from 198.133.219.25: bytes=32 time<1ms TTL=255

Ping statistics for 198.133.219.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping www.google.com

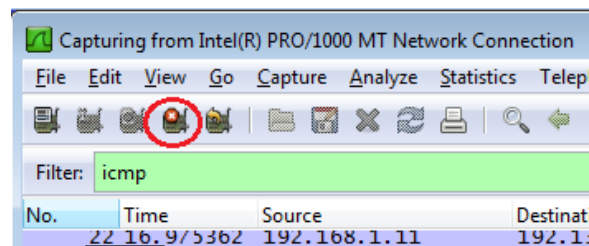
Pinging www.google.com [74.125.129.99] with 32 bytes of data:
Reply from 74.125.129.99: bytes=32 time=1ms TTL=255
Reply from 74.125.129.99: bytes=32 time<1ms TTL=255
Reply from 74.125.129.99: bytes=32 time<1ms TTL=255
Reply from 74.125.129.99: bytes=32 time<1ms TTL=255

Ping statistics for 74.125.129.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>_
```

Note: When you ping the URLs listed, notice that the Domain Name Server (DNS) translates the URL to an IP address. Note the IP address received for each URL.

- r. You can stop capturing data by clicking the **Stop Capture** icon.



Examining and analyzing the data from the remote hosts.

- s. Review the captured data in Wireshark, examine the IP and MAC addresses of the three locations that you pinged. List the destination IP and MAC addresses for all three locations in the space provided.

1st Location: IP: _____._____._____._____ MAC: ____:____:____:____:____:_____

2nd Location: IP: _____._____._____._____ MAC: ____:____:____:____:____:_____

3rd Location: IP: _____._____._____._____ MAC: ____:____:____:____:____:_____

- t. What is significant about this information?

- u. How does this information differ from the local ping information you received in Part 1?

Reflection

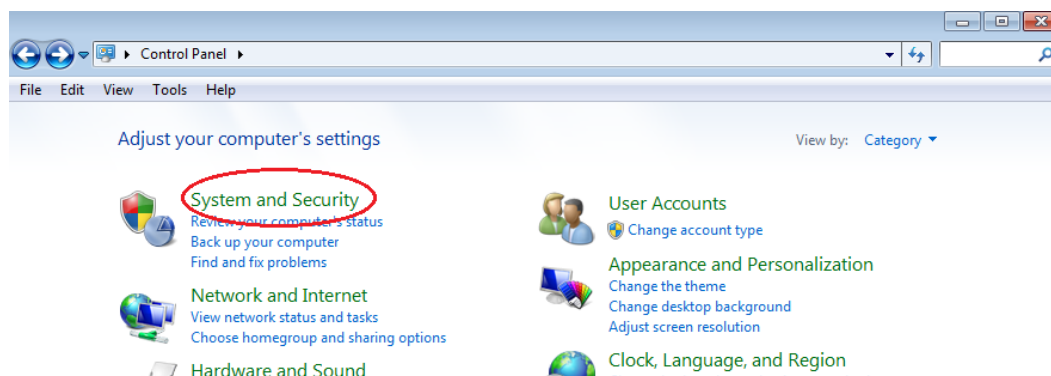
Why does Wireshark show the actual MAC address of the local hosts, but not the actual MAC address for the remote hosts?

Appendix A: Allowing ICMP Traffic through a Firewall

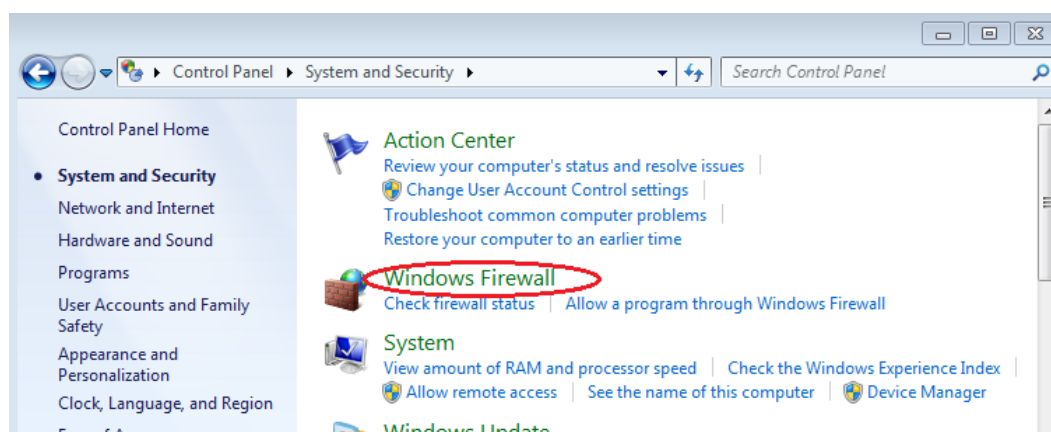
If the members of your team are unable to ping your PC, the firewall may be blocking those requests. This appendix describes how to create a rule in the firewall to allow ping requests. It also describes how to disable the new ICMP rule after you have completed the lab.

Create a new inbound rule allowing ICMP traffic through the firewall.

- v. From the Control Panel, click the **System and Security** option.



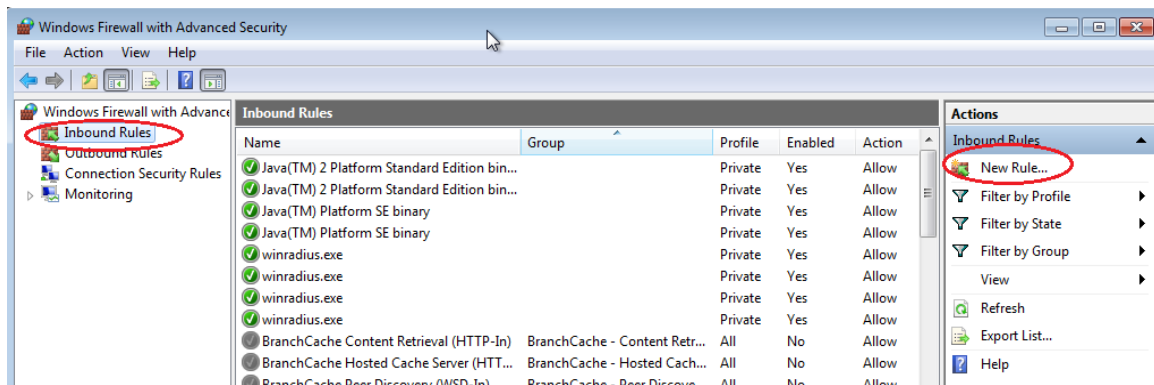
- w. From the System and Security window, click **Windows Firewall**.



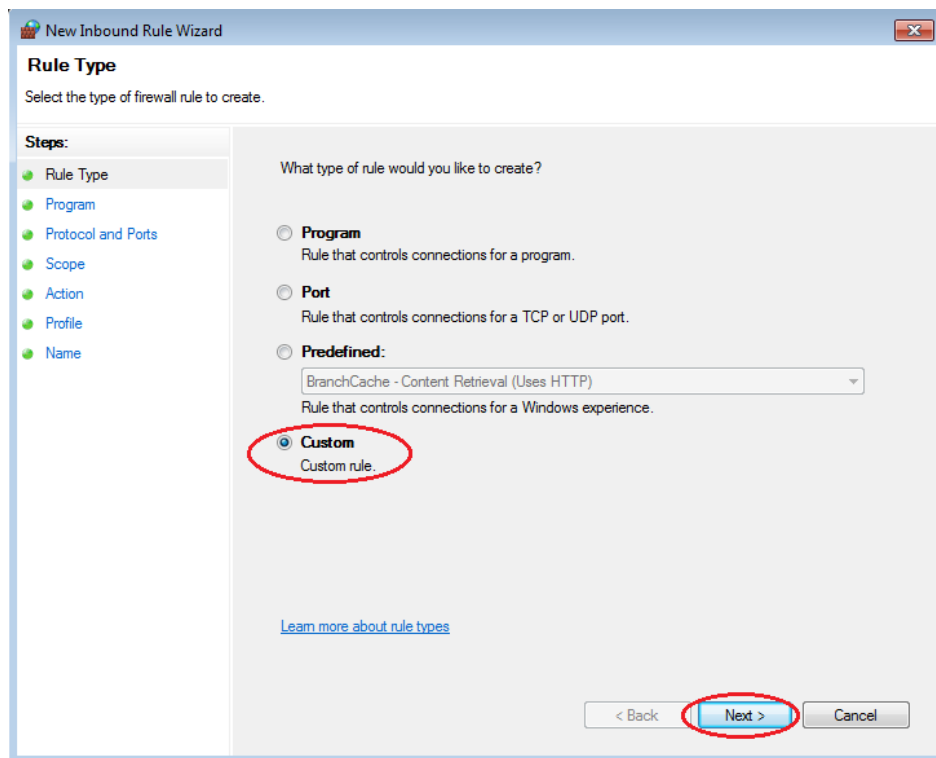
- x. In the left pane of the Windows Firewall window, click **Advanced settings**.



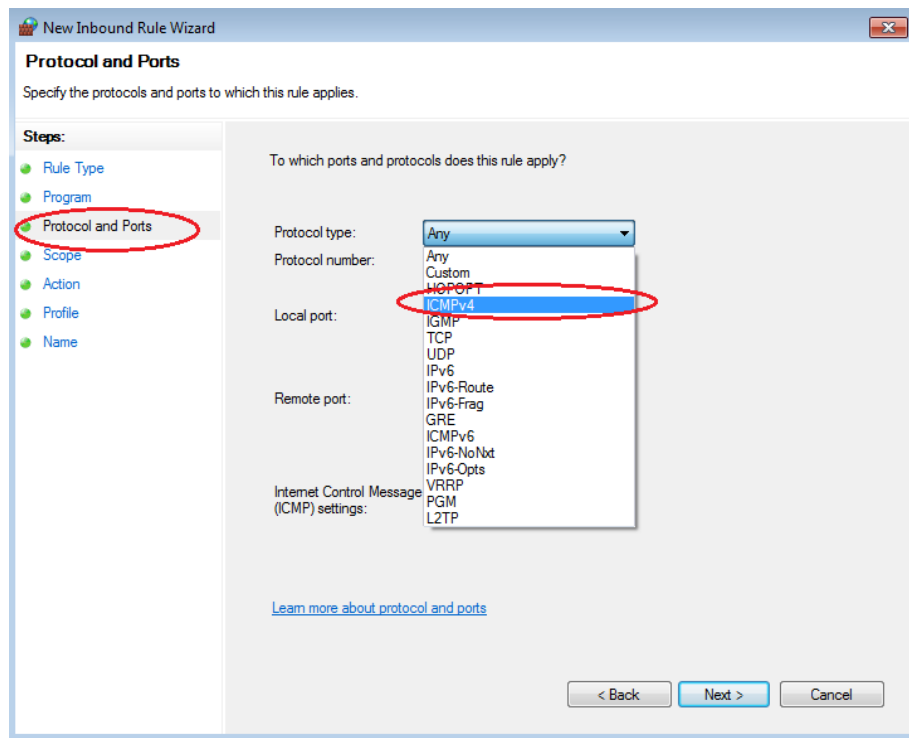
- y. On the Advanced Security window, choose the **Inbound Rules** option on the left sidebar and then click **New Rule...** on the right sidebar.



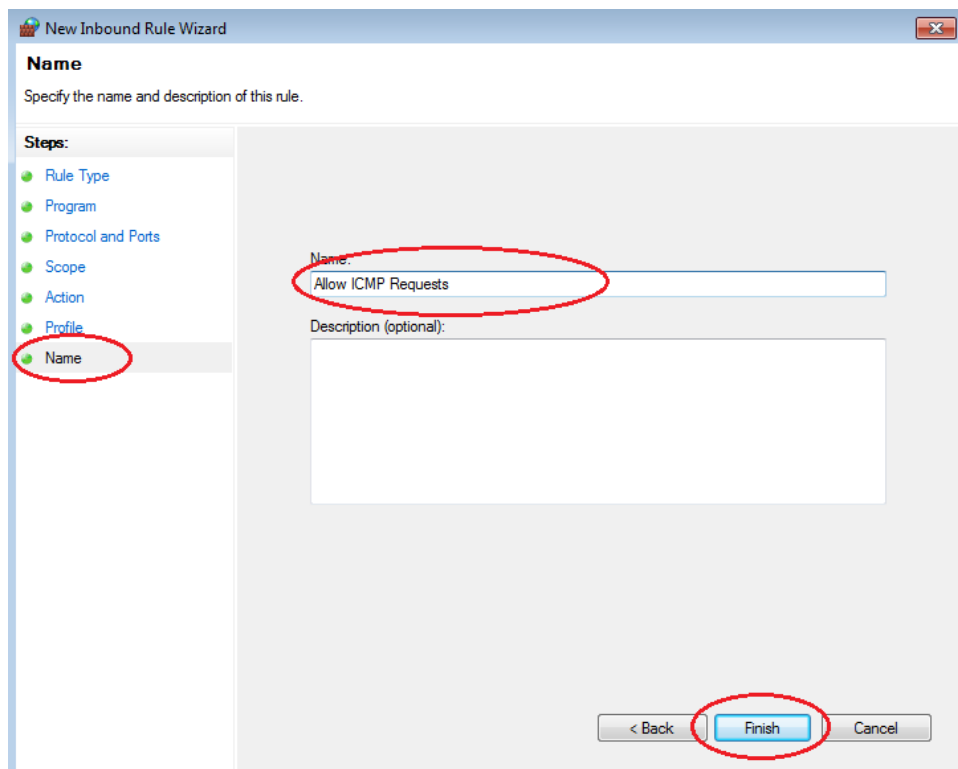
- z. This launches the New Inbound Rule wizard. On the Rule Type screen, click the **Custom** radio button and click **Next**



- aa. In the left pane, click the **Protocol and Ports** option and using the Protocol type drop-down menu, select **ICMPv4**, and then click **Next**.



- bb. In the left pane, click the **Name** option and in the Name field, type **Allow ICMP Requests**. Click **Finish**.

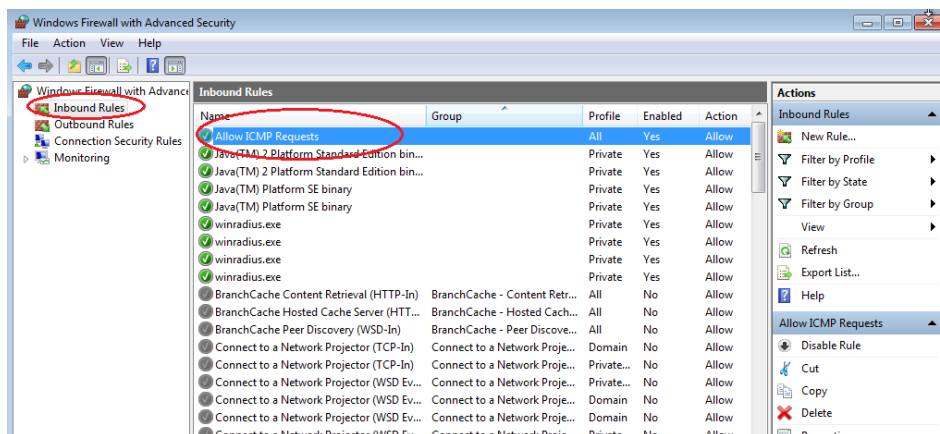


This new rule should allow your team members to receive ping replies from your PC.

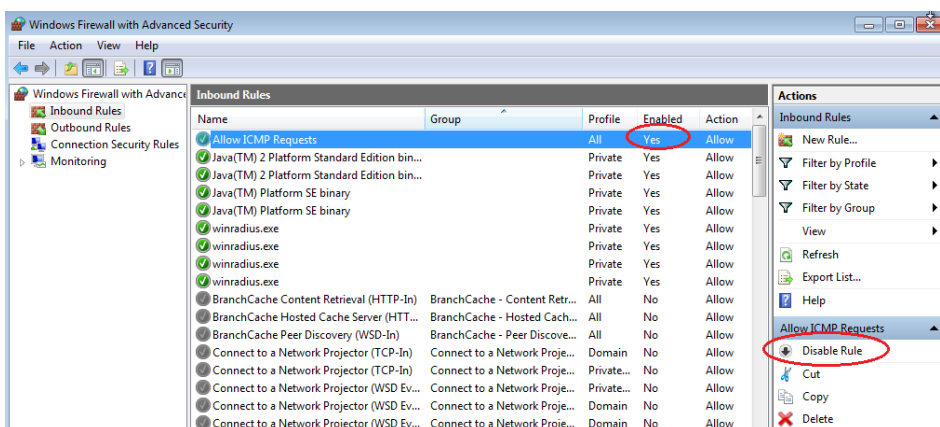
Disabling or deleting the new ICMP rule.

After the lab is complete, you may want to disable or even delete the new rule you created in Step 1. Using the **Disable Rule** option allows you to enable the rule again at a later date. Deleting the rule permanently deletes it from the list of Inbound Rules.

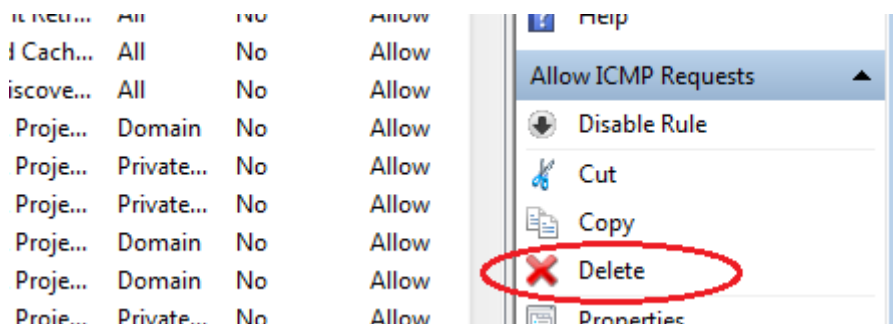
- cc. On the Advanced Security window, click **Inbound Rules** in the left pane and then locate the rule you created in Step 1.



- dd. To disable the rule, click the **Disable Rule** option. When you choose this option, you will see this option change to **Enable Rule**. You can toggle back and forth between Disable Rule and Enable Rule; the status of the rule also shows in the Enabled column of the Inbound Rules list.

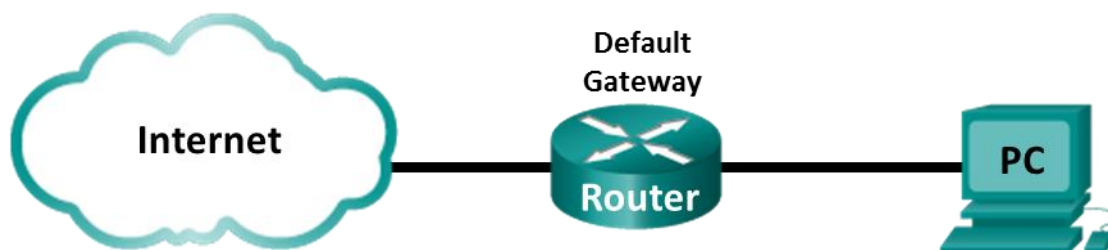


- ee. To permanently delete the ICMP rule, click **Delete**. If you choose this option, you must re-create the rule again to allow ICMP replies.



Lab 6 – Using Wireshark to Examine Ethernet Frames

Topology



Objectives

Part 1: Examine the Header Fields in an Ethernet II Frame

Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

Background / Scenario

When upper layer protocols communicate with each other, data flows down the Open Systems Interconnection (OSI) layers and is encapsulated into a Layer 2 frame. The frame composition is dependent on the media access type. For example, if the upper layer protocols are TCP and IP and the media access is Ethernet, then the Layer 2 frame encapsulation will be Ethernet II. This is typical for a LAN environment.

When learning about Layer 2 concepts, it is helpful to analyze frame header information. In the first part of this lab, you will review the fields contained in an Ethernet II frame. In Part 2, you will use Wireshark to capture and analyze Ethernet II frame header fields for local and remote traffic.

Required Resources

1 PC (Windows 7 or 8 with Internet access with Wireshark installed)

Part 1 – Examine the Header Fields in an Ethernet II Frame

In Part 1, you will examine the header fields and content in an Ethernet II Frame. A Wireshark capture will be used to examine the contents in those fields.

Review the Ethernet II header field descriptions and lengths.

Preamble	Destination Address	Source Address	Frame Type	Data	FCS
8 Bytes	6 Bytes	6 Bytes	2 Bytes	46 – 1500 Bytes	4 Bytes

Examine the network configuration of the PC.

This PC host IP address is 192.168.1.17 and the default gateway has an IP address of 192.168.1.1.

```
Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . : 
Description . . . . . : Broadcom 802.11a/b/g WLAN
Physical Address. . . . . : 00-1A-73-EA-63-8C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::a858:5f3e:35e2:d38f%13(Preferred)
IPv4 Address. . . . . : 192.168.1.17(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, June 16, 2015 6:59:54 AM
Lease Expires . . . . . : Wednesday, June 17, 2015 6:59:54 AM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 234887795
DHCPv6 Client DUID. . . . . : 00-01-00-01-1B-07-0A-E1-00-1E-EC-15-74-C2

DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

Examine Ethernet frames in a Wireshark capture.

The Wireshark capture below shows the packets generated by a ping being issued from a PC host to its default gateway. A filter has been applied to Wireshark to view the ARP and ICMP protocols only. The session begins with an ARP query for the MAC address of the gateway router, followed by four ping requests and replies.

The image shows a Wireshark network capture with a filter of 'arp or icmp'. The packet list shows several packets: an ARP request (No. 9), an ARP reply (No. 10), and four ICMP echo (ping) requests and replies (Nos. 11, 12, 14, 15). The packet details pane is expanded for Frame 9, showing the Ethernet II header (Source: GemtekTe_ea:63:8c, Destination: Broadcast) and the ARP (Type: ARP) protocol details. The packet bytes pane shows the raw data of the ARP request.

No.	Time	Source	Destination	Protocol	Length	Info
9	2.497611000	GemtekTe_ea:63:8c	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.17
10	2.502719000	Netgear_ea:b1:7a	GemtekTe_ea:63:8c	ARP	42	192.168.1.1 is at 80:37:73:ea:b1:7a
11	2.502767000	192.168.1.17	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=19/4864,
12	2.503610000	192.168.1.1	192.168.1.17	ICMP	74	Echo (ping) reply id=0x0001, seq=19/4864,
14	3.499098000	192.168.1.17	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=20/5120,
15	3.501917000	192.168.1.1	192.168.1.17	ICMP	74	Echo (ping) reply id=0x0001, seq=20/5120,

Frame 9: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

Ethernet II, Src: GemtekTe_ea:63:8c (00:1a:73:ea:63:8c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- Source: GemtekTe_ea:63:8c (00:1a:73:ea:63:8c)
- Type: ARP (0x0806)

Address Resolution Protocol (request)

Offset	Hex	ASCII
0000	ff ff ff ff ff ff 00 1a 73 ea 63 8c 08 06 00 01	s.c.....
0010	08 00 06 04 00 01 00 1a 73 ea 63 8c c0 a8 01 11	s.c.....
0020	00 00 00 00 00 00 c0 a8 01 01	

Examine the Ethernet II header contents of an ARP request.

The following table takes the first frame in the Wireshark capture and displays the data in the Ethernet II header fields.

Field	Value	Description						
Preamble	Not shown in capture	This field contains synchronizing bits, processed by the NIC hardware.						
Destination Address	Broadcast (ff:ff:ff:ff:ff:ff)	Layer 2 addresses for the frame. Each address is 48 bits long, or 6 octets, expressed as 12 hexadecimal digits, 0–9, A–F. A common format is 12:34:56:78:9A:BC. The first six hex numbers indicate the manufacturer of the network interface card (NIC), the last six hex numbers are the serial number of the NIC. The destination address may be a broadcast, which contains all ones, or a unicast. The source address is always unicast.						
Source Address	GemtekTe_ea:63:8c (00:1a:73:ea:63:8c)							
Frame Type	0x0806	For Ethernet II frames, this field contains a hexadecimal value that is used to indicate the type of upper-layer protocol in the data field. There are numerous upper-layer protocols supported by Ethernet II. Two common frame types are: <table><tr><th>Value</th><th>Description</th></tr><tr><td>0x0800</td><td>IPv4 Protocol</td></tr><tr><td>0x0806</td><td>Address resolution protocol (ARP)</td></tr></table>	Value	Description	0x0800	IPv4 Protocol	0x0806	Address resolution protocol (ARP)
Value	Description							
0x0800	IPv4 Protocol							
0x0806	Address resolution protocol (ARP)							
Data	ARP	Contains the encapsulated upper-level protocol. The data field is between 46 – 1,500 bytes.						
FCS	Not shown in capture	Frame Check Sequence, used by the NIC to identify errors during transmission. The value is computed by the sending machine, encompassing frame addresses, type, and data field. It is verified by the receiver.						

What is significant about the contents of the destination address field?

Why does the PC send out a broadcast ARP prior to sending the first ping request?

What is the MAC address of the source in the first frame? _____

What is the Vendor ID (OUI) of the Source's NIC? _____

What portion of the MAC address is the OUI?

What is the Source's NIC serial number? _____

Use Wireshark to Capture and Analyze Ethernet Frames

In Part 2, you will use Wireshark to capture local and remote Ethernet frames. You will then examine the information that is contained in the frame header fields.

Determine the IP address of the default gateway on your PC.

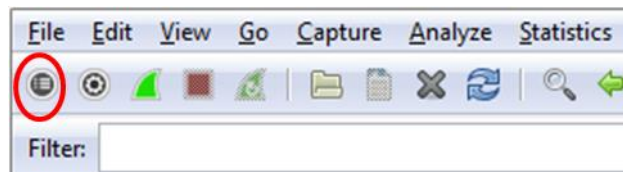
Open a command prompt window and issue the **ipconfig** command.

What is the IP Address of the PC Default Gateway? _____

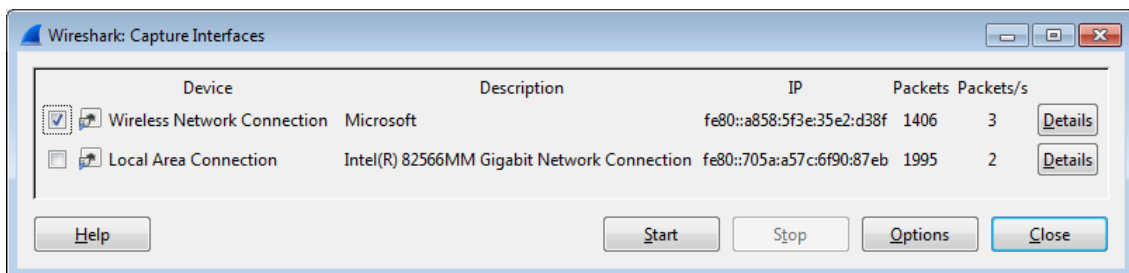
Start capturing traffic on your PC's NIC.

ff. Open Wireshark.

gg. On the Wireshark Network Analyzer toolbar, click the **Interface List** icon.



hh. On the Wireshark: Capture Interfaces window, select the interface to start traffic capturing by clicking the appropriate check box, and then click **Start**. If you are uncertain of what interface to check, click **Details** for more information about each interface listed.



ii. Observe the traffic that appears in the Packet List window.

The image shows the 'Wireshark: Packet List' window. It displays a list of captured packets with columns: No., Time, Source, Destination, Protocol, Length, and Info. The list shows various protocols including DNS, ARP, ICMPv6, and IGMPv3. The 'Filter' field is empty, and the 'Expression...' field is also empty.

No.	Time	Source	Destination	Protocol	Length	Info
17	3.691404000	192.168.1.17	192.168.1.1	DNS	85	Standard query 0x0c33 A teredo.ipv6.microso
18	3.702954000	192.168.1.1	192.168.1.17	DNS	150	Standard query response 0x0c33 CNAME teredo
19	3.752602000	GemtekTe_ea:63:8Broadcast		ARP	42	who has 192.168.1.1? Tell 192.168.1.17
20	3.754732000	Netgear_ea:b1:7:GemtekTe_ea:63		ARP	42	192.168.1.1 is at 80:37:73:ea:b1:7a
21	3.768583000	fe80::a858:5f3e:ff02::16		ICMPv6	90	Multicast Listener Report Message v2
22	3.768843000	192.168.1.17	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
23	3.795917000	GemtekTe_ea:63:8Broadcast		ARP	42	who has 192.168.1.1? Tell 192.168.1.17
24	3.800804000	Netgear_ea:b1:7:GemtekTe_ea:63		ARP	42	192.168.1.1 is at 80:37:73:ea:b1:7a

Filter Wireshark to display only ICMP traffic.

You can use the filter in Wireshark to block visibility of unwanted traffic. The filter does not block the capture of unwanted data; it only filters what to display on the screen. For now, only ICMP traffic is to be displayed.

In the Wireshark **Filter** box, type **icmp**. The box should turn green if you typed the filter correctly. If the box is green, click **Apply** to apply the filter.

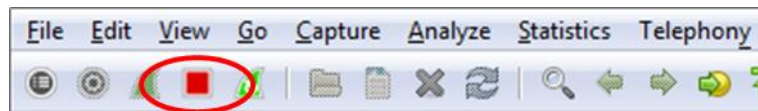


From the command prompt window, ping the default gateway of your PC.

From the command window, ping the default gateway using the IP address that you recorded in Step 1.

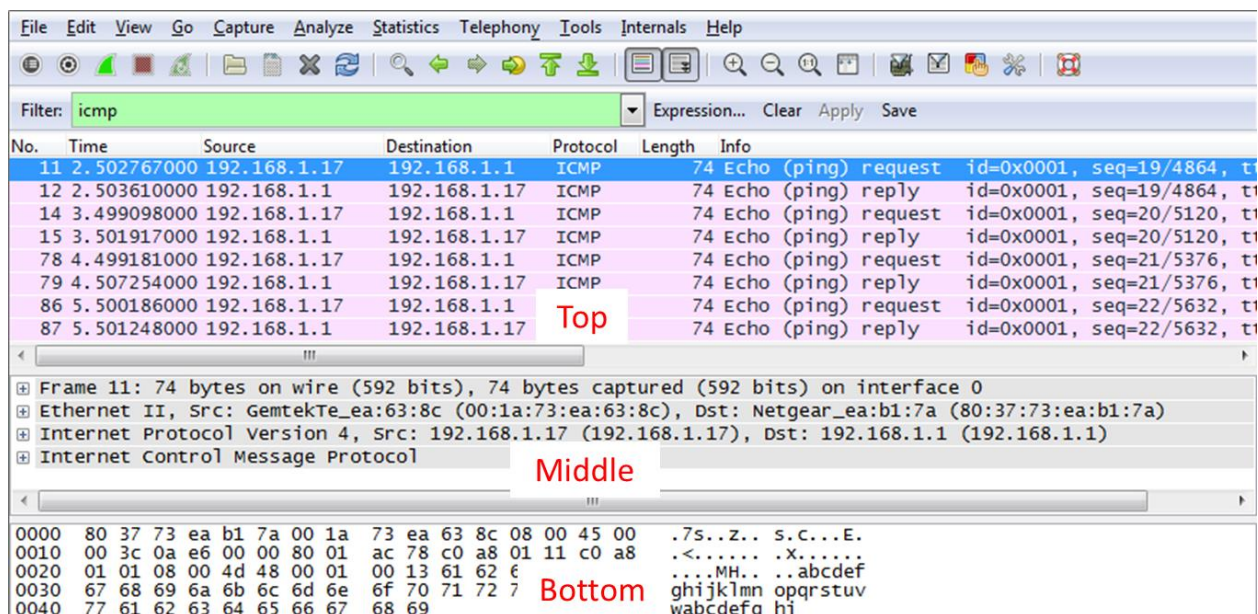
Stop capturing traffic on the NIC.

Click the **Stop Capture** icon to stop capturing traffic.



Examine the first Echo (ping) request in Wireshark.

The Wireshark main window is divided into three sections: the Packet List pane (top), the Packet Details pane (middle), and the Packet Bytes pane (bottom). If you selected the correct interface for packet capturing in Step 3, Wireshark should display the ICMP information in the Packet List pane of Wireshark, similar to the following example.



jj. In the Packet List pane (top section), click the first frame listed. You should see **Echo (ping) request** under the **Info** heading. This should highlight the line blue.

kk. Examine the first line in the Packet Details pane (middle section). This line displays the length of the frame; 74 bytes in this example.

- ll. The second line in the Packet Details pane shows that it is an Ethernet II frame. The source and destination MAC addresses are also displayed.

What is the MAC address of the PC's NIC? _____

What is the default gateway's MAC address? _____

- mm. You can click the plus (+) sign at the beginning of the second line to obtain more information about the Ethernet II frame. Notice that the plus sign changes to a minus (-) sign.

What type of frame is displayed? _____

- nn. The last two lines displayed in the middle section provide information about the data field of the frame. Notice that the data contains the source and destination IPv4 address information.

What is the source IP address? _____

What is the destination IP address? _____

- oo. You can click any line in the middle section to highlight that part of the frame (hex and ASCII) in the Packet Bytes pane (bottom section). Click the **Internet Control Message Protocol** line in the middle section and examine what is highlighted in the Packet Bytes pane.

+ Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0	
- Ethernet II, Src: GemtekTe_ea:63:8c (00:1a:73:ea:63:8c), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)	
+ Destination: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)	
+ Source: GemtekTe_ea:63:8c (00:1a:73:ea:63:8c)	
Type: IP (0x0800)	
+ Internet Protocol Version 4, Src: 192.168.1.17 (192.168.1.17), Dst: 192.168.1.1 (192.168.1.1)	
- Internet Control Message Protocol	
Type: 8 (Echo (ping) request)	
Code: 0	
Checksum: 0x4d48 [correct]	
!!!	
0000	80 37 73 ea b1 7a 00 1a 73 ea 63 8c 08 00 45 00 .7s..Z..s.c...E.
0010	00 3c 0a e6 00 00 80 01 ac 78 c0 a8 01 11 c0 a8 .<.....X.....
0020	01 01 08 00 4d 48 00 01 00 13 61 62 63 64 65 66 ..MH...abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69 wabcdefg hi

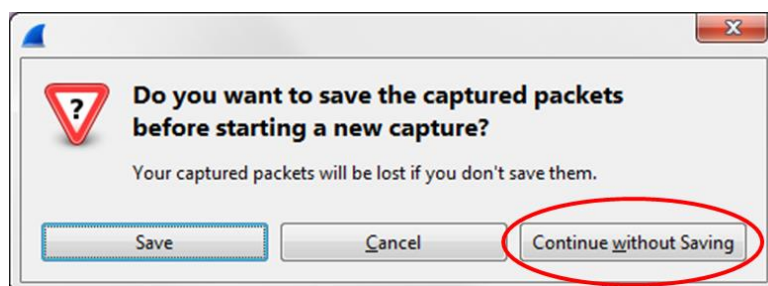
What do the last two highlighted octets spell? _____

- pp. Click the next frame in the top section and examine an Echo reply frame. Notice that the source and destination MAC addresses have reversed, because this frame was sent from the default gateway router as a reply to the first ping.

What device and MAC address is displayed as the destination address?

Restart packet capture in Wireshark.

Click the **Start Capture** icon to start a new Wireshark capture. You will receive a popup window asking if you would like to save the previous captured packets to a file before starting a new capture. Click **Continue without Saving**.



In the command prompt window, ping www.cisco.com.

Stop capturing packets.

Examine the new data in the packet list pane of Wireshark.

In the first echo (ping) request frame, what are the source and destination MAC addresses?

Source: _____

Destination: _____

What are the source and destination IP addresses contained in the data field of the frame?

Source: _____

Destination: _____

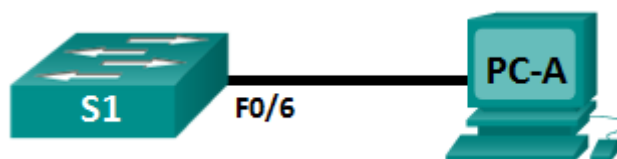
Compare these addresses to the addresses you received in Step 6. The only address that changed is the destination IP address. Why has the destination IP address changed, while the destination MAC address remained the same?

Reflection

Wireshark does not display the preamble field of a frame header. What does the preamble contain?

Lab 7 – Viewing Network Device MAC Addresses

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Devices and Verify Connectivity

Part 2: Display, Describe, and Analyze Ethernet MAC Addresses

Background / Scenario

Every device on an Ethernet LAN is identified by a Layer 2 MAC address. This address is assigned by the manufacturer and stored in the firmware of the NIC. This lab will explore and analyze the components that make up a MAC address, and how you can find this information on a switch and a PC.

You will cable the equipment as shown in the topology. You will configure the switch and PC to match the addressing table. You will verify your configurations by testing for network connectivity.

After the devices have been configured and network connectivity has been verified, you will use various commands to retrieve information from the devices to answer questions about your network equipment.

Note: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs.

Note: Make sure that the switches have been erased and have no startup configurations. If you are unsure, ask your instructor.

Required Resources

1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)

1 PC (Windows 7 or 8 with a terminal emulation program, such as Tera Term)

Console cable to configure the Cisco switch via the console ports

Ethernet cables as shown in the topology

Part 1 – Configure Devices and Verify Connectivity

In this part, you will set up the network topology and configure basic settings, such as the interface IP addresses and device name. For device name and address information, refer to the Topology and Addressing Table.

Cable the network as shown in the topology.

Attach the devices shown in the topology and cable as necessary.

- b. Power on all the devices in the topology.

Configure the IPv4 address for the PC.

- c. Configure the IPv4 address, subnet mask, and default gateway address for PC-A.
- d. From the command prompt on PC-A, ping the switch address.

Were the pings successful? Explain.

Configure basic settings for the switch.

In this step, you will configure the device name and the IP address, and disable DNS lookup on the switch.

- e. Console into the switch and enter global configuration mode.

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

- f. Assign a hostname to the switch based on the Addressing Table.

```
Switch(config)# hostname S1
```

- g. Disable DNS lookup.

```
S1(config)# no ip domain-lookup
```

- h. Configure and enable the SVI interface for VLAN 1.

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.1 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
*Mar  1 00:07:59.048: %SYS-5-CONFIG_I: Configured from console by console
```

Verify network connectivity.

Ping the switch from PC-A. Were the pings successful?

Display, Describe, and Analyze Ethernet MAC Addresses

Every device on an Ethernet LAN has a MAC address that is assigned by the manufacturer and stored in the firmware of the NIC. Ethernet MAC addresses are 48-bits long. They are displayed using six sets of hexadecimal digits that are usually separated by dashes, colons, or periods. The following example shows the same MAC address using the three different notation methods:

00-05-9A-3C-78-00 00:05:9A:3C:78:00 0005.9A3C.7800

Note: MAC addresses are also called physical addresses, hardware addresses, or Ethernet hardware addresses.

You will issue commands to display the MAC addresses on a PC and a switch, and you will analyze the properties of each one.

Analyze the MAC address for the PC-A NIC.

Before you analyze the MAC address on PC-A, look at an example from a different PC NIC. You can issue the **ipconfig /all** command to view the MAC address of your NIC. An example screen output is shown below. When using the **ipconfig /all** command, notice that MAC addresses are referred to as

physical addresses. Reading the MAC address from left to right, the first six hex digits refer to the vendor (manufacturer) of this device. These first six hex digits (3 bytes) are also known as the organizationally unique identifier (OUI). This 3-byte code is assigned to the vendor by the IEEE organization. To find the manufacturer, you can use a tool like www.macvendorlookup.com or go to the IEEE web site to find the registered OUI vendor codes. The IEEE web site address for OUI information is <http://standards.ieee.org/develop/regauth/oui/public.html>. The last six digits are the NIC serial number assigned by the manufacturer.

- a. Using the output from the **ipconfig /all** command, answer the following questions.

```
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) 82577LM Gigabit Network Connection
Physical Address. . . . . : 5C-26-0A-24-2A-60
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b875:731b:3c7b:c0b1%10(Preferred)
IPv4 Address. . . . . : 192.168.1.3(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 246920024
```

What is the OUI portion of the MAC address for this device?

What is the serial number portion of the MAC address for this device?

Using the example above, find the name of the vendor that manufactured this NIC.

- b. From the command prompt on PC-A, issue the **ipconfig /all** command and identify the OUI portion of the MAC address for the NIC of PC-A.

Identify the serial number portion of the MAC address for the NIC of PC-A.

Identify the name of the vendor that manufactured the NIC of PC-A.

Analyze the MAC address for the S1 F0/6 interface.

You can use a variety of commands to display MAC addresses on the switch.

- c. Console into S1 and use the **show interfaces vlan 1** command to find the MAC address information. A sample is shown below. Use output generated by your switch to answer the questions.

```
S1# show interfaces vlan 1
Vlan1 is up, line protocol is up
  Hardware is EtherSVI, address is 001b.0c6d.8f40 (bia 001b.0c6d.8f40)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:14:51, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
```

```

5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts (0 IP multicasts)
  0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  34 packets output, 11119 bytes, 0 underruns
  0 output errors, 2 interface resets
  0 unknown protocol drops
  0 output buffer failures, 0 output buffers swapped out

```

What is the MAC address for VLAN 1 on S1?

What is the MAC serial number for VLAN 1?

What is the OUI for VLAN 1?

Based on this OUI, what is the name of the vendor?

What does bia stand for?

Why does the output show the same MAC address twice?

- d. Another way to display the MAC address on the switch is to use the **show arp** command. Use the **show arp** command to display MAC address information. This command maps the Layer 2 address to its corresponding Layer 3 address. A sample is shown below. Use output generated by your switch to answer the questions.

```

S1# show arp
Protocol  Address          Age (min)  Hardware Addr  Type   Interface
Internet  192.168.1.1      -         001b.0c6d.8f40  ARPA   Vlan1
Internet  192.168.1.3      0         5c26.0a24.2a60  ARPA   Vlan1

```

What Layer 2 addresses are displayed on S1?

What Layer 3 addresses are displayed on S1?

View the MAC addresses on the switch.

Issue the **show mac address-table** command on S1. A sample is shown below. Use output generated by your switch to answer the questions.

```

S1# show mac address-table
Mac Address Table

```

```
-----
```

Vlan	Mac Address	Type	Ports
----	-----	-----	-----
All	0100.0ccc.cccc	STATIC	CPU
All	0100.0ccc.cccd	STATIC	CPU
All	0180.c200.0000	STATIC	CPU
All	0180.c200.0001	STATIC	CPU
All	0180.c200.0002	STATIC	CPU
All	0180.c200.0003	STATIC	CPU
All	0180.c200.0004	STATIC	CPU
All	0180.c200.0005	STATIC	CPU
All	0180.c200.0006	STATIC	CPU
All	0180.c200.0007	STATIC	CPU
All	0180.c200.0008	STATIC	CPU
All	0180.c200.0009	STATIC	CPU
All	0180.c200.000a	STATIC	CPU
All	0180.c200.000b	STATIC	CPU
All	0180.c200.000c	STATIC	CPU
All	0180.c200.000d	STATIC	CPU
All	0180.c200.000e	STATIC	CPU
All	0180.c200.000f	STATIC	CPU
All	0180.c200.0010	STATIC	CPU
All	ffff.ffff.ffff	STATIC	CPU
1	5c26.0a24.2a60	DYNAMIC	Fa0/6

Total Mac Addresses for this criterion: 21

Did the switch display the MAC address of PC-A? If you answered yes, what port was it on?

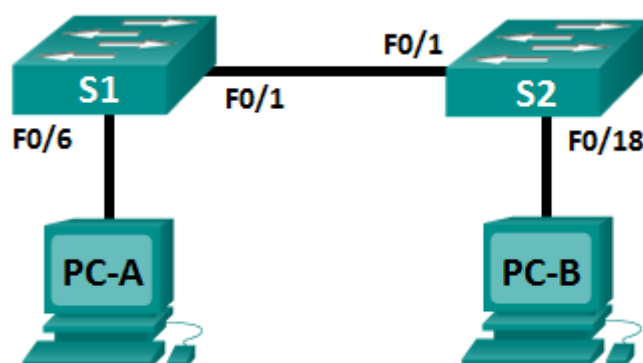
Reflection

Can you have broadcasts at the Layer 2 level? If so, what would the MAC address be?

Why would you need to know the MAC address of a device?

Lab 8 – Viewing the Switch MAC Address Table

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	N/A
PC-B	NIC	192.168.1.2	255.255.255.0	N/A

Objectives

Part 1: Build and Configure the Network

Part 2: Examine the Switch MAC Address Table

Background / Scenario

The purpose of a Layer 2 LAN switch is to deliver Ethernet frames to host devices on the local network. The switch records host MAC addresses that are visible on the network, and maps those MAC addresses to its own Ethernet switch ports. This process is called building the MAC address table. When a switch receives a frame from a PC, it examines the frame's source and destination MAC addresses. The source MAC address is recorded and mapped to the switch port from which it arrived. Then the destination MAC address is looked up in the MAC address table. If the destination MAC address is a known address, then the frame is forwarded out of the corresponding switch port associated with that MAC address. If the MAC address is unknown, then the frame is broadcasted out of all switch ports, except the one from which it came. It is important to observe and understand the function of a switch and how it delivers data on the network. The way a switch operates has implications for network administrators whose job it is to ensure secure and consistent network communication.

Switches are used to interconnect and deliver information to computers on local area networks. Switches deliver Ethernet frames to host devices identified by network interface card MAC addresses.

In Part 1, you will build a multi-switch topology with a trunk linking the two switches. In Part 2, you will ping various devices and observe how the two switches build their MAC address tables.

Note: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Note: Make sure that the switches have been erased and have no startup configurations. If you are unsure contact your instructor.

Required Resources

- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: The Fast Ethernet interfaces on Cisco 2960 switches are autosensing and an Ethernet straight-through cable may be used between switches S1 and S2. If using another model Cisco switch, it may be necessary to use an Ethernet crossover cable.

Part 1 – Build and Configure the Network

Cable the network according to the topology.

Configure PC hosts.

Initialize and reload switches as necessary.

Configure basic settings for each switch.

- e. Configure device name as shown in the topology.
- f. Configure IP address as listed in Addressing Table.
- g. Assign **cisco** as the console and vty passwords.
- h. Assign **class** as the privileged EXEC password.

Part 2 – Examine the Switch MAC Address Table

A switch learns MAC addresses and builds the MAC address table, as network devices initiate communication on the network.

Record network device MAC addresses.

- i. Open a command prompt on PC-A and PC-B and type **ipconfig /all**. What are the Ethernet adapter physical addresses?

PC-A MAC Address:

PC-B MAC Address:

- j. Console into switch S1 and S2 and type the **show interface F0/1** command on each switch. On the second line of command output, what is the hardware addresses (or burned-in address [bia])?

S1 Fast Ethernet 0/1 MAC Address:

S2 Fast Ethernet 0/1 MAC Address:

Display the switch MAC address table.

Console into switch S2 and view the MAC address table, both before and after running network communication tests with ping.

- k. Establish a console connection to S2 and enter privileged EXEC mode.
- l. In privileged EXEC mode, type the **show mac address-table** command and press Enter.

S2# **show mac address-table**

Even though there has been no network communication initiated across the network (i.e., no use of ping), it is possible that the switch has learned MAC addresses from its connection to the PC and the other switch.

Are there any MAC addresses recorded in the MAC address table?

What MAC addresses are recorded in the table? To which switch ports are they mapped and to which devices do they belong? Ignore MAC addresses that are mapped to the CPU.

If you had not previously recorded MAC addresses of network devices in Step 1, how could you tell which devices the MAC addresses belong to, using only the output from the **show mac address-table** command? Does it work in all scenarios?

Clear the S2 MAC address table and display the MAC address table again.

- m. In privileged EXEC mode, type the **clear mac address-table dynamic** command and press **Enter**.

S2# **clear mac address-table dynamic**

- n. Quickly type the **show mac address-table** command again. Does the MAC address table have any addresses in it for VLAN 1? Are there other MAC addresses listed?

Wait 10 seconds, type the **show mac address-table** command, and press Enter. Are there new addresses in the MAC address table? _____

From PC-B, ping the devices on the network and observe the switch MAC address table.

- o. From PC-B, open a command prompt and type **arp -a**. Not including multicast or broadcast addresses, how many device IP-to-MAC address pairs have been learned by ARP?

- p. From the PC-B command prompt, ping PC-A, S1, and S2. Did all devices have successful replies? If not, check your cabling and IP configurations.

- q. From a console connection to S2, enter the **show mac address-table** command. Has the switch added additional MAC addresses to the MAC address table? If so, which addresses and devices?

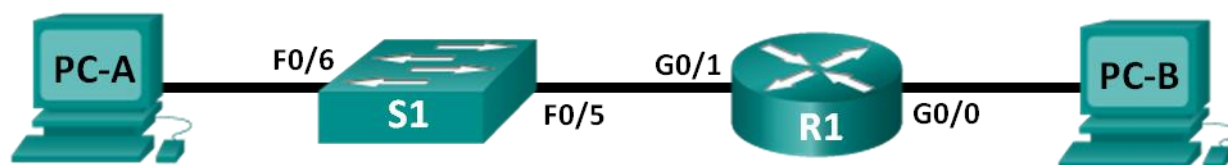
From PC-B, open a command prompt and retype **arp -a**. Does the PC-B ARP cache have additional entries for all network devices that were sent pings?

Reflection

On Ethernet networks, data is delivered to devices by their MAC addresses. For this to happen, switches and PCs dynamically build ARP caches and MAC address tables. With only a few computers on the network this process seems fairly easy. What might be some of the challenges on larger networks?

Lab 9 – Building a Switch and Router Network

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Devices and Verify Connectivity

Part 3: Display Device Information

Background / Scenario

This is a comprehensive lab to review previously covered IOS commands. In this lab, you will cable the equipment as shown in the topology diagram. You will then configure the devices to match the addressing table. After the configurations have been saved, you will verify your configurations by testing for network connectivity.

After the devices have been configured and network connectivity has been verified, you will use IOS commands to retrieve information from the devices to answer questions about your network equipment.

This lab provides minimal assistance with the actual commands necessary to configure the router. Test your knowledge by trying to configure the devices without referring to the content or previous activities.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the **Error! Reference source not found.** at the end of this lab for the correct interface identifiers.

Note: Ensure that the routers and switches have been erased and have no startup configurations. Consult with your instructor for the procedure to initialize and reload a router and switch.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: The Gigabit Ethernet interfaces on Cisco 1941 routers are autosensing and an Ethernet straight-through cable may be used between the router and PC-B. If using another model Cisco router, it may be necessary to use an Ethernet crossover cable.

Part 1 – Set Up Topology and Initialize Devices

Cable the network as shown in the topology.

- a. Attach the devices shown in the topology diagram, and cable, as necessary.
- b. Power on all the devices in the topology.

Initialize and reload the router and switch.

If configuration files were previously saved on the router and switch, initialize and reload these devices back to their basic configurations.

Part 2 – Configure Devices and Verify Connectivity

In Part 2, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords. Refer to the Topology and Addressing Table at the beginning of this lab for device names and address information.

Assign static IP information to the PC interfaces.

- a. Configure the IP address, subnet mask, and default gateway settings on PC-A.
- b. Configure the IP address, subnet mask, and default gateway settings on PC-B.
- c. Ping PC-B from a command prompt window on PC-A.

Why were the pings not successful?

Configure the router.

- a. Console into the router and enable privileged EXEC mode.
- b. Enter configuration mode.
- c. Assign a device name to the router.
- d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- e. Assign **class** as the privileged EXEC encrypted password.
- f. Assign **cisco** as the console password and enable login.
- g. Assign **cisco** as the VTY password and enable login.
- h. Encrypt the clear text passwords.
- i. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
- j. Configure and activate both interfaces on the router.
- k. Configure an interface description for each interface indicating which device is connected to it.
- l. Save the running configuration to the startup configuration file.
- m. Set the clock on the router.

Note: Use the question mark (?) to help with the correct sequence of parameters needed to execute this command.

- n. Ping PC-B from a command prompt window on PC-A.

Were the pings successful? Why?

Display Device Information

In Part 3, you will use **show** commands to retrieve information from the router and switch.

Retrieve hardware and software information from the network devices.

Use the show version command to answer the following questions about the router.

What is the name of the IOS image that the router is running?

How much DRAM memory does the router have?

How much NVRAM memory does the router have?

How much Flash memory does the router have?

Use the show version command to answer the following questions about the switch.

What is the name of the IOS image that the switch is running?

How much dynamic random access memory (DRAM) does the switch have?

How much nonvolatile random-access memory (NVRAM) does the switch have?

What is the model number of the switch?

Display the routing table on the router.

Use the show ip route command on the router to answer the following questions.

What code is used in the routing table to indicate a directly connected network? _____

How many route entries are coded with a C code in the routing table? _____

What interface types are associated to the C coded routes?

Display interface information on the router.

Use the **show interface g0/1** to answer the following questions.

What is the operational status of the G0/1 interface?

What is the Media Access Control (MAC) address of the G0/1 interface?

How is the Internet address displayed in this command?

Display a summary list of the interfaces on the router and switch.

There are several commands that can be used to verify an interface configuration. One of the most useful of these is the **show ip interface brief** command. The command output displays a summary list of the interfaces on the device and provides immediate feedback to the status of each interface.

Enter the **show ip interface brief** command on the router.

```
R1# show ip interface brief
Interface                IP-Address      OK? Method Status
Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0       192.168.0.1     YES manual  up
GigabitEthernet0/1       192.168.1.1     YES manual  up
Serial0/0/0              unassigned      YES unset  administratively down down
Serial0/0/1              unassigned      YES unset  administratively down down
R1#
```

Enter the **show ip interface brief** command on the switch.

```
Switch# show ip interface brief
Interface                IP-Address      OK? Method Status
Protocol
Vlan1                   unassigned      YES manual  up
FastEthernet0/1         unassigned      YES unset  down
FastEthernet0/2         unassigned      YES unset  down
FastEthernet0/3         unassigned      YES unset  down
FastEthernet0/4         unassigned      YES unset  down
FastEthernet0/5         unassigned      YES unset  up
FastEthernet0/6         unassigned      YES unset  up
FastEthernet0/7         unassigned      YES unset  down
FastEthernet0/8         unassigned      YES unset  down
FastEthernet0/9         unassigned      YES unset  down
FastEthernet0/10        unassigned      YES unset  down
FastEthernet0/11        unassigned      YES unset  down
FastEthernet0/12        unassigned      YES unset  down
FastEthernet0/13        unassigned      YES unset  down
FastEthernet0/14        unassigned      YES unset  down
FastEthernet0/15        unassigned      YES unset  down
FastEthernet0/16        unassigned      YES unset  down
FastEthernet0/17        unassigned      YES unset  down
FastEthernet0/18        unassigned      YES unset  down
FastEthernet0/19        unassigned      YES unset  down
FastEthernet0/20        unassigned      YES unset  down
FastEthernet0/21        unassigned      YES unset  down
FastEthernet0/22        unassigned      YES unset  down
FastEthernet0/23        unassigned      YES unset  down
FastEthernet0/24        unassigned      YES unset  down
GigabitEthernet0/1      unassigned      YES unset  down
GigabitEthernet0/2      unassigned      YES unset  down
```

Reflection

1. If the G0/1 interface showed administratively down, what interface configuration command would you use to turn the interface up?

2. What would happen if you had incorrectly configured interface G0/1 on the router with an IP address of 192.168.1.2?

Lab 10 – Converting IPv4 Addresses to Binary

Objectives

Part 1: Convert IPv4 Addresses from Dotted Decimal to Binary

Part 2: Use Bitwise ANDing Operation to Determine Network Addresses

Part 3: Apply Network Address Calculations

Background / Scenario

Every IPv4 address is comprised of two parts: a network portion and a host portion. The network portion of an address is the same for all devices that reside in the same network. The host portion identifies a specific host within a given network. The subnet mask is used to determine the network portion of an IP address. Devices on the same network can communicate directly; devices on different networks require an intermediary Layer 3 device, such as a router, to communicate.

To understand the operation of devices on a network, we need to look at addresses the way devices do—in binary notation. To do this, we must convert the dotted decimal form of an IP address and its subnet mask to binary notation. After this has been done, we can use the bitwise ANDing operation to determine the network address.

This lab provides instructions on how to determine the network and host portion of IP addresses by converting addresses and subnet masks from dotted decimal to binary, and then using the bitwise ANDing operation. You will then apply this information to identify addresses in the network.

Convert IPv4 Addresses from Dotted Decimal to Binary

In Part 1, you will convert decimal numbers to their binary equivalent. After you have mastered this activity, you will convert IPv4 addresses and subnet masks from dotted decimal to their binary form.

Convert decimal numbers to their binary equivalent.

Fill in the following table by converting the decimal number to an 8-bit binary number. The first number has been completed for your reference. Recall that the eight binary bit values in an octet are based on the powers of 2, and from left to right are 128, 64, 32, 16, 8, 4, 2, and 1.

Decimal	Binary
192	11000000
168	
10	
255	
2	

Convert the IPv4 addresses to their binary equivalent.

An IPv4 address can be converted using the same technique you used above. Fill in the table below with the binary equivalent of the addresses provided. To make your answers easier to read, separate the binary octets with a period.

Decimal	Binary
192.168.10.10	11000000.10101000.00001010.00001010
209.165.200.229	
172.16.18.183	
10.86.252.17	
255.255.255.128	
255.255.192.0	

Use Bitwise ANDing Operation to Determine Network Addresses

In Part 2, you will use the bitwise ANDing operation to calculate the network address for the provided host addresses. You will first need to convert an IPv4 decimal address and subnet mask to their binary equivalent. Once you have the binary form of the network address, convert it to its decimal form.

Note: The ANDing process compares the binary value in each bit position of the 32-bit host IP with the corresponding position in the 32-bit subnet mask. If there two 0s or a 0 and a 1, the ANDing result is 0. If there are two 1s, the result is a 1, as shown in the example here.

Determine the number of bits to use to calculate the network address.

Description	Decimal	Binary
IP Address	192.168.10.131	11000000.10101000.00001010.10000011
Subnet Mask	255.255.255.192	11111111.11111111.11111111.11000000
Network Address	192.168.10.128	11000000.10101000.00001010.10000000

How do you determine what bits to use to calculate the network address?

In the example above, how many bits are used to calculate the network address?

Use the ANDing operation to determine the network address.

- o. Enter the missing information into the table below:

Description	Decimal	Binary
IP Address	172.16.145.29	
Subnet Mask	255.255.0.0	
Network Address		

- p. Enter the missing information into the table below:

Description	Decimal	Binary
IP Address	192.168.10.10	
Subnet Mask	255.255.255.0	
Network Address		

- q. Enter the missing information into the table below:

Description	Decimal	Binary
IP Address	192.168.68.210	
Subnet Mask	255.255.255.128	
Network Address		

- r. Enter the missing information into the table below:

Description	Decimal	Binary
IP Address	172.16.188.15	
Subnet Mask	255.255.240.0	
Network Address		

- s. Enter the missing information into the table below:

Description	Decimal	Binary
IP Address	10.172.2.8	
Subnet Mask	255.224.0.0	
Network Address		

Apply Network Address Calculations

In Part 3, you must calculate the network address for the given IP addresses and subnet masks. After you have the network address, you should be able to determine the responses needed to complete the lab.

Determine whether IP addresses are on same network.

- t. You are configuring two PCs for your network. PC-A is given an IP address of 192.168.1.18, and PC-B is given an IP address of 192.168.1.33. Both PCs receive a subnet mask of 255.255.255.240.

What is the network address for PC-A? _____

What is the network address for PC-B? _____

Will these PCs be able to communicate directly with each other? _____

What is the highest address that can be given to PC-B that allows it to be on the same network as PC-A?

- u. You are configuring two PCs for your network. PC-A is given an IP address of 10.0.0.16, and PC-B is given an IP address of 10.1.14.68. Both PCs receive a subnet mask of 255.254.0.0.

What is the network address for PC-A? _____

What is the network address for PC-B? _____

Will these PCs be able to communicate directly with each other? _____

What is the lowest address that can be given to PC-B that allows it to be on the same network as PC-A?

Identify the default gateway address.

- v. Your company has a policy to use the first IP address in a network as the default gateway address. A host on the local-area network (LAN) has an IP address of 172.16.140.24 and a subnet mask of 255.255.192.0.

What is the network address for this network?

What is the default gateway address for this host?

- w. Your company has a policy to use the first IP address in a network as the default gateway address. You have been instructed to configure a new server with an IP address of 192.168.184.227 and a subnet mask of 255.255.255.248.

What is the network address for this network?

What is the default gateway for this server?

Reflection

Why is the subnet mask important in determining the network address?

Lab 11 – Identifying IPv4 Addresses

Objectives

Part 1: Identify IPv4 Addresses

Part 2: Classify IPv4 Addresses

Background / Scenario

In this lab, you will examine the structure of Internet Protocol version 4 (IPv4) addresses. You will identify the various types of IPv4 addresses and the components that help comprise the address, such as network portion, host portion, and subnet mask. Types of addresses covered include public, private, unicast, and multicast.

Required Resources

- Device with Internet access
- Optional: IPv4 address calculator

Identify IPv4 Addresses

In Part 1, you will be given several IPv4 addresses and will complete tables with appropriate information.

Analyze the table shown below and identify the network portion and host portion of the given IPv4 addresses.

The first two rows show examples of how the table should be completed.

Key for table:

N = all 8 bits for an octet are in the network portion of the address

n = a bit in the network portion of the address

H = all 8 bits for an octet are in the host portion of the address

h = a bit in the host portion of the address

IP Address/Prefix	Network/Host N,n = Network, H,h = Host	Subnet Mask	Network Address
192.168.10.10/24	N.N.N.H	255.255.255.0	192.168.10.0
10.101.99.17/23	N.N.nnnnnnnh.H	255.255.254.0	10.101.98.0
209.165.200.227/27			
172.31.45.252/24			
10.1.8.200/26			
172.16.117.77/20			
10.1.1.101/25			
209.165.202.140/27			
192.168.28.45/28			

Analyze the table below and list the range of host and broadcast addresses given a network/prefix mask pair.

The first row shows an example of how the table should be completed.

IP Address/Prefix	First Host Address	Last Host Address	Broadcast Address
192.168.10.10/24	192.168.10.1	192.168.10.254	192.168.10.255
10.101.99.17/23			
209.165.200.227/27			
172.31.45.252/24			
10.1.8.200/26			
172.16.117.77/20			
10.1.1.101/25			
209.165.202.140/27			
192.168.28.45/28			

Classify IPv4 Addresses

In Part 2, you will identify and classify several examples of IPv4 addresses.

Analyze the table shown below and identify the type of address (network, host, multicast, or broadcast address).

The first row shows an example of how the table should be completed.

IP Address	Subnet Mask	Address Type
10.1.1.1	255.255.255.252	host
192.168.33.63	255.255.255.192	
239.192.1.100	255.252.0.0	
172.25.12.52	255.255.255.0	
10.255.0.0	255.0.0.0	
172.16.128.48	255.255.255.240	
209.165.202.159	255.255.255.224	
172.16.0.255	255.255.0.0	
224.10.1.11	255.255.255.0	

Analyze the table shown below and identify the address as public or private.

IP Address/Prefix	Public or Private
209.165.201.30/27	
192.168.255.253/24	
10.100.11.103/16	
172.30.1.100/28	
192.31.7.11/24	
172.20.18.150/22	
128.107.10.1/16	
192.135.250.10/24	
64.104.0.11/16	

Analyze the table shown below and identify whether the address/prefix pair is a valid host address.

IP Address/Prefix	Valid Host Address?	Reason
127.1.0.10/24		
172.16.255.0/16		
241.19.10.100/24		
192.168.0.254/24		
192.31.7.255/24		
64.102.255.255/14		
224.0.0.5/16		
10.0.255.255/8		
198.133.219.8/24		

Reflection

Why should we continue to study and learn about IPv4 addressing if the available IPv4 address space is depleted?

Lab 12 – Calculating IPv4 Subnets

Objectives

Part 1: Determine IPv4 Address Subnetting

Part 2: Calculate IPv4 Address Subnetting

Background / Scenario

The ability to work with IPv4 subnets and determine network and host information based on a given IP address and subnet mask is critical to understanding how IPv4 networks operate. The first part is designed to reinforce how to compute network IP address information from a given IP address and subnet mask. When given an IP address and subnet mask, you will be able to determine other information about the subnet.

Required Resources

- 1 PC (Windows 7 or 8 with Internet access)
- Optional: IPv4 address calculator

Determine IPv4 Address Subnetting

In Part 1, you will determine the network and broadcast addresses, as well as the number of hosts, given an IPv4 address and subnet mask.

REVIEW: To determine the network address, perform binary ANDing on the IPv4 address using the subnet mask provided. The result will be the network address. Hint: If the subnet mask has decimal value 255 in an octet, the result will ALWAYS be the original value of that octet. If the subnet mask has decimal value 0 in an octet, the result will ALWAYS be 0 for that octet.

Example:

IP Address	192.168.10.10
Subnet Mask	255.255.255.0
	=====
Result (Network)	192.168.10.0

Knowing this, you may only have to perform binary ANDing on an octet that does not have 255 or 0 in its subnet mask portion.

Example:

IP Address	172.30.239.145
Subnet Mask	255.255.192.0

Analyzing this example, you can see that you only have to perform binary ANDing on the third octet. The first two octets will result in 172.30 due to the subnet mask. The fourth octet will result in 0 due to the subnet mask.

IP Address	172.30.239.145
Subnet Mask	255.255.192.0
	=====
Result (Network)	172.30.?.0

Perform binary ANDing on the third octet.

Decimal	Binary
239	11101111
192	11000000

=====

Result	192	11000000
---------------	------------	----------

Analyzing this example again produces the following result:

IP Address	172.30.239.145
Subnet Mask	255.255.192.0
=====	
Result (Network)	172.30.192.0

Continuing with this example, determining the number of hosts per network can be calculated by analyzing the subnet mask. The subnet mask will be represented in dotted decimal format, such as 255.255.192.0, or in network prefix format, such as /18. An IPv4 address always has 32 bits. Subtracting the number of bits used for the network portion (as represented by the subnet mask) gives you the number of bits used for hosts.

Using our example above, the subnet mask 255.255.192.0 is equivalent to /18 in prefix notation. Subtracting 18 network bits from 32 bits results in 14 bits left for the host portion. From there, it is a simple calculation:

$$2^{(\text{number of host bits})} - 2 = \text{Number of hosts}$$

$$2^{14} = 16,384 - 2 = 16,382 \text{ hosts}$$

Determine the network and broadcast addresses and number of host bits and hosts for the given IPv4 addresses and prefixes in the following table.

IPv4 Address/Prefix	Network Address	Broadcast Address	Total Number of Host Bits	Total Number of Hosts
192.168.100.25/28				
172.30.10.130/30				
10.1.113.75/19				
198.133.219.250/24				
128.107.14.191/22				
172.16.104.99/27				

Calculate IPv4 Address Subnetting

When given an IPv4 address, the original subnet mask and the new subnet mask, you will be able to determine:

- Network address of this subnet
- Broadcast address of this subnet
- Range of host addresses of this subnet
- Number of subnets created
- Number of hosts per subnet

The following example shows a sample problem along with the solution for solving this problem:

Given:	
Host IP Address:	172.16.77.120
Original Subnet Mask	255.255.0.0
New Subnet Mask:	255.255.240.0
Find:	
Number of Subnet Bits	4
Number of Subnets Created	16
Number of Host Bits per Subnet	12
Number of Hosts per Subnet	4,094
Network Address of this Subnet	172.16.64.0
IPv4 Address of First Host on this Subnet	172.16.64.1
IPv4 Address of Last Host on this Subnet	172.16.79.254
IPv4 Broadcast Address on this Subnet	172.16.79.255

Let's analyze how this table was completed.

The original subnet mask was 255.255.0.0 or /16. The new subnet mask is 255.255.240.0 or /20. The resulting difference is 4 bits. Because 4 bits were borrowed, we can determine that 16 subnets were created because $2^4 = 16$.

The new mask of 255.255.240.0 or /20 leaves 12 bits for hosts. With 12 bits left for hosts, we use the following formula: $2^{12} = 4,096 - 2 = 4,094$ hosts per subnet.

Binary ANDing will help you determine the subnet for this problem, which results in the network 172.16.64.0.

Finally, you need to determine the first host, last host, and broadcast address for each subnet. One method to determine the host range is to use binary math for the host portion of the address. In our example, the last 12 bits of the address is the host portion. The first host would have all significant bits set to zero and the least significant bit set to 1. The last host would have all significant bits set to 1 and the least significant bit set to 0. In this example, the host portion of the address resides in the 3rd and 4th octets.

Description	1 st Octet	2 nd Octet	3 rd Octet	4 th Octet	Description
Network/Host	nnnnnnnn	nnnnnnnn	nnnnhhhh	hhhhhhhh	Subnet Mask
Binary	10101100	00010000	01000000	00000001	First Host
Decimal	172	16	64	1	First Host
Binary	10101100	00010000	01001111	11111110	Last Host
Decimal	172	16	79	254	Last Host
Binary	10101100	00010000	01001111	11111111	Broadcast
Decimal	172	16	79	255	Broadcast

Step 2: Fill out the tables below with appropriate answers given the IPv4 address, original subnet mask, and new subnet mask.

a. **Problem 1:**

Given:	
Host IP Address:	192.168.200.139
Original Subnet Mask	255.255.255.0
New Subnet Mask:	255.255.255.224
Find:	
Number of Subnet Bits	
Number of Subnets Created	
Number of Host Bits per Subnet	
Number of Hosts per Subnet	
Network Address of this Subnet	
IPv4 Address of First Host on this Subnet	
IPv4 Address of Last Host on this Subnet	
IPv4 Broadcast Address on this Subnet	

b. Problem 2:

Given:	
Host IP Address:	10.101.99.228
Original Subnet Mask	255.0.0.0
New Subnet Mask:	255.255.128.0
Find:	
Number of Subnet Bits	
Number of Subnets Created	
Number of Host Bits per Subnet	
Number of Hosts per Subnet	
Network Address of this Subnet	
IPv4 Address of First Host on this Subnet	
IPv4 Address of Last Host on this Subnet	
IPv4 Broadcast Address on this Subnet	

c. Problem 3:

Given:	
Host IP Address:	172.22.32.12
Original Subnet Mask	255.255.0.0
New Subnet Mask:	255.255.224.0
Find:	
Number of Subnet Bits	
Number of Subnets Created	
Number of Host Bits per Subnet	
Number of Hosts per Subnet	
Network Address of this Subnet	
IPv4 Address of First Host on this Subnet	
IPv4 Address of Last Host on this Subnet	
IPv4 Broadcast Address on this Subnet	

d. Problem 4:

Given:	
Host IP Address:	192.168.1.245
Original Subnet Mask	255.255.255.0
New Subnet Mask:	255.255.255.252
Find:	
Number of Subnet Bits	
Number of Subnets Created	
Number of Host Bits per Subnet	
Number of Hosts per Subnet	
Network Address of this Subnet	
IPv4 Address of First Host on this Subnet	
IPv4 Address of Last Host on this Subnet	
IPv4 Broadcast Address on this Subnet	

e. Problem 5:

Given:	
Host IP Address:	128.107.0.55
Original Subnet Mask	255.255.0.0
New Subnet Mask:	255.255.255.0
Find:	
Number of Subnet Bits	
Number of Subnets Created	
Number of Host Bits per Subnet	
Number of Hosts per Subnet	
Network Address of this Subnet	
IPv4 Address of First Host on this Subnet	
IPv4 Address of Last Host on this Subnet	
IPv4 Broadcast Address on this Subnet	

f. **Problem 6:**

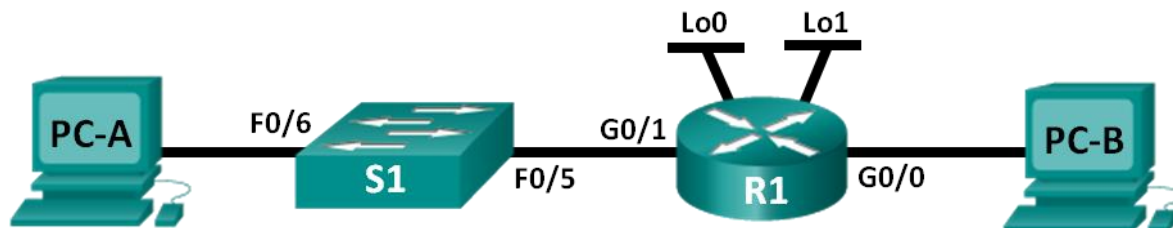
Given:	
Host IP Address:	192.135.250.180
Original Subnet Mask	255.255.255.0
New Subnet Mask:	255.255.255.248
Find:	
Number of Subnet Bits	
Number of Subnets Created	
Number of Host Bits per Subnet	
Number of Hosts per Subnet	
Network Address of this Subnet	
IPv4 Address of First Host on this Subnet	
IPv4 Address of Last Host on this Subnet	
IPv4 Broadcast Address on this Subnet	

Reflection

Why is the subnet mask so important when analyzing an IPv4 address?

Lab 13 – Designing and Implementing a Sub netted IPv4 Addressing Scheme

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0			N/A
	G0/1			N/A
	Lo0			N/A
	Lo1			N/A
S1	VLAN 1	N/A	N/A	N/A
PC-A	NIC			
PC-B	NIC			

Objectives

Part 1: Design a Network Subnetting Scheme

Part 2: Configure the Devices

Part 3: Test and Troubleshoot the Network

Background / Scenario

In this lab, starting from a single network address and network mask, you will subnet the network into multiple subnets. The subnet scheme should be based on the number of host computers required in each subnet, as well as other network considerations, like future network host expansion.

After you have created a subnetting scheme and completed the network diagram by filling in the host and interface IP addresses, you will configure the host PCs and router interfaces, including loopback interfaces. The loopback interfaces are created to simulate additional LANs attached to router R1.

After the network devices and host PCs have been configured, you will use the **ping** command to test for network connectivity.

This lab provides minimal assistance with the actual commands necessary to configure the router. However, the required commands are provided in Appendix A. Test your knowledge by trying to configure the devices without referring to the appendix.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced

might vary from what is shown in the labs. Refer to the Router Interface Summary Table at this end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: The Gigabit Ethernet interfaces on Cisco 1941 routers are autosensing. An Ethernet straight-through cable may be used between the router and PC-B. If using another Cisco router model, it may be necessary to use an Ethernet crossover cable.

Design a Network Subnetting Scheme

Create a subnetting scheme that meets the required number of subnets and required number of host addresses.

In this scenario, you are a network administrator for a small subdivision within a larger company. You must create multiple subnets out of the 192.168.0.0/24 network address space to meet the following requirements:

- The first subnet is the employee network. You need a minimum of 25 host IP addresses.
- The second subnet is the administration network. You need a minimum of 10 IP addresses.
- The third and fourth subnets are reserved as virtual networks on virtual router interfaces, loopback 0 and loopback 1. These virtual router interfaces simulate LANs attached to R1.
- You also need two additional unused subnets for future network expansion.

Note: Variable length subnet masks will not be used. All of the device subnet masks will be the same length.

Answer the following questions to help create a subnetting scheme that meets the stated network requirements:

- 1) How many host addresses are needed in the largest required subnet? _____
- 2) What is the minimum number of subnets required? _____
- 3) The network that you are tasked to subnet is 192.168.0.0/24. What is the /24 subnet mask in binary?

- 4) The subnet mask is made up of two portions, the network portion, and the host portion. This is represented in the binary by the ones and the zeros in the subnet mask.
In the network mask, what do the ones represent?

In the network mask, what do the zeros represent?

- 5) To subnet a network, bits from the host portion of the original network mask are changed into subnet bits. The number of subnet bits defines the number of subnets. Given each of the possible subnet masks depicted in the following binary format, how many subnets and how many hosts are created in each example?

Hint: Remember that the number of host bits (to the power of 2) defines the number of hosts per subnet (minus 2), and the number of subnet bits (to the power of two) defines the number of subnets. The subnet bits (depicted in bold type face) are the bits that have been borrowed beyond the original network mask of /24. The /24 is the slash prefix notation and corresponds to a dotted decimal mask of 255.255.255.0.

(/25) 11111111.11111111.11111111.**10000000**

Dotted decimal subnet mask equivalent: _____

Number of subnets? _____, Number of hosts? _____

(/26) 11111111.11111111.11111111.**11000000**

Dotted decimal subnet mask equivalent: _____

Number of subnets? _____, Number of hosts? _____

(/27) 11111111.11111111.11111111.**11100000**

Dotted decimal subnet mask equivalent: _____

Number of subnets? _____ Number of hosts? _____

(/28) 11111111.11111111.11111111.**11110000**

Dotted decimal subnet mask equivalent: _____

Number of subnets? _____ Number of hosts? _____

(/29) 11111111.11111111.11111111.**11111000**

Dotted decimal subnet mask equivalent: _____

Number of subnets? _____ Number of hosts? _____

(/30) 11111111.11111111.11111111.**11111100**

Dotted decimal subnet mask equivalent: _____

Number of subnets? _____ Number of hosts? _____

- 6) Considering your answers, which subnet masks meet the required number of minimum host addresses?

- 7) Considering your answers, which subnet masks meets the minimum number of subnets required?

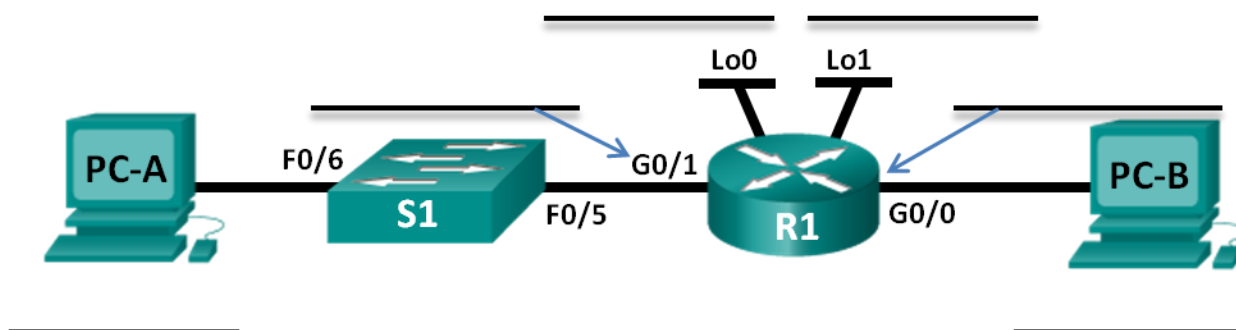
- 8) Considering your answers, which subnet mask meets both the required minimum number of hosts and the minimum number of subnets required?

- 9) When you have determined which subnet mask meets all of the stated network requirements, you will derive each of the subnets starting from the original network address. List the subnets from first to last below. Remember that the first subnet is 192.168.0.0 with the newly acquired subnet mask.

Subnet Address	/ Prefix	Subnet Mask (dotted decimal)
_____	/ ____	_____
_____	/ ____	_____
_____	/ ____	_____
_____	/ ____	_____
_____	/ ____	_____
_____	/ ____	_____
_____	/ ____	_____
_____	/ ____	_____
_____	/ ____	_____
_____	/ ____	_____
_____	/ ____	_____

Complete the diagram showing where the host IP addresses will be applied.

On the following lines provided, fill in the IP addresses and subnets masks in slash prefix notation. On the router, use the first usable address in each subnet for each of the interfaces, Gigabit Ethernet 0/0, Gigabit Ethernet 0/1, loopback 0, and loopback 1. Fill in an IP address for both PC-A and PC-B. Also enter this information into the Addressing Table on Page 1.



Configure the Devices

In Part 2, set up the network topology and configure basic settings on the PCs and router, such as the router Gigabit Ethernet interface IP addresses, and the PC's IP addresses, subnet masks, and default gateways. Refer to the Addressing Table for device names and address information.

Note: Appendix A provides configuration details for the steps in Part 2. You should attempt to complete Part 2 prior to reviewing Appendix A.

Configure the router.

- a. Enter into privileged EXEC mode and then global config mode.
- b. Assign the **R1** as the hostname for the router.
- c. Configure both the **G0/0** and **G0/1** interfaces with IP addresses and subnet masks, and then enable them.
- d. Loopback interfaces are created to simulate additional LANs on R1 router. Configure the loopback interfaces with IP addresses and subnet masks. After they are created, loopback interfaces are enabled, by default. (To create the loopback addresses, enter the command **interface loopback 0** at the global config mode)

Note: You can create additional loopbacks for testing with different addressing schemes, if desired.

- e. Save the running configuration to the startup configuration file.

Configure the PC interfaces.

- a. Configure the IP address, subnet mask, and default gateway settings on PC-A.
- b. Configure the IP address, subnet mask, and default gateway settings on PC-B.

Test and Troubleshoot the Network

In Part 3, you will use the **ping** command to test network connectivity.

- a. Test to see if PC-A can communicate with its default gateway. From PC-A, open a command prompt and ping the IP address of the router Gigabit Ethernet 0/1 interface. Do you get a reply?

- b. Test to see if PC-B can communicate with its default gateway. From PC-B, open a command prompt and ping the IP address of the router Gigabit Ethernet 0/0 interface. Do you get a reply?

- c. Test to see if PC-A can communicate with PC-B. From PC-A, open a command prompt and ping the IP address of PC-B. Do you get a reply? _____
- d. If you answered “no” to any of the preceding questions, then you should go back and check all of your IP address and subnet mask configurations, and ensure that the default gateways have been correctly configured on PC-A and PC-B.
- e. If you verify that all of the settings are correct, and you can still not ping successfully, then there are a few additional factors that can block ICMP pings. On PC-A and PC-B within Windows, make sure that the Windows Firewall is turned off for the Work, Home, and Public networks.
- f. Experiment by purposely misconfiguring the gateway address on PC-A to 10.0.0.1. What happens when you try and ping from PC-B to PC-A? Do you receive a reply?

Reflection

1. Subnetting one larger network into multiple smaller subnetworks allows for greater flexibility and security in network design. However, what do you think some of the drawbacks are when the subnets are limited to being the same size?

2. Why do you think the gateway/router IP address is usually the first usable IP address in the network?

Appendix A: Configuration Details for Steps in Part 2

Configure the router.

- a. Console into the router and enable privileged EXEC mode.

```
Router> enable
Router#
```

- b. Enter into configuration mode.

```
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

- c. Assign a device name to the router.

```
Router(config)# hostname R1
R1(config)#
```

- d. Configure both the **G0/0** and **G0/1** interfaces with IP addresses and subnet masks, and enable them.

```
R1(config)# interface g0/0
R1(config-if)# ip address <ip address> <subnet mask>
R1(config-if)# no shutdown
R1(config-if)# interface g0/1
R1(config-if)# ip address <ip address> <subnet mask>
R1(config-if)# no shutdown
```

- e. Loopback interfaces are created to simulate additional LANs off of router R1. Configure the loopback interfaces with IP addresses and subnet masks. When they are created, loopback interfaces are enabled, by default.

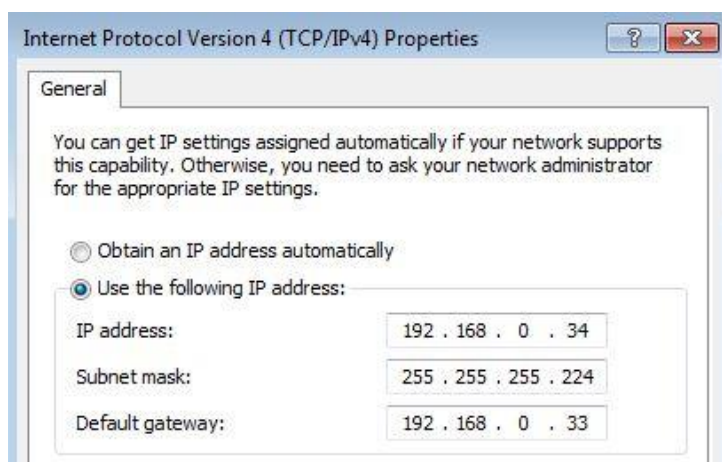
```
R1(config)# interface loopback 0
R1(config-if)# ip address <ip address> <subnet mask>
R1(config-if)# interface loopback 1
R1(config-if)# ip address <ip address> <subnet mask>
R1(config-if)# end
```

- f. Save the running configuration to the startup configuration file.

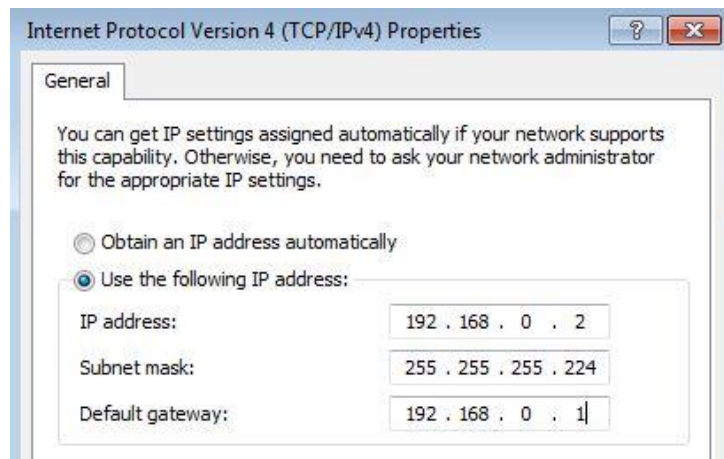
```
R1# copy running-config startup-config
```

Configure the PC interfaces.

- a. Configure the IP address, subnet mask, and default gateway settings on PC-A.

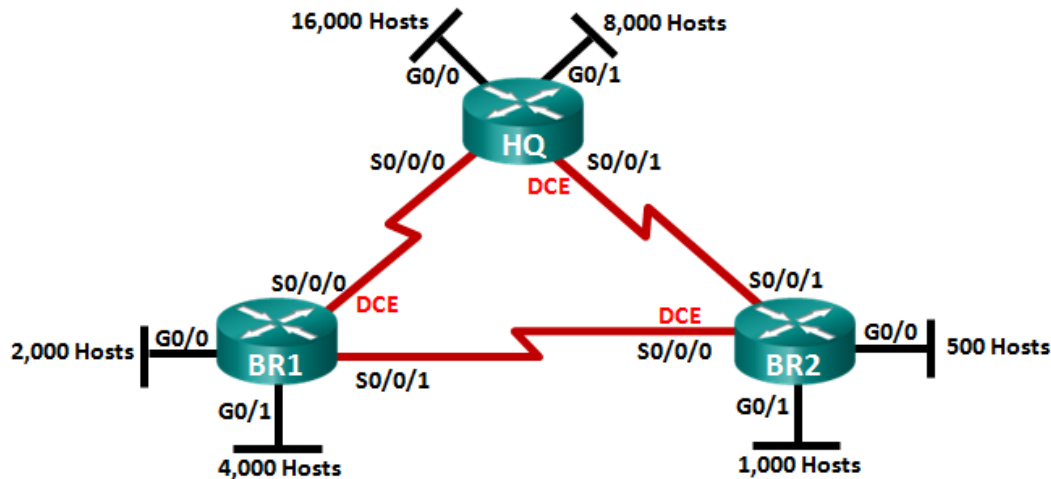


- b. Configure the IP address, subnet mask, and default gateway settings on PC-B.



Lab 14 – Designing and Implementing a VLSM Addressing Scheme

Topology



Objectives

- Part 1: Examine Network Requirements
- Part 2: Design the VLSM Address Scheme
- Part 3: Cable and Configure the IPv4 Network

Background / Scenario

Variable Length Subnet Mask (VLSM) was designed to avoid wasting IP addresses. With VLSM, a network is subnetted and then re-subnetted. This process can be repeated multiple times to create subnets of various sizes based on the number of hosts required in each subnet. Effective use of VLSM requires address planning.

In this lab, use the 172.16.128.0/17 network address to develop an address scheme for the network displayed in the topology diagram. VLSM is used to meet the IPv4 addressing requirements. After you have designed the VLSM address scheme, you will configure the interfaces on the routers with the appropriate IP address information.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). Other routers and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 routers (Cisco 1941 with Cisco IOS software, Release 15.2(4)M3 universal image or comparable)
- 1 PC (with terminal emulation program, such as Tera Term, to configure routers)
- Console cable to configure the Cisco IOS devices via the console ports
- Ethernet (optional) and serial cables, as shown in the topology
- Windows Calculator (optional)

Examine Network Requirements

In Part 1, you will examine the network requirements to develop a VLSM address scheme for the network displayed in the topology diagram using the 172.16.128.0/17 network address.

Note: You can use the Windows Calculator application and the www.ipcalc.org IP subnet calculator to help with your calculations.

Determine how many host addresses and subnets are available.

How many host addresses are available in a /17 network? _____

What is the total number of host addresses needed in the topology diagram? _____

How many subnets are needed in the network topology? _____

Determine the largest subnet.

What is the subnet description (e.g. BR1 G0/1 LAN or BR1-HQ WAN link)? _____

How many IP addresses are required in the largest subnet? _____

What subnet mask can support that many host addresses?

How many total host addresses can that subnet mask support? _____

Can you subnet the 172.16.128.0/17 network address to support this subnet? _____

What are the two network addresses that would result from this subnetting?

Use the first network address for this subnet.

Determine the second largest subnet.

What is the subnet description? _____

How many IP addresses are required for the second largest subnet? _____

What subnet mask can support that many host addresses?

How many total host addresses can that subnet mask support? _____

Can you subnet the remaining subnet again and still support this subnet? _____

What are the two network addresses that would result from this subnetting?

Use the first network address for this subnet.

Determine the next largest subnet.

What is the subnet description? _____

How many IP addresses are required for the next largest subnet? _____

What subnet mask can support that many host addresses?

How many total host addresses can that subnet mask support? _____

Can you subnet the remaining subnet again and still support this subnet? _____

What are the two network addresses that would result from this subnetting?

Use the first network address for this subnet.

Determine the next largest subnet.

What is the subnet description? _____

How many IP addresses are required for the next largest subnet? _____

What subnet mask can support that many host addresses?

How many total host addresses can that subnet mask support? _____

Can you subnet the remaining subnet again and still support this subnet? _____

What are the two network addresses that would result from this subnetting?

Use the first network address for this subnet.

Determine the next largest subnet.

What is the subnet description? _____

How many IP addresses are required for the next largest subnet? _____

What subnet mask can support that many host addresses?

How many total host addresses can that subnet mask support? _____

Can you subnet the remaining subnet again and still support this subnet? _____

What are the two network addresses that would result from this subnetting?

Use the first network address for this subnet.

Determine the next largest subnet.

What is the subnet description? _____

How many IP addresses are required for the next largest subnet? _____

What subnet mask can support that many host addresses?

How many total host addresses can that subnet mask support? _____

Can you subnet the remaining subnet again and still support this subnet? _____

What are the two network addresses that would result from this subnetting?

Use the first network address for this subnet.

Determine the subnets needed to support the serial links.

How many host addresses are required for each serial subnet link? _____

What subnet mask can support that many host addresses?

- _____
- a. Continue subnetting the first subnet of each new subnet until you have four /30 subnets. Write the first three network addresses of these /30 subnets below.

- b. Enter the subnet descriptions for these three subnets below.

Design the VLSM Address Scheme

Calculate the subnet information.

Use the information that you obtained in Part 1 to fill in the following table.

Subnet Description	Number of Hosts Needed	Network Address /CIDR	First Host Address	Broadcast Address
HQ G0/0	16,000			
HQ G0/1	8,000			
BR1 G0/1	4,000			
BR1 G0/0	2,000			
BR2 G0/1	1,000			
BR2 G0/0	500			
HQ S0/0/0 – BR1 S0/0/0	2			
HQ S0/0/1 – BR2 S0/0/1	2			
BR1 S0/0/1 – BR2 S0/0/0	2			

Complete the device interface address table.

Assign the first host address in the subnet to the Ethernet interfaces. HQ should be given the first host address on the Serial links to BR1 and BR2. BR1 should be given the first host address for the serial link to BR2.

Device	Interface	IP Address	Subnet Mask	Device Interface
HQ	G0/0			16,000 Host LAN
	G0/1			8,000 Host LAN
	S0/0/0			BR1 S0/0/0
	S0/0/1			BR2 S0/0/1
BR1	G0/0			2,000 Host LAN
	G0/1			4,000 Host LAN
	S0/0/0			HQ S0/0/0
	S0/0/1			BR2 S0/0/0
BR2	G0/0			500 Host LAN
	G0/1			1,000 Host LAN
	S0/0/0			BR1 S0/0/1
	S0/0/1			HQ S0/0/1

Cable and Configure the IPv4 Network

In Part 3, you will cable the network topology and configure the three routers using the VLSM address scheme that you developed in Part 2.

Cable the network as shown in the topology.

Configure basic settings on each router.

- Assign the device name to the router.
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.
- Assign **cisco** as the VTY password and enable login.
- Encrypt the clear text passwords.
- Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.

Configure the interfaces on each router.

- Assign an IP address and subnet mask to each interface using the table that you completed in Part 2.
- Configure an interface description for each interface.
- Set the clocking rate on all DCE serial interfaces to 128000.

```
HQ(config-if)# clock rate 128000
```
- Activate the interfaces.

Save the configuration on all devices.

Test Connectivity.

- From HQ, ping BR1's S0/0/0 interface address.

- b. From HQ, ping BR2's S0/0/1 interface address.
- c. From BR1, ping BR2's S0/0/0 interface address.
- d. Troubleshoot connectivity issues if pings were not successful.

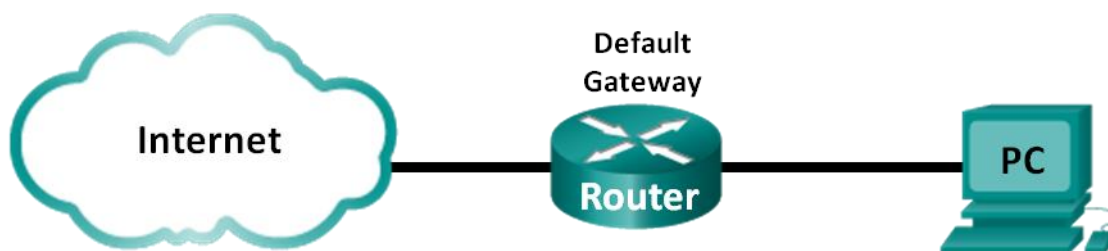
Note: Pings to the GigabitEthernet interfaces on other routers will not be successful. The LANs defined for the GigabitEthernet interfaces are simulated. Because no devices are attached to these LANs they will be in down/down state. A routing protocol needs to be in place for other devices to be aware of those subnets. The GigabitEthernet interfaces also need to be in an up/up state before a routing protocol can add the subnets to the routing table. These interfaces will remain in a down/down state until a device is connected to the other end of the Ethernet interface cable. The focus of this lab is on VLSM and configuring the interfaces.

Reflection

Can you think of a shortcut for calculating the network addresses of consecutive /30 subnets?

Lab 15 – Identifying IPv6 Addresses

Topology



Objectives

Part 1: Identify the Different Types of IPv6 Addresses

Part 2: Examine a Host IPv6 Network Interface and Address

Part 3: Practice IPv6 Address Abbreviation

Background / Scenario

With the depletion of the Internet Protocol version 4 (IPv4) network address space and the adoption and transition to IPv6, networking professionals must understand how both IPv4 and IPv6 networks function. Many devices and applications already support IPv6. This includes extensive Cisco device Internetwork Operating System (IOS) support and workstation/server operating system support, such as that found in Windows and Linux.

This lab focuses on IPv6 addresses and the components of the address. In Part 1, you will identify the IPv6 address types, and in Part 2, you will view the IPv6 settings on a PC. In Part 3, you will practice IPv6 address abbreviation.

Required Resources

- 1 PC (Windows 7 or 8 with Internet access)

Identify the Different Types of IPv6 Addresses

In Part 1, you will review the characteristics of IPv6 addresses to identify the different types of IPv6 addresses.

Review the different types of IPv6 addresses.

An IPv6 address is 128 bits long. It is most often presented as 32 hexadecimal characters. Each hexadecimal character is the equivalent of 4 bits ($4 \times 32 = 128$). A non-abbreviated IPv6 host address is shown here:

2001:0DB8:0001:0000:0000:0000:0001

A hextet is the hexadecimal, IPv6 version of an IPv4 octet. An IPv4 address is 4 octets long, separated by dots. An IPv6 address is 8 hextets long, separated by colons.

An IPv4 address is 4 octets and is commonly written or displayed in decimal notation.

255.255.255.255

An IPv6 address is 8 hextets and is commonly written or displayed in hexadecimal notation.

FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

In an IPv4 address, each individual octet is 8 binary digits (bits). Four octets equals one 32-bit IPv4 address.

11111111 = 255

11111111.11111111.11111111.11111111 = 255.255.255.255

In an IPv6 address, each individual hextet is 16 bits long. Eight hextets equals one 128-bit IPv6 address.

1111111111111111 = FFFF

1111111111111111.1111111111111111.1111111111111111.1111111111111111.

1111111111111111.1111111111111111.1111111111111111.1111111111111111 =

FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

If we read an IPv6 address starting from the left, the first (or far left) hextet identifies the IPv6 address type. For example, if the IPv6 address has all zeros in the far left hextet, then the address is possibly a loopback address.

0000:0000:0000:0000:0000:0000:0000:0001 = loopback address

::1 = loopback address abbreviated

As another example, if the IPv6 address has FE80 in the first hextet, then the address is a link-local address.

FE80:0000:0000:0000:C5B7:CB51:3C00:D6CE = link-local address

FE80::C5B7:CB51:3C00:D6CE = link-local address abbreviated

Study the chart below to help you identify the different types of IPv6 address based on the numbers in the first hextet.

First Hextet (Far Left)	Type of IPv6 Address
0000 to 00FF	Loopback address, any address, unspecified address, or IPv4-compatible
2000 to 3FFF	Global unicast address (a routable address in a range of addresses that is currently being handed out by the Internet Assigned Numbers Authority [IANA])
FE80 to FEBF	Link-local (a unicast address which identifies the host computer on the local network)
FC00 to FCFF	Unique-local (a unicast address which can be assigned to a host to identify it as being part of a specific subnet on the local network)
FF00 to FFFF	Multicast address

There are other IPv6 address types that are either not yet widely implemented, or have already become deprecated, and are no longer supported. For instance, an **anycast address** is new to IPv6 and can be used by routers to facilitate load sharing and provide alternate path flexibility if a router becomes unavailable. Only routers should respond to an anycast address. Alternatively, **site-local addresses** have been deprecated and replaced by unique-local addresses. Site-local addresses were identified by the numbers FEC0 in the initial hextet.

In IPv6 networks, there are no network (wire) addresses or broadcast addresses as there are in IPv4 networks.

Match the IPv6 address to its type.

Match the IPv6 addresses to their corresponding address type. Notice that the addresses have been compressed to their abbreviated notation and that the slash network prefix number is not shown. Some answer choices must be used more than once.

IPv6 Address	Answer
2001:0DB8:1:ACAD::FE55:6789:B210	1. ____
::1	2. ____
FC00:22:A:2::CD4:23E4:76FA	3. ____
2033:DB8:1:1:22:A33D:259A:21FE	4. ____
FE80::3201:CC01:65B1	5. ____
FF00::	6. ____
FF00::DB7:4322:A231:67C	7. ____
FF02::2	8. ____

Answer Choices

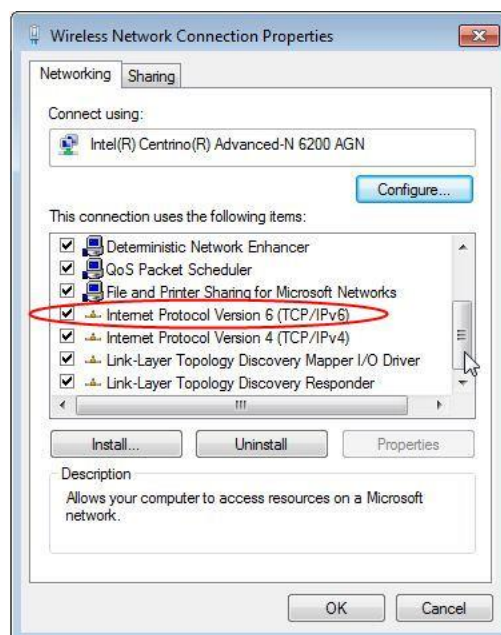
- a. Loopback address
- b. Global unicast address
- c. Link-local address
- d. Unique-local address
- e. Multicast address

Examine a Host IPv6 Network Interface and Address

In Part 2, you will check the IPv6 network settings of your PC to identify your network interface IPv6 address.

Check your PC IPv6 network address settings.

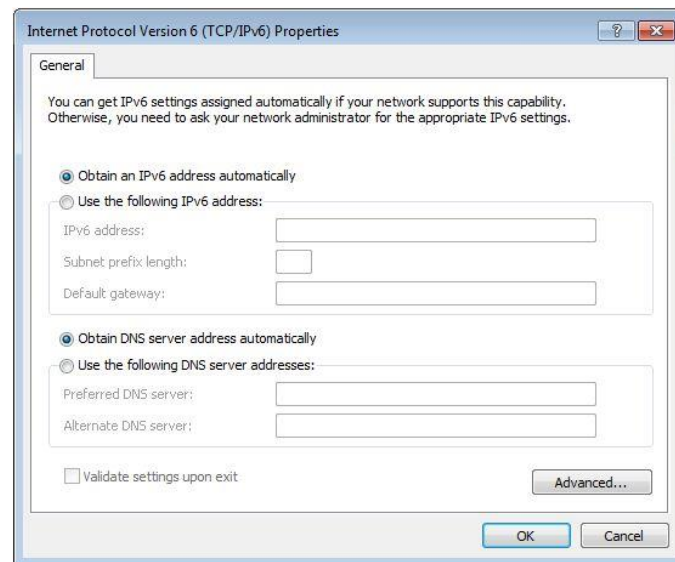
- a. Verify that the IPv6 protocol is installed and active on your PC-A (check your Local Area Connection settings).
- b. Click the Windows **Start** button and then **Control Panel** and change **View by: Category** to **View by: Small icons**.
- c. Click the **Network and Sharing Center** icon.
- d. On the left side of the window, click **Change adapter settings**. You should now see icons representing your installed network adapters. Right-click your active network interface (it may be a **Local Area Connection** or a **Wireless Network Connection**), and then click **Properties**.
- e. You should now see your Network Connection Properties window. Scroll through the list of items to determine whether IPv6 is present, which indicates that it is installed, and if it is also check marked, which indicates that it is active.



- f. Select the item **Internet Protocol Version 6 (TCP/IPv6)** and click **Properties**. You should see the IPv6 settings for your network interface. Your IPv6 properties window is likely set to **Obtain an IPv6**

address automatically. This does not mean that IPv6 relies on the Dynamic Host Configuration Protocol (DHCP). Instead of using DHCP, IPv6 looks to the local router for IPv6 network information and then auto-configures its own IPv6 addresses. To manually configure IPv6, you must provide the IPv6 address, the subnet prefix length, and the default gateway.

Note: The local router can refer host requests for IPv6 information, especially Domain Name System (DNS) information, to a DHCPv6 server on the network.



- g. After you have verified that IPv6 is installed and active on your PC, you should check your IPv6 address information. To do this, click the **Start** button, type **cmd** in the *Search programs and files* form box, and press Enter. This opens a Windows command prompt window.
- h. Type **ipconfig /all** and press Enter. Your output should look similar to this:

```
C:\Users\user> ipconfig /all
```

```
Windows IP Configuration
```

```
<output omitted>
```

```
Wireless LAN adapter Wireless Network Connection:
```

```

Connection-specific DNS Suffix  . : 
Description . . . . . : Intel(R) Centrino(R) Advanced-N 6200 AGN
Physical Address. . . . . : 02-37-10-41-FB-48
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8d4f:4f4d:3237:95e2%14 (Preferred)
IPv4 Address. . . . . : 192.168.2.106 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Sunday, January 06, 2013 9:47:36 AM
Lease Expires . . . . . : Monday, January 07, 2013 9:47:38 AM
Default Gateway . . . . . : 192.168.2.1
DHCP Server . . . . . : 192.168.2.1
DHCPv6 IAID . . . . . : 335554320
DHCPv6 Client DUID. . . . . : 00-01-00-01-14-57-84-B1-1C-C1-DE-91-C3-5D

DNS Servers . . . . . : 192.168.1.1
                       8.8.4.4

```

<output omitted>

- i. You can see from the output that the client PC has an IPv6 link-local address with a randomly generated interface ID. What does it indicate about the network regarding IPv6 global unicast address, IPv6 unique-local address, or IPv6 gateway address?

- j. What kind of IPv6 addresses did you find when using **ipconfig /all**?

Practice IPv6 Address Abbreviation

In Part 3, you will study and review rules for IPv6 address abbreviation to correctly compress and decompress IPv6 addresses.

Study and review the rules for IPv6 address abbreviation.

Rule 1: In an IPv6 address, a string of four zeros (0s) in a hextet can be abbreviated as a single zero.

2001:0404:0001:1000:0000:0000:0EF0:BC00

2001:0404:0001:1000:0:0:0EF0:BC00 (abbreviated with single zeros)

Rule 2: In an IPv6 address, the leading zeros in each hextet can be omitted, trailing zeros cannot be omitted.

2001:0404:0001:1000:0000:0000:0EF0:BC00

2001:404:1:1000:0:0:EF0:BC00 (abbreviated with leading zeros omitted)

Rule 3: In an IPv6 address, a single continuous string of four or more zeros can be abbreviated as a double colon (::). The double colon abbreviation can only be used one time in an IP address.

2001:0404:0001:1000:0000:0000:0EF0:BC00

2001:404:1:1000::EF0:BC00 (abbreviated with leading zeroes omitted and continuous zeros replaced with a double colon)

The image below illustrates these rules of IPv6 address abbreviation:

```
FF01:0000:0000:0000:0000:0000:0000:1
= FF01:0:0:0:0:0:0:1
= FF01::1
```

```
E3D7:0000:0000:0000:51F4:00C8:C0A8:6420
= E3D7::51F4:C8:C0A8:6420
```

```
3FFE:0501:0008:0000:0260:97FF:FE40:EFAB
= 3FFE:501:8:0:260:97FF:FE40:EFAB
= 3FFE:501:8::260:97FF:FE40:EFAB
```

Practice compressing and decompressing IPv6 addresses.

Using the rules of IPv6 address abbreviation, either compress or decompress the following addresses:

1) 2002:0EC0:0200:0001:0000:04EB:44CE:08A2

2) FE80:0000:0000:0001:0000:60BB:008E:7402

3) FE80::7042:B3D7:3DEC:84B8

4) FF00::

5) 2001:0030:0001:ACAD:0000:330E:10C2:32BF

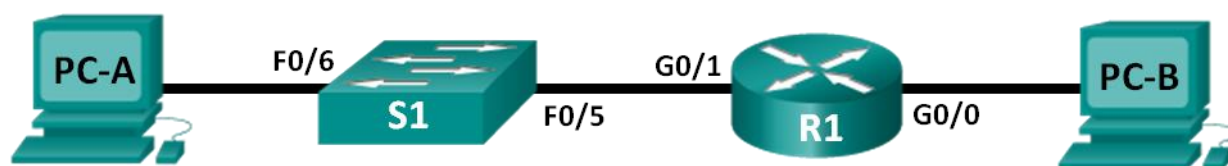
Reflection

1. How do you think you must support IPv6 in the future?

2. Do you think IPv4 networks continue on, or will everyone eventually switch over to IPv6? How long do you think it will take?

Lab 16 – Configuring IPv6 Addresses on Network Devices

Topology



Addressing Table

Device	Interface	IPv6 Address	Prefix Length	Default Gateway
R1	G0/0	2001:DB8:ACAD:A::1	64	N/A
	G0/1	2001:DB8:ACAD:1::1	64	N/A
S1	VLAN 1	2001:DB8:ACAD:1::B	64	N/A
PC-A	NIC	2001:DB8:ACAD:1::3	64	FE80::1
PC-B	NIC	2001:DB8:ACAD:A::3	64	FE80::1

Objectives

Part 1: Set Up Topology and Configure Basic Router and Switch Settings

Part 2: Configure IPv6 Addresses Manually

Part 3: Verify End-to-End Connectivity

Background / Scenario

Knowledge of the Internet Protocol version 6 (IPv6) multicast groups can be helpful when assigning IPv6 addresses manually. Understanding how the all-router multicast group is assigned and how to control address assignments for the Solicited Nodes multicast group can prevent IPv6 routing issues and help ensure best practices are implemented.

In this lab, you will configure hosts and device interfaces with IPv6 addresses and explore how the all-router multicast group is assigned to a router. You will use **show** commands to view IPv6 unicast and multicast addresses. You will also verify end-to-end connectivity using the **ping** and **traceroute** commands.

Note: The routers used with CCNA hands-on labs are Cisco 1941 ISRs with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS software, Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports

- Ethernet cables as shown in the topology

Note: The Gigabit Ethernet interfaces on Cisco 1941 routers are autosensing and an Ethernet straight-through cable may be used between the router and PC-B. If using another model Cisco router, it may be necessary to use an Ethernet crossover cable.

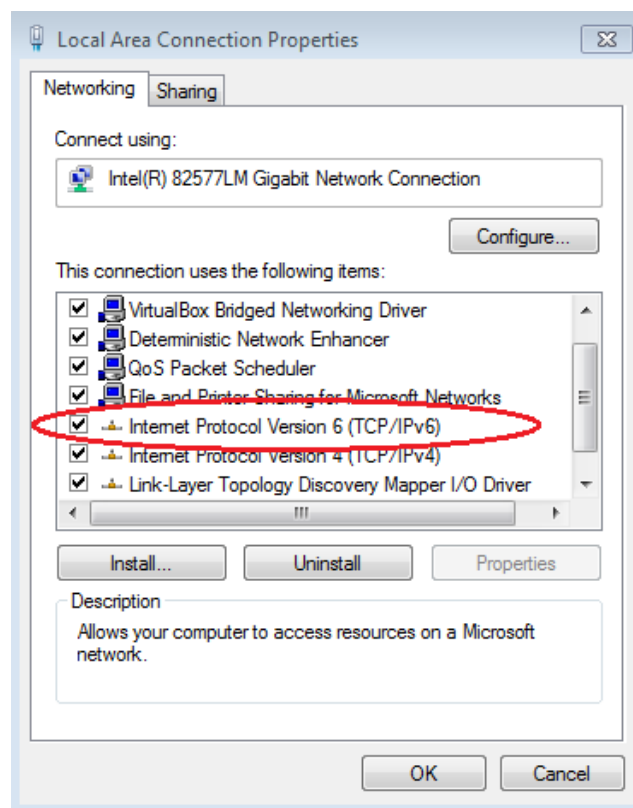
Set Up Topology and Configure Basic Router and Switch Settings

Cable the network as shown in the topology.

Initialize and reload the router and switch.

Verify that the PC interfaces are configured to use the IPv6 protocol.

Verify that the IPv6 protocol is active on both PCs by ensuring that the **Internet Protocol Version 6 (TCP/IPv6)** check box is selected in the Local Area Connection Properties window.



Configure the router.

- Console into the router and enable privileged EXEC mode.
- Assign the device name to the router.
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.
- Assign **cisco** as the VTY password and enable login.
- Encrypt the clear text passwords.
- Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

- i. Save the running configuration to the startup configuration file.

Configure the switch.

- a. Console into the switch and enable privileged EXEC mode.
- b. Assign the device name to the switch.
- c. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.
- d. Assign **class** as the privileged EXEC encrypted password.
- e. Assign **cisco** as the console password and enable login.
- f. Assign **cisco** as the VTY password and enable login.
- g. Encrypt the clear text passwords.
- h. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
- i. Save the running configuration to the startup configuration file.

Configure IPv6 Addresses Manually

Assign the IPv6 addresses to Ethernet interfaces on R1.

- a. Assign the IPv6 global unicast addresses, listed in the Addressing Table, to both Ethernet interfaces on R1.

```
R1(config)# interface g0/0
R1(config-if)# ipv6 address 2001:db8:acad:a::1/64
R1(config-if)# no shutdown
R1(config-if)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# end
R1#
```

- b. Issue the **show ipv6 interface brief** command to verify that the correct IPv6 unicast address is assigned to each interface.

```
R1# show ipv6 interface brief
Em0/0 [administratively down/down]
    unassigned
GigabitEthernet0/0 [up/up]
    FE80::D68C:B5FF:FECE:A0C0
    2001:DB8:ACAD:A::1
GigabitEthernet0/1 [up/up]
    FE80::D68C:B5FF:FECE:A0C1
    2001:DB8:ACAD:1::1
<output omitted>
```

- c. Issue the **show ipv6 interface g0/0** command. Notice that the interface is listing two Solicited Nodes multicast groups, because the IPv6 link-local (FE80) Interface ID was not manually configured to match the IPv6 unicast Interface ID.

Note: The link-local address displayed is based on EUI-64 addressing, which automatically uses the interface Media Access Control (MAC) address to create a 128-bit IPv6 link-local address.

```
R1# show ipv6 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::D68C:B5FF:FECE:A0C0
  No Virtual link-local address(es):
```

```

Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::1:FF00:1
  FF02::1:FFCE:A0C0
MTU is 1500 bytes
<output omitted>

```

- d. To get the link-local address to match the unicast address on the interface, manually enter the link-local addresses on each of the Ethernet interfaces on R1.

```

R1# config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface g0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# interface g0/1
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# end
R1#

```

Note: Each router interface belongs to a separate network. Packets with a link-local address never leave the local network; therefore, you can use the same link-local address on both interfaces.

- e. Re-issue the **show ipv6 interface g0/0** command. Notice that the link-local address has been changed to **FE80::1** and that there is only one Solicited Nodes multicast group listed.

```

R1# show ipv6 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
  MTU is 1500 bytes
<output omitted>

```

What multicast groups have been assigned to interface G0/0?

Enable IPv6 routing on R1.

- f. On a PC-B command prompt, enter the **ipconfig** command to examine IPv6 address information assigned to the PC interface.

Has an IPv6 unicast address been assigned to the network interface card (NIC) on PC-B? _____

- g. Enable IPv6 routing on R1 using the **IPv6 unicast-routing** command.

```

R1 # configure terminal
R1(config)# ipv6 unicast-routing
R1(config)# exit
R1#
*Dec 17 18:29:07.415: %SYS-5-CONFIG_I: Configured from console by console

```

- h. Use the **show ipv6 interface g0/0** command to see what multicast groups are assigned to interface G0/0. Notice that the all-router multicast group (FF02::2) now appears in the group list for interface G0/0.

Note: This will allow the PCs to obtain their IP address and default gateway information automatically using Stateless Address Autoconfiguration (SLAAC).

R1# **show ipv6 interface g0/0**

```
GigabitEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
<output omitted>
```

- i. Now that R1 is part of the all-router multicast group, re-issue the **ipconfig** command on PC-B. Examine the IPv6 address information.

Why did PC-B receive the Global Routing Prefix and Subnet ID that you configured on R1?

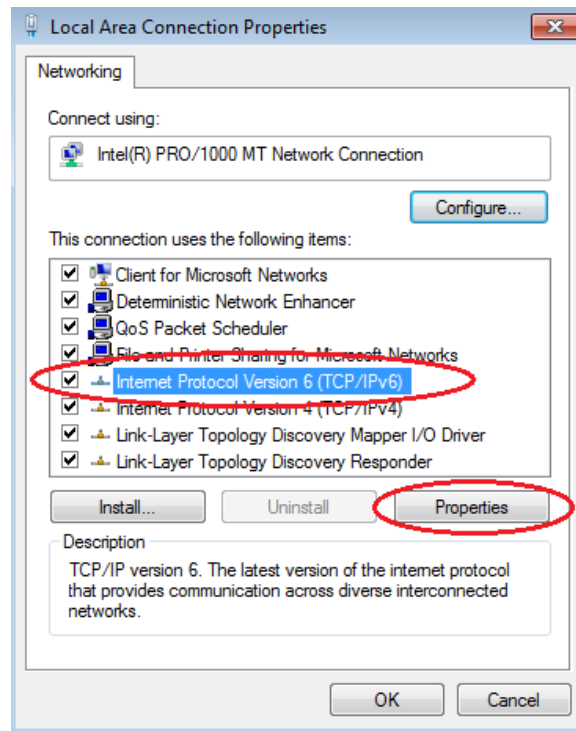
Assign IPv6 addresses to the management interface (SVI) on S1.

- j. Assign the IPv6 address listed in the Addressing Table to the management interface (VLAN 1) on S1. Also assign a link-local address for this interface. IPv6 command syntax is the same as on the router.
- k. Verify that the IPv6 addresses are properly assigned to the management interface using the **show ipv6 interface vlan1** command.

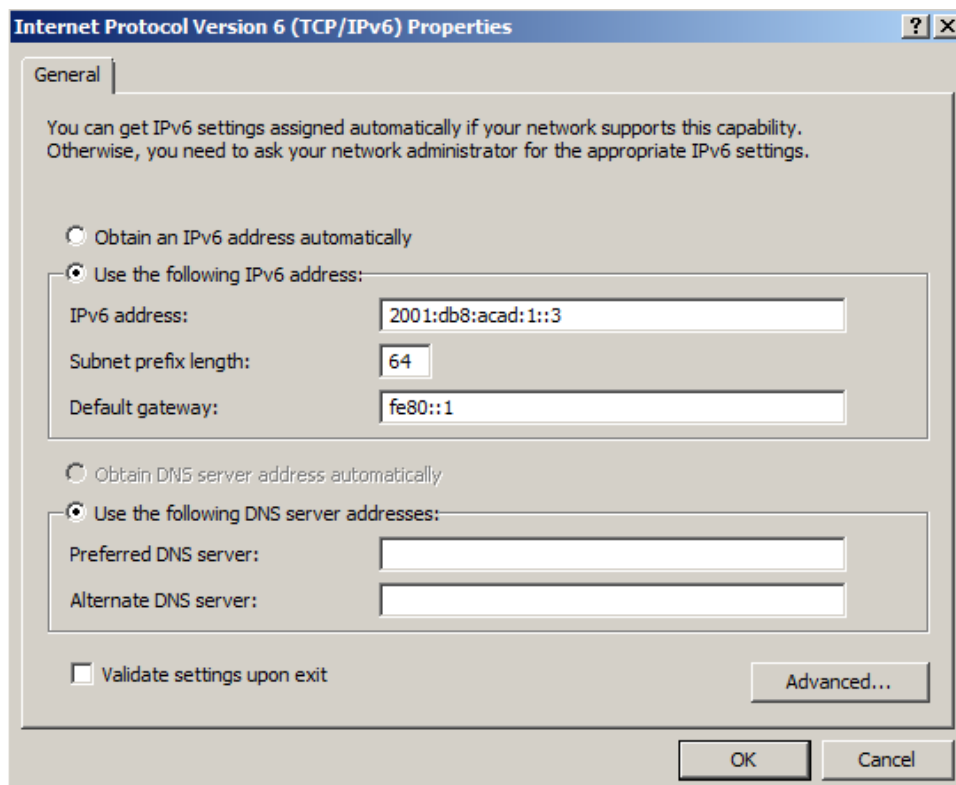
Note: The default 2960 Switch Database Manager (SDM) template does not support IPv6. It may be necessary to issue the command **sdm prefer dual-ipv4-and-ipv6 default** to enable IPv6 addressing before applying an IPv6 address to the VLAN 1 SVI.

Assign static IPv6 addresses to the PCs.

- l. Open the Local Area Connection Properties window on PC-A. Select **Internet Protocol Version 6 (TCP/IPv6)** and click **Properties**.



- m. Click the **Use the following IPv6 address** radio button. Refer to the Addressing Table and enter the **IPv6 address**, **Subnet prefix length**, and **Default gateway** information. Click **OK**.



- n. Click **Close** to close the Local Area Connection Properties window.
- o. Repeat Steps 4a to c to enter the static IPv6 information on PC-B. For the correct IPv6 address information, refer to the Addressing Table.
- p. Issue the **ipconfig** command from the command line on PC-B to verify the IPv6 address information.

Verify End-to-End Connectivity

- q. From PC-A, ping **FE80::1**. This is the link-local address assigned to G0/1 on R1.

```
C:\>ping fe80::1

Pinging fe80::1 with 32 bytes of data:
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms

Ping statistics for fe80::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Note: You can also test connectivity by using the global unicast address, instead of the link-local address.

- r. Ping the S1 management interface from PC-A.

```
C:\>ping 2001:db8:acad:1::b

Pinging 2001:db8:acad:1::b with 32 bytes of data:
Reply from 2001:db8:acad:1::b: time=14ms
Reply from 2001:db8:acad:1::b: time=2ms
Reply from 2001:db8:acad:1::b: time=2ms
Reply from 2001:db8:acad:1::b: time=3ms

Ping statistics for 2001:db8:acad:1::b:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 14ms, Average = 5ms

C:\>
```

- s. Use the **tracert** command on PC-A to verify that you have end-to-end connectivity to PC-B.

```
C:\>tracert 2001:db8:acad:a::3

Tracing route to 2001:db8:acad:a::3 over a maximum of 30 hops

  1  <1 ms    <1 ms    <1 ms    2001:db8:acad:1::1
  2   5 ms    <1 ms    <1 ms    2001:db8:acad:a::3

Trace complete.

C:\>
```

- t. From PC-B, ping PC-A.

```
C:\>ping 2001:db8:acad:1::3

Pinging 2001:db8:acad:1::3 with 32 bytes of data:
Reply from 2001:db8:acad:1::3: time<1ms
Reply from 2001:db8:acad:1::3: time<1ms
Reply from 2001:db8:acad:1::3: time<1ms
Reply from 2001:db8:acad:1::3: time<1ms

Ping statistics for 2001:db8:acad:1::3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

- u. From PC-B, ping the link-local address for G0/0 on R1.

```
C:\>ping fe80::1

Pinging fe80::1 with 32 bytes of data:
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms

Ping statistics for fe80::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Note: If end-to-end connectivity is not established, troubleshoot your IPv6 address assignments to verify that you entered the addresses correctly on all devices.

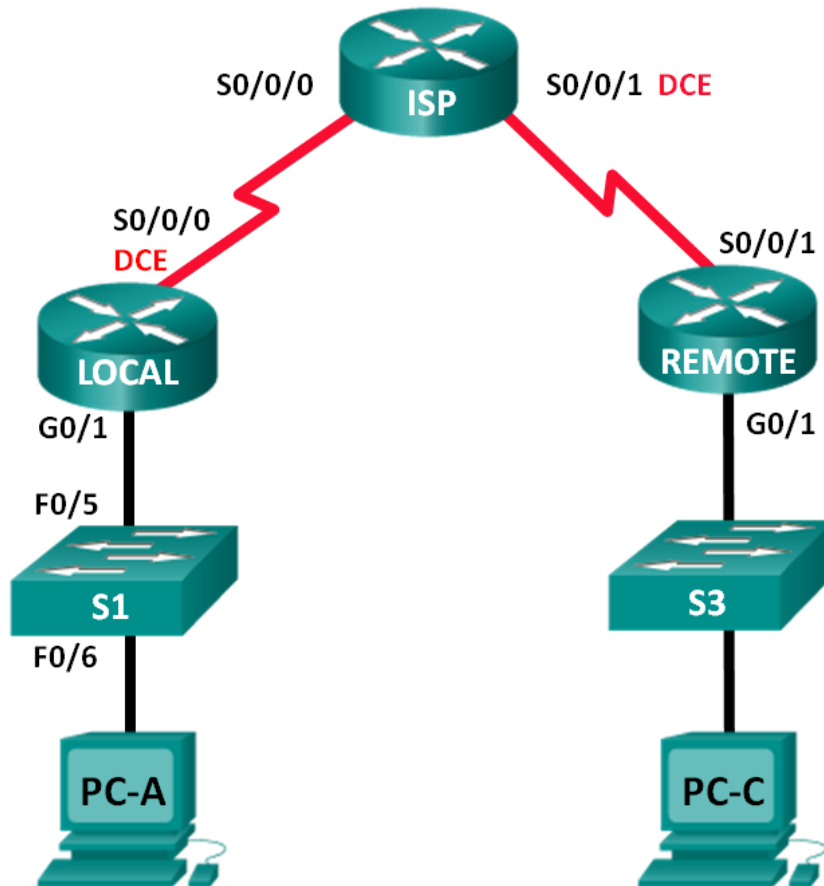
Reflection

3. Why can the same link-local address, FE80::1, be assigned to both Ethernet interfaces on R1?

4. What is the Subnet ID of the IPv6 unicast address 2001:db8:acad::aaaa:1234/64?

Lab 17 – Testing Network Connectivity with Ping and Traceroute

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
LOCAL	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
REMOTE	G0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.3.11	255.255.255.0	192.168.3.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Objectives

Part 1: Build and Configure the Network

Part 2: Use Ping Command for Basic Network Testing

Part 3: Use Tracert and Traceroute Commands for Basic Network Testing

Part 4: Troubleshoot the Topology

Background / Scenario

Ping and traceroute are two tools that are indispensable when testing TCP/IP network connectivity. Ping is a network administration utility used to test the reachability of a device on an IP network. This utility also measures the round-trip time for messages sent from the originating host to a destination computer. The ping utility is available on Windows, Unix-like operating systems (OS), and the Cisco Internetwork Operating System (IOS).

The traceroute utility is a network diagnostic tool for displaying the route and measuring the transit delays of packets travelling an IP network. The tracert utility is available on Windows, and a similar utility, traceroute, is available on Unix-like OS and Cisco IOS.

In this lab, the **ping** and **traceroute** commands are examined and command options are explored to modify the command behavior. Cisco devices and PCs are used in this lab for command exploration. Cisco routers will use Enhanced Interior Gateway Routing Protocol (EIGRP) to route packets between networks. The necessary Cisco device configurations are provided in this lab.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Build and Configure the Network

In Part 1, you will set up the network in the topology and configure the PCs and Cisco devices. The initial configurations for the routers and switches are provided for your reference. In this topology, EIGRP is used to route packets between networks.

Cable the network as shown in the topology.

Erase the configurations on the routers and switches, and reload the devices.

Configure PC IP addresses and default gateways according to the Addressing Table.

Configure the LOCAL, ISP, and REMOTE routers using the initial configurations provided below.

At the switch or router global config mode prompt, copy and paste the configuration for each device. Save the configuration to startup-config.

Initial configurations for the LOCAL router:

```
hostname LOCAL
no ip domain-lookup
interface s0/0/0
    ip address 10.1.1.1 255.255.255.252
    clock rate 56000
    no shutdown
interface g0/1
    ip add 192.168.1.1 255.255.255.0
    no shutdown
router eigrp 1
    network 10.1.1.0 0.0.0.3
    network 192.168.1.0 0.0.0.255
    no auto-summary
```

Initial configurations for ISP:

```
hostname ISP
no ip domain-lookup
interface s0/0/0
    ip address 10.1.1.2 255.255.255.252
    no shutdown
interface s0/0/1
    ip add 10.2.2.2 255.255.255.252
    clock rate 56000
    no shutdown
router eigrp 1
    network 10.1.1.0 0.0.0.3
    network 10.2.2.0 0.0.0.3
    no auto-summary
end
```

Initial configurations for REMOTE:

```
hostname REMOTE
no ip domain-lookup
interface s0/0/1
    ip address 10.2.2.1 255.255.255.252
    no shutdown
interface g0/1
    ip add 192.168.3.1 255.255.255.0
```

```

no shutdown
router eigrp 1
network 10.2.2.0 0.0.0.3
network 192.168.3.0 0.0.0.255
no auto-summary
end

```

Configure the S1 and S3 switches with the initial configurations.

Initial configurations for S1:

```

hostname S1
no ip domain-lookup
interface vlan 1
ip add 192.168.1.11 255.255.255.0
no shutdown
exit
ip default-gateway 192.168.1.1
end

```

Initial configurations for S3:

```

hostname S3
no ip domain-lookup
interface vlan 1
ip add 192.168.3.11 255.255.255.0
no shutdown
exit
ip default-gateway 192.168.3.1
end

```

Configure an IP host table on the LOCAL router.

The IP host table allows you to use a hostname to connect to a remote device rather than an IP address. The host table provides name resolution for the device with the following configurations. Copy and paste the following configurations for the LOCAL router. The configurations will allow you to use the hostnames for **ping** and **traceroute** commands on the LOCAL router.

```

ip host REMOTE 10.2.2.1 192.168.3.1
ip host ISP 10.1.1.2 10.2.2.2
ip host LOCAL 192.168.1.1 10.1.1.1
ip host PC-C 192.168.3.3
ip host PC-A 192.168.1.3
ip host S1 192.168.1.11
ip host S3 192.168.3.11
end

```

Use Ping Command for Basic Network Testing

In Part 2 of this lab, use the **ping** command to verify end-to-end connectivity. Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and then waiting for an ICMP response. It can record the round trip time and any packet loss.

You will examine the results with the **ping** command and the additional ping options that are available on Windows-based PCs and Cisco devices.

Test network connectivity from the LOCAL network using PC-A.

All the pings from PC-A to other devices in the topology should be successful. If they are not, check the topology and the cabling, as well as the configuration of the Cisco devices and the PCs.

- a. Ping from PC-A to its default gateway (LOCAL's GigabitEthernet 0/1 interface).

```
C:\Users\User1> ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

In this example, four (4) ICMP requests, 32 bytes each, were sent and the responses were received in less than one millisecond with no packet loss. The transmission and reply time increases as the ICMP requests and responses are processed by more devices during the journey to and from the final destination.

- b. From PC-A, ping the addresses listed in the following table and record the average round trip time and Time to Live (TTL).

Destination	Average Round Trip Time (ms)	TTL
192.168.1.1 (LOCAL)		
192.168.1.11 (S1)		
10.1.1.1 (LOCAL)		
10.1.1.2 (ISP)		
10.2.2.2 (ISP)		
10.2.2.1 (REMOTE)		
192.168.3.1 (REMOTE)		
192.168.3.11 (S3)		
192.168.3.3 (PC-C)		

Notice the average round trip time to 192.168.3.3 (PC-C). The time increased because the ICMP requests were processed by three routers before PC-A received the reply from PC-C.

```
C:\Users\User1> ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 40ms, Maximum = 41ms, Average = 40ms
```

Use extended ping commands on a PC.

The default **ping** command sends four requests at 32 bytes each. It waits 4,000 milliseconds (4 seconds) for each response to be returned before displaying the "Request timed out" message. The **ping** command can be fine tuned for troubleshooting a network.

- a. At the command prompt, type **ping** and press Enter.

```
C:\Users\User1> ping
```

```
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
          [-r count] [-s count] [[-j host-list] | [-k host-list]]
          [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name
```

Options:

-t	Ping the specified host until stopped. To see statistics and continue - type Control-Break; To stop - type Control-C.
-a	Resolve addresses to hostnames.
-n count	Number of echo requests to send.
-l size	Send buffer size.
-f	Set Don't Fragment flag in packet (IPv4-only).
-i TTL	Time To Live.
-v TOS	Type Of Service (IPv4-only. This setting has been deprecated and has no effect on the type of service field in the IP

Header).

-r count	Record route for count hops (IPv4-only).
-s count	Timestamp for count hops (IPv4-only).
-j host-list	Loose source route along host-list (IPv4-only).
-k host-list	Strict source route along host-list (IPv4-only).
-w timeout	Timeout in milliseconds to wait for each reply.
-R	Use routing header to test reverse route also (IPv6-only).
-S srcaddr	Source address to use.
-4	Force using IPv4.
-6	Force using IPv6.

- b. Using the **-t** option, ping PC-C to verify that PC-C is reachable.

```
C:\Users\User1> ping -t 192.168.3.3
```

```
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
```

```
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
```

To illustrate the results when a host is unreachable, disconnect the cable between the REMOTE router and the S3 switch, or shut down the GigabitEthernet 0/1 interface on the REMOTE router.

```
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
```

```
Reply from 192.168.1.3: Destination host unreachable.
```

```
Reply from 192.168.1.3: Destination host unreachable.
```

While the network is functioning correctly, the **ping** command can determine whether the destination responded and how long it took to receive a reply from the destination. If a network connectivity problem exists, the **ping** command displays an error message.

- c. Reconnect the Ethernet cable or enable the GigabitEthernet interface on the REMOTE router (using the **no shutdown** command) before moving onto the next step. After about 30 seconds, the ping should be successful again.

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
```

- d. Press **Ctrl+C** to stop the ping command.

Test network connectivity from the LOCAL network using Cisco devices.

The **ping** command is also available on Cisco devices. In this step, the **ping** command is examined using the LOCAL router and the S1 switch.

- a. Ping PC-C on the REMOTE network using the IP address of 192.168.3.3 from the LOCAL router.

```
LOCAL# ping 192.168.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/64/68 ms
```

The exclamation point (!) indicates that the ping was successful from the LOCAL router to PC-C. The round trip takes an average of 64 ms with no packet loss, as indicated by a 100% success rate.

- b. Because a local host table was configured on the LOCAL router, you can ping PC-C on the REMOTE network using the hostname configured from the LOCAL router.

```
LOCAL# ping PC-C
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/63/64 ms
```

- c. There are more options available for the **ping** command. At the CLI, type **ping** and press Enter. Input **192.168.3.3** or **PC-C** for the Target IP address. Press Enter to accept the default value for other options.

```
LOCAL# ping
Protocol [ip]:
Target IP address: PC-C
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/63/64 ms
```

- d. You can use an extended ping to observe when there is a network issue. Start the **ping** command to 192.168.3.3 with a repeat count of 500. Then, disconnect the cable between the REMOTE router and the S3 switch or shut down the GigabitEthernet 0/1 interface on the REMOTE router.

Reconnect the Ethernet cable or enable the GigabitEthernet interface on the REMOTE router after the exclamation points (!) have replaced by the letter U and periods (.). After about 30 seconds, the ping should be successful again. Press **Ctrl+Shift+6** to stop the **ping** command if desired.

Use the tracert command from PC-A to PC-C.

- a. At the command prompt, type **tracert 192.168.3.3**.

```
C:\Users\User1> tracert 192.168.3.3
Tracing route to PC-C [192.168.3.3]
Over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2    24 ms    24 ms    24 ms    10.1.1.2
  3    48 ms    48 ms    48 ms    10.2.2.1
  4    59 ms    59 ms    59 ms    PC-C [192.168.3.3]
```

Trace complete.

The tracert results indicates the path from PC-A to PC-C is from PC-A to LOCAL to ISP to REMOTE to PC-C. The path to PC-C traveled through three router hops to the final destination of PC-C.

Explore additional options for the tracert command.

- b. At the command prompt, type **tracert** and press Enter.

```
C:\Users\User1> tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
           [-R] [-S srcaddr] [-4] [-6] target_name

Options:
  -d                        Do not resolve addresses to hostnames.
  -h maximum_hops          Maximum number of hops to search for target.
  -j host-list              Loose source route along host-list (IPv4-only).
  -w timeout                Wait timeout milliseconds for each reply.
  -R                        Trace round-trip path (IPv6-only).
  -S srcaddr                Source address to use (IPv6-only).
  -4                        Force using IPv4.
  -6                        Force using IPv6.
```

- c. Use the **-d** option. Notice that the IP address of 192.168.3.3 is not resolved as PC-C.

```
C:\Users\User1> tracert -d 192.168.3.3
Tracing route to 192.168.3.3 over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2    24 ms    24 ms    24 ms    10.1.1.2
  3    48 ms    48 ms    48 ms    10.2.2.1
  4    59 ms    59 ms    59 ms    192.168.3.3
```

Trace complete.

Use the traceroute command from the LOCAL router to PC-C.

- d. At the command prompt, type **traceroute 192.168.3.3** or **traceroute PC-C** on the LOCAL router. The hostnames are resolved because a local IP host table was configured on the LOCAL router.

```
LOCAL# traceroute 192.168.3.3
Type escape sequence to abort.
```

```
Tracing the route to PC-C (192.168.3.3)
VRF info: (vrf in name/id, vrf out name/id)
  1 ISP (10.1.1.2) 16 msec 16 msec 16 msec
  2 REMOTE (10.2.2.1) 28 msec 32 msec 28 msec
  3 PC-C (192.168.3.3) 32 msec 28 msec 32 msec
```

```
LOCAL# traceroute PC-C
Type escape sequence to abort.
Tracing the route to PC-C (192.168.3.3)
VRF info: (vrf in name/id, vrf out name/id)
  1 ISP (10.1.1.2) 16 msec 16 msec 16 msec
  2 REMOTE (10.2.2.1) 28 msec 32 msec 28 msec
  3 PC-C (192.168.3.3) 32 msec 32 msec 28 msec
```

Use the traceroute command from the S1 switch to PC-C.

- e. On the S1 switch, type **traceroute 192.168.3.3**. The hostnames are not displayed in the traceroute results because a local IP host table was not configured on this switch.

```
S1# traceroute 192.168.3.3
Type escape sequence to abort.
Tracing the route to 192.168.3.3
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.1.1 1007 msec 0 msec 0 msec
  2 10.1.1.2 17 msec 17 msec 16 msec
  3 10.2.2.1 34 msec 33 msec 26 msec
  4 192.168.3.3 33 msec 34 msec 33 msec
```

The **traceroute** command has additional options. You can use the **?** or just press Enter after typing **traceroute** at the prompt to explore these options.

The following link provides more information regarding the **ping** and **traceroute** commands for a Cisco device:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800a6057.shtml

Troubleshoot the Topology

Erase the configurations on the REMOTE router.

Reload the REMOTE router.

Copy and paste the following configuration into the REMOTE router.

```
hostname REMOTE
no ip domain-lookup
interface s0/0/1
  ip address 10.2.2.1 255.255.255.252
  no shutdown
interface g0/1
  ip add 192.168.8.1 255.255.255.0
  no shutdown
router eigrp 1
  network 10.2.2.0 0.0.0.3
  network 192.168.3.0 0.0.0.255
  no auto-summary
end
```

From the LOCAL network, use ping and tracert or traceroute commands to troubleshoot and correct the problem on the REMOTE network.

- a. Use the **ping** and **tracert** commands from PC-A.

You can use the **tracert** command to determine end-to-end network connectivity. This tracert result indicates that PC-A can reach its default gateway of 192.168.1.1, but PC-A does not have network connectivity with PC-C.

```
C:\Users\User1> tracert 192.168.3.3
```

```
Tracing route to 192.168.3.3 over a maximum of 30 hops
 1    <1 ms    <1 ms    <1 ms    192.168.1.1
 2    192.168.1.1  reports: Destination host unreachable.
```

```
Trace complete.
```

One way to locate the network issue is to ping each hop in the network to PC-C. First determine if PC-A can reach the ISP router Serial 0/0/1 interface with an IP address of 10.2.2.2.

```
C:\Users\Utraser1> ping 10.2.2.2
```

```
Pinging 10.2.2.2 with 32 bytes of data:
Reply from 10.2.2.2: bytes=32 time=41ms TTL=254
Reply from 10.2.2.2: bytes=32 time=41ms TTL=254
Reply from 10.2.2.2: bytes=32 time=41ms TTL=254
Reply from 10.2.2.2: bytes=32 time=41ms TTL=254
```

```
Ping statistics for 10.2.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 21ms, Average = 20ms
```

The ping was successful to the ISP router. The next hop in the network is the REMOTE router. Ping the REMOTE router Serial 0/0/1 interface with an IP address of 10.2.2.1.

```
C:\Users\User1> ping 10.2.2.1
```

```
Pinging 10.2.2.1 with 32 bytes of data:
Reply from 10.2.2.1: bytes=32 time=41ms TTL=253
Reply from 10.2.2.1: bytes=32 time=41ms TTL=253
Reply from 10.2.2.1: bytes=32 time=41ms TTL=253
Reply from 10.2.2.1: bytes=32 time=41ms TTL=253
```

```
Ping statistics for 10.2.2.1:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 41ms, Average = 40ms
```

PC-A can reach the REMOTE router. Based on the successful ping results from PC-A to the REMOTE router, the network connectivity issue is with 192.168.3.0/24 network. Ping the default gateway to PC-C, which is the GigabitEthernet 0/1 interface of the REMOTE router.

```
C:\Users\User1> ping 192.168.3.1
```

```
Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
```

```
Ping statistics for 192.168.3.1:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

PC-A cannot reach the GigabitEthernet 0/1 interface of the REMOTE router, as displayed by the results from the **ping** command.

The S3 switch can also be pinged from PC-A to verify the location of the networking connectivity issue by typing **ping 192.168.3.11** at the command prompt. Because PC-A cannot reach GigabitEthernet 0/1 of the REMOTE router, PC-A probably cannot ping the S3 switch successfully, as indicated by the results below.

```
C:\Users\User1> ping 192.168.3.11
```

```
Pinging 192.168.3.11 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
```

```
Ping statistics for 192.168.3.11:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

The tracert and ping results conclude that PC-A can reach the LOCAL, ISP, and REMOTE routers, but not PC-C or the S3 switch, nor the default gateway for PC-C.

- b. Use the **show** commands to examine the running configurations for the the REMOTE router.

```
REMOTE# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down down
GigabitEthernet0/0	unassigned	YES	unset	administratively down down
GigabitEthernet0/1	192.168.8.1	YES	manual	up up
Serial0/0/0	unassigned	YES	unset	administratively down down
Serial0/0/1	10.2.2.1	YES	manual	up up

```
REMOTE# show run
<output omitted>
interface GigabitEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  ip address 192.168.8.1 255.255.255.0
  duplex auto
  speed auto
!
interface Serial0/0/0
  no ip address
  shutdown
  clock rate 2000000
!
interface Serial0/0/1
  ip address 10.2.2.1 255.255.255.252
<output omitted>
```

The outputs of the **show run** and **show ip interface brief** commands indicate that the GigabitEthernet 0/1 interface is up/up, but was configured with an incorrect IP address.

- c. Correct the IP address for GigabitEthernet 0/1.

```
REMOTE# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
REMOTE(config)# interface GigabitEthernet 0/1
REMOTE(config-if)# ip address 192.168.3.1 255.255.255.0
```

- d. Verify that PC-A can ping and tracert to PC-C.

```
C:\Users\User1> ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=44ms TTL=125
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 40ms, Maximum = 44ms, Average = 41ms
```

```
C:\Users\User1> tracert 192.168.3.3
```

```
Tracing route to PC-C [192.168.3.3]  
Over a maximum of 30 hops:
```

1	<1 ms	<1 ms	<1 ms	192.168.1.1
2	24 ms	24 ms	24 ms	10.1.1.2
3	48 ms	48 ms	48 ms	10.2.2.1
4	59 ms	59 ms	59 ms	PC-C [192.168.3.3]

```
Trace complete.
```

Note: This can also be accomplished using **ping** and **tracert** commands from the CLI on the the LOCAL router and the S1 switch after verifying that there are no network connectivity issues on the 192.168.1.0/24 network.

Reflection

1. What could prevent ping or traceroute responses from reaching the originating device beside network connectivity issues?

2. If you ping a non-existent address on the remote network, such as 192.168.3.4, what is the message displayed by the **ping** command? What does this mean? If you ping a valid host address and receive this response, what should you check?

3. If you ping an address that does not exist in any network in your topology, such as 192.168.5.3, from a Windows-based PC, what is the message displayed by the **ping** command? What does this message indicate?

Lab 18 – Mapping the Internet

Objectives

Part 1: Test Network Connectivity Using Ping

Part 2: Trace a Route to a Remote Server Using Windows Tracert

Background

Route tracing computer software is a utility that lists the networks data has to traverse from the user's originating end device to a distant destination network.

This network tool is typically executed at the command line as:

```
tracert <destination network name or end device address>
```

(Microsoft Windows systems)

or

```
traceroute <destination network name or end device address>
```

(UNIX and similar systems)

Route tracing utilities allow a user to determine the path or routes as well as the delay across an IP network. Several tools exist to perform this function.

The **traceroute** (or **tracert**) tool is often used for network troubleshooting. By showing a list of routers traversed, it allows the user to identify the path taken to reach a particular destination on the network or across internetworks. Each router represents a point where one network connects to another network and through which the data packet was forwarded. The number of routers is known as the number of "hops" the data traveled from source to destination.

The displayed list can help identify data flow problems when trying to access a service such as a website. It can also be useful when performing tasks such as downloading data. If there are multiple websites (mirrors) available for the same data file, one can trace each mirror to get a good idea of which mirror would be the fastest to use.

Two trace routes between the same source and destination conducted some time apart may produce different results. This is due to the "meshed" nature of the interconnected networks that comprise the Internet and the Internet Protocols ability to select different pathways over which to send packets.

Command-line-based route tracing tools are usually embedded with the operating system of the end device.

Scenario

Using an Internet connection, you will use three route tracing utilities to examine the Internet pathway to destination networks. This activity should be performed on a computer that has Internet access and access to the command line. First, you will use the Windows embedded tracert utility.

Required Resources

1 PC (Windows 7 or 8 with Internet access)

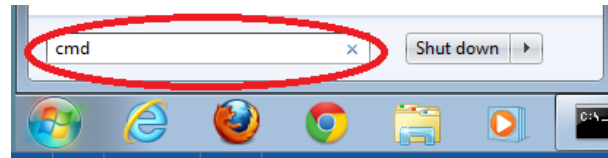
Test Network Connectivity Using Ping

Determine whether the remote server is reachable.

To trace the route to a distant network, the PC used must have a working connection to the Internet.

- a. The first tool we will use is ping. Ping is a tool used to test whether a host is reachable. Packets of information are sent to the remote host with instructions to reply. Your local PC measures whether a response is received to each packet, and how long it takes for those packets to cross the network. The name ping comes from active sonar technology in which a pulse of sound is sent underwater and bounced off of terrain or other ships.

- b. From your PC, click the **Windows Start** icon, type **cmd** in the **Search programs and files** box, and then press Enter.



- c. At the command-line prompt, type **ping www.cisco.com**.

```
C:\>ping www.cisco.com

Pinging e144.dsccb.akamaiedge.net [23.1.48.170] with 32 bytes of data:
Reply from 23.1.48.170: bytes=32 time=56ms TTL=57
Reply from 23.1.48.170: bytes=32 time=55ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57

Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

- d. The first output line displays the Fully Qualified Domain Name (FQDN) e144.dsccb.akamaiedge.net. This is followed by the IP address 23.1.48.170. Cisco hosts the same web content on different servers throughout the world (known as mirrors). Therefore, depending upon where you are geographically, the FQDN and the IP address will be different.
- e. From this portion of the output:

```
Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

Four pings were sent and a reply was received from each ping. Because each ping was responded to, there was 0% packet loss. On average, it took 54 ms (54 milliseconds) for the packets to cross the network. A millisecond is 1/1,000th of a second.

Streaming video and online games are two applications that suffer when there is packet loss, or a slow network connection. A more accurate determination of an Internet connection speed can be determined by sending 100 pings, instead of the default 4. Here is how to do that:

```
C:\>ping -n 100 www.cisco.com
```

And here is what the output from that looks like:

```
Ping statistics for 23.45.0.170:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 46ms, Maximum = 53ms, Average = 49ms
```

- f. Now ping Regional Internet Registry (RIR) websites located in different parts of the world:

For Africa:

```
C:\> ping www.afrinic.net
```

```
C:\>ping www.afrinic.net

Pinging www.afrinic.net [196.216.2.136] with 32 bytes of data:
Reply from 196.216.2.136: bytes=32 time=314ms TTL=111
Reply from 196.216.2.136: bytes=32 time=312ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111

Ping statistics for 196.216.2.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 312ms, Maximum = 314ms, Average = 313ms
```

For Australia:

```
C:\> ping www.apnic.net
```

```
C:\>ping www.apnic.net

Pinging www.apnic.net [202.12.29.194] with 32 bytes of data:
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=287ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49

Ping statistics for 202.12.29.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 286ms, Maximum = 287ms, Average = 286ms
```

For Europe:

```
C:\> ping www.ripe.net
```

```
C:\>ping www.ripe.net

Pinging www.ripe.net [193.0.6.139] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 193.0.6.139:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

For South America:

```
C:\> ping www.lacnic.net
```

```
C:\>ping www.lacnic.net

Pinging www.lacnic.net [200.3.14.147] with 32 bytes of data:
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=157ms TTL=51

Ping statistics for 200.3.14.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 157ms, Maximum = 158ms, Average = 157ms
```

All these pings were run from a computer located in the United States. What happens to the average ping time in milliseconds when data is traveling within the same continent (North America) as compared to data from North America traveling to different continents?

What is interesting about the pings that were sent to the European website?

Trace a Route to a Remote Server Using Tracert

Determine what route across the Internet traffic takes to the remote server.

Now that basic reachability has been verified by using the ping tool, it is helpful to look more closely at each network segment that is crossed. To do this, the **tracert** tool will be used.

- a. At the command-line prompt, type **tracert www.cisco.com**.

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    dslrouter.westell.com [192.168.1.1]
  2  38 ms     38 ms     37 ms     10.18.20.1
  3  37 ms     37 ms     37 ms     G3-0-9-2204.ALBVNY-LCR-02.verizon-gni.net [130.81.196.190]
  4  43 ms     43 ms     42 ms     so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81.22.46]
  5  43 ms     43 ms     65 ms     0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6  45 ms     45 ms     45 ms     0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7  46 ms     48 ms     46 ms     TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]
  8  45 ms     45 ms     45 ms     a23-1-144-170.deploy.akamaitechnologies.com [23.1.144.170]

Trace complete.
```

- b. Save the tracert output in a text file as follows:
- 1) Right-click the title bar of the Command Prompt window and choose **Edit > Select All**.
 - 2) Right-click the title bar of the Command Prompt window again and choose **Edit > Copy**.
 - 3) Open the **Windows Notepad** program: **Windows Start** icon > **All Programs > Accessories > Notepad**.
 - 4) To paste the output into Notepad, choose **Edit > Paste**.
 - 5) Choose **File > Save As** and save the Notepad file to your desktop as **tracert1.txt**.

- c. Run **tracert** for each destination website and save the output in sequentially numbered files.

```
C:\> tracert www.afrinic.net
C:\> tracert www.lacnic.net
```

- d. Interpreting **tracert** outputs.

Routes traced can go through many hops and a number of different Internet Service Providers (ISPs), depending on the size of your ISP, and the location of the source and destination hosts. Each “hop” represents a router. A router is a specialized type of computer used to direct traffic across the Internet. Imagine taking an automobile trip across several countries using many highways. At different

points in the trip, you come to a fork in the road in which you have the option to select from several different highways. Now further imagine that there is a device at each fork in the road that directs you to take the correct highway to your final destination. That is what a router does for packets on a network.

Because computers talk in numbers, rather than words, routers are uniquely identified using IP addresses (numbers with the format x.x.x.x). The **tracert** tool shows you what path through the network a packet of information takes to reach its final destination. The **tracert** tool also gives you an idea of how fast traffic is going on each segment of the network. Three packets are sent to each router in the path, and the return time is measured in milliseconds. Now use this information to analyze the **tracert** results to www.cisco.com. Below is the entire traceroute:

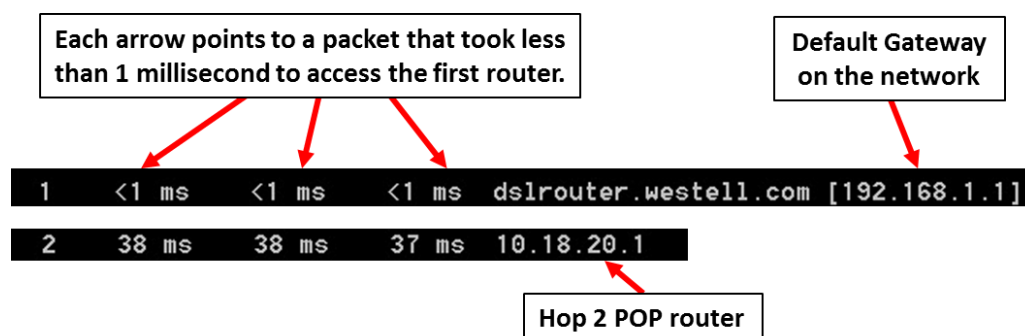
```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    dslrouter.westell.com [192.168.1.1]
  2  38 ms    38 ms    37 ms    10.18.20.1
  3  37 ms    37 ms    37 ms    G3-0-9-2204.ALBVNY-LCR-02.verizon-gni.net [130.81.196.190]
  4  43 ms    43 ms    42 ms    so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81.22.46]
  5  43 ms    43 ms    65 ms    0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6  45 ms    45 ms    45 ms    0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7  46 ms    48 ms    46 ms    TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]
  8  45 ms    45 ms    45 ms    a23-1-144-170.deploy.akamaitechnologies.com [23.1.144.170]

Trace complete.
```

Below is the breakdown:



In the example output shown above, the tracert packets travel from the source PC to the local router default gateway (hop 1: 192.168.1.1) to the ISPs Point of Presence (POP) router (hop 2: 10.18.20.1). Every ISP has numerous POP routers. These POP routers are at the edge of the ISP's network and are the means by which customers connect to the Internet. The packets travel along the Verizon network for two hops and then jump to a router that belongs to alter.net. This could mean that the packets have traveled to another ISP. This is significant because sometimes there is packet loss in the transition between ISPs, or sometimes one ISP is slower than another. How could we determine if alter.net is another ISP or the same ISP?

- e. There is an Internet tool known as whois. The whois tool allows us to determine who owns a domain name. A web-based whois tool is found at <http://whois.domaintools.com/>. This domain is also owned by Verizon according to the web-based whois tool.

```

Registrant:
Verizon Business Global LLC
Verizon Business Global LLC
One Verizon Way
Basking Ridge NJ 07920
US
domainlegalcontact@verizon.com +1.7033513164 Fax: +1.7033513669

Domain Name: alter.net

```

To summarize, Internet traffic starts at a home PC and travels through the home router (hop 1). It then connects to the ISP and travels through its network (hops 2-7) until it arrives at the remote server (hop 8). This is a relatively unusual example in which there is only one ISP involved from start to finish. It is typical to have two or more ISP involved as displayed in the following examples.

- f. Now examine an example that involves Internet traffic crossing multiple ISPs. Below is the tracert for www.afrinic.net:

```

C:\>tracert www.afrinic.net

Tracing route to www.afrinic.net [196.216.2.136]
over a maximum of 30 hops:

  1    1 ms    <1 ms    <1 ms    dslrouter.westell.com [192.168.1.1]
  2   39 ms   38 ms   37 ms   10.18.20.1
  3   40 ms   38 ms   39 ms   G4-0-0-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.197.182]
  4   44 ms   43 ms   43 ms   so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5   43 ms   43 ms   42 ms   0.so-4-0-0.XT2.NYC4.ALTER.NET [152.63.9.249]
  6   43 ms   71 ms   43 ms   0.ae4.BR3.NYC4.ALTER.NET [152.63.16.185]
  7   47 ms   47 ms   47 ms   te-7-3-0.edge2.NewYork2.level3.net [4.68.111.137
]
  8   43 ms   55 ms   43 ms   vlan51.ebr1.NewYork2.Level3.net [4.69.138.222]
  9   52 ms   51 ms   51 ms   ae-3-3.ebr2.Washington1.Level3.net [4.69.132.89]

10  130 ms   132 ms   132 ms   ae-42-42.ebr2.Paris1.Level3.net [4.69.137.53]
11  139 ms   145 ms   140 ms   ae-46-46.ebr1.Frankfurt1.Level3.net [4.69.143.13
7]
12  148 ms   140 ms   152 ms   ae-91-91.csw4.Frankfurt1.Level3.net [4.69.140.14
]
13  144 ms   144 ms   146 ms   ae-92-92.ebr2.Frankfurt1.Level3.net [4.69.140.29
]
14  151 ms   150 ms   150 ms   ae-23-23.ebr2.London1.Level3.net [4.69.148.193]
15  150 ms   150 ms   150 ms   ae-58-223.csw2.London1.Level3.net [4.69.153.138]
16  156 ms   156 ms   156 ms   ae-227-3603.edge3.London1.Level3.net [4.69.166.1
54]
17  157 ms   159 ms   160 ms   195.50.124.34
18  353 ms   340 ms   341 ms   168.209.201.74
19  333 ms   333 ms   332 ms   csw4-pk1-gi1-1.ip.isnet.net [196.26.0.101]
20  331 ms   331 ms   331 ms   196.37.155.180
21  318 ms   316 ms   318 ms   fa1-0-1.ar02.jnb.afrinic.net [196.216.3.132]
22  332 ms   334 ms   332 ms   196.216.2.136

Trace complete.

```

What happens at hop 7? Is level3.net the same ISP as hops 2-6, or a different ISP? Use the whois tool to answer this question.

What happens in hop 10 to the amount of time it takes for a packet to travel between Washington D.C. and Paris, as compared with the earlier hops 1-9?

What happens in hop 18? Do a whois lookup on 168.209.201.74 using the whois tool. Who owns this network?

g. Type **tracert www.lacnic.net**.

```
C:\>tracert www.lacnic.net

Tracing route to www.lacnic.net [200.3.14.147]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    dslrouter.westell.com [192.168.1.1]
  1  38 ms     38 ms     37 ms     10.18.20.1
  2  38 ms     38 ms     39 ms     G3-0-9-2204.ALBVNY-LCR-02.verizon-gni.net [130.81.196.190]
  3  42 ms     43 ms     42 ms     so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81.22.46]
  4  82 ms     47 ms     47 ms     0.ae2.BR3.NYC4.ALTER.NET [152.63.16.49]
  5  46 ms     47 ms     56 ms     204.255.168.194
  6  157 ms    158 ms    157 ms    ge-1-1-0.100.gw1.gc.registro.br [159.63.48.38]
  7  156 ms    157 ms    157 ms    xe-5-0-1-0.core1.gc.registro.br [200.160.0.174]
  8  161 ms    161 ms    161 ms    xe-4-0-0-0.core2.nu.registro.br [200.160.0.164]
  9  158 ms    157 ms    157 ms    ae0-0.ar3.nu.registro.br [200.160.0.249]
 10 176 ms    176 ms    170 ms    gw02.lacnic.registro.br [200.160.0.213]
 11 158 ms    158 ms    158 ms    200.3.12.36
 12 157 ms    158 ms    157 ms    200.3.14.147
 13

Trace complete.
```

What happens in hop 7?

Reflection

What are the functional differences between the commands ping and tracert?

Lab 19 – Accessing Network Devices with SSH

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure the Router for SSH Access

Part 3: Configure the Switch for SSH Access

Part 4: SSH from the CLI on the Switch

Background / Scenario

In the past, Telnet was the most common network protocol used to remotely configure network devices. Telnet does not encrypt the information between the client and server. This allows a network sniffer to intercept passwords and configuration information.

Secure Shell (SSH) is a network protocol that establishes a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals. SSH is most often used to log in to a remote device and execute commands; however, it can also transfer files using the associated Secure FTP (SFTP) or Secure Copy (SCP) protocols.

The network devices that are communicating must be configured to support SSH in order for SSH to function. In this lab, you will enable the SSH server on a router and then connect to that router using a PC with an SSH client installed. On a local network, the connection is normally made using Ethernet and IP.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)

- 1 PC (Windows 7 or 8 with terminal emulation program, such as Tera Term, and Wireshark installed)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords on the router.

Cable the network as shown in the topology.

Initialize and reload the router and switch.

Configure the router.

- Console into the router and enable privileged EXEC mode.
- Enter configuration mode.
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.
- Assign **cisco** as the VTY password and enable login.
- Encrypt the plaintext passwords.
- Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.
- Configure and activate the G0/1 interface on the router using the information contained in the Addressing Table.
- Save the running configuration to the startup configuration file.

Configure PC-A.

- Configure PC-A with an IP address and subnet mask.
- Configure a default gateway for PC-A.

Verify network connectivity.

Ping R1 from PC-A. If the ping fails, troubleshoot the connection.

Configure the Router for SSH Access

Using Telnet to connect to a network device is a security risk because all information is transmitted in a clear text format. SSH encrypts the session data and provides device authentication, which is why SSH is recommended for remote connections. In Part 2, you will configure the router to accept SSH connections over the VTY lines.

Configure device authentication.

The device name and domain are used as part of the crypto key when it is generated. Therefore, these names must be entered prior to issuing the **crypto key** command.

- Configure device name.
`Router(config)# hostname R1`
- Configure the domain for the device.
`R1(config)# ip domain-name ccna-lab.com`

Configure the encryption key method.

```
R1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

R1(config)#
*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Configure a local database username.

```
R1(config)# username admin privilege 15 secret adminpass
```

Note: A privilege level of 15 gives the user administrator rights.

Enable SSH on the VTY lines.

- Enable Telnet and SSH on the inbound VTY lines using the **transport input** command.

```
R1(config)# line vty 0 4
R1(config-line)# transport input telnet ssh
```

- Change the login method to use the local database for user verification.

```
R1(config-line)# login local
R1(config-line)# end
R1#
```

Save the running configuration to the startup configuration file.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Establish an SSH connection to the router.

- Start Tera Term from PC-A.
- Establish an SSH session to R1. Use the username **admin** and password **adminpass**. You should be able to establish an SSH session with R1.

Configure the Switch for SSH Access

In Part 3, you will configure the switch in the topology to accept SSH connections. After the switch has been configured, establish an SSH session using Tera Term.

Configure the basic settings on the switch.

- Console into the switch and enable privileged EXEC mode.
- Enter configuration mode.
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.

- f. Assign **cisco** as the VTY password and enable login.
- g. Encrypt the plain text passwords.
- h. Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.
- i. Configure and activate the VLAN 1 interface on the switch according to the Addressing Table.
- j. Save the running configuration to the startup configuration file.

Configure the switch for SSH connectivity.

Use the same commands that you used to configure SSH on the router in Part 2 to configure SSH for the switch.

- a. Configure the device name as listed in the Addressing Table.
- b. Configure the domain for the device.

```
S1(config)# ip domain-name ccna-lab.com
```
- c. Configure the encryption key method.

```
S1(config)# crypto key generate rsa modulus 1024
```
- d. Configure a local database username.

```
S1(config)# username admin privilege 15 secret adminpass
```
- e. Enable Telnet and SSH on the VTY lines.

```
S1(config)# line vty 0 15
S1(config-line)# transport input telnet ssh
```
- f. Change the login method to use the local database for user verification.

```
S1(config-line)# login local
S1(config-line)# end
```

Establish an SSH connection to the switch.

Start Tera Term from PC-A, and then SSH to the SVI interface on S1.

Are you able to establish an SSH session with the switch?

SSH From the CLI on the Switch

The SSH client is built into the Cisco IOS and can be run from the CLI. In Part 4, you will SSH to the router from the CLI on the switch.

View the parameters available for the Cisco IOS SSH client.

Use the question mark (?) to display the parameter options available with the **ssh** command.

```
S1# ssh ?
-c      Select encryption algorithm
-l      Log in using this user name
-m      Select HMAC algorithm
-o      Specify options
-p      Connect to this port
-v      Specify SSH Protocol Version
-vrf    Specify vrf name
WORD    IP address or hostname of a remote system
```

SSH to R1 from S1.

- a. You must use the **-l admin** option when you SSH to R1. This allows you to log in as user **admin**. When prompted, enter **adminpass** for the password.

```
S1# ssh -l admin 192.168.1.1
Password:
*****
Warning: Unauthorized Access is Prohibited!
*****
```

```
R1#
```

- b. You can return to S1 without closing the SSH session to R1 by pressing **Ctrl+Shift+6**. Release the **Ctrl+Shift+6** keys and press **x**. The switch privileged EXEC prompt displays.

```
R1#
```

```
S1#
```

- c. To return to the SSH session on R1, press Enter on a blank CLI line. You may need to press Enter a second time to see the router CLI prompt.

```
S1#
[Resuming connection 1 to 192.168.1.1 ... ]
```

```
R1#
```

- d. To end the SSH session on R1, type **exit** at the router prompt.

```
R1# exit
```

```
[Connection to 192.168.1.1 closed by foreign host]
```

```
S1#
```

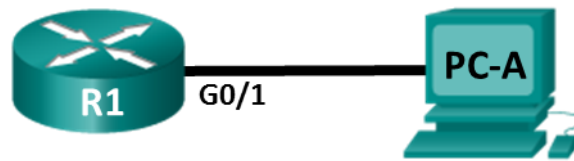
What versions of SSH are supported from the CLI?

Reflection

How would you provide multiple users, each with their own username, access to a network device?

Lab 20 – Examining Telnet and SSH in Wireshark

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

- Part 1: Configure the Devices for SSH Access
- Part 2: Examine a Telnet Session with Wireshark
- Part 3: Examine a SSH Session with Wireshark

Background / Scenario

In this lab, you will configure a router to accept SSH connectivity, and use Wireshark to capture and view Telnet and SSH sessions. This will demonstrate the importance of encryption with SSH.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 PC (Windows 7 or 8 with terminal emulation program, such as Tera Term, and Wireshark installed)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Configure the Devices for SSH Access

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords on the router.

Cable the network as shown in the topology.

Initialize and reload the router.

Configure the basic settings on the router.

- a. Console into the router and enable privileged EXEC mode.
- b. Enter configuration mode.
- c. Configure device name as listed in the Addressing Table.
- d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- e. Assign **class** as the privileged EXEC encrypted password.
- f. Assign **cisco** as the console password and enable login.
- g. Assign **cisco** as the VTY password and enable login.
- h. Encrypt the plain text passwords.
- i. Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.
- j. Configure and activate the G0/1 interface using the information contained in the Addressing Table.

Configure R1 for SSH access.

- a. Configure the domain for the device.

```
R1(config)# ip domain-name ccna-lab.com
```
- b. Configure the encryption key method.

```
R1(config)# crypto key generate rsa modulus 1024
```
- c. Configure a local database username.

```
R1(config)# username admin privilege 15 secret adminpass
```
- d. Enable Telnet and SSH on the VTY lines.

```
R1(config)# line vty 0 4  
R1(config-line)# transport input telnet ssh
```
- e. Change the login method to use the local database for user verification.

```
R1(config-line)# login local  
R1(config-line)# end
```

Save the running configuration to the startup configuration file.

Configure PC-A.

- a. Configure PC-A with an IP address and subnet mask.
- b. Configure a default gateway for PC-A.

Verify network connectivity.

Ping R1 from PC-A. If the ping fails, troubleshoot the connection.

Examine a Telnet Session with Wireshark

In Part 2, you will use Wireshark to capture and view the transmitted data of a Telnet session on the router. You will use Tera Term to telnet to R1, sign in, and then issue the **show run** command on the router.

Note: If a Telnet/SSH client software package is not installed on your PC, you must install one before continuing. Two popular freeware Telnet/SSH packages are Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) and PuTTY (www.putty.org).

Note: Telnet is not available from the command prompt in Windows 7, by default. To enable Telnet for use in the command prompt window, click **Start > Control Panel > Programs > Programs and Features > Turn Windows features on or off**. Click the **Telnet Client** check box, and then click **OK**.

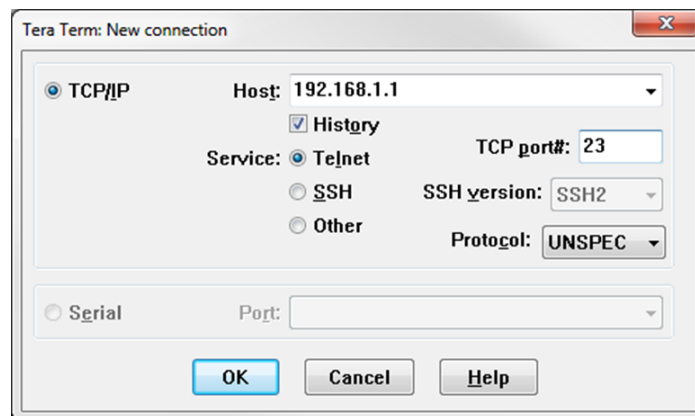
Capture data.

- Start Wireshark.
- Start capturing data on the LAN interface.

Note: If you are unable to start the capture on the LAN interface, you may need to open Wireshark using the **Run as Administrator** option.

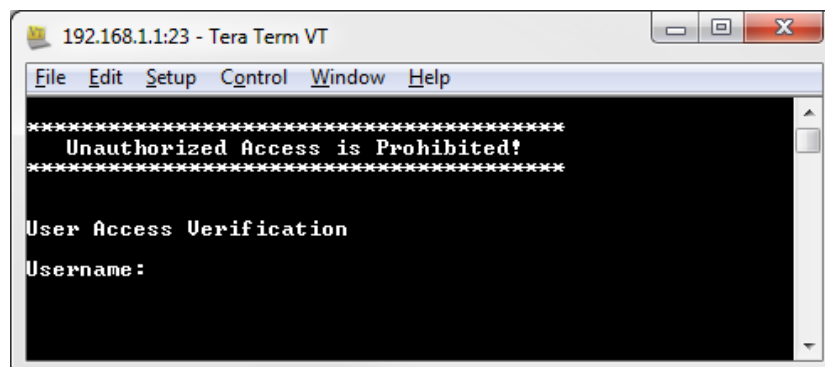
Start a Telnet session to the router.

- Open Tera Term and select the **Telnet** Service radio button and in the Host field, enter **192.168.1.1**.



What is the default TCP port for Telnet sessions? _____

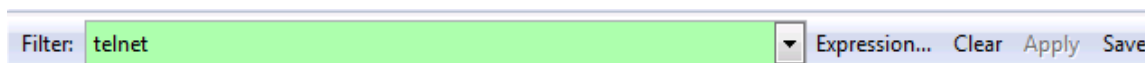
- At the Username: prompt, enter **admin** and at the Password: prompt, enter **adminpass**. These prompts are generated because you configured the VTY lines to use the local database with the **login local** command.



- Issue the **show run** command.
R1# **show run**
- Enter **exit** to exit the Telnet session and out of Tera Term.
R1# **exit**

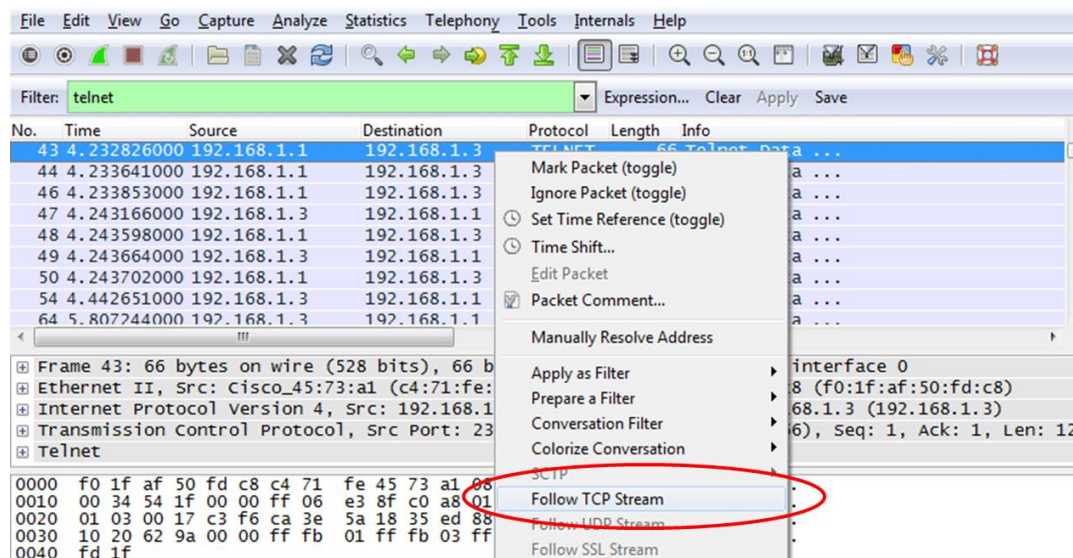
Stop the Wireshark capture.

Apply a Telnet filter on the Wireshark capture data.

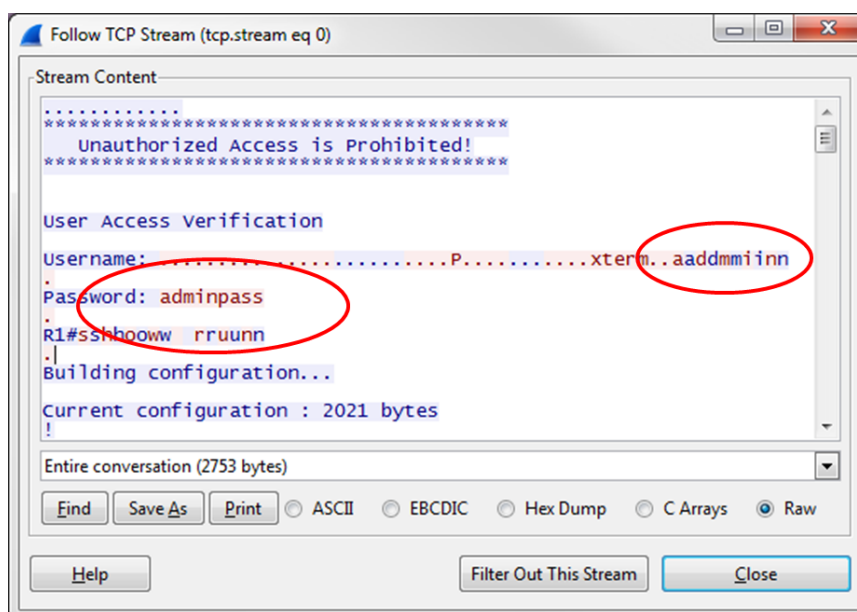


Use the Follow TCP Stream feature in Wireshark to view the Telnet session.

- a. Right-click one of the **Telnet** lines in the **Packet list** section of Wireshark, and from the drop-down list, select **Follow TCP Stream**.



- b. The Follow TCP Stream window displays the data for your Telnet session with the router. The entire session is displayed in clear text, including your password. Notice that the username and **show run** command that you entered are displayed with duplicate characters. This is caused by the echo setting in Telnet to allow you to view the characters that you type on the screen.



- c. After you have finished reviewing your Telnet session in the **Follow TCP Stream** window, click **Close**.

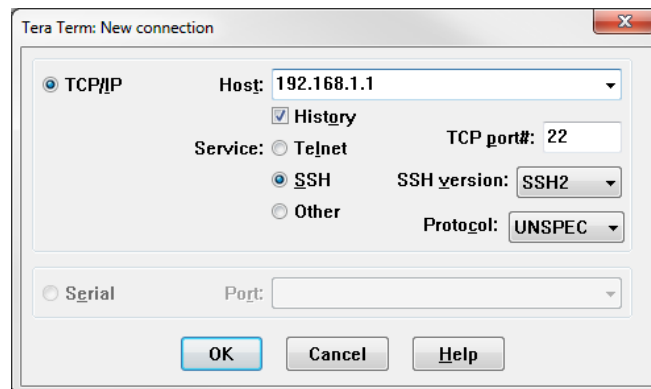
Examine an SSH Session with Wireshark

In Part 4, you will use the Tera Term software to establish an SSH session with the router. Wireshark will be used to capture and view the data of this SSH session.

Open Wireshark and start capturing data on the LAN interface.

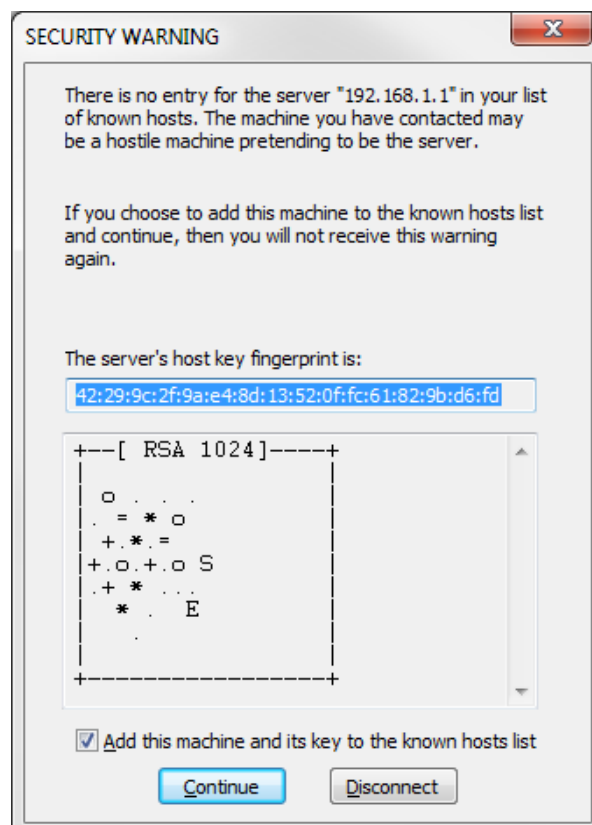
Start an SSH session on the router.

- a. Open Tera Term and enter the G0/1 interface IP address of R1 in the Host: field of the Tera Term: New Connection window. Ensure that the **SSH** radio button is selected and then click **OK** to connect to the router.

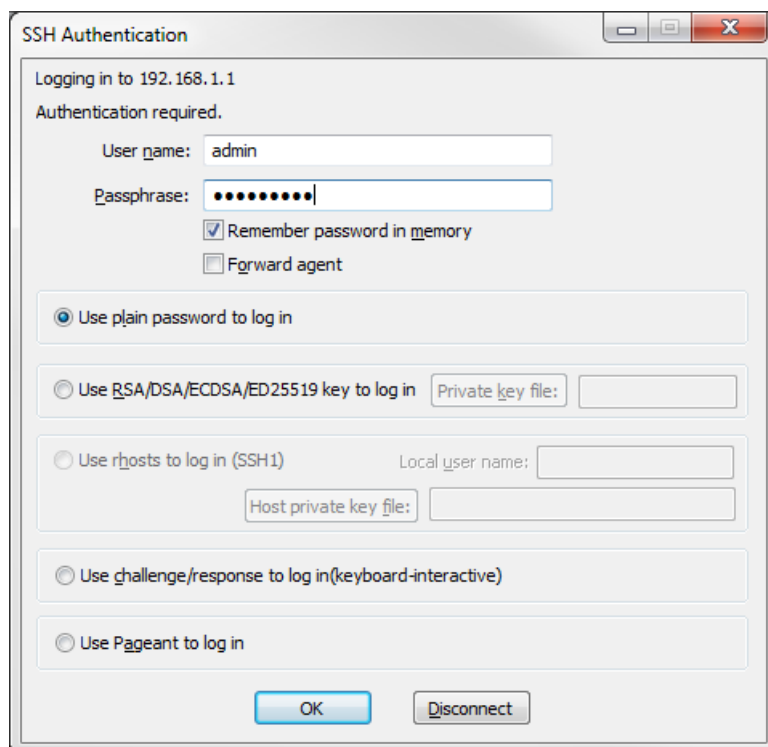


What is the default TCP port used for SSH sessions? _____

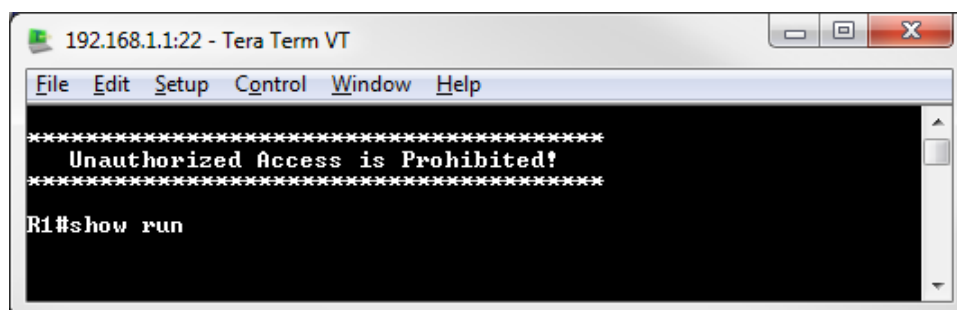
- b. The first time you establish a SSH session to a device, a **SECURITY WARNING** is generated to let you know that you have not connected to this device before. This message is part of the authentication process. Read the security warning and click **Continue**.



In the SSH Authentication window, enter **admin** for the username and **adminpass** for the passphrase. Click **OK** to sign into the router.



- c. You have established an SSH session on the router. The Tera Term software looks very similar to a command window. At the command prompt, issue the **show run** command.

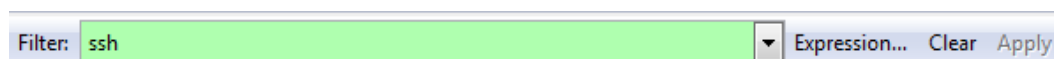


- d. Exit the SSH session by issuing the **exit** command.

R1# **exit**

Stop the Wireshark capture.

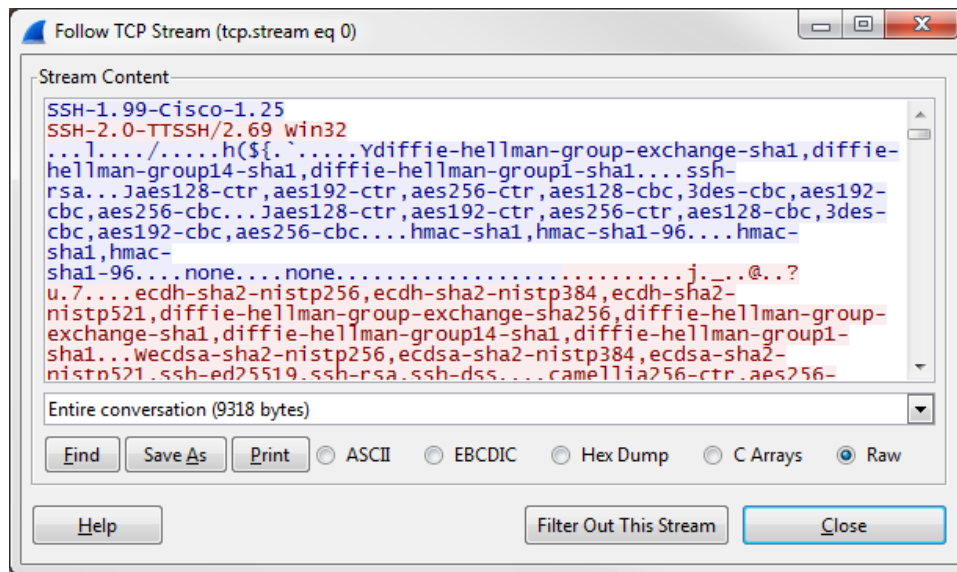
Apply an SSH filter on the Wireshark Capture data.



Use the Follow TCP Stream feature in Wireshark to view the SSH session.

- a. Right-click one of the **SSHv2** lines in the **Packet list** section of Wireshark, and in the drop-down list, select the **Follow TCP Stream** option.

- b. Examine the **Follow TCP Stream** window of your SSH session. The data has been encrypted and is unreadable. Compare the data in your SSH session to the data of your Telnet session.



Why is SSH preferred over Telnet for remote connections?

- c. After examining your SSH session, click **Close**.
- d. Close Wireshark.

Reflection

How would you provide multiple users, each with their own username, access to a network device?

Lab 21 – Securing Network Devices

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure Basic Security Measures on the Router

Part 3: Configure Basic Security Measures on the Switch

Background / Scenario

It is recommended that all network devices be configured with at least a minimum set of best practice security commands. This includes end user devices, servers, and network devices, such as routers and switches.

In this lab, you will configure the network devices in the topology to accept SSH sessions for remote management. You will also use the IOS CLI to configure common, basic best practice security measures. You will then test the security measures to verify that they are properly implemented and working correctly.

Note: The routers used with CCNA hands-on labs are Cisco 1941 ISRs with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS software, release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords on the devices.

Cable the network as shown in the topology.

Attach the devices shown in the topology and cable as necessary.

Initialize and reload the router and switch.

Configure the router and switch.

- Console into the device and enable privileged EXEC mode.
- Assign the device name according to the Addressing Table.
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.
- Assign **cisco** as the VTY password and enable login.
- Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
- Configure and activate the G0/1 interface on the router using the information contained in the Addressing Table.
- Configure the default SVI on the switch with the IP address information according to the Addressing Table.
- Save the running configuration to the startup configuration file.

Configure Basic Security Measures on the Router

Encrypt the clear text passwords.

```
R1(config)# service password-encryption
```

Strengthen passwords.

An administrator should ensure that passwords meet the standard guidelines for strong passwords. These guidelines could include combining letters, numbers and special characters in the password and setting a minimum length.

Note: Best practice guidelines require the use of strong passwords, such as those shown here, in a production environment. However, the other labs in this course use the cisco and class passwords for ease in performing the labs.

- Change the privileged EXEC encrypted password to meet guidelines.

```
R1(config)# enable secret Enablep@55
```

- Require that a minimum of 10 characters be used for all passwords.

```
R1(config)# security passwords min-length 10
```

Enable SSH connections.

- Assign the domain name as **CCNA-lab.com**.

```
R1(config)# ip domain-name CCNA-lab.com
```

- b. Create a local user database entry to use when connecting to the router via SSH. The password should meet strong password standards, and the user should have user EXEC access. If privilege level is not specified in the command, the user will have user EXEC (level 15) access by default.

```
R1(config)# username SSHadmin privilege 1 secret Admin1p@55
```

- c. Configure the transport input for the VTY lines so that they accept SSH connections, but do not allow Telnet connections.

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
```

- d. The VTY lines should use the local user database for authentication.

```
R1(config-line)# login local
R1(config-line)# exit
```

- e. Generate a RSA crypto key using a modulus of 1024 bits.

```
R1(config)# crypto key generate rsa modulus 1024
```

Secure the console and VTY lines.

- a. You can set the router to log out of a connection that has been idle for a specified time. If a network administrator was logged into a networking device and was suddenly called away, this command automatically logs the user out after the specified time. The following commands cause the line to log out after five minutes of inactivity.

```
R1(config)# line console 0
R1(config-line)# exec-timeout 5 0
R1(config-line)# line vty 0 4
R1(config-line)# exec-timeout 5 0
R1(config-line)# exit
R1(config)#
```

- b. The following command impedes brute force login attempts. The router blocks login attempts for 30 seconds if someone fails two attempts within 120 seconds. This timer is set especially low for the purpose of this lab.

```
R1(config)# login block-for 30 attempts 2 within 120
```

What does the **2 within 120** mean in the above command?

What does the **block-for 30** mean in the above command?

Verify that all unused ports are disabled.

Router ports are disabled by default, but it is always prudent to verify that all unused ports are in an administratively down state. This can be quickly checked by issuing the **show ip interface brief** command. Any unused ports that are not in an administratively down state should be disabled using the **shutdown** command in interface configuration mode.

R1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status
Embedded-Service-Engine0/0	unassigned	YES	NVRAM	administratively down down
GigabitEthernet0/0	unassigned	YES	NVRAM	administratively down down
GigabitEthernet0/1	192.168.1.1	YES	manual	up up
Serial0/0/0	unassigned	YES	NVRAM	administratively down down
Serial0/0/1	unassigned	YES	NVRAM	administratively down down

R1#

Verify that your security measures have been implemented correctly.

- a. Use Tera Term to telnet to R1.

Does R1 accept the Telnet connection? Explain.

- b. Use Tera Term to SSH to R1.

Does R1 accept the SSH connection? _____

- c. Intentionally mistype the user and password information to see if login access is blocked after two attempts.

What happened after you failed to login the second time?

- d. From your console session on the router, issue the **show login** command to view the login status. In the example below, the **show login** command was issued within the 30 second login blocking period and shows that the router is in Quiet-Mode. The router will not accept any login attempts for 14 more seconds.

R1# **show login**

```
A default login delay of 1 second is applied.  
No Quiet-Mode access list has been configured.
```

```
Router enabled to watch for login Attacks.  
If more than 2 login failures occur in 120 seconds or less,  
logins will be disabled for 30 seconds.
```

```
Router presently in Quiet-Mode.  
Will remain in Quiet-Mode for 14 seconds.  
Denying logins from all sources.
```

R1#

- e. After the 30 seconds has expired, SSH to R1 again and login using the **SSHadmin** username and **Admin1p@55** for the password.

After you successfully logged in, what was displayed? _____

- f. Enter privileged EXEC mode and use **Enablep@55** for the password.

If you mistype this password, are you disconnected from your SSH session after two failed attempts within 120 seconds? Explain.

- g. Issue the **show running-config** command at the privileged EXEC prompt to view the security settings you have applied.

Configure Basic Security Measures on the Switch

Encrypt the clear text passwords.

```
S1(config)# service password-encryption
```

Strengthen Passwords on the switch.

Change the privileged EXEC encrypted password to meet strong password guidelines.

```
S1(config)# enable secret Enablep@55
```

Note: The security **password min-length** command is not available on the 2960 switch.

Enable SSH Connections.

- a. Assign the domain-name as **CCNA-lab.com**

```
S1(config)# ip domain-name CCNA-lab.com
```

- b. Create a local user database entry for use when connecting to the switch via SSH. The password should meet strong password standards, and the user should have user EXEC access. If privilege level is not specified in the command, the user will have user EXEC (level 1) access by default.

```
S1(config)# username SSHadmin privilege 1 secret Admin1p@55
```

- c. Configure the transport input for the VTY lines to allow SSH connections but not allow Telnet connections.

```
S1(config)# line vty 0 15
```

```
S1(config-line)# transport input ssh
```

- d. The VTY lines should use the local user database for authentication.

```
S1(config-line)# login local
```

```
S1(config-line)# exit
```

- e. Generate an RSA crypto key using a modulus of 1024 bits.

```
S1(config)# crypto key generate rsa modulus 1024
```

Secure the console and VTY lines.

- a. Configure the switch to log out a line that has been idle for 10 minutes.

```
S1(config)# line console 0
```

```
S1(config-line)# exec-timeout 10 0
```

```
S1(config-line)# line vty 0 15
```

```
S1(config-line)# exec-timeout 10 0
```

```
S1(config-line)# exit
```

```
S1(config)#
```

- b. To impede brute force login attempts, configure the switch to block login access for 30 seconds if there are 2 failed attempts within 120 seconds. This timer is set especially low for the purpose of this lab.

```
S1(config)# login block-for 30 attempts 2 within 120
```

```
S1(config)# end
```

Verify all unused ports are disabled.

Switch ports are enabled, by default. Shut down all ports that are not in use on the switch.

- a. You can verify the switch port status using the **show ip interface brief** command.

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

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.11	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	down	down
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	down
FastEthernet0/20	unassigned	YES	unset	down	down
FastEthernet0/21	unassigned	YES	unset	down	down
FastEthernet0/22	unassigned	YES	unset	down	down
FastEthernet0/23	unassigned	YES	unset	down	down
FastEthernet0/24	unassigned	YES	unset	down	down
GigabitEthernet0/1	unassigned	YES	unset	down	down
GigabitEthernet0/2	unassigned	YES	unset	down	down

```
S1#
```

- b. Use the **interface range** command to shut down multiple interfaces at a time.

```
S1(config)# interface range f0/1-4 , f0/7-24 , g0/1-2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

- c. Verify that all inactive interfaces have been administratively shut down.

S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.11	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
FastEthernet0/2	unassigned	YES	unset	administratively down	down
FastEthernet0/3	unassigned	YES	unset	administratively down	down
FastEthernet0/4	unassigned	YES	unset	administratively down	down
FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	administratively down	down
FastEthernet0/8	unassigned	YES	unset	administratively down	down
FastEthernet0/9	unassigned	YES	unset	administratively down	down
FastEthernet0/10	unassigned	YES	unset	administratively down	down
FastEthernet0/11	unassigned	YES	unset	administratively down	down
FastEthernet0/12	unassigned	YES	unset	administratively down	down
FastEthernet0/13	unassigned	YES	unset	administratively down	down
FastEthernet0/14	unassigned	YES	unset	administratively down	down
FastEthernet0/15	unassigned	YES	unset	administratively down	down
FastEthernet0/16	unassigned	YES	unset	administratively down	down
FastEthernet0/17	unassigned	YES	unset	administratively down	down
FastEthernet0/18	unassigned	YES	unset	administratively down	down
FastEthernet0/19	unassigned	YES	unset	administratively down	down
FastEthernet0/20	unassigned	YES	unset	administratively down	down
FastEthernet0/21	unassigned	YES	unset	administratively down	down
FastEthernet0/22	unassigned	YES	unset	administratively down	down
FastEthernet0/23	unassigned	YES	unset	administratively down	down
FastEthernet0/24	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down

S1#

Verify that your security measures have been implemented correctly.

- Verify that Telnet has been disabled on the switch.
- SSH to the switch and intentionally mistype the user and password information to see if login access is blocked.
- After the 30 seconds has expired, SSH to S1 again and log in using the **SSHadmin** username and **Admin1p@55** for the password.
Did the banner appear after you successfully logged in? _____
- Enter privileged EXEC mode using **Enablep@55** as the password.
- Issue the **show running-config** command at the privileged EXEC prompt to view the security settings you have applied.

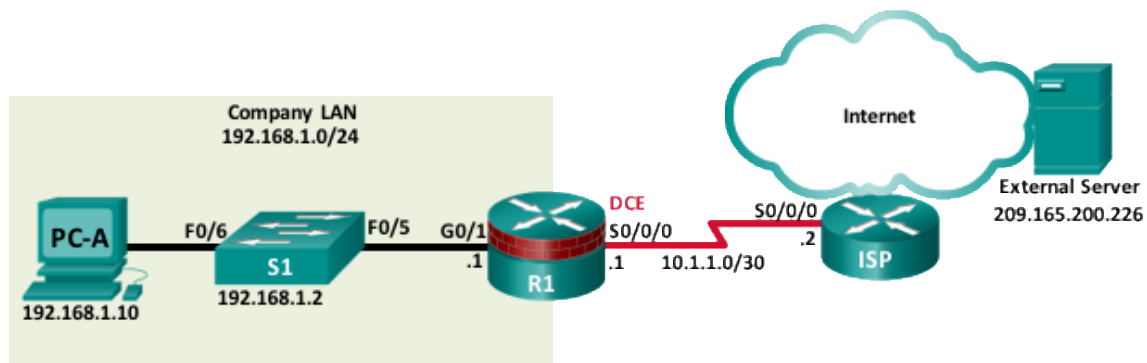
Reflection

- The **password cisco** command was entered for the console and VTY lines in your basic configuration in Part 1. When is this password used after the best practice security measures have been applied?

- Are preconfigured passwords shorter than 10 characters affected by the **security passwords min-length 10** command?

Lab 22 – Troubleshooting Connectivity Issues

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	Lo0	209.165.200.226	255.255.255.255	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objectives

Part 1: Identify the Problem

Part 2: Implement Network Changes

Part 3: Verify Full Functionality

Part 4: Document Findings and Configuration Changes

Background / Scenario

In this lab, the company that you work for is experiencing problems with their Local Area Network (LAN). You have been asked to troubleshoot and resolve the network issues. In Part 1, you will connect to devices on the LAN and use troubleshooting tools to identify the network issues, establish a theory of probable cause, and test that theory. In Part 2, you will establish a plan of action to resolve and implement a solution. In Part 3, you will verify full functionality has been restored. Part 4 provides space for you to document your troubleshooting findings along with the configuration changes that you made to the LAN devices.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions may be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Required Resources

- 2 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Ethernet and Serial cables as shown in the topology

Troubleshooting Configurations

The following settings must be configured on the devices shown in the topology. Paste the configurations onto the specified devices prior to starting the lab.

S1:

```
no ip domain-lookup
hostname S1
ip domain-name ccna-lab.com
username admin01 privilege 15 secret 9
$9$lJgfiLCHj.Xp/q$hA2w.oyQPTMhBGPeR.FZo3NZRJ9T1FdqvgRCFyBYnNs
interface FastEthernet0/1
shutdown
interface FastEthernet0/2
shutdown
interface FastEthernet0/3
shutdown
interface FastEthernet0/4
shutdown
interface FastEthernet0/5
duplex full
interface Vlan1
ip address 192.168.1.2 255.255.255.0
line vty 0 4
login local
transport input ssh
line vty 5 15
login local
transport input ssh
crypto key generate rsa general-keys modulus 1024
end
```

R1:

```
hostname R1
no ip domain-lookup
ip domain-name ccna-lab.com
username admin01 privilege 15 secret 9
$9$8a4jGjbPPpeeoE$WyPsIiOaYT4ATlJzrR6T9E6vIdESOGF.NYX53arPmtA
interface GigabitEthernet0/0
shutdown
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
duplex half
speed auto
no shutdown
interface Serial0/0/0
ip address 10.1.2.1 255.255.255.252
no shutdown
```

```
interface Serial0/0/1
  no ip address
  shutdown
line vty 0 4
  login local
  transport input ssh
crypto key generate rsa general-keys modulus 1024
end
```

ISP:

```
hostname ISP
no ip domain-lookup
interface Serial0/0/0
  ip address 10.1.1.2 255.255.255.252
  no shut
interface Lo0
  ip address 209.165.200.226 255.255.255.255
ip route 0.0.0.0 0.0.0.0 10.1.1.1
end
```

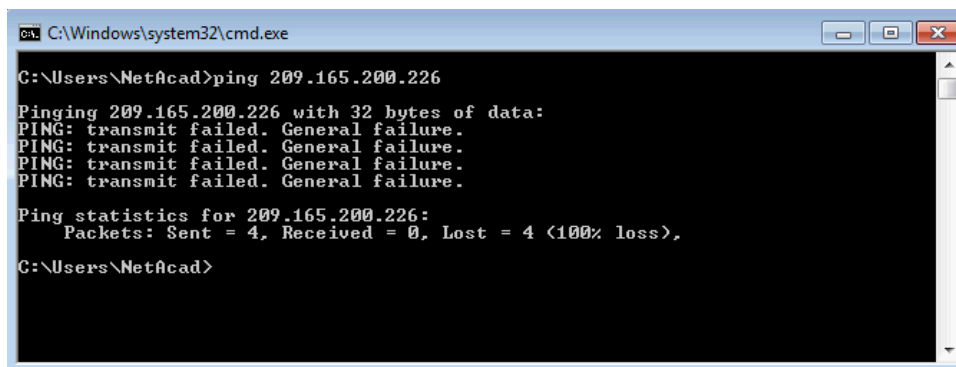
Identify the Problem.

The only available information about the network problem is that the users are experiencing slow response times and that they are not able to reach an external device on the Internet at IP address 209.165.200.226. To determine probable cause(s) for these network issues, you will need to utilize network commands and tools on the LAN equipment shown in the topology.

Note: The user name **admin01** with a password of **cisco12345** will be required to log into the network equipment.

Troubleshoot from the PC.

- a. From the PC command prompt, **ping** the external server IP Address **209.165.200.226**.



- b. Use the **ipconfig** command to determine the network settings on the PC.

```

C:\Windows\system32\cmd.exe

C:\Users\NetAcad>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e9f5:e056:806:f9a0%11
    IPv4 Address. . . . . : 192.168.1.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Tunnel adapter isatap.{E2FC1866-B195-460A-BF40-F04F42A38FFE}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 11:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

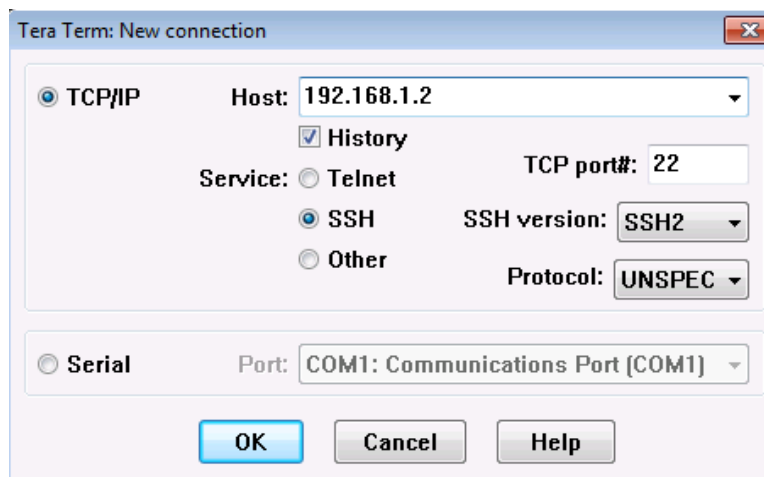
C:\Users\NetAcad>_

```

Troubleshoot from S1 using a SSH client session.

Note: Any SSH client software can be used. Tera Term is used in the examples in this lab.

- SSH to S1 using its IP Address of 192.168.1.2 and log into the switch using **admin01** for the user name and **cisco12345** for the password.



- Issue the **terminal monitor** command on S1 to allow log messages to be sent to the VTY line of your SSH session. After a few seconds you notice the following error message being displayed in your SSH window.

```

S1# terminal monitor
S1#
*Mar  1 02:08:11.338: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
FastEthernet0/5 (not half duplex), with R1.ccna-lab.com GigabitEthernet0/1
(half duplex).
S1#

```

- On S1, issue the **show interface f0/5** command to view the duplex setting of the interface.

```

S1# show interface f0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0cd9.96e8.8a05 (bia 0cd9.96e8.8a05)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set

```

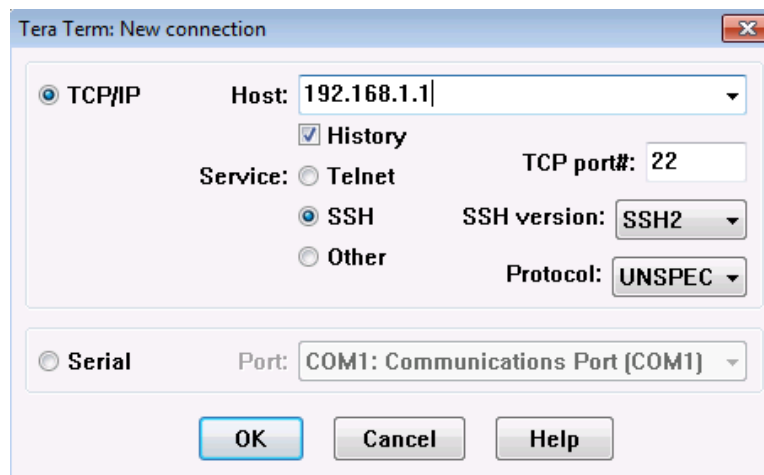
```

Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is 10/100BaseTX
input flow-control is off, output flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:35, output 00:00:01, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  849 packets input, 104642 bytes, 0 no buffer
    Received 123 broadcasts (122 multicasts)
      0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 122 multicast, 0 pause input
    0 input packets with dribble condition detected
  4489 packets output, 361270 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out
S1#

```

Troubleshoot on R1 using an SSH client.

- a. SSH to R1's LAN interface and log in using **admin01** for the user name and **cisco12345** as the password.



- b. Issue the **terminal monitor** command on R1 to allow log messages to be sent to the VTY line of your SSH session for R1. After a few seconds the duplex mismatch message appears on R1's SSH session.

```
R1# terminal monitor
```

```
R1#
```

```
*Nov 23 16:12:36.623: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
GigabitEthernet0/1 (not full duplex), with S1.ccna-lab.com FastEthernet0/5 (full
duplex).
```

```
R1#
```

- c. Issue the **show interface G0/1** command on R1 to display the duplex setting.

```
R1# show interfaces g0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is d48c.b5ce.a0c1 (bia d48c.b5ce.a0c1)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:15, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    641 packets input, 101892 bytes, 0 no buffer
    Received 453 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 361 multicast, 0 pause input
    1043 packets output, 123698 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    235 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out
R1#
```

- d. Issue the **ping 209.165.200.226** command on R1 to test connectivity to the external server.

```
R1# ping 209.165.200.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#
```

- e. Issue the **show ip interface brief** command on R1 to verify interface IP Address settings.

```
R1# show ip interface brief
Interface                                IP-Address      OK? Method Status
Protocol
Embedded-Service-Engine0/0              unassigned      YES unset  administratively down down
GigabitEthernet0/0                      unassigned      YES unset  administratively down down
GigabitEthernet0/1                      192.168.1.1     YES manual up
Serial0/0/0                             10.1.2.1        YES manual up
Serial0/0/1                             unassigned      YES unset  administratively down down
R1#
```

- f. Issue the **show ip route** command on R1 to verify the router's default gateway setting.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
 a - application route
 + - replicated route, % - next hop override

Gateway of last resort is not set

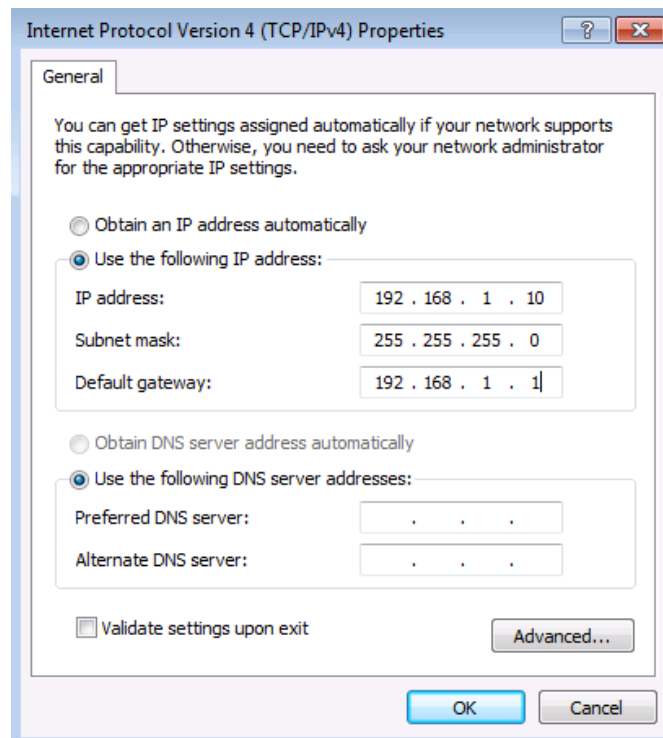
```

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.2.0/30 is directly connected, Serial0/0/0
L       10.1.2.1/32 is directly connected, Serial0/0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
R1#
  
```

List the probable causes for the network problems that employees are experiencing.

Implement Network Changes

You have communicated the problems that you discovered in Part 1 to your supervisor. She has approved these changes and has requested that you implement them. Set the Default Gateway on the PC to 192.168.1.1.



Set the duplex setting for interface G0/1 on R1 to full duplex.

```
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
*Nov 23 17:23:36.879: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
GigabitEthernet0/1 (not full duplex), with S1.ccna-lab.com FastEthernet0/5
(full duplex).
R1(config)#
R1(config)# interface g0/1
R1(config-if)# duplex full
R1(config-if)# exit
*Nov 23 17:24:08.039: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state
to down
R1(config)#
*Nov 23 17:24:10.363: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state
to up
*Nov 23 17:24:10.459: %SYS-5-CONFIG_I: Configured from console by console
R1(config)#
```

Reconfigure the IP address for S0/0/0 to IP Address 10.1.1.1/30 on R1.

```
R1(config)# interface s0/0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.252
R1(config-if)# exit
```

Configure the Gateway of last resort on R1 with a 10.1.1.2 default route.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2
R1(config)# end
```

Verify Full Functionality

Verify that full functionality has been restored.

Verify that all interfaces and routes have been set correctly and that routing has been restored on R1.

- Issue the **show ip route** command to verify that the default gateway has been set correctly.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
```

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

```
S*    0.0.0.0/0 [1/0] via 10.1.1.2
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      10.1.1.0/30 is directly connected, Serial0/0/0
```

```

L      10.1.1.1/32 is directly connected, Serial0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.1.0/24 is directly connected, GigabitEthernet0/1
L      192.168.1.1/32 is directly connected, GigabitEthernet0/1
R1#

```

- b. Issue the **show ip interface s0/0/0** command to verify that the IP Address on S0/0/0 is set correctly.

```

R1# show ip interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  <output omitted>
  IPv4 WCCP Redirect exclude is disabled
R1#

```

- c. Issue the **ping 209.165.200.226** command to verify that the external server is reachable now.

```

R1# ping 209.165.200.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1#

```

- d. Issue the **show interface g0/1** command to verify that the duplex setting is full duplex.

```

R1# show interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is d48c.b5ce.a0c1 (bia d48c.b5ce.a0c1)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:04, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    559 packets input, 74066 bytes, 0 no buffer
    Received 279 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 208 multicast, 0 pause input
    742 packets output, 81462 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    133 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    1 lost carrier, 0 no carrier, 0 pause output

```

```
0 output buffer failures, 0 output buffers swapped out
```

R1#

Verify End-to-End connectivity from the LAN PC.

- Issue the **ipconfig** command from the command prompt on the PC.

```
C:\Windows\system32\cmd.exe

C:\Users\NetAcad>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e9f5:e056:806:f9a0%11
    IPv4 Address. . . . . : 192.168.1.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter isatap.{E2FC1866-B195-460A-BF40-F04F42A38FFE}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 11:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\NetAcad>
```

- b. Issue the **ping 209.165.200.226** command from the CMD window on the PC

```
C:\Windows\system32\cmd.exe
C:\Users\NetAcad>ping 209.165.200.226

Pinging 209.165.200.226 with 32 bytes of data:
Reply from 209.165.200.226: bytes=32 time=1ms TTL=254
Reply from 209.165.200.226: bytes=32 time=1ms TTL=254
Reply from 209.165.200.226: bytes=32 time=1ms TTL=254
Reply from 209.165.200.226: bytes=32 time=1ms TTL=254

Ping statistics for 209.165.200.226:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\NetAcad>
C:\Users\NetAcad>
```

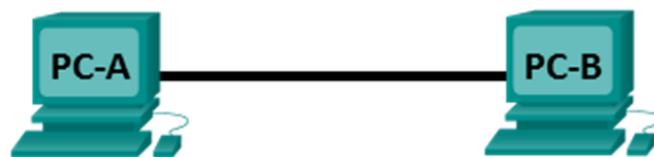
Document Findings and Configuration Changes

Use the space provided below to document the issues found during your troubleshooting and the configurations changes made to resolve those issues.

[illegible]

Lab 23 – Building an Ethernet Crossover Cable

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC-A	NIC	192.168.10.1	255.255.255.0	N/A
PC-B	NIC	192.168.10.2	255.255.255.0	N/A

Objectives

Part 1: Analyze Ethernet Cabling Standards and Pinouts

Part 2: Build an Ethernet Crossover Cable

Part 3: Test an Ethernet Crossover Cable

Background / Scenario

In this lab, you will build and terminate an Ethernet crossover cable and test it by connecting two PCs together and pinging between them. You will first analyze the Telecommunications Industry Association/Electronic Industries Association (TIA/EIA) 568-A and 568-B standards and how they apply to Ethernet cables. You will then construct an Ethernet crossover cable and test it. Finally, you will use the cable you just constructed to connect two PCs together and test it by pinging between them.

Note: With autosensing capabilities available on many devices, such as the Cisco 1941 Integrated Services Router (ISR) switch, you may see straight-through cables connecting like devices.

Required Resources

- One length of cable, either Category 5 or 5e. Cable length should be 0.6 to 0.9m (2 to 3 ft.)
- 2 RJ-45 connectors
- RJ-45 crimping tool
- Wire cutter
- Wire stripper
- Ethernet cable tester (optional)
- 2 PCs (Windows 7 or 8)

Analyze Ethernet Cabling Standards and Pinouts

The TIA/EIA has specified unshielded twisted pair (UTP) cabling standards for use in LAN cabling environments. TIA/EIA 568-A and 568-B stipulates the commercial cabling standards for LAN installations; these are the standards most commonly used in LAN cabling for organizations and they determine which color wire is used on each pin.

With a crossover cable, the second and third pairs on the RJ-45 connector at one end of the cable are reversed at the other end, which reverses the send and receive pairs. The cable pinouts are the 568-A standard on one end and the 568-B standard on the other end. Crossover cables are normally used to

connect hubs to hubs or switches to switches, but they can also be used to directly connect two hosts to create a simple network.

Note: With modern networking devices, a straight-through cable can often be used even when connecting like devices because of their autosensing feature. With autosensing, the interfaces detect whether the send and receive circuit pairs are correctly connected. If they are not, the interfaces reverse one end of the connection. Autosensing also alters the speed of the interfaces to match the slowest one. For example, if connecting a Gigabit Ethernet (1000 Mb/s) router interface to a Fast Ethernet (100 Mb/s) switch interface, the connection uses Fast Ethernet.

The Cisco 2960 switch has autosensing turned on, by default; therefore, connecting two 2960 switches together works with either a crossover or a straight-through cable. With some older switches, this is not the case and a crossover cable must be used.

In addition, the Cisco 1941 router Gigabit Ethernet interfaces are autosensing and a straight-through cable may be used to connect a PC directly to the router interface (bypassing the switch). With some older routers, this is not the case and a crossover cable must be used.

When directly connecting two hosts, it is generally advisable to use a crossover cable.

Analyze diagrams and tables for the TIA/EIA 568-A standard Ethernet cable.

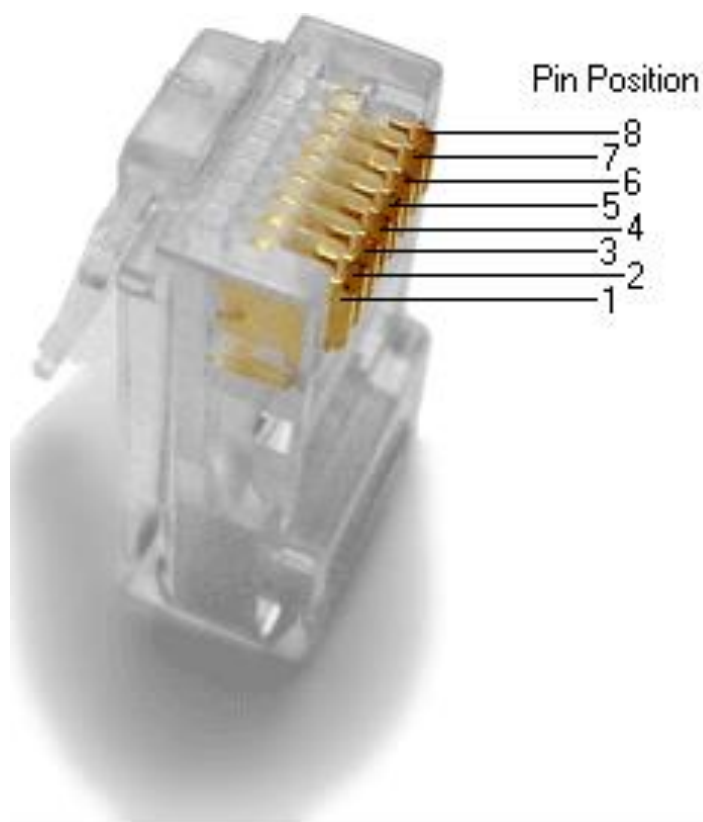
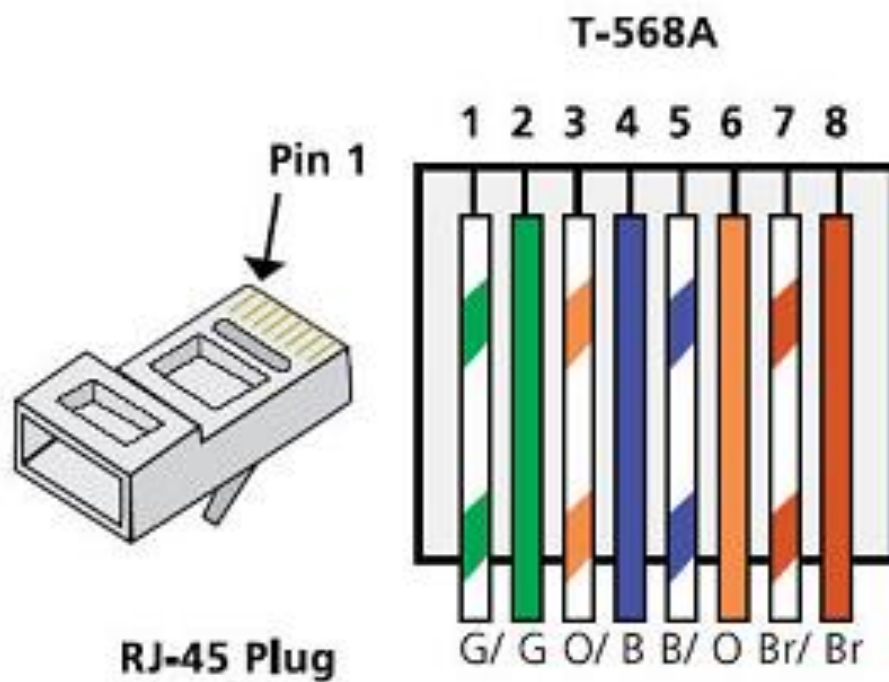
The following table and diagrams display the color scheme and pinouts, as well as the function of the four pairs of wires used for the 568-A standard.

Note: In LAN installations using 100Base-T (100 Mb/s), only two pairs out of the four are used.

568-A 10/100/1000Base-TX Ethernet

Pin Number	Pair Number	Wire Color	10Base-T Signal 100Base-TX Signal	1000Base-T Signal
1	2	White/Green	Transmit	BI_DA+
2	2	Green	Transmit	BI_DA-
3	3	White/Orange	Receive	BI_DB+
4	1	Blue	Not Used	BI_DC+
5	1	White/Blue	Not Used	BI_DC-
6	3	Orange	Receive	BI_DB-
7	4	White/Brown	Not Used	BI_DD+
8	4	Brown	Not Used	BI_DD-

The following diagrams display how the wire color and pinouts align with an RJ-45 jack for the 568-A standard.



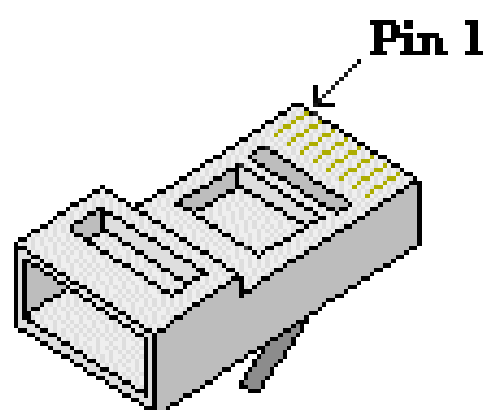
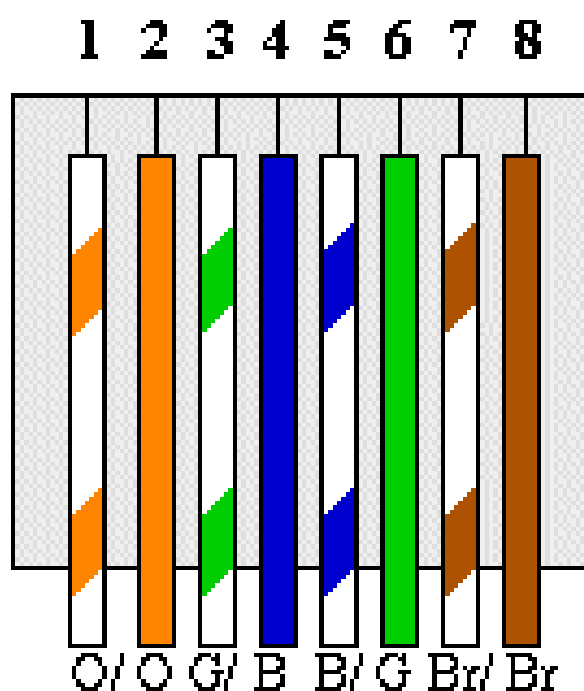
Analyze diagrams and tables for the TIA/EIA 568-B standard Ethernet cable.

The following table and diagram display the color scheme and pinouts for the 568-B standard.

568-B 10/100/1000-BaseTX Ethernet

Pin Number	Pair Number	Wire Color	10Base-T Signal 100Base-TX Signal	1000Base-T Signal
1	2	White/Orange	Transmit	BI_DA+
2	2	Orange	Transmit	BI_DA-
3	3	White/Green	Receive	BI_DB+
4	1	Blue	Not Used	BI_DC+
5	1	White/Blue	Not Used	BI_DC-
6	3	Green	Receive	BI_DB-
7	4	White/Brown	Not Used	BI_DD+
8	4	Brown	Not Used	BI_DD-

T-568B

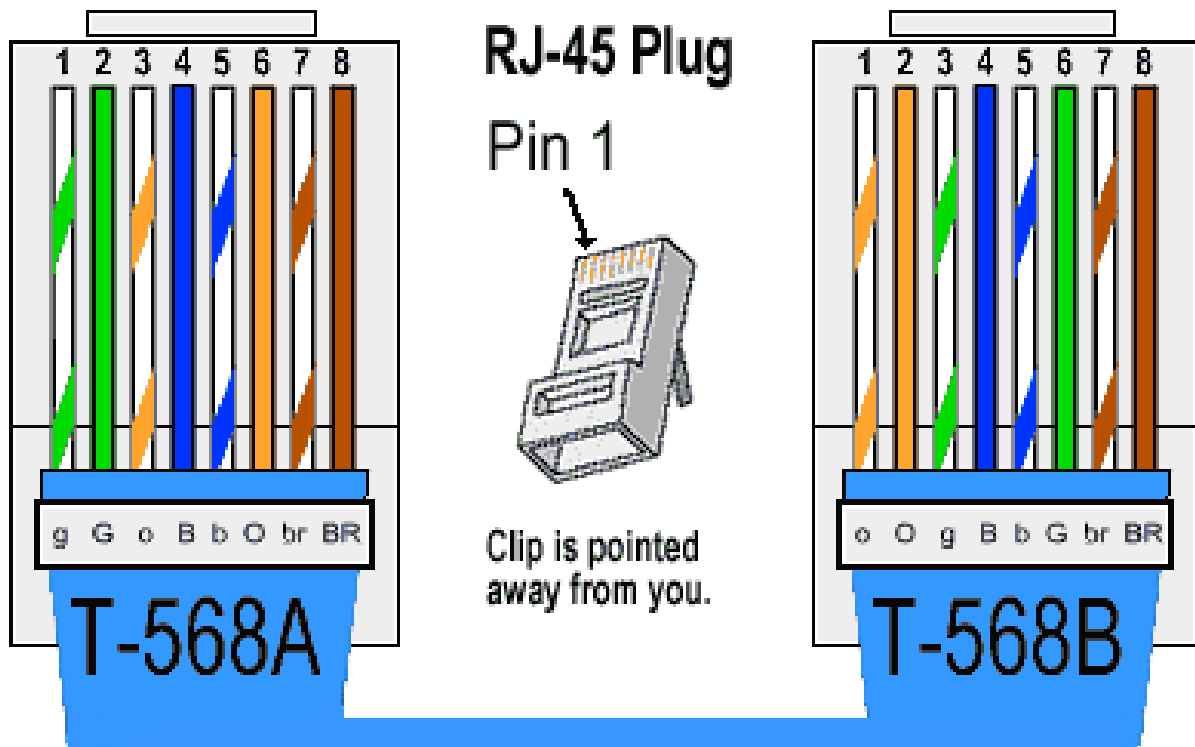


RJ-45 Plug

Build an Ethernet Crossover Cable

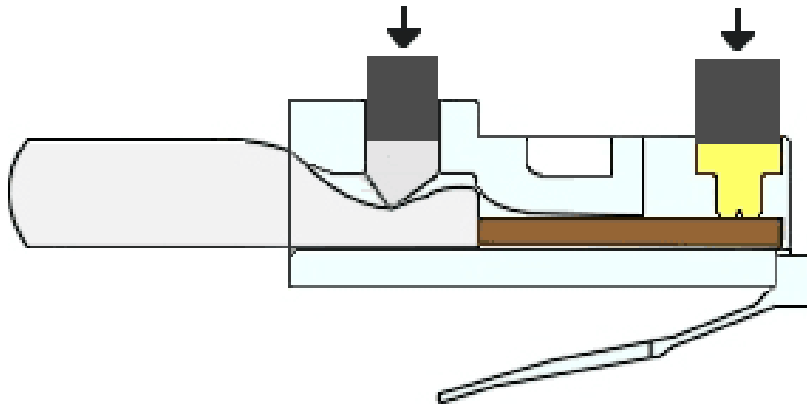
A crossover cable has the second and third pairs on the RJ-45 connector at one end, reversed at the other end (refer to the table in Part 1, Step 2). The cable pinouts are the 568-A standard on one end and the 568-B standard on the other end. The two following diagrams illustrate this concept.

RJ-45 Crossover Ethernet Cable



Build and terminate a TIA/EIA 568-A cable end.

- Determine the cable length required. (Your instructor will let you know the cable length you should make.)
Note: If you were making a cable in a production environment, the general guideline is to add another 12 in. (30.48 cm) to the length.
- Cut off a piece of cable to the desired length and using your wire stripper, remove 5.08 cm (2 in.) of the cable jacket from both ends.
- Hold the four pairs of twisted cables tightly where the jacket was cut away. Reorganize the cable pairs into the order of the 568-A wiring standard. Refer to the diagrams, if necessary. Take as much care as possible to maintain the twists in the cable; this provides noise cancellation.
- Flatten, straighten, and line up the wires using your thumb and forefinger.
- Ensure that the cable wires are still in the correct order for the 568-A standard. Using your wire cutters, trim the four pairs in a straight line to within 1.25 to 1.9 cm (1/2 to 3/4 in.).
- Place an RJ-45 connector on the end of your cable, with the prong on the underside pointing downward. Firmly insert the wires into the RJ-45 connector. All wires should be seen at the end of the connector in their proper positions. If the wires are not extending to the end of the connector, take the cable out, rearrange the wires as necessary, and reinsert the wires back into the RJ-45 connector.
- If everything is correct, insert the RJ-45 connector with cable into the crimper. Crimp down hard enough to force the contacts on the RJ-45 connector through the insulation on the wires, thus completing the conducting path. See the following diagram for an example.



Build and terminate a TIA/EIA 568-B cable end.

Repeat steps 1a to 1g using the 568-B color wiring scheme for the other end.

Test an Ethernet Crossover Cable

Test the cable.

Many cable testers will test for length and mapping of wires. If the cable tester has a wire map feature, it verifies which pins on one end of the cable are connected to which pins on the other end.

If your instructor has a cable tester, test the crossover cable for functionality. If it fails, check with your instructor first as to whether you should re-cable the ends and re-test.

Connect two PCs together via NICs using your Ethernet crossover cable.

- Working with a lab partner, set your PC to one of the IP addresses shown in the Addressing Table (see page 1). For example, if your PC is **PC-A**, your IP address should be set to **192.168.10.1** with a **24-bit subnet mask**. Your partner's IP address should be **192.168.10.2**. The default gateway address can be left empty.
- Using the crossover cable you made, connect the two PCs together via their NICs.
- On the PC-A command prompt, ping the PC-B IP address.

Note: The Windows firewall may have to be temporarily disabled for pings to be successful. If the firewall is disabled, make sure you re-enable it at the conclusion of this lab.

- Repeat the process and ping from PC-B to PC-A.

Assuming IP addressing and firewall are not issues, your pings should be successful if the cables were properly made.

Reflection

- Which part of making cables did you find the most difficult?

- Why do you have to learn how to make a cable if you can easily buy pre-made cables?
