CCNA Semester 1 labs

Part 1 of 2

Labs for chapters 1 – 7

2.3.3.3 Lab - Building a Simple Network

2.3.3.4 Lab - Configuring a Switch Management Address

3.4.1.2 Lab - Using Wireshark to View Network Traffic

5.1.1.7 Lab - Using Wireshark to Examine Ethernet Frames

5.1.2.8 Lab - Viewing Network Device MAC Addresses

5.2.1.7 Lab - Viewing the Switch MAC Address Table

6.5.1.2 Lab - Building a Switch and Router Network

7.1.4.9 Lab - Identifying IPv4 Addresses

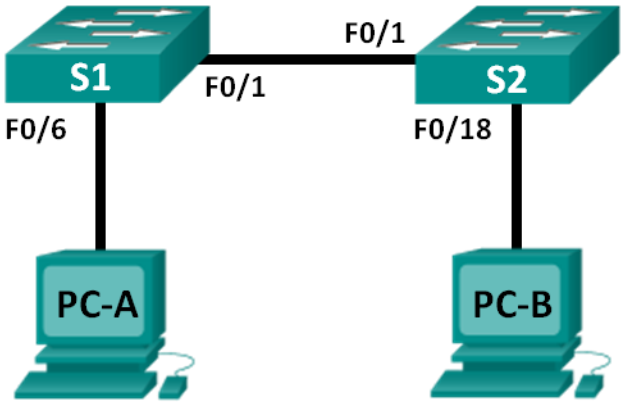
7.2.5.3 Lab - Identifying IPv6 Addresses

7.2.5.4 Lab - Configuring IPv6 Addresses on Network Devices

7.3.2.8 Lab - Mapping the Internet

Lab - 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

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

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

Step 1: 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.

Step 2: 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.

Step 3: Connect the PCs to their respective switches.

a. 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.

b. 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.

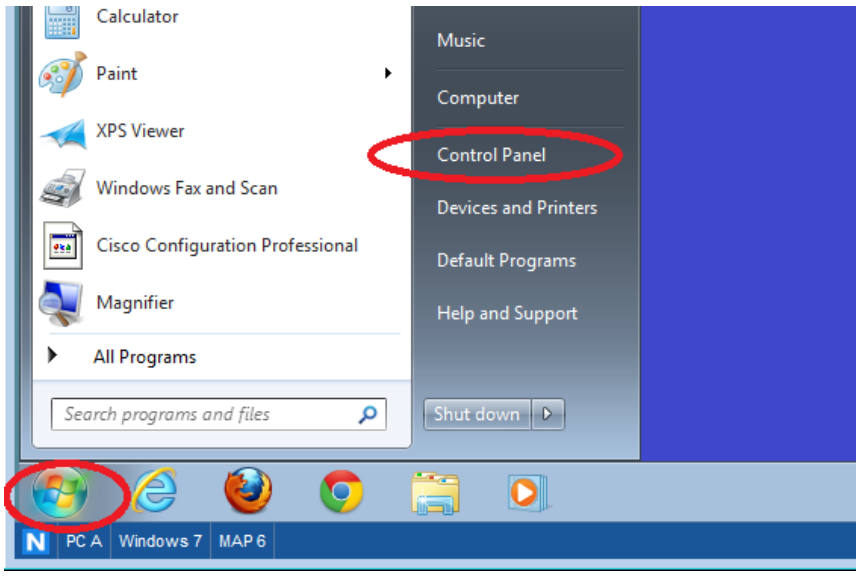
Step 4: Visually inspect network connections.

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

Part 2: Configure PC Hosts

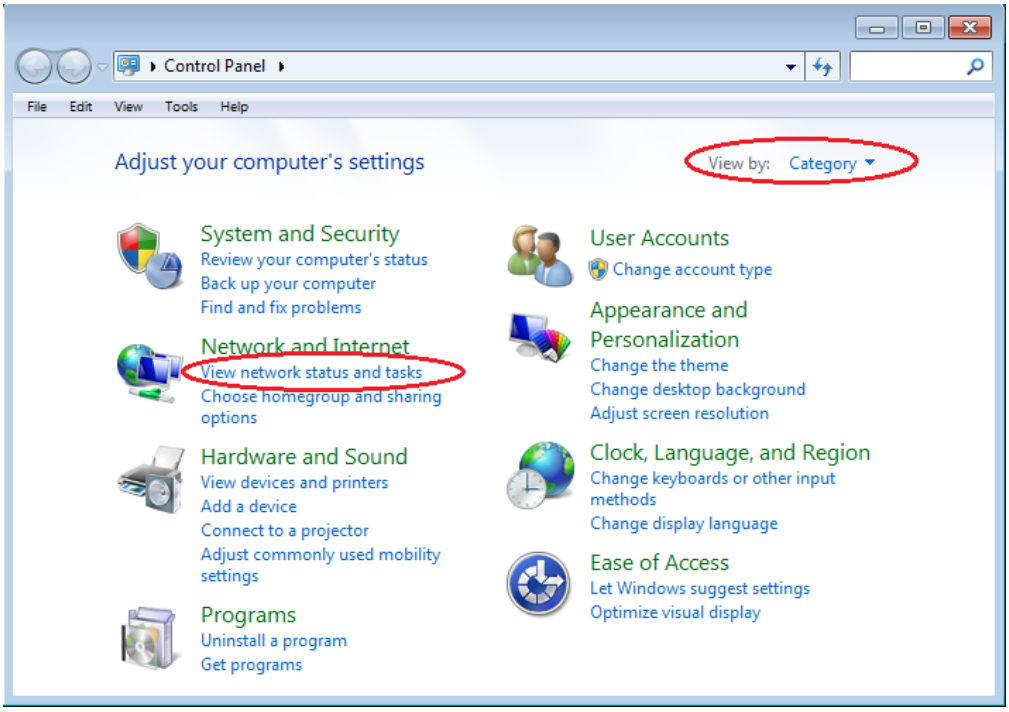
Step 1: Configure static IP address information on the PCs.

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

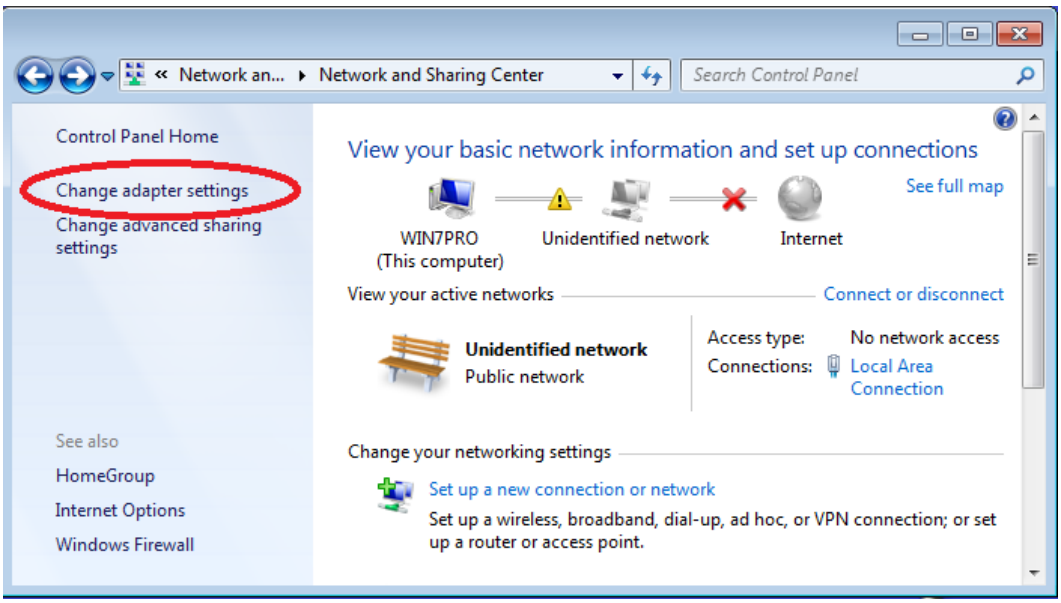


b. In the Network and Internet section, click the **View network status and tasks** link.

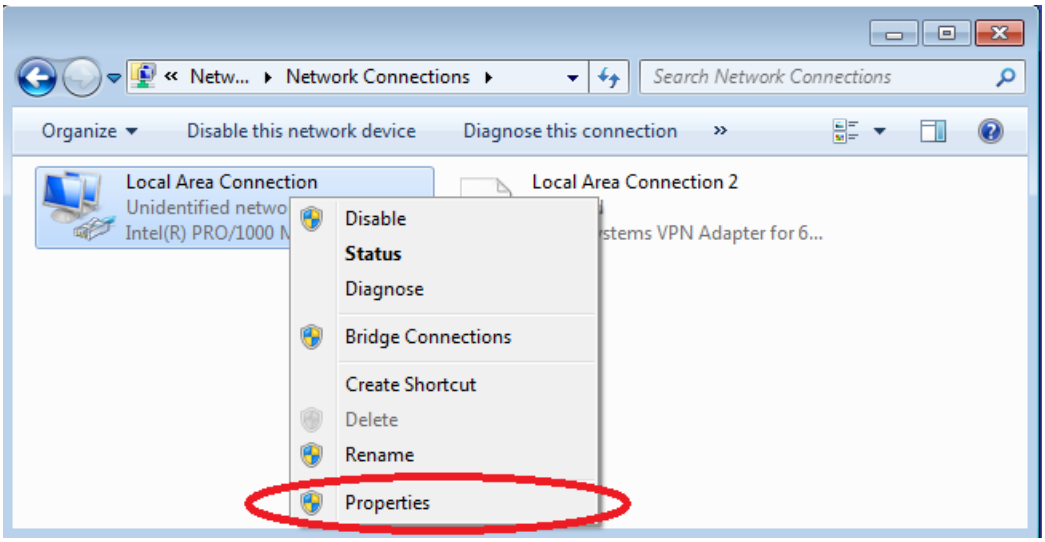
Note: If the Control Panel displays a list of icons, click the drop-down option next to the **View by**: and change this option to display by **Category**.



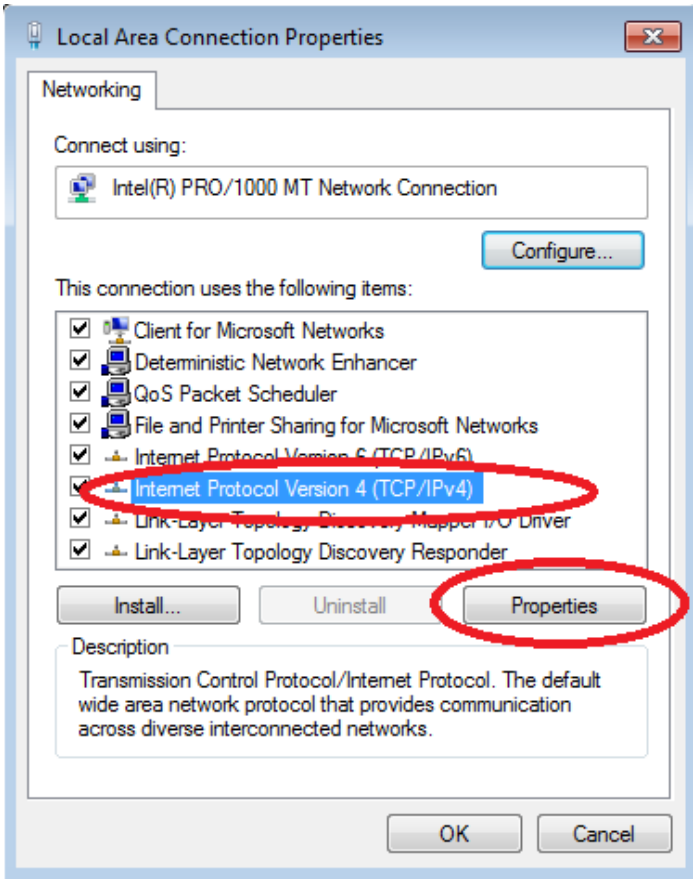
c. In the left pane of the Network and Sharing Center window, click the **Change adapter settings** link.



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

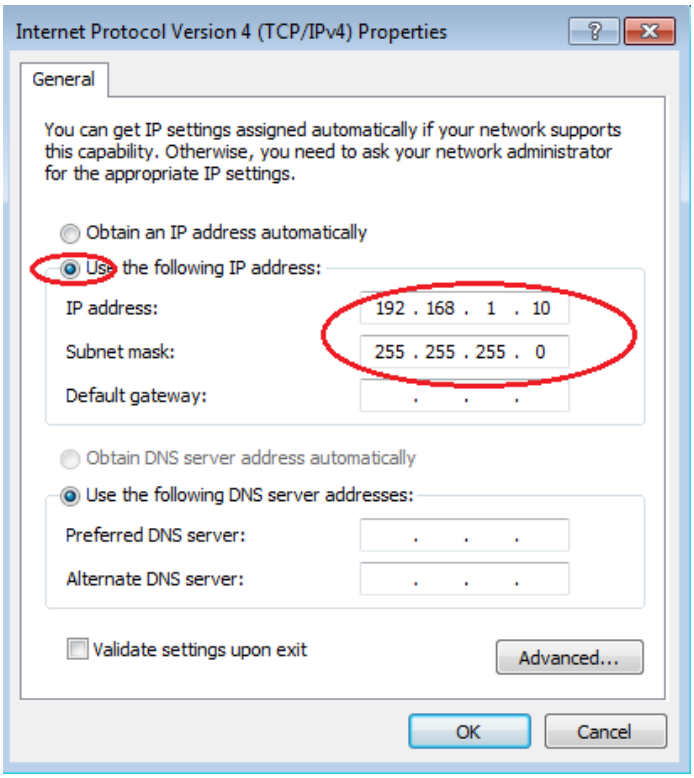


e. Select the **Internet Protocol Version 4 (TCP/IPv4)** option and then click **Properties**.



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

f. 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.

g. 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.

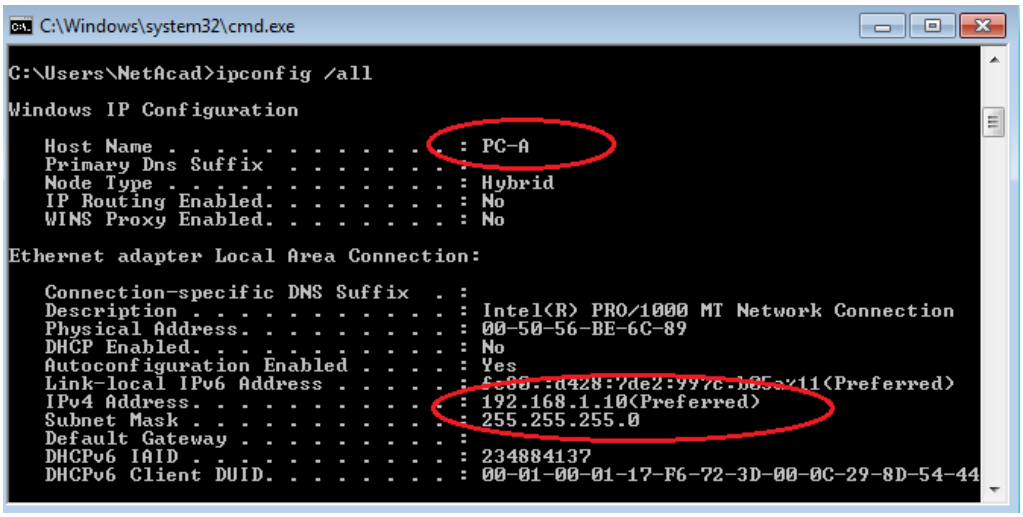
h. Repeat the previous steps to enter the IP address information for PC-B.

Step 2: Verify PC settings and connectivity.

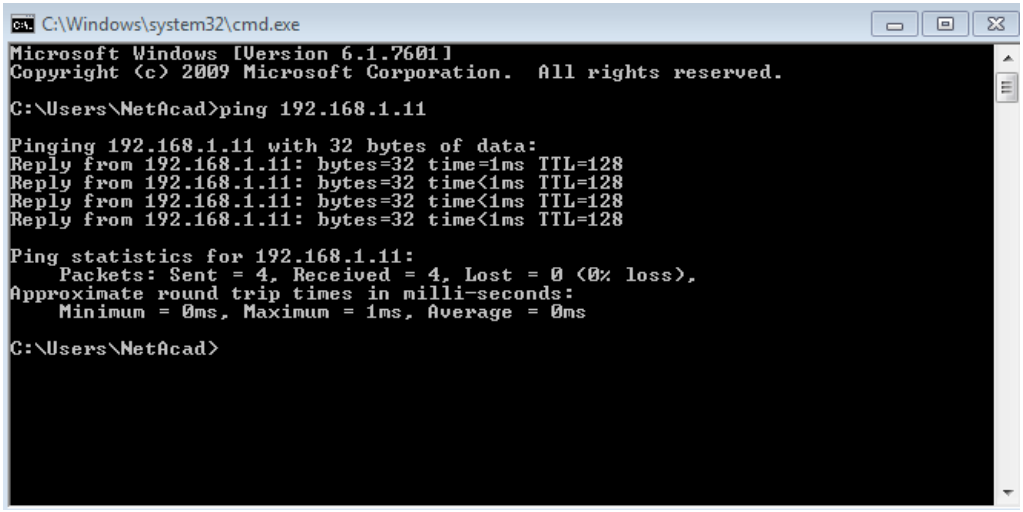
Use the command prompt (**cmd.exe**) window to verify the PC settings and connectivity.

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

b. 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. Type **ping 192.168.1.11** and press Enter.



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.

Part 3: Configure and Verify Basic Switch Settings

Step 1: Console into the switch.

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

Step 2: 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.

Step 3: 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.

Step 4: Give the switch a name.

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

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

Step 5: 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)#
```

Step 6: 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)#
```

Step 7: 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#
```

Step 8: 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#
```

Step 9: 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/kLkDq9BGho1QM5EnRtoyr8cHAUg.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#
```

Step 10: 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#
```

Step 11: 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                  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#
```

Step 12: Repeat Steps 1 to 12 to configure switch S2.

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

Step 13: Record the interface status for the following interfaces.

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

Why are some FastEthernet ports on the switches are up and others are down?

_____

_____

Reflection

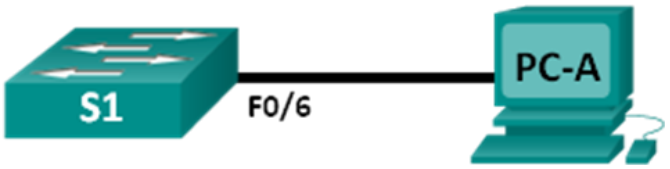
What could prevent a ping from being sent between the PCs?

_____

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

Lab - 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

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.

Step 1: Cable the network.

a. Cable the network as shown in the topology.

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

Step 2: 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.

a. 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#
```

b. 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.

c. Enter global configuration mode and assign the switch hostname.

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

d. Configure the switch password access.

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

e. Prevent unwanted DNS lookups.

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

f. Configure a login MOTD banner.

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

g. 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?

_____

h. 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.

i. 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)#
```

j. 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)#
```

k. 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
```

Step 3: Configure an IP address on PC-A.

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.

Part 2: 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.

Step 1: Display the S1 device configuration.

a. 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 06YFDUHH61wAE/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
```

b. 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
```

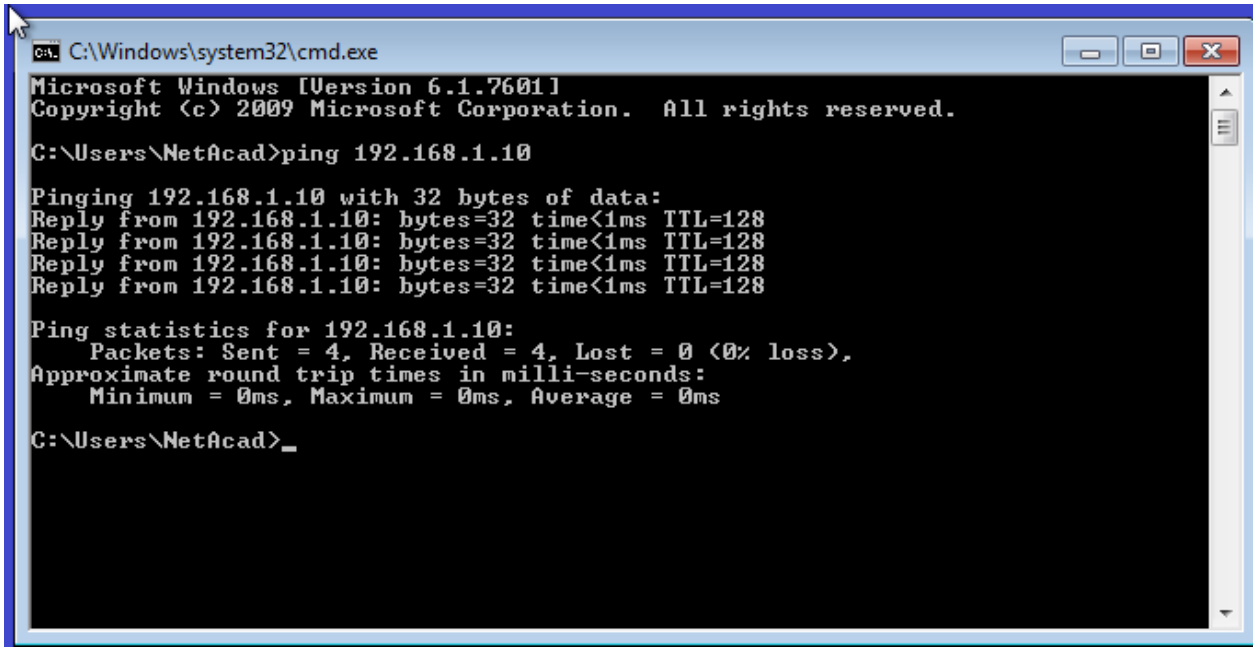
Step 2: Test end-to-end connectivity.

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.

a. Ping the PC-A address first.

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

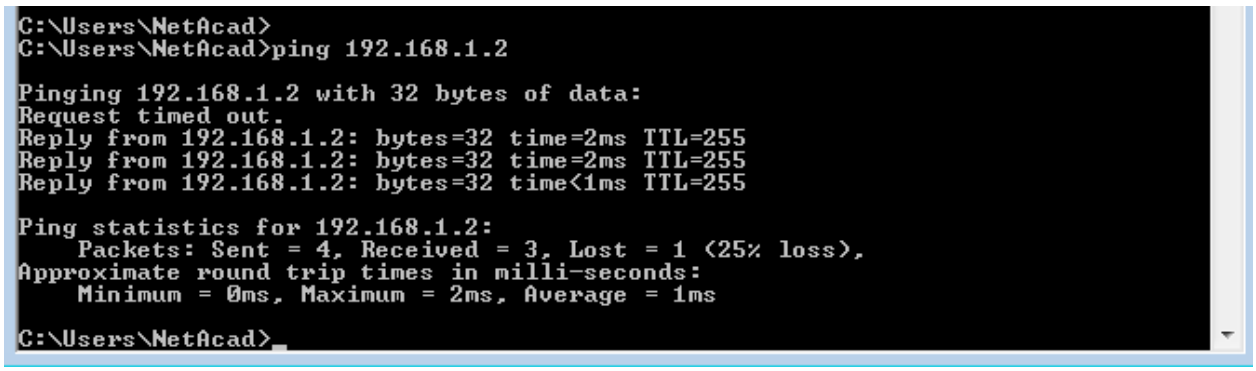
Your output should be similar to the following screen:



b. 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.



Step 3: 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.

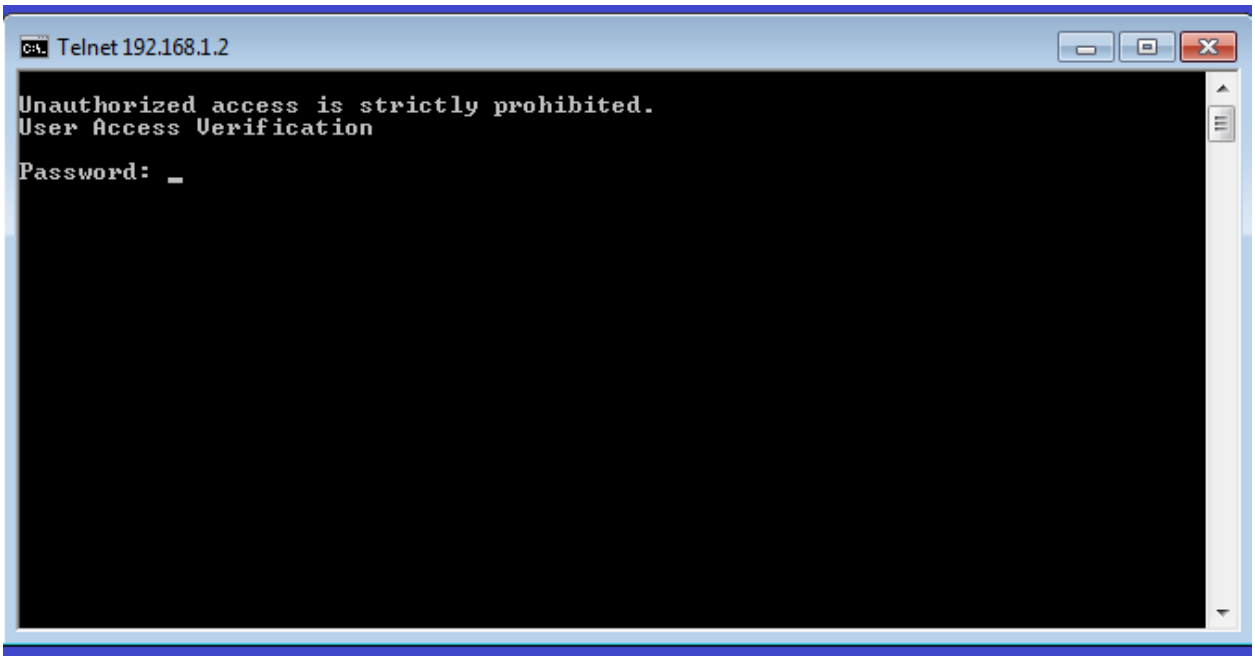
Note: Windows 7 does not natively support Telnet. The administrator must enable this protocol. To install the Telnet client, open a command prompt window and type **pkgmgr /iu:"TelnetClient"**.

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

a. 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:



b. 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.

Step 4: Save the configuration file.

a. 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#
```

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

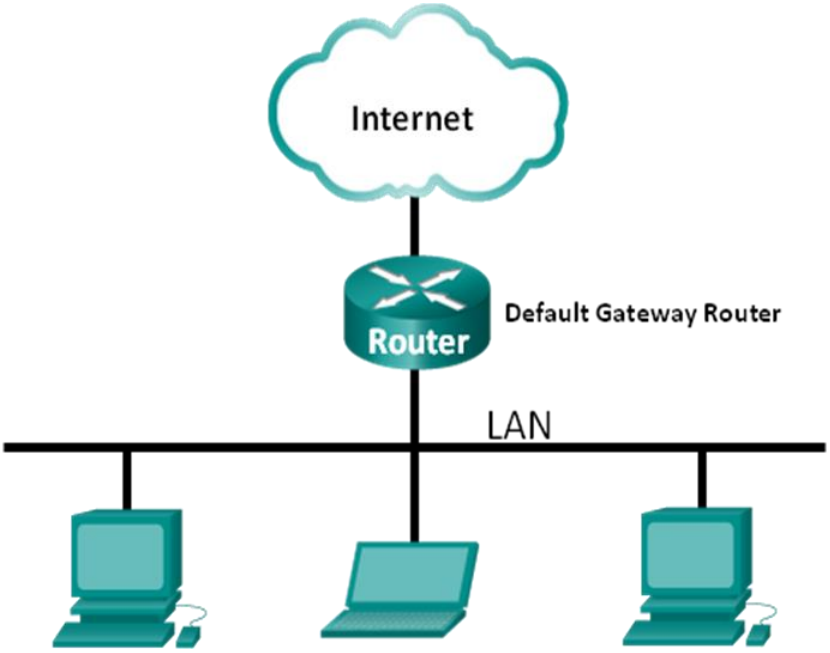
Reflection

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

_____

Lab - 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

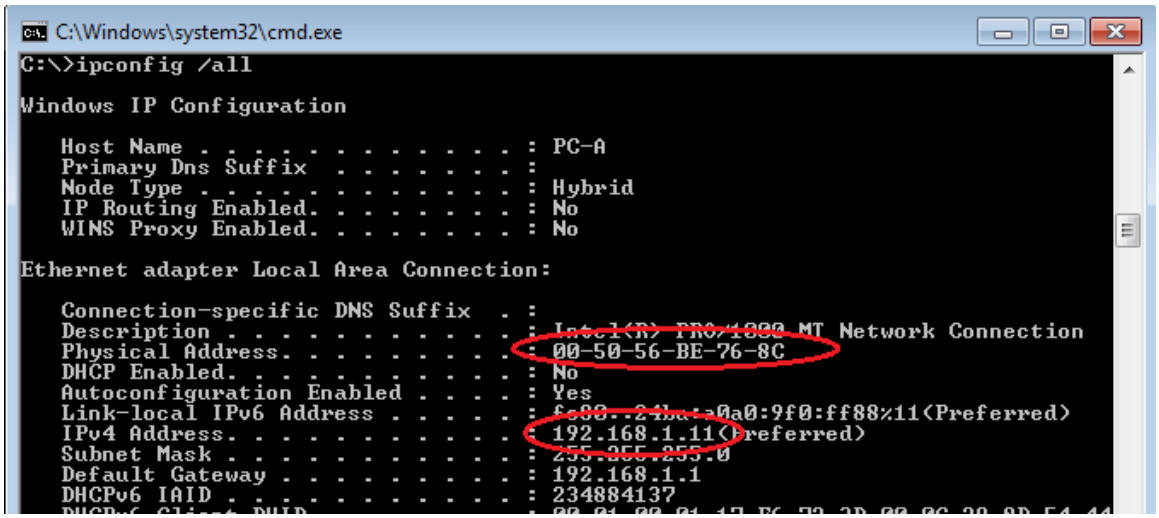
In Part 1 of this lab, you will ping another PC on the LAN and capture ICMP requests and replies in Wireshark. You will also look inside the frames captured for specific information. This analysis should help to clarify how packet headers are used to transport data to their destination.

Step 1: 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.

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

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

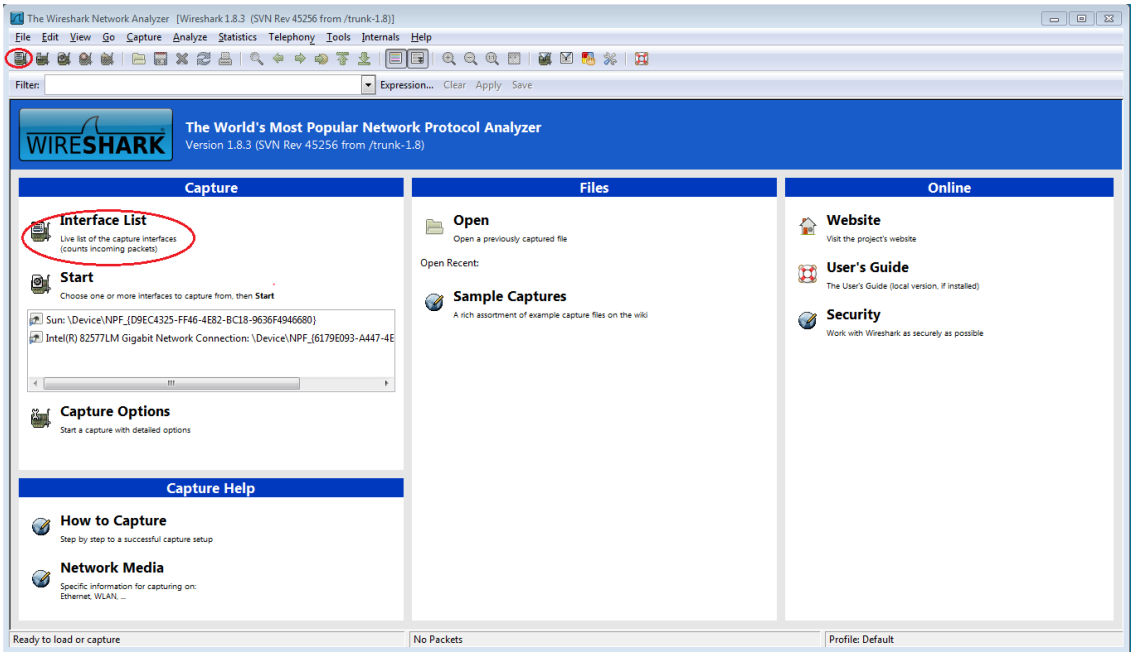


c. Ask a team member for their PC's IP address and provide your PC's IP address to them. Do not provide them with your MAC address at this time.

Step 2: Start Wireshark and begin capturing data.

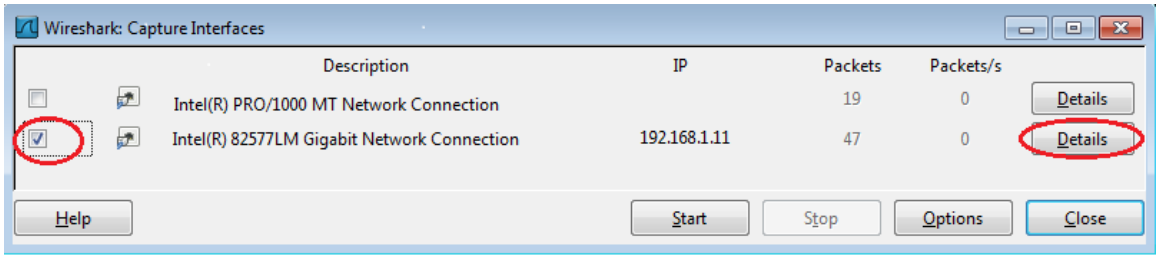
a. On your PC, click the Windows **Start** button to see Wireshark listed as one of the programs on the pop-up menu. Double-click **Wireshark**.

b. After Wireshark starts, click **Interface List**.

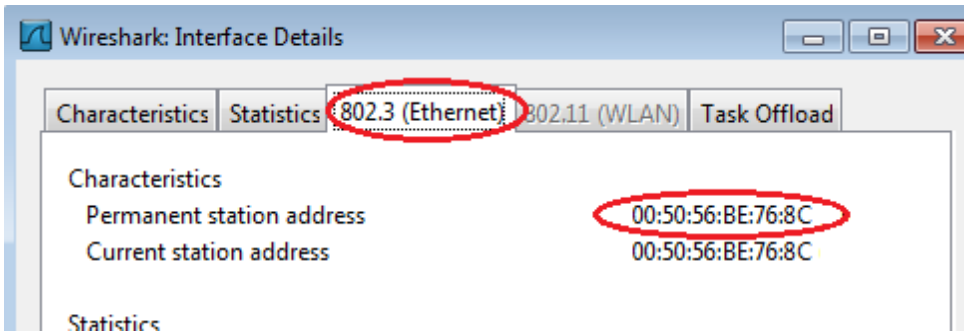


Note: Clicking the first interface icon in the row of icons also opens the Interface List.

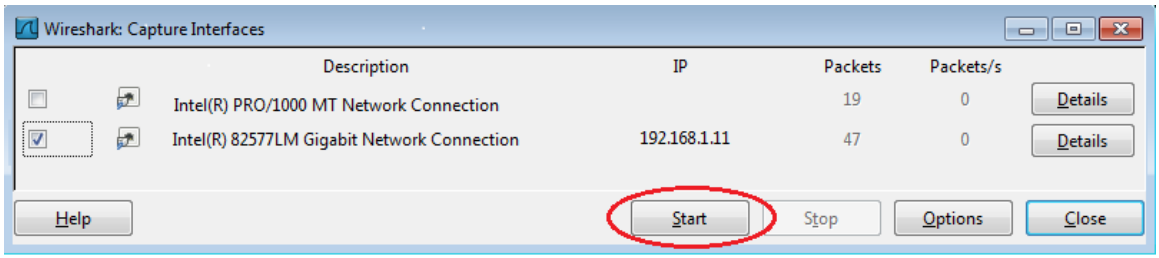
c. On the Wireshark: Capture Interfaces window, click the check box next to the interface connected to your LAN.



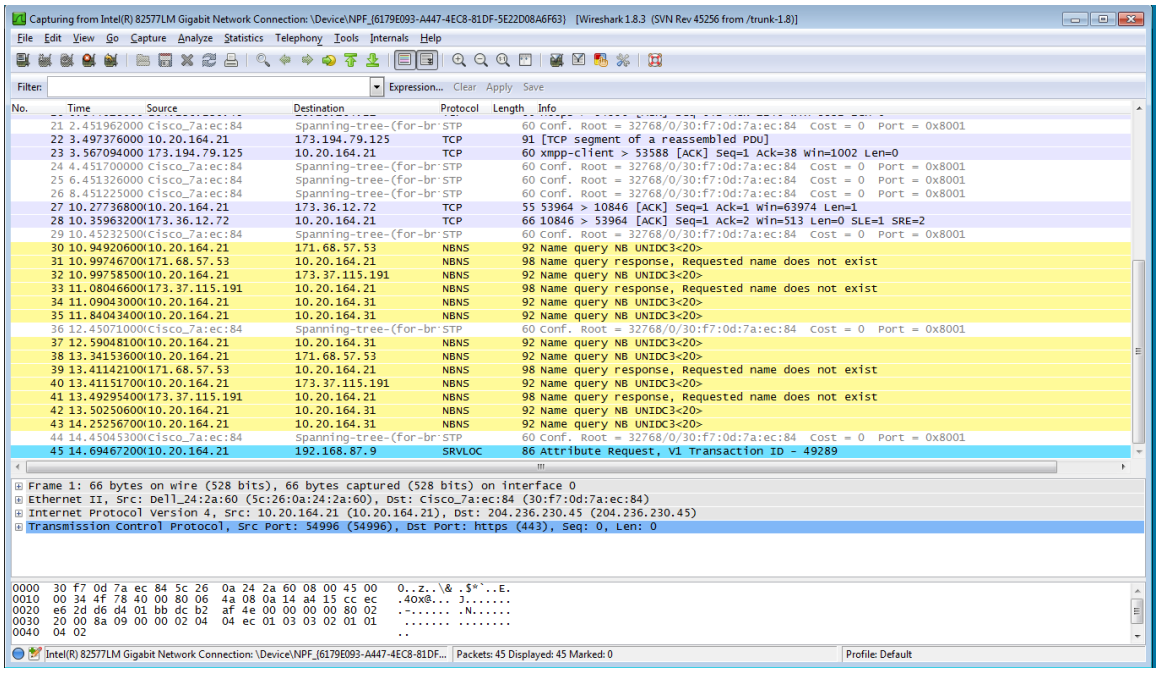
Note: If multiple interfaces are listed and you are unsure which interface to check, click the **Details** button, and then click the **802.3 (Ethernet)** tab. Verify that the MAC address matches what you noted in Step 1b. Close the Interface Details window after verifying the correct interface.



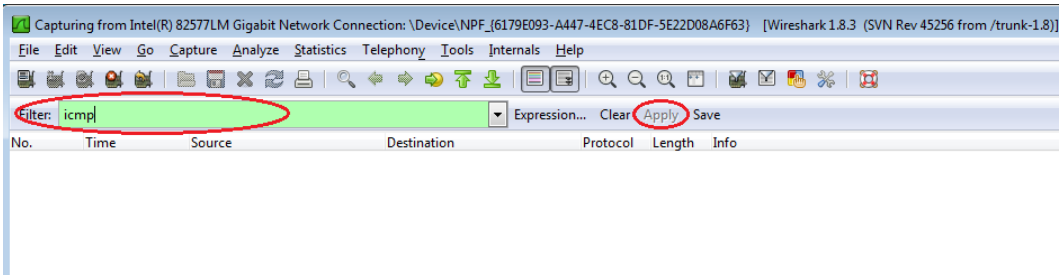
d. After you have checked the correct interface, click **Start** to start the data capture.



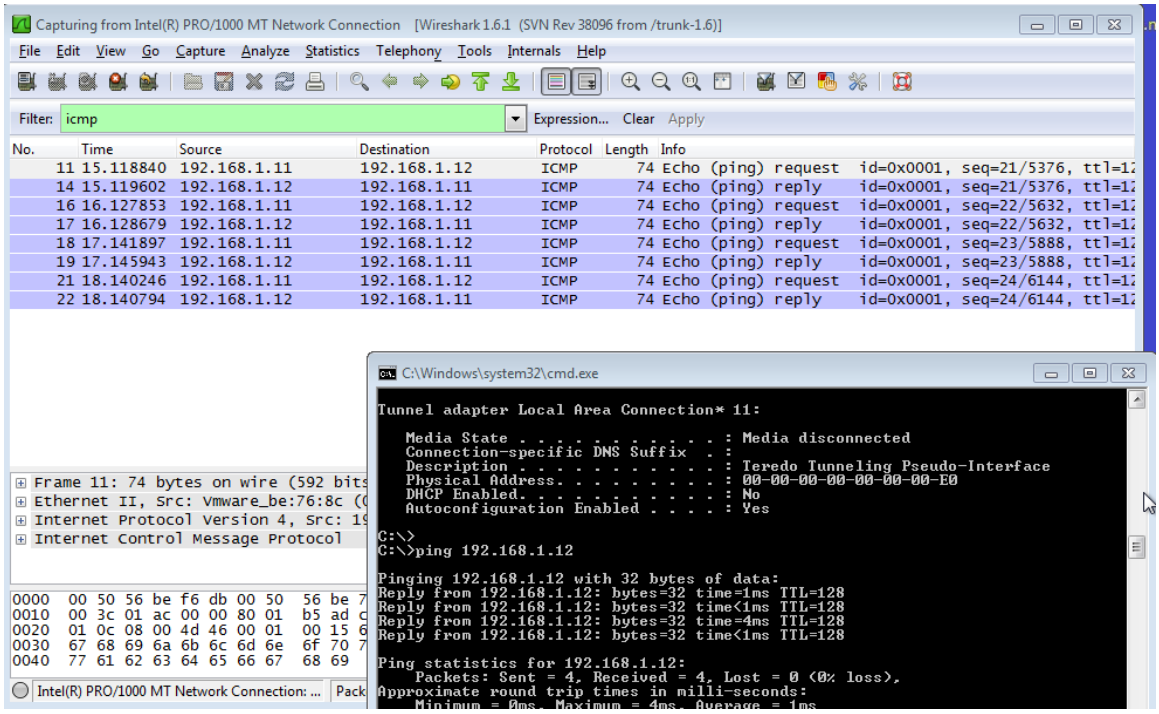
Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol.



e. 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.

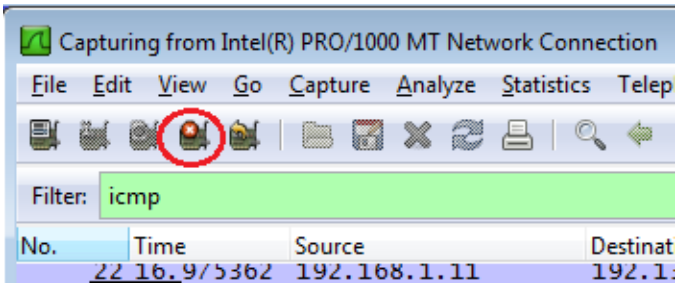


f. This filter causes all data in the top window to disappear, but you are still capturing the traffic on the interface. Bring up the command prompt window that you opened earlier and ping the IP address that you received from your team member. Notice that you start seeing data appear in the top window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



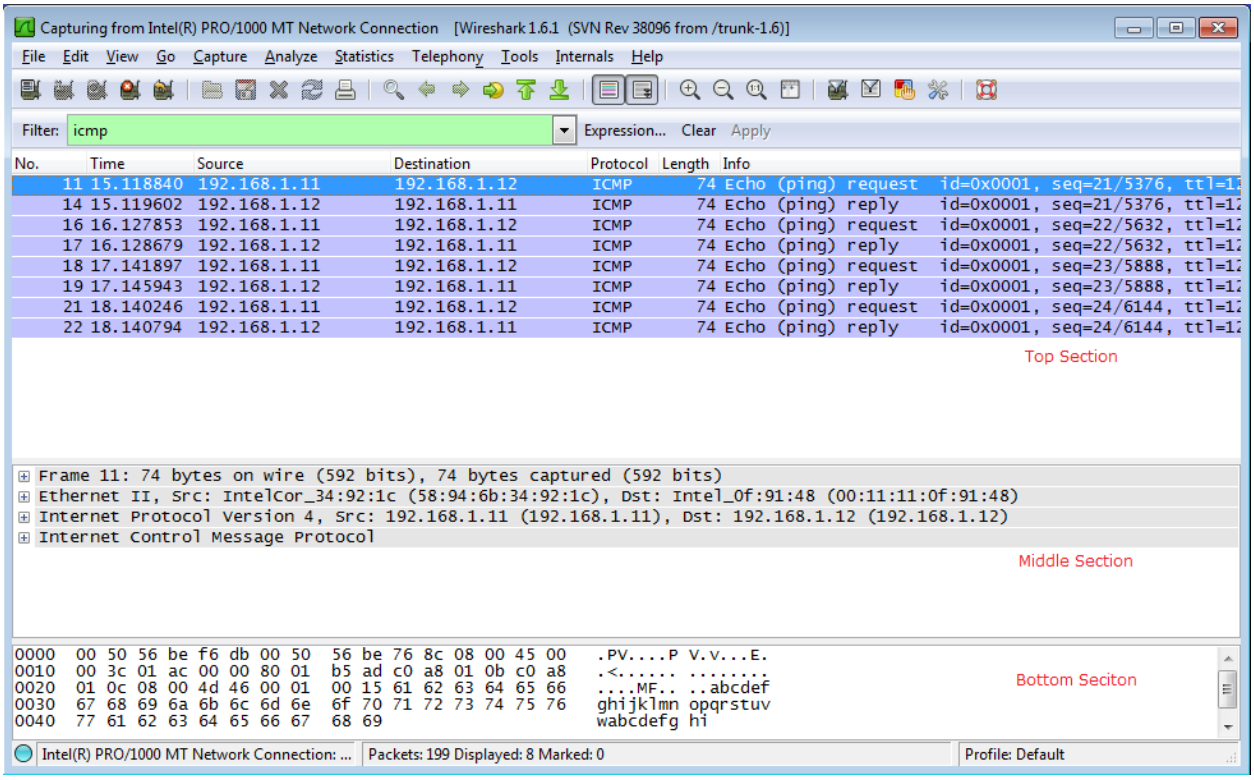
Note: If your team member's PC does not reply to your pings, this may be because their PC firewall is blocking these requests. Please see Error! Reference source not found. for information on how to allow ICMP traffic through the firewall using Windows 7.

g. Stop capturing data by clicking the **Stop Capture** icon.

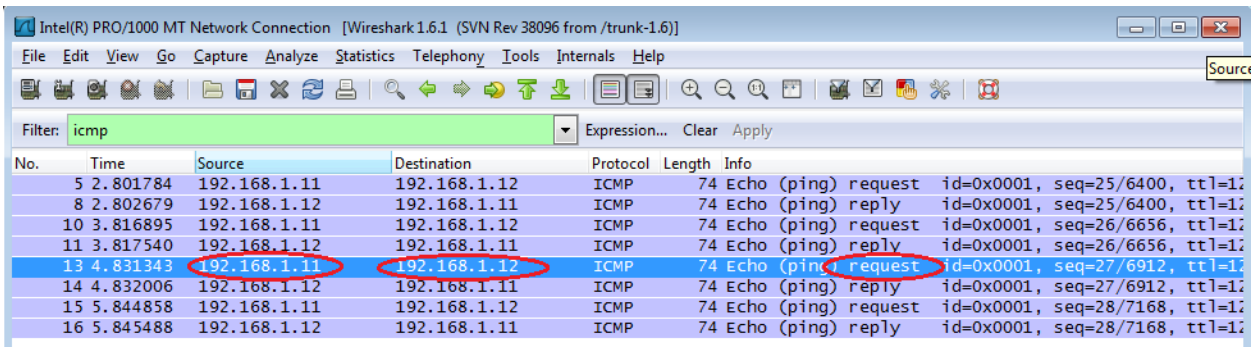


Step 3: Examine the captured data.

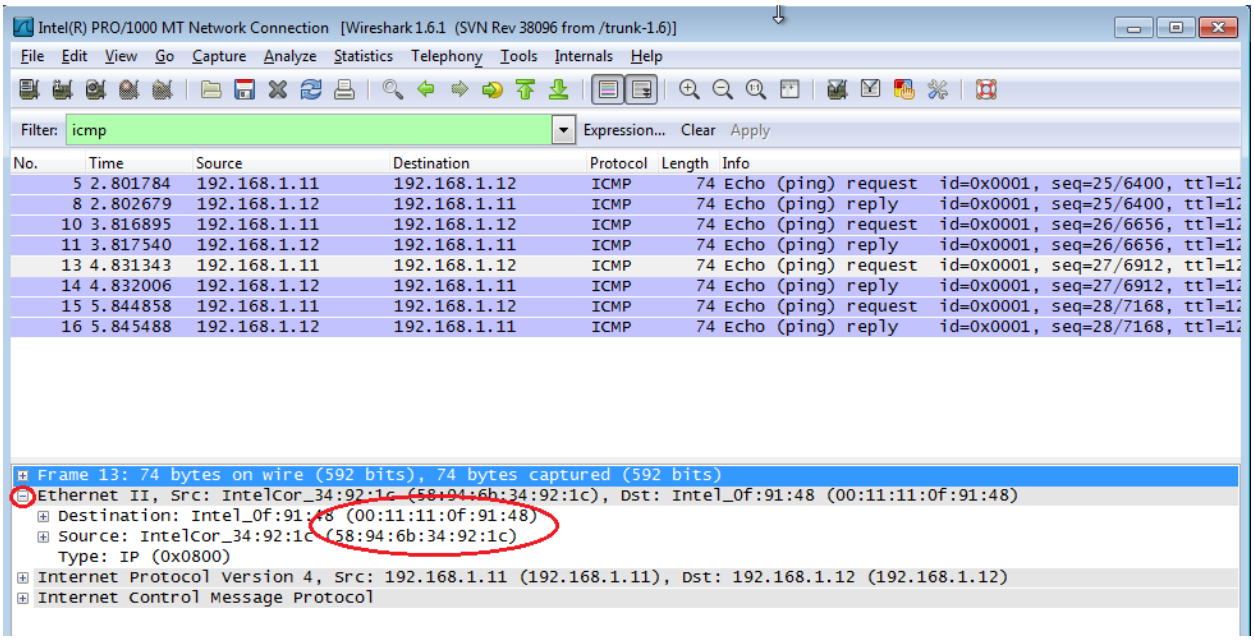
In Step 3, examine the data that was generated by the ping requests of your team member's PC. Wireshark data is displayed in three sections: 1) The top section displays the list of PDU frames captured with a summary of the IP packet information listed, 2) the middle section lists PDU information for 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.



a. 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.



b. 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?

_____

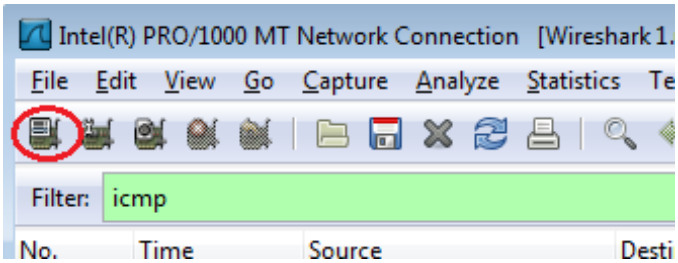
Note: In the preceding example of a captured ICMP request, ICMP data is encapsulated inside an IPv4 packet PDU (IPv4 header) which is then encapsulated in an Ethernet II frame PDU (Ethernet II header) for transmission on the LAN.

Part 2: Capture and Analyze Remote ICMP Data in Wireshark

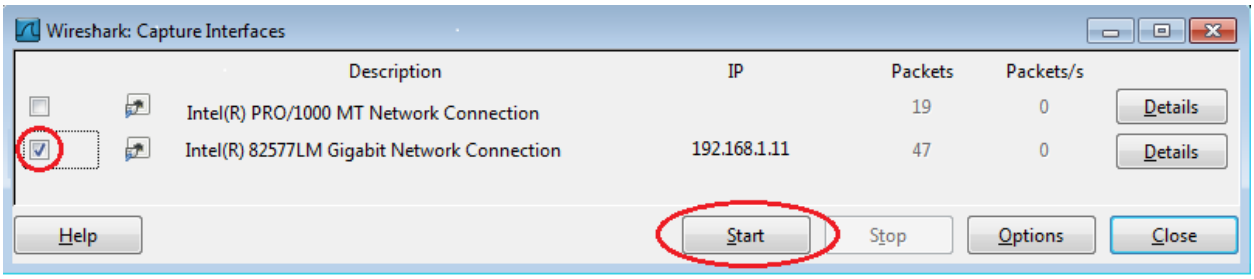
In Part 2, you will ping remote hosts (hosts not on the LAN) and examine the generated data from those pings. You will then determine what is different about this data from the data examined in Part 1.

Step 1: Start capturing data on the interface.

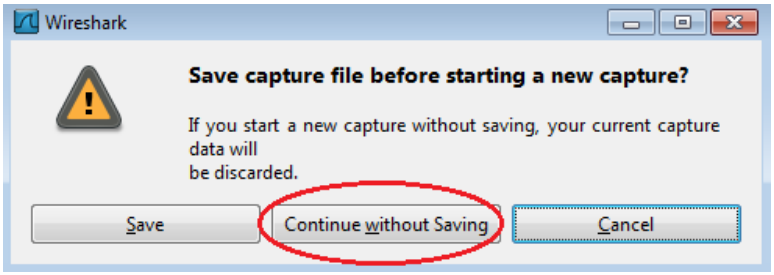
a. Click the **Interface List** icon to bring up the list PC interfaces again.



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

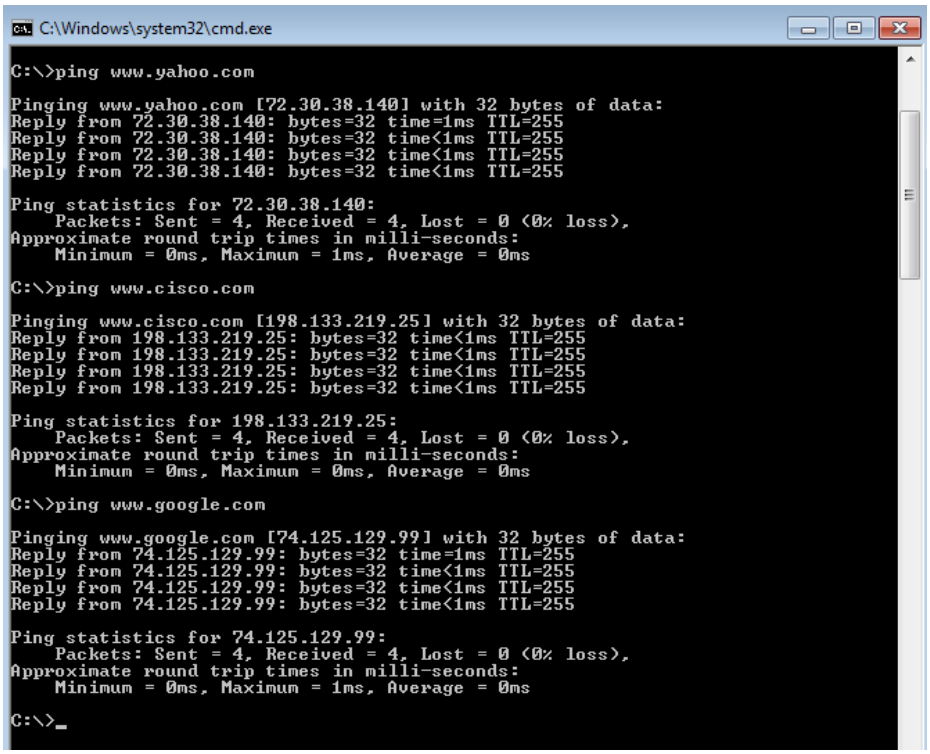


c. A window prompts to save the previously captured data before starting another capture. It is not necessary to save this data. Click **Continue without Saving**.



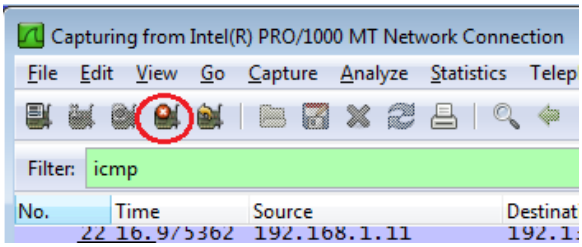
d. With the capture active, ping the following three website URLs:

1) www.yahoo.com
2) www.cisco.com
3) www.google.com



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.

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



Step 2: Examining and analyzing the data from the remote hosts.

a. 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: ____:____:____:____:____:____

b. What is significant about this information?

_____

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

_____

_____

Reflection

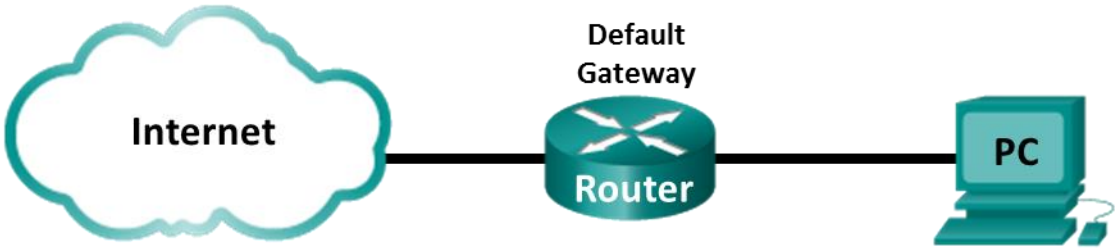
Why does Wireshark show the actual MAC address of the local hosts, but not the actual MAC address for the remote hosts?

_____

_____

Lab – 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.

Step 1: 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

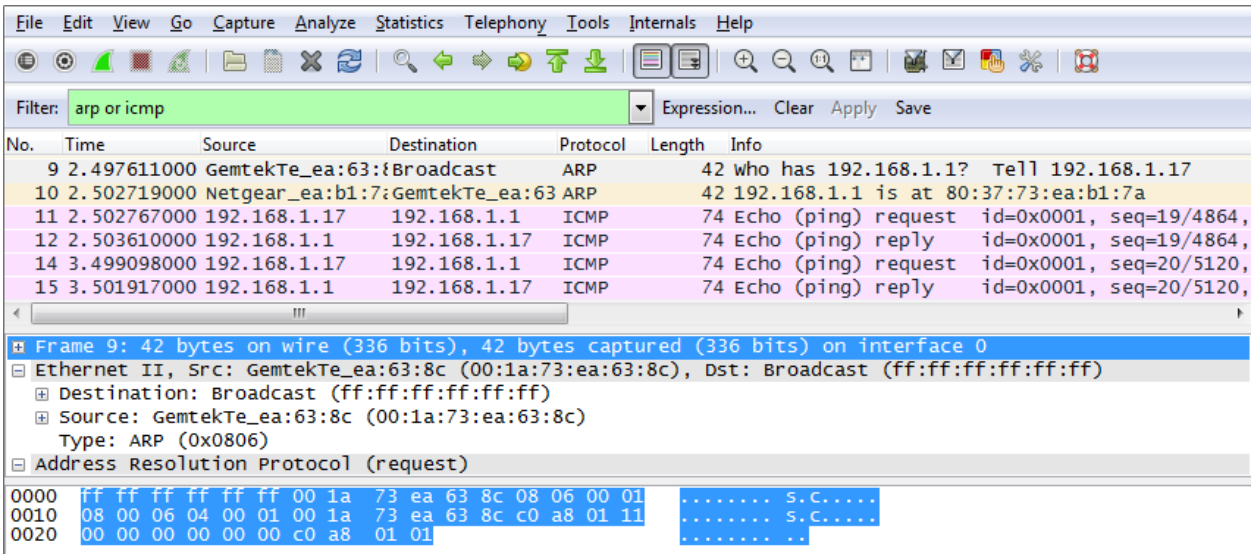
Step 2: Examine the network configuration of the PC.

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
```

Step 3: 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.



Step 4: 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: 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? _____

Part 2: 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.

Step 1: Determine the IP address of the default gateway on your PC.

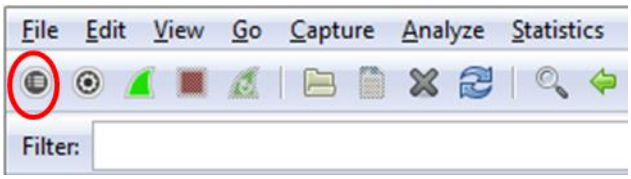
Open a command prompt window and issue the **ipconfig** command.

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

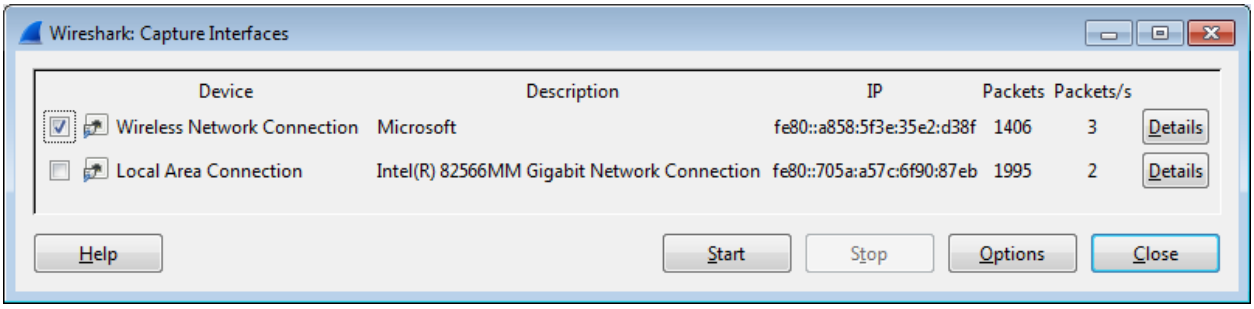
Step 2: Start capturing traffic on your PC's NIC.

a. Open Wireshark.

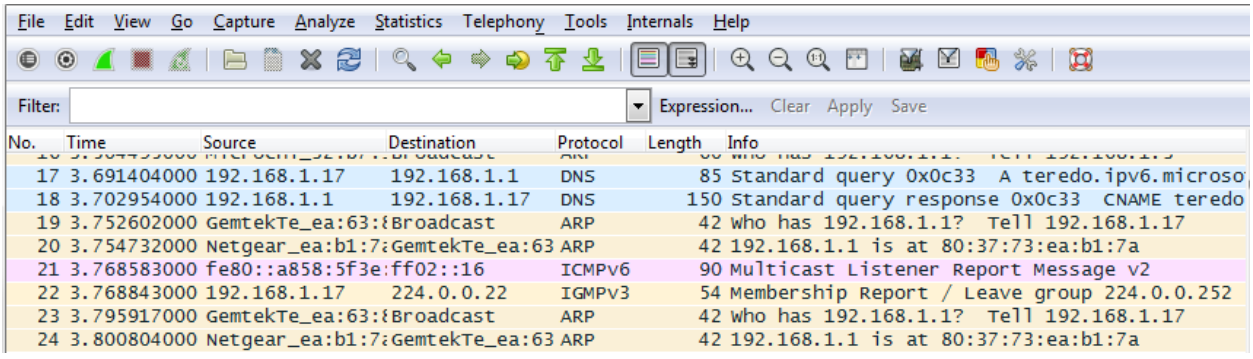
b. On the Wireshark Network Analyzer toolbar, click the **Interface List** icon.



c. 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.



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



Step 3: 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.

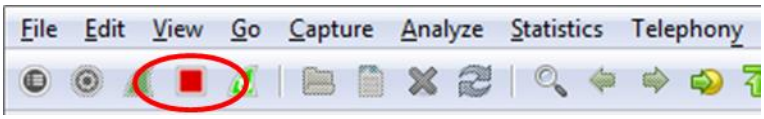
In the Wireshark **Filter** box, type **icmp**. The box should turn green if you typed the filter correctly. If the box is green, click **Apply** to apply the filter.

Step 4: 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.

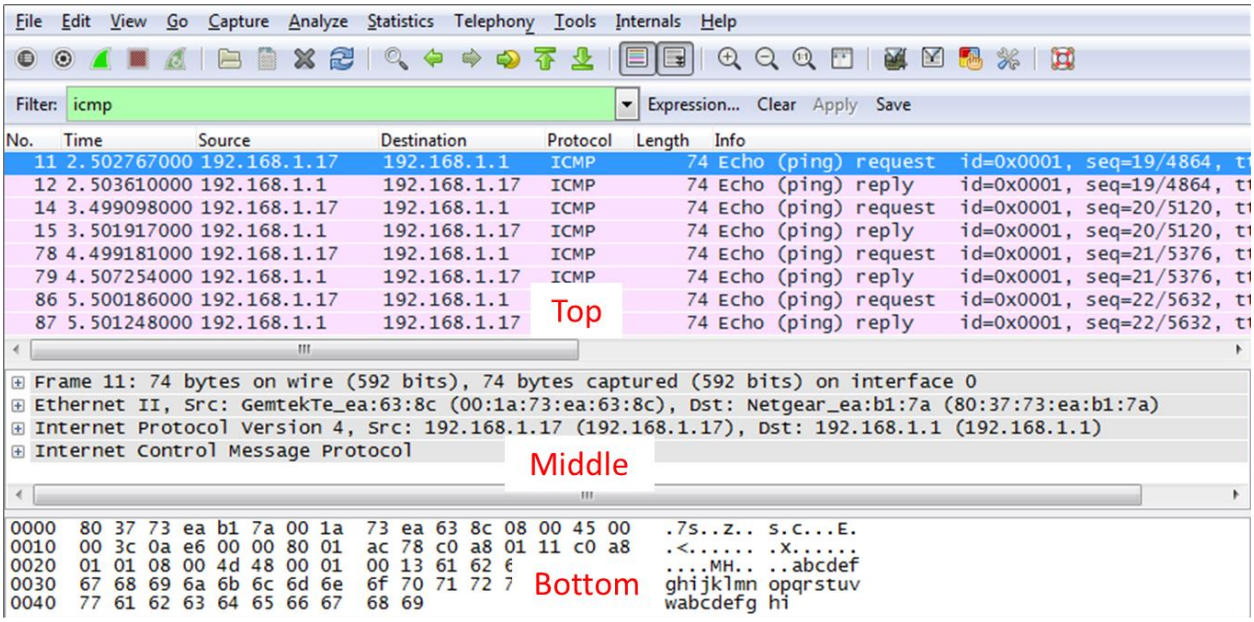
Step 5: Stop capturing traffic on the NIC.

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



Step 6: 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.



a. 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.

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

c. 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? _____

d. 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.

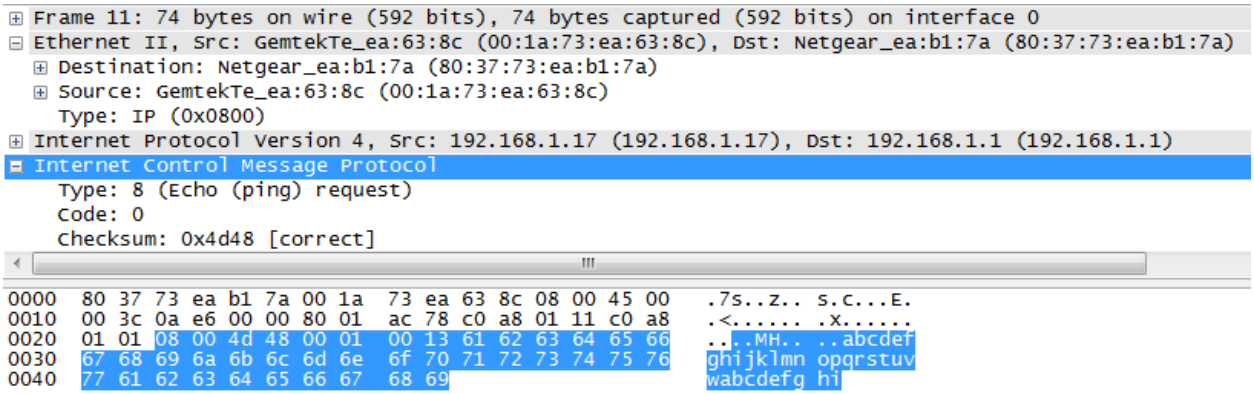
What type of frame is displayed? _____

e. 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? _____

f. 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.



What do the last two highlighted octets spell? _____

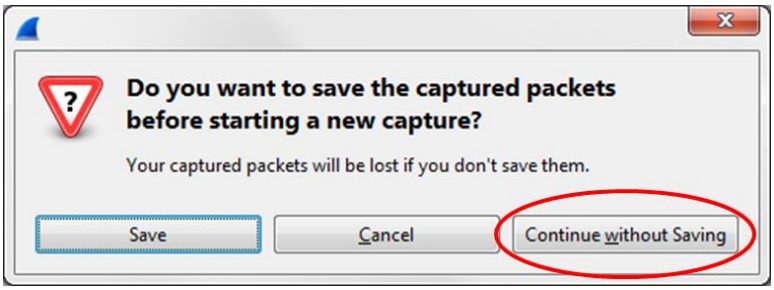
g. Click the next frame in the top section and examine an Echo reply frame. Notice that the source and destination MAC addresses have reversed, because this frame was sent from the default gateway router as a reply to the first ping.

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

_____

Step 7: 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**.



Step 8: In the command prompt window, ping www.cisco.com.

Step 9: Stop capturing packets.

Step 10: 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

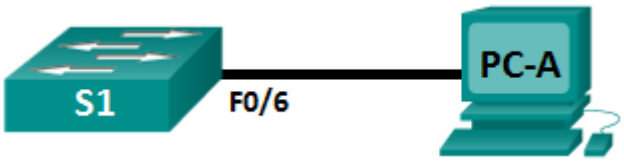
Wireshark does not display the preamble field of a frame header. What does the preamble contain?

_____

_____

Lab – 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.

Step 1: Cable the network as shown in the topology.

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

b. Power on all the devices in the topology.

Step 2: Configure the IPv4 address for the PC.

a. Configure the IPv4 address, subnet mask, and default gateway address for PC-A.

b. From the command prompt on PC-A, ping the switch address.

Were the pings successful? Explain.

_____

Step 3: 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.

a. 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)#
```

b. Assign a hostname to the switch based on the Addressing Table.

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

c. Disable DNS lookup.

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

d. 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
```

Step 4: Verify network connectivity.

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

Part 2: 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.

Step 1: 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 . . . . . . . . . . . : 240920074
```

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.

_____

Step 2: Analyze the MAC address for the S1 F0/6 interface.

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

a. 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?

_____

b. 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?

_____

Step 3: 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

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

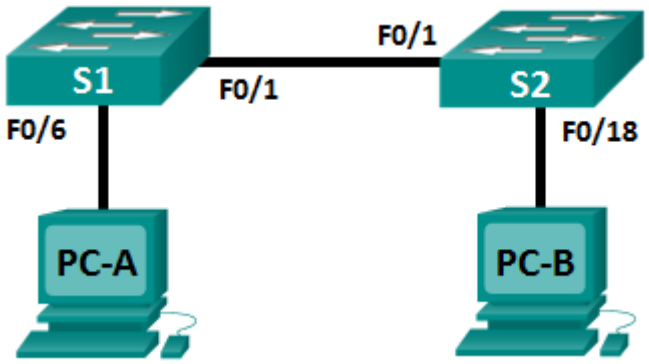
   _____

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

   _____

Lab – 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

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

Step 1: Cable the network according to the topology.

Step 2: Configure PC hosts.

Step 3: Initialize and reload switches as necessary.

Step 4: Configure basic settings for each switch.

a. Configure device name as shown in the topology.

b. Configure IP address as listed in Addressing Table.

c. Assign **cisco** as the console and vty passwords.

d. 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.

Step 1: Record network device MAC addresses.

a. 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: _____

b. 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: _____

Step 2: 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.

a. Establish a console connection to S2 and enter privileged EXEC mode.

b. 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?

_____

_____

_____

_____

Step 3: Clear the S2 MAC address table and display the MAC address table again.

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

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

b. 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? _____

Step 4: From PC-B, ping the devices on the network and observe the switch MAC address table.

a. 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?

_____

b. 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.

_____

_____

c. 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?

_____

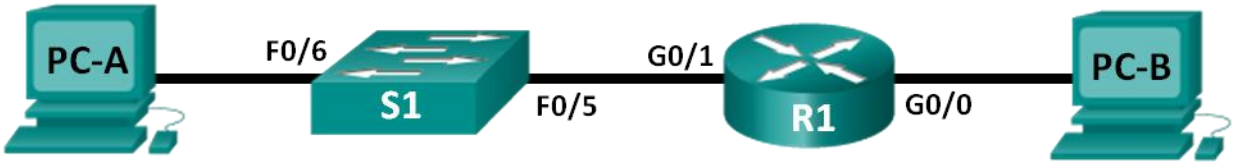
Reflection

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 - 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

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

Step 1: 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.

Step 2: 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. For information on how to initialize and reload these devices, refer to Appendix B.

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.

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

Step 1: 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?

_____

Step 2: 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?

_____

_____

_____

Part 3: Display Device Information

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

Step 1: Retrieve hardware and software information from the network devices.

a. 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?

_____

b. 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?

_____

Step 2: 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?

_____

Step 3: 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?

_____

Step 4: 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.

a. 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                    up
GigabitEthernet0/1         192.168.1.1     YES manual up                    up
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                unassigned      YES unset  administratively down down
R1#
```

b. 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                    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
Switch#
```

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– 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

Part 1: Identify IPv4 Addresses

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

Step 1: 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			

Step 2: 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			

Part 2: Classify IPv4 Addresses

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

Step 1: 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	

Step 2: 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	

Step 3: 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

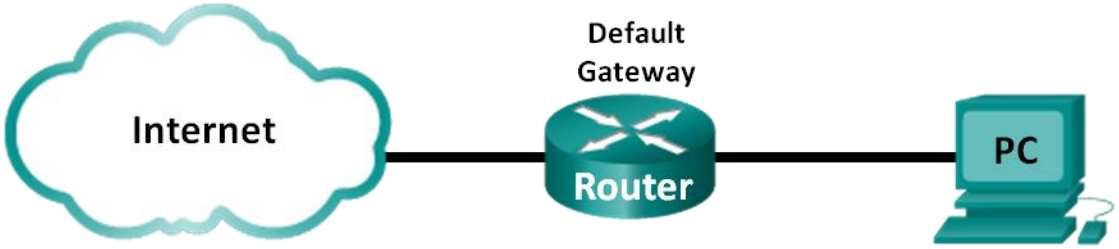
Why should we continue to study and learn about IPv4 addressing if the available IPv4 address space is depleted?

_____

_____

Lab – 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

Required Resources

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

Part 1: 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.

Step 1: 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 x 32 = 128). A non-abbreviated IPv6 host address is shown here:

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

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.

Step 2: 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

Part 2: 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.

Step 1: Check your PC IPv6 network address settings.

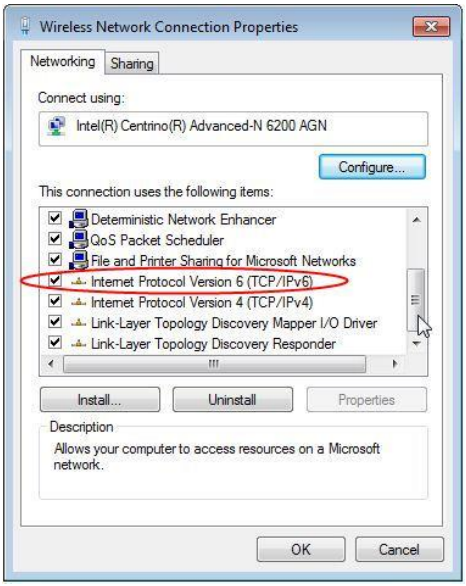
a. Verify that the IPv6 protocol is installed and active on your PC-A (check your Local Area Connection settings).

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.

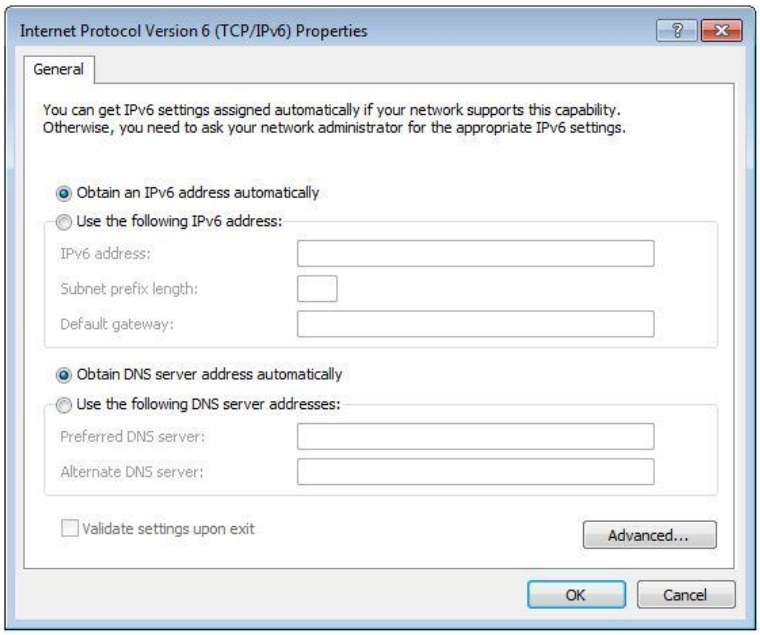
d. On the left side of the window, click **Change adapter settings**. You should now see icons representing your installed network adapters. Right-click your active network interface (it may be a **Local Area Connection** or a **Wireless Network Connection**), and then click **Properties**.

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**?

_____

_____

Part 3: Practice IPv6 Address Abbreviation

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

Step 1: 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:**0**404:**000**1:1000:0000:0000:**0**EF0: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
```

Step 2: 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?

   _____

   _____

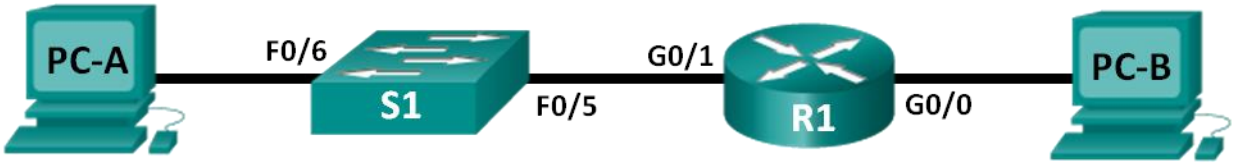
2. Do you think IPv4 networks continue on, or will everyone eventually switch over to IPv6? How long do you think it will take?

   _____

   _____

Lab - 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.

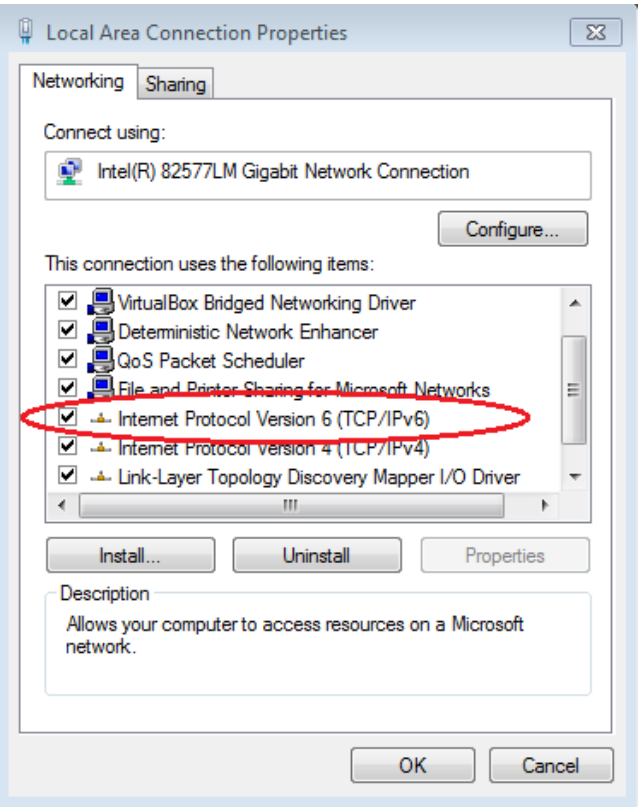
Part 1: Set Up Topology and Configure Basic Router and Switch Settings

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the router and switch.

Step 3: 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.



Step 4: Configure the router.

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

b. Assign the device name to the router.

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.

Step 5: 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.

Part 2: Configure IPv6 Addresses Manually

Step 1: 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?

_____

Step 2: Enable IPv6 routing on R1.

a. 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? _____

b. 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
```

c. 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>
```

d. 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?

_____

_____

Step 3: Assign IPv6 addresses to the management interface (SVI) on S1.

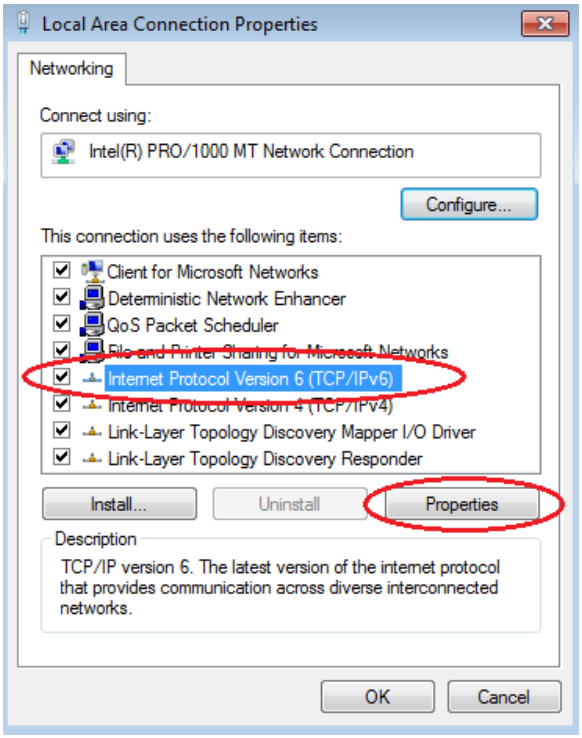
a. Assign the IPv6 address listed in the Addressing Table to the management interface (VLAN 1) on S1. Also assign a link-local address for this interface. IPv6 command syntax is the same as on the router.

b. Verify that the IPv6 addresses are properly assigned to the management interface using the **show ipv6 interface vlan1** command.

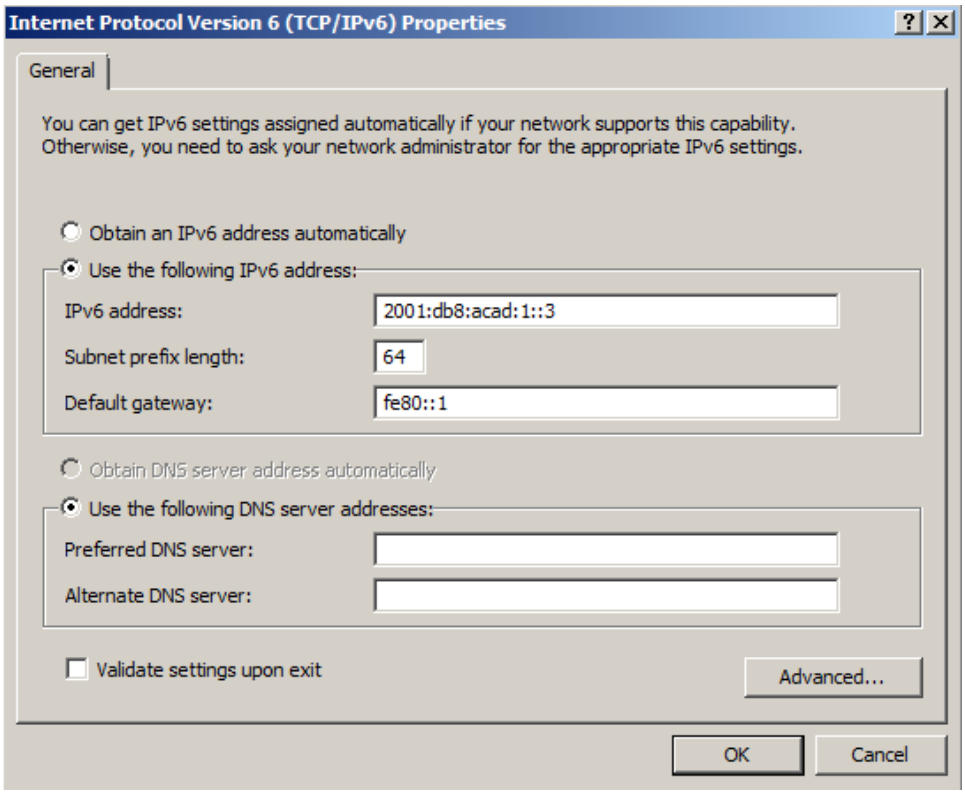
Note: The default 2960 Switch Database Manager (SDM) template does not support IPv6. It may be necessary to issue the command **sdm prefer dual-ipv4-and-ipv6 default** to enable IPv6 addressing before applying an IPv6 address to the VLAN 1 SVI.

Step 4: Assign static IPv6 addresses to the PCs.

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



b. 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**.



c. Click **Close** to close the Local Area Connection Properties window.

d. 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.

e. Issue the **ipconfig** command from the command line on PC-B to verify the IPv6 address information.

Part 3: Verify End-to-End Connectivity

a. 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.

b. 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:\>_
```

c. 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:\>
```

d. 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:\>
```

e. 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

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

   _____

   _____

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

   _____

Lab - 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)

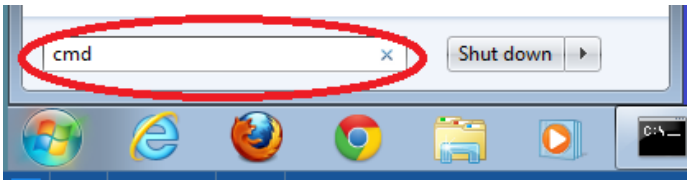
Part 1: Test Network Connectivity Using Ping

Step 1: 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.dscb.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.dscb.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?

_____

_____

Part 2: Trace a Route to a Remote Server Using Tracert

Step 1: 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.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  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
```

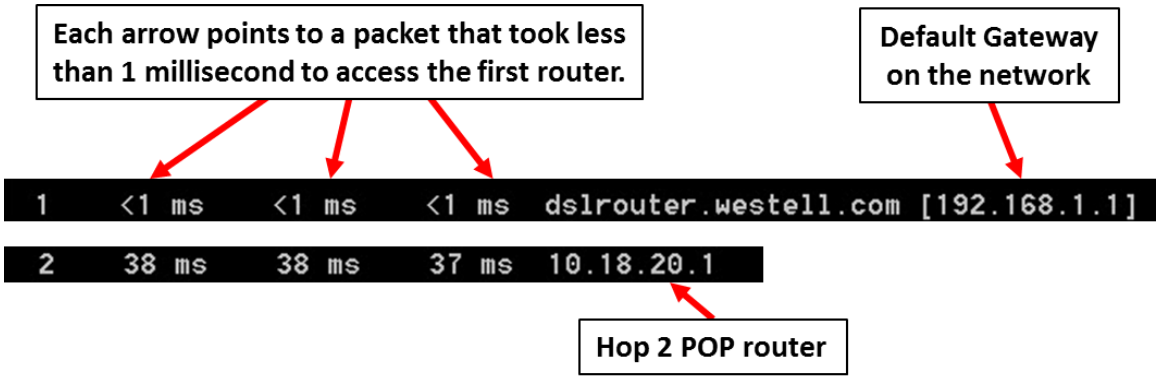
d. Interpreting **tracert** outputs.

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.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  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-pkl-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:

  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    38 ms    38 ms    39 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    42 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    82 ms    47 ms    47 ms  0.ae2.BR3.NYC4.ALTER.NET [152.63.16.49]
  6    46 ms    47 ms    56 ms  204.255.168.194
  7   157 ms   158 ms   157 ms  ge-1-1-0.100.gw1.gc.registro.br [159.63.48.38]
  8   156 ms   157 ms   157 ms  xe-5-0-1-0.core1.gc.registro.br [200.160.0.174]

  9   161 ms   161 ms   161 ms  xe-4-0-0-0.core2.nu.registro.br [200.160.0.164]

 10   158 ms   157 ms   157 ms  ae0-0.ar3.nu.registro.br [200.160.0.249]
 11   176 ms   176 ms   170 ms  gw02.lacnic.registro.br [200.160.0.213]
 12   158 ms   158 ms   158 ms  200.3.12.36
 13   157 ms   158 ms   157 ms  200.3.14.147

Trace complete.
```

What happens in hop 7?

_____

_____

_____

Reflection

What are the functional differences between the commands ping and tracert?

_____

_____