

Practical – Week 2

Objectives:

The aim of this week's practical includes:

- To build a simple network and learn how to do basic switch and end device configuration
- To learn how to use Wireshark to inspect network traffic
- To consolidate the understanding of TCP/IP and OSI models

Tasks:

Accordingly, you will need to complete the following two labs in this week's practical class:

1. Build a simple network
2. Use Wireshark to view network traffic

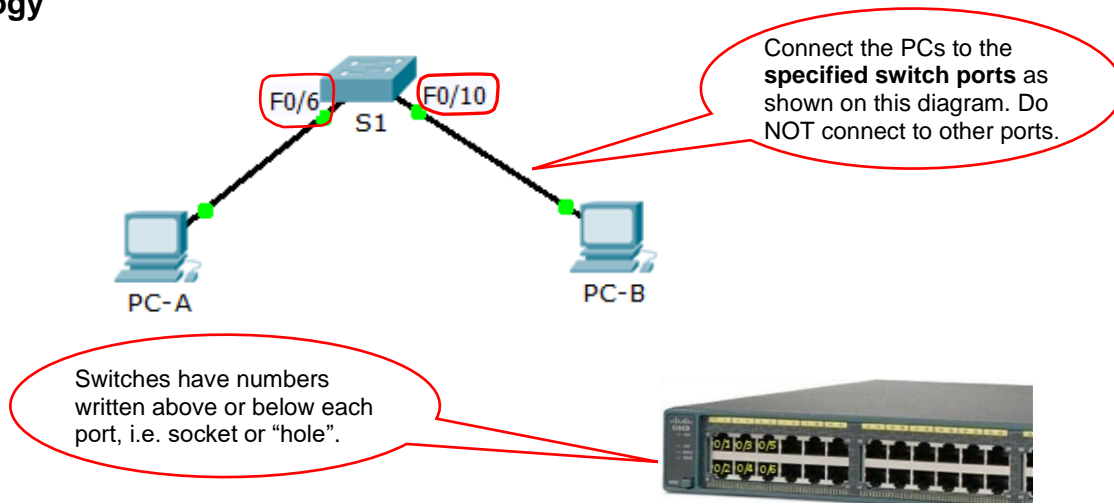
Instructions of the tasks are given in the next pages.

Assessment:

This week's Practical is assessed in class, and it is worth 1% of the total score of the course.

Lab - Build a Simple Network

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A
PC-A	NIC	192.168.1.10	255.255.255.0	N/A
PC-B	NIC	192.168.1.11	255.255.255.0	N/A

Objectives

Part 1: Set Up the Network Topology

- Identify cables and ports for use in the network.
- Cable a physical lab topology.

Part 2: Configure PC Hosts

- Enter static IP address information on the LAN interface of the hosts.
- Verify that PCs can communicate using the **ping** utility.

Part 3: Access a Cisco Switch through the Serial Console Port

- Connect to a Cisco switch using a serial console cable.
- Establish a console session using a terminal emulator, such as Tera Term.

Part 4: Configure and Verify Basic Switch Settings

- Configure the switch with hostname, local passwords, and login banner.
- Set the switch's management address to allow remote switch management
- Display the running switch configuration.
- Display the IOS version for the running switch.
- Display the status of the interfaces.

Background / Scenario

In this lab, you will build a simple network with two hosts and a switch. You will apply IP addressing to the PCs to enable communication between them and use the **ping** utility to verify connectivity.

You will practice how to access a Cisco switch via a direct local connection from a PC's serial port to the console port of the switch, using a terminal emulation program, Tera Term installed on the PC. You will also configure the PC serial port settings for the Tera Term console connection. After you have established a console connection with the Cisco switch, you will configure basic settings of the switch, including hostname, local passwords, and login banner. Use **show** commands to display the running configuration, IOS version, and interface status of the switch.

A Cisco device can also be managed via a remote connection. A Cisco switch has a special interface, known as a switch virtual interface (SVI). The SVI can be configured with an IP address, commonly referred to as the management address. The management address is used for remote access to the switch to display or configure settings. In this lab, you will configure the SVI of the switch, and demonstrate the use of a management IP address for remote switch management.

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

- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs with terminal emulation program, such as Tera Term
- Console cable to configure the Cisco IOS devices via the console port
- Ethernet cables as shown in the topology

Part 1: Set Up the Network Topology

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 switch does not have a power switch. It will power on as soon as you plug in the power cord.

Step 2: Connect the PCs to the switch

Refer to the **Topology Diagram on page 1** of the lab instruction

- Connect one end of the first Ethernet cable to the NIC port on PC-A. Connect the other end of the cable to **F0/6** on S1. After connecting the PC to the switch, you should see the light for F0/6 turn amber and then green, indicating that PC-A has been connected correctly.
- Connect one end of the second Ethernet cable to the NIC port on PC-B. Connect the other end of the cable to **F0/10** on S1. After connecting the PC to the switch, you should see the light for F0/10 turn amber and then green, indicating that the PC-B has been connected correctly.

Note: In our networking laboratory (i.e. practical classroom), following these steps to use an Ethernet cable to connect a PC to a specified Ethernet port, e.g. F0/6 or F0/10 port of a switch:

- 1) Plug the Ethernet cable to the NIC port on the PC.
- 2) **If the switch is on your desk**, plug the other end of the Ethernet cable into the Ethernet port at the front of the switch.

If the switch is on a rack at the front of the classroom, continue with (i) to (iv) below:

- (i) Plug the other end of the Ethernet cable into a yellow, blue, green, or red (but NOT a black/white) socket on the pole/wall in front of you.
- (ii) Remember the socket label and colour (e.g. A3, red)
- (iii) Go to the rack where the switch is mounted, at the front of the rack, find on the patch panel the socket with the same label and colour (A3, red in this example)
- (iv) use a straight-through cable to connect the socket found on the patch panel to the specified Ethernet port, e.g. F0/6 or F0/10 at the front of the rack.

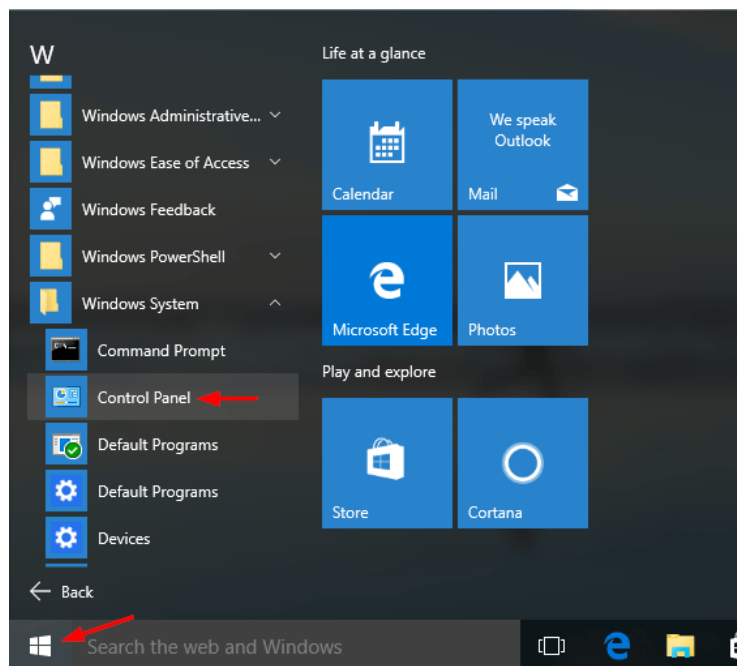
Step 3: Visually inspect network connections.

After cabling the network devices, take a moment to carefully verify the connections to minimize the time required to troubleshoot network connectivity issues later. **If you are unsure if the connections are correct, ask your practical supervisor to help.**

Part 2: Configure PC Hosts

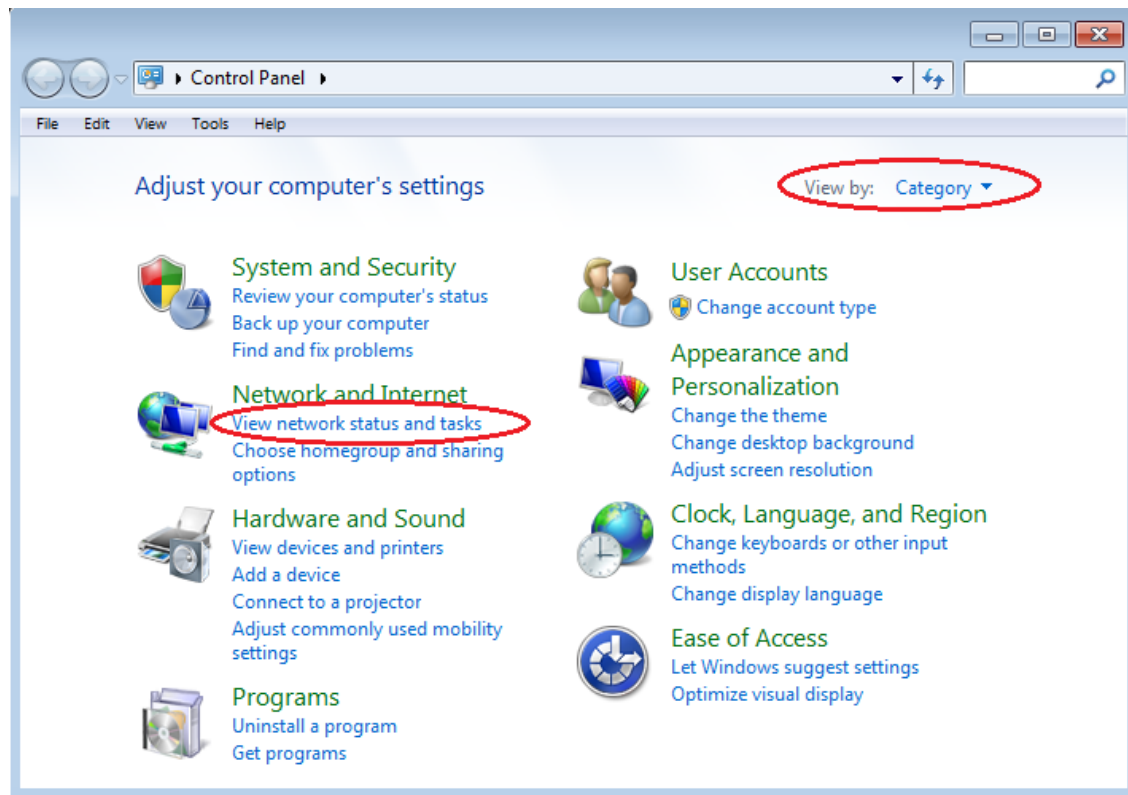
Step 1: Configure static IP address information on the PCs.

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

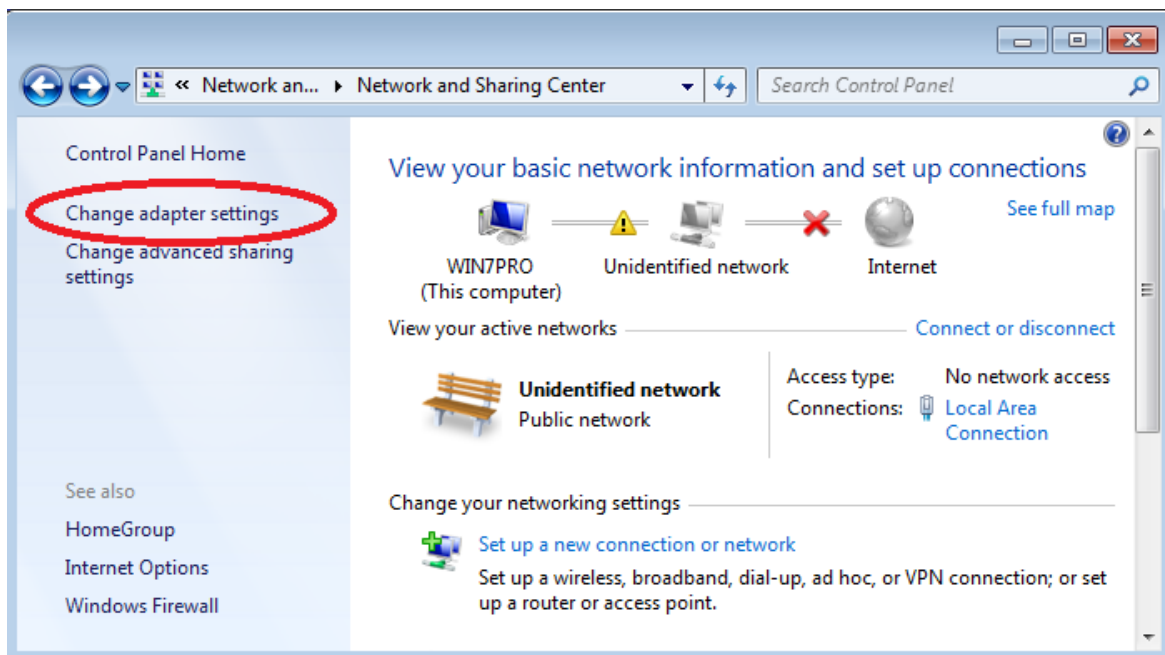


- b. In the Network and Internet section, click the **View network status and tasks** link.

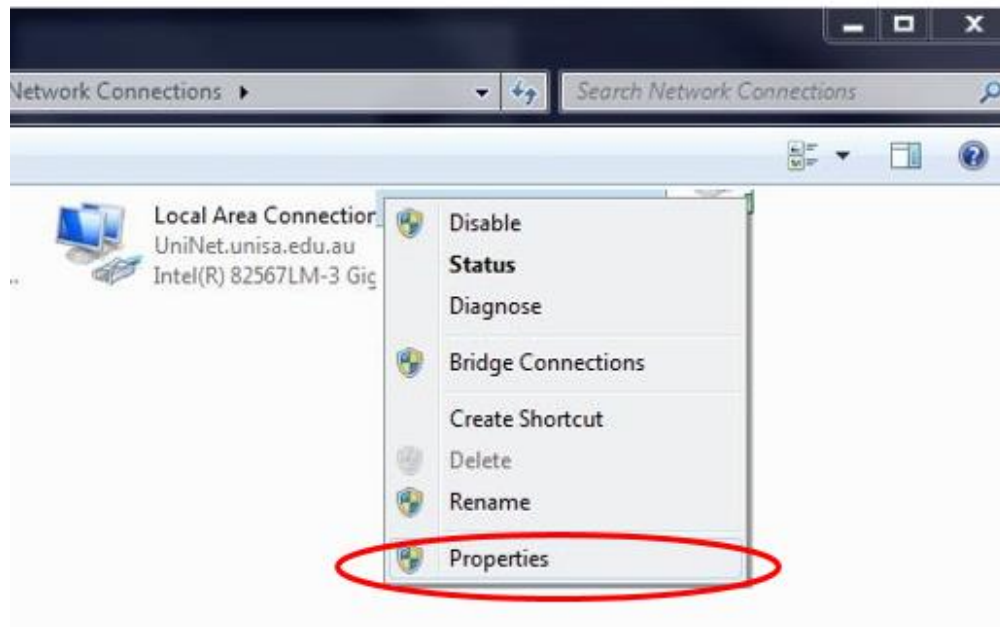
Note: If the Control Panel displays a list of icons, click the drop-down option next to the **View by:** and change this option to display by **Category**.



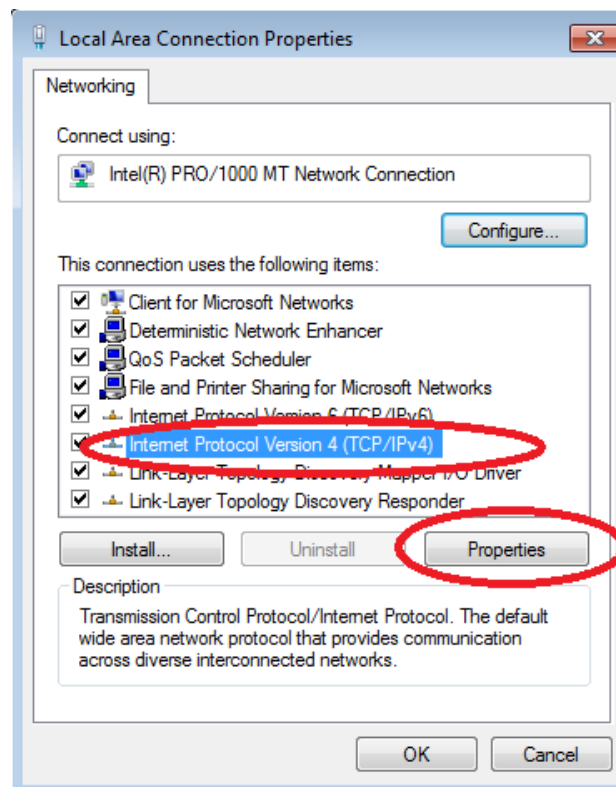
- c. In the left pane of the Network and Sharing Center window, click the **Change adapter settings** link.



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

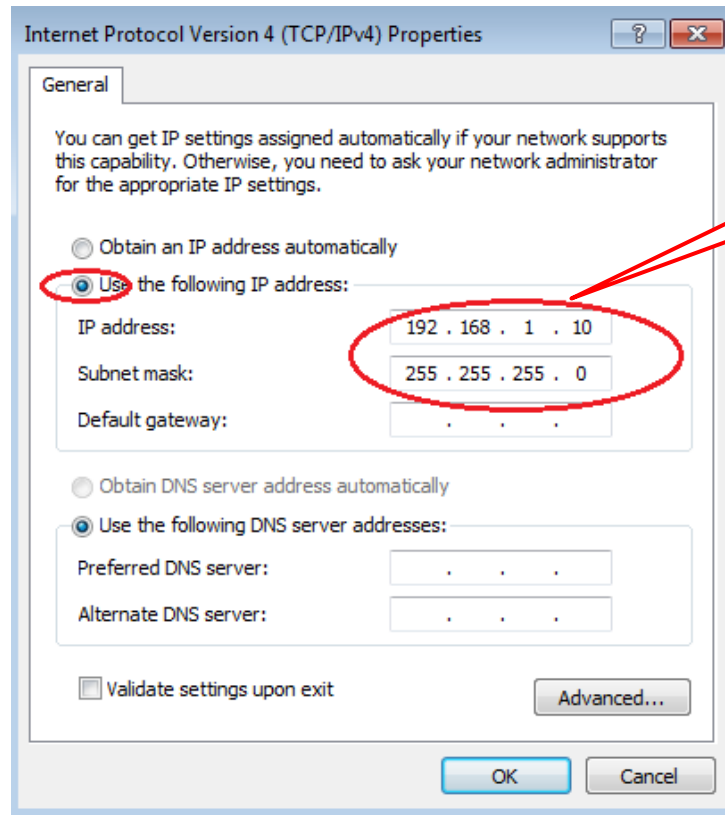


- e. Select the **Internet Protocol Version 4 (TCP/IPv4)** option and then click **Properties**.



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 and subnet mask, as per the IP addressing table shown on Page 1 of this document.



- g. Click "Ok" to close the **Internet Protocol Version 4 (TCP/IPv4) Properties** window and then click "Close" to close the **Local Area Connection Properties** window (i.e. the window opened in step e above) to apply the configured IP address.

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 it is not required for PC-A and PC-B to communicate as the two PCs are in the same IP network. However, when two PCs are in different networks, a router will be needed and each of the PCs will need to have their gateway configured.

- h. After all the IP information has been entered, click **OK**. Then click **OK** on the **Local Area Connection Properties window** to assign the IP address to the LAN adapter.
- i. Repeat the previous steps to enter the IP address information for PC-B. For PC-B's IP address information, see the Addressing Table given at the start of this lab instruction.

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.



Lab - Build a Simple Network

- 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:\Windows\system32\cmd.exe

C:\Users\NetAcad>ipconfig /all

Windows IP Configuration

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

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  : 
   Description . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . : 00-50-56-BE-6C-89
   DHCP Enabled. . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d428:7de2:997c-b05a%11(Preferred)
   IPv4 Address. . . . . : 192.168.1.10(Preferred)
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 
   DHCPv6 IAID . . . . . : 234884137
   DHCPv6 Client DUID. . . . . : 00-01-00-01-17-F6-72-3D-00-0C-29-8D-54-44
```

- c. From PC-A, ping PC-B by typing **ping 192.168.1.11** and press Enter.

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

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

C:\Users\NetAcad>ping 192.168.1.11

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

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

C:\Users\NetAcad>
```

- d. From PC-B, ping PC-A by repeating the previous steps (**Note:** enter PC-A's IP address as the parameter of the ping command)

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: Make a console connection from PC-A to the switch

Console into the Switch from PC-A. (Refer to week 1 practical instruction on the steps of making a console connection from a PC to a switch)

Step 2: Enter privileged EXEC mode.

You can only access limited number of commands in user EXEC mode. To access more commands, you need to enter the privileged EXEC mode. The privileged EXEC command set includes those commands contained in user EXEC mode and the **configure** command through which access to the remaining command

modes are gained. To enter privileged EXEC mode from user 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: Set and verify console password

- a. To secure access to the console line, access config-line mode and set the console password to **cisco**.

```
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

When you set the console password, if you forgot to enter the command "login", what would happen?

- b. Exit privileged mode to verify that the console port password is in effect.

```
S1# exit
Switch con0 is now available
Press RETURN to get started.

User Access Verification
Password:
S1>
```

- c. Enter the console password you have set, i.e. **cisco**, and enter the global configuration mode.

```
S1> enable
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#
```

Step 7: Set and verify enable secret password

- a. To prevent unauthorized access to the privileged EXEC mode, encrypt password needs to be set up. Set the password as **class**

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

- b. Type **Exit** twice to log out of the switch.
- c. Press <Enter> and you will now be asked for a password:

```
User Access Verification
Password:
```

This password is the console password you configured for **line con 0**. Enter this password to return to user EXEC mode.

- d. Enter the privileged EXEC mode.

```
S1> enable
Password:
```

This password is the encrypted password you configured for access to the privileged EXEC mode, i.e. **class**. Enter the password to enter privileged EXEC mode.

Step 8: Enter a login MOTD banner.

- a. 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 #
S1(config)# exit
S1#
```

- b. Verify your access setting by moving between modes.

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

- a. 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 because it is hidden from view. Press Enter after typing in the password.

Step 9: Configure the Switch Management Interface

- 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)#
```

- 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 10: Verify the status of your SVI management interface.

- Use the show ip interface brief command to show the status of the interfaces, including the management interface, VLAN 1. Your VLAN 1 interface should be up and have an IP address assigned. Notice that switch ports F0/6 and F0/10 are also up because PC-A and PC-B are connected to them respectively. 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	up	up
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

Lab - Build a Simple Network

FastEthernet0/24	unassigned	YES	unset	down	down
GigabitEthernet0/1	unassigned	YES	unset	down	down
GigabitEthernet0/2	unassigned	YES	unset	down	down

- b. Record the interface status for the following interfaces.

Interface	S1	
	Status	Protocol
F0/6		
F0/10		
VLAN 1		

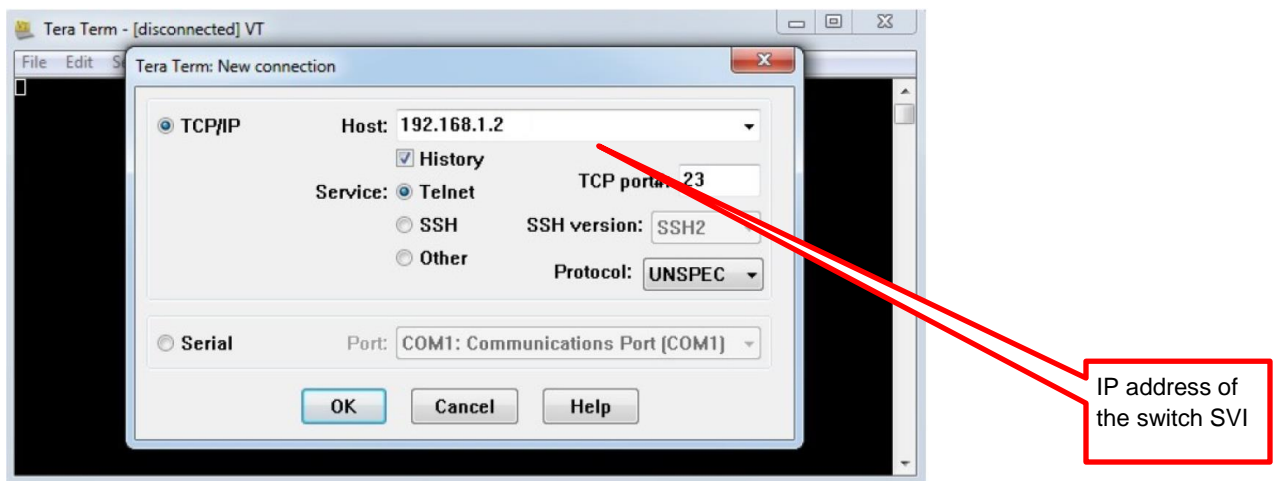
Why are some FastEthernet ports on the switch up and others down?

Step 11: Test and verify remote management of S1.

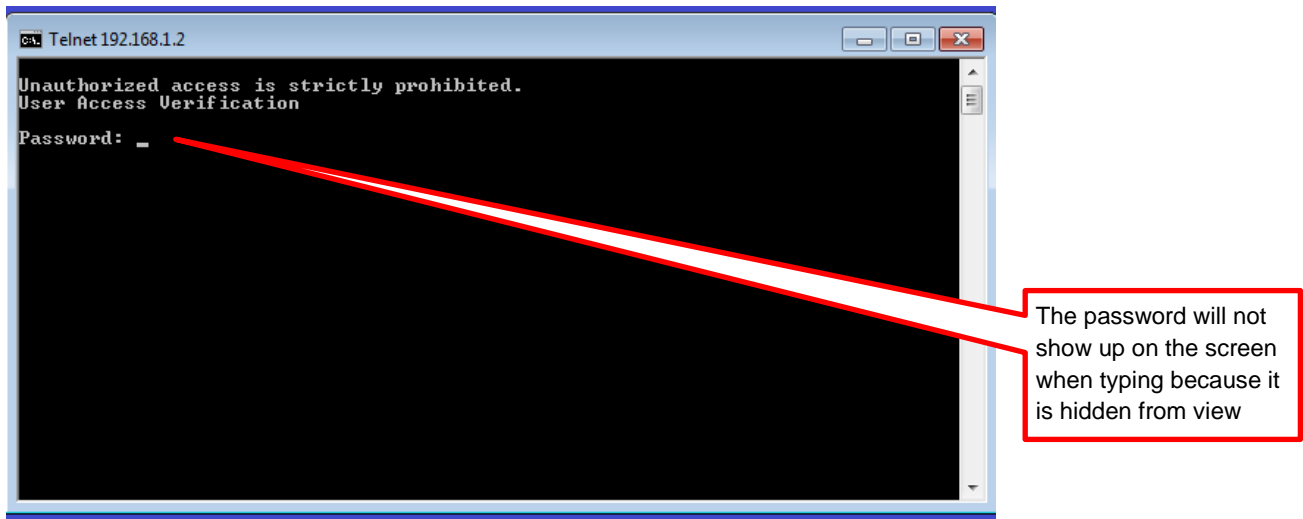
You will now use the Telnet option in Tera Term to remotely access the switch S1 using the SVI management address from **PC-B**.

(Note that in this lab, PC-B 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 plain text. In subsequent labs, you will use Secure Shell (SSH) to remotely access network devices.)

- a. Start Tera Term on PC-B
- b. In the New Connection dialog box, select TCP/IP (rather than the Serial connection used for console connection), then select Telnet, and **type in the IP address of the switch** as shown, Press OK.



- c. You should see a window like the one shown below. Enter the password configured previously (cisco). After entering the password, you will be at the user EXEC mode prompt.



- d. Type **enable** at the prompt. Enter the **class** password to enter privileged EXEC mode.
- e. Enter global configuration mode and change the hostname of the switch to S-B
- ```
S1# config t
S1(config)# hostname S-B
S-B(config)#
```

Now in the Tera Term console window on PC-A press Enter. What is the switch name shown in the window?

### Step 12: 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 Part 4 are highlighted below.

```
S-B# show running-config
Building configuration...
!
Current configuration : 1508 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S-B
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
```

```
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 192.168.1.2 255.255.255.0
!
banner motd ^C
```

```
Unauthorized access is strictly prohibited. ^C
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
end
```

If you were asked to save the running configuration such that it can be loaded when the switch is restarted, what command would you use? (*Please do **NOT** save the running configuration, only answer this question by writing down the command below*)

---

### Step 13: Encrypt the console and vty passwords.

As you noticed in the output of the show running-config command, the **enable secret** password was encrypted, but the **console and vty** passwords were still in plain text. We will now encrypt these plain text passwords using the **service password-encryption** command.

```
S-B# config t
S-B(config)# service password-encryption
S-B(config)# exit
```

Enter the show running-config command again, did you see any difference in the passwords displayed?

---

---

### Step 14: 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.

```
S-B# show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE
SOFTWARE (fcl)
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
(fcl)

S-B 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

## Lab - Build a Simple Network

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](mailto: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  
S-B#

**Ask your practical supervisor to check your work, before moving to the cleanup step blow.**

### Clean up!

Now you've completed the lab. Congratulations! For the smooth running of next class, **please do the following before leaving the classroom:**

- Initialize and reload the switch (see next page for the instruction)
- When the switch has been reloaded, put any cables back to the correct port (i.e. the network cable should be connected to the University network and the console cable taken out of the data point/socket).
- Remove the cables from the rack and the switch/router (if used) and put them into the drawer.



Your practical supervisor may ask you to initialize and reload the switch you have used. Appendix A provides the steps for initializing and reloading a switch.

*However, DO NOT do this step UNTIL your work has been checked by your supervisor and you are required to initialize and reload the switch.*

### Appendix A: Initializing and Reloading a Switch

(Note: Your practical supervisor may ask you to skip steps 1 to 3 below as the switches used may not have VLANs step up.)

#### Step 1: Connect to the switch.

Console into the switch and enter privileged EXEC mode.

```
Switch> enable
Switch#
```

#### Step 2: Determine if there have been any virtual local-area networks (VLANs) created.

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

```
Switch# show flash
```

```
Directory of flash:/
```

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

```
32514048 bytes total (20886528 bytes free)
```

```
Switch#
```

#### Step 3: Delete the VLAN file.

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

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

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

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

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

#### Step 4: Erase the startup configuration file.

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

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

```
[OK]
Erase of nvram: complete
Switch#
```

### Step 5: Reload the switch.

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

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

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

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

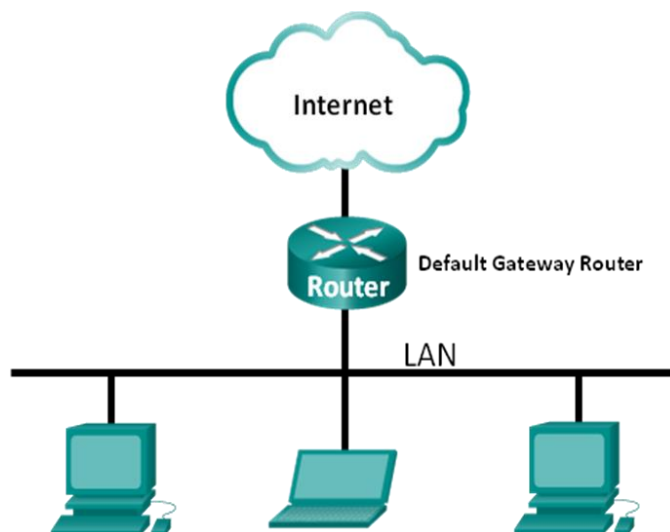
### Step 6: Bypass the initial configuration dialog.

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

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

# Lab - Using Wireshark to View Network Traffic

## Topology



## Objectives

### Part 1: Capture and Analyze Local ICMP Data in Wireshark

- Start and stop data capture of ping traffic to local hosts.
- Locate the IP and MAC address information in captured PDUs.

### Part 2: Capture and Analyze Remote ICMP Data in Wireshark

- Start and stop data capture of ping traffic to remote hosts.
- Locate the IP and MAC address information in captured PDUs.
- Explain why MAC addresses for remote hosts are different than the MAC addresses of local hosts.

## 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. This lab provides instructions for downloading and installing Wireshark, although it may already be installed. In this lab, you will use Wireshark to capture ICMP data packet IP addresses and Ethernet frame MAC addresses.

## Required Resources

- 1 PC with Internet access
- (optional) 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 or your default gateway 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.

**(Note:** Ping can be used to test whether a host is reachable. When a Ping command is issued, a series of ICMP (Internet Control Message Protocol) echo request packets are sent to the target host being “pinged”, and the target host would respond with ICMP response packets if it is reachable.)

### 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.

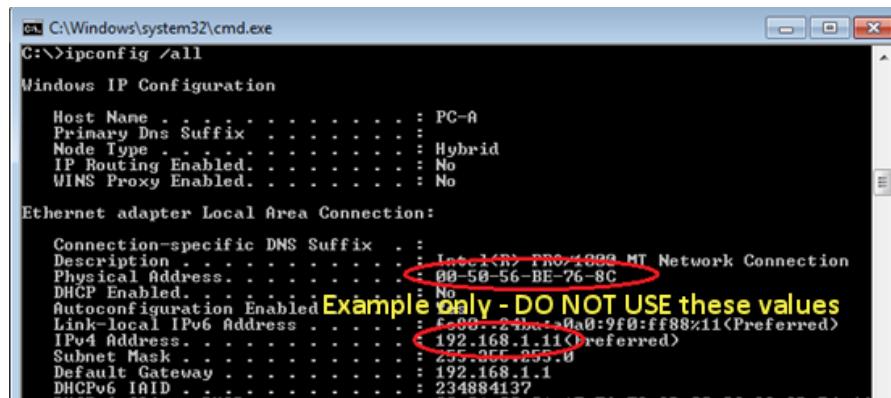
- Open a command window, type **ipconfig /all**, and then press Enter.
- Note your PC interface's IP address and MAC (physical) address.

IP address: \_\_\_\_\_

MAC (physical address): \_\_\_\_\_

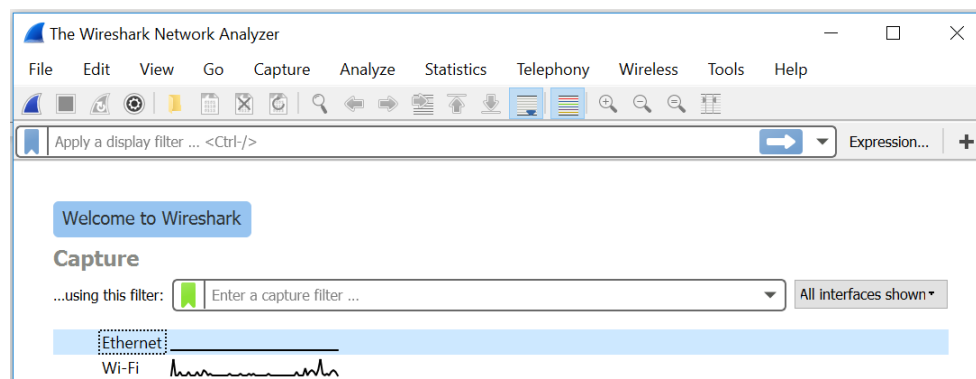
- c. Note your default gateway's IP address too.

IP address: \_\_\_\_\_




## Step 2: Start Wireshark and begin capturing data.

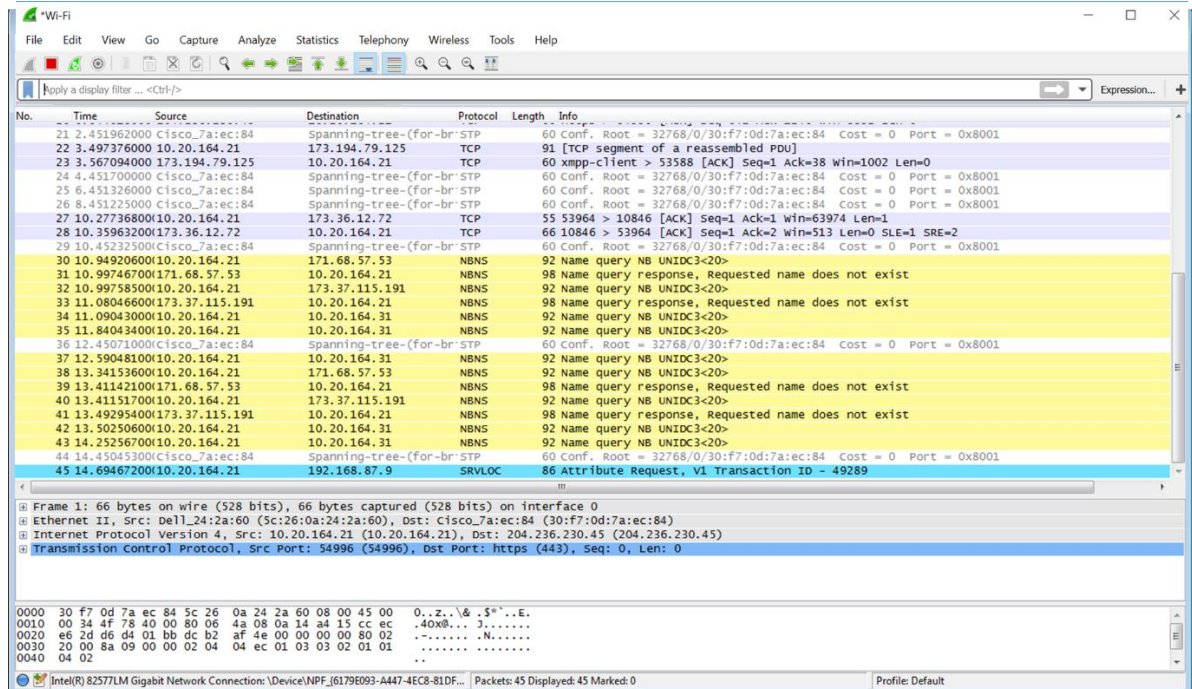
- On your PC, click the Windows **Start** button to see Wireshark listed as one of the programs on the pop-up menu. Double-click **Wireshark**.
- After Wireshark starts, you will see one or more network interfaces as shown below. (Note: when you are in the networking lab at UniSA, you will probably not see any wireless connection, so **choose the Ethernet connection** instead.)



## Using Wireshark to View Network Traffic

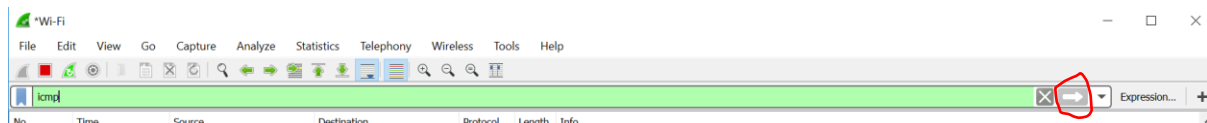
- c. After you have checked the correct interface, in the menu, choose **Capture > Start** or press the  icon to start the data capture.

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



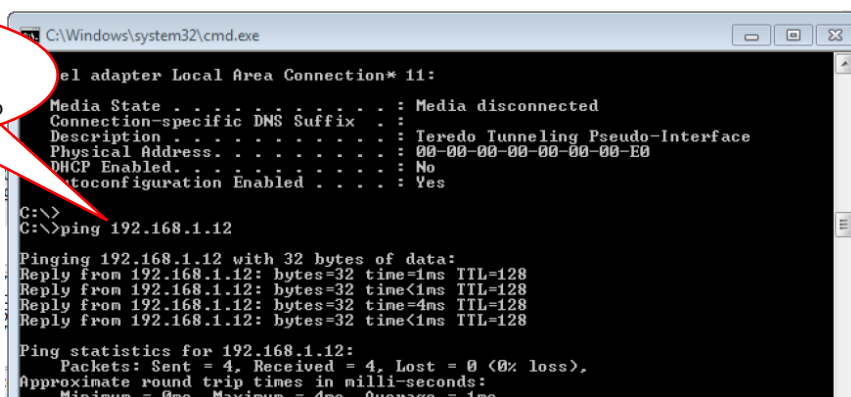
This information can scroll by very quickly depending on what communication is taking place between your PC and the LAN. We can **apply a filter to make it easier to view and work with the data** that is being captured by Wireshark. For this lab, we are only interested in displaying ICMP (ping) PDUs.

- d. Type **icmp** (in lower case) in the Filter box at the top of Wireshark and press Enter or click on the right arrow to view only ICMP (ping) PDUs.



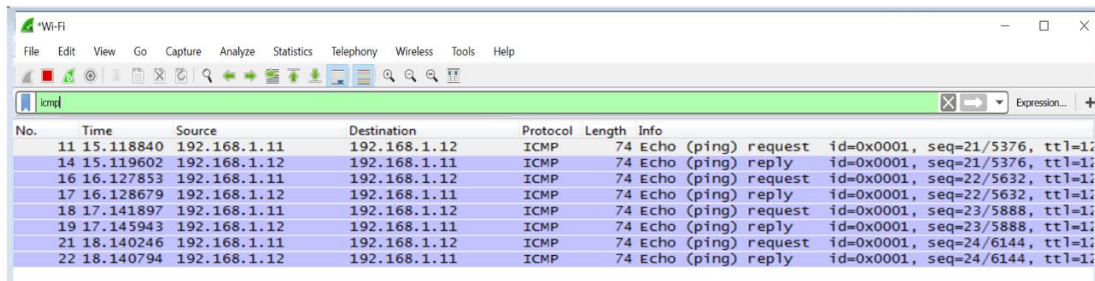
- e. This filter causes all data in the top window to disappear, but you are still capturing the traffic on the interface. You will see output on the screen AFTER the next step is done.
- f. Bring up the command prompt (cmd) window that you opened earlier in Step 1 and **ping your default gateway** or another PC in your network if you know its IP address.

Use your default gateway address identified in Part 1, Step



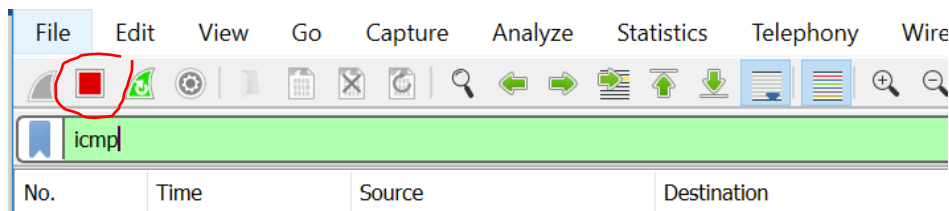
## Using Wireshark to View Network Traffic

Notice that you start seeing data appear in the top window of Wireshark again.



**Note:** If the other PC does not reply to your pings, this may be because their PC firewall is blocking these requests. You could temporarily allow ICMP traffic on that PC, but remember to restore the firewall setting immediately after the lab.

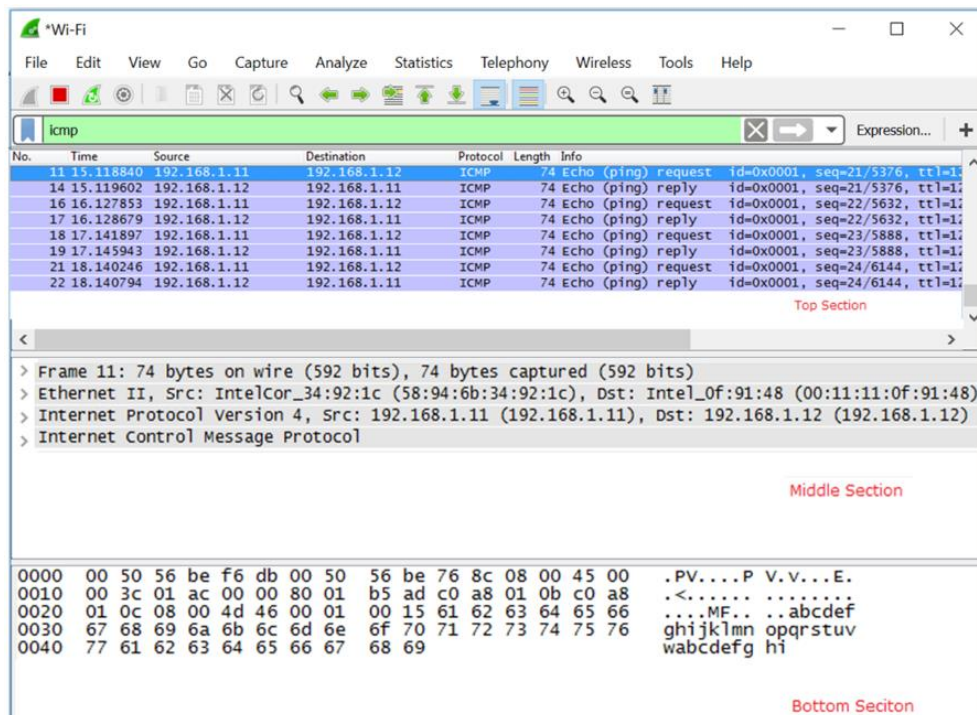
- g. Stop capturing data by clicking the **Stop Capture** icon.



### Step 3: Examine the captured data.

In this step, you will examine the data that was generated by the ping. Note that Wireshark data is displayed in three sections:

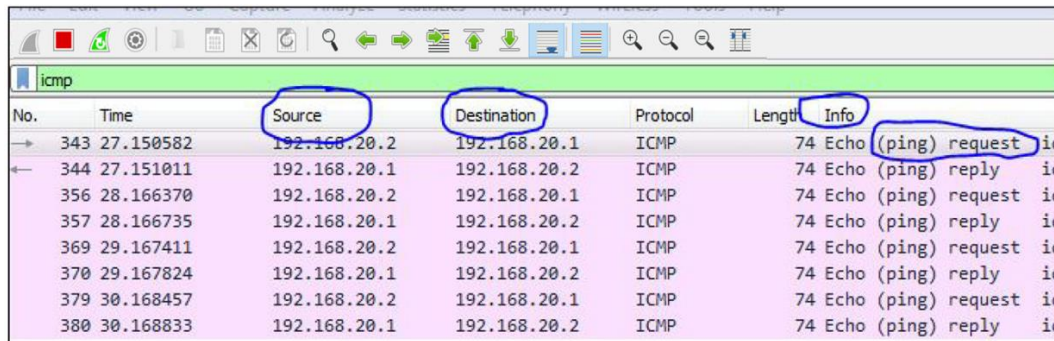
- The **top section** displays the list of PDU frames captured with a summary of the IP packet information
- The **middle section** lists PDU information for the frame selected in the top part of the screen and separates a captured PDU frame by its protocol layers
- The **bottom section** displays the raw data of each layer. The raw data is displayed in both hexadecimal and decimal form.





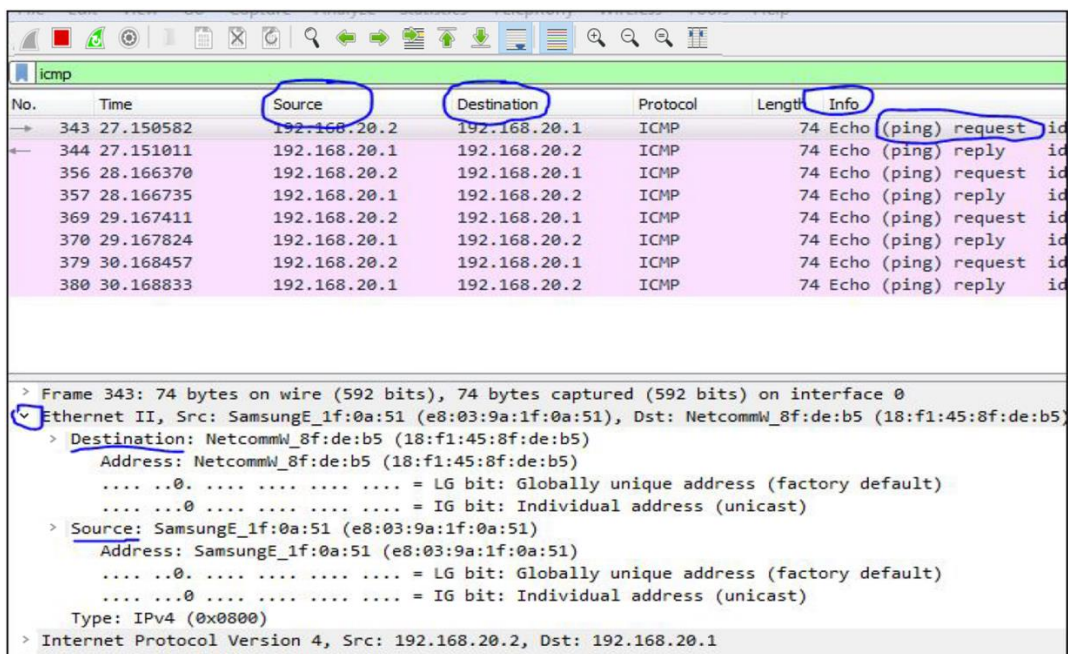
## Using Wireshark to View Network Traffic

- Click the first ICMP (ping) request PDU row in the top section of Wireshark. Notice that the **Source** column has your PC's IP address, and the **Destination** column contains the IP address of the target host you pinged.



| No.   | Time      | Source       | Destination  | Protocol | Length | Info                   |
|-------|-----------|--------------|--------------|----------|--------|------------------------|
| → 343 | 27.150582 | 192.168.20.2 | 192.168.20.1 | ICMP     | 74     | Echo (ping) request id |
| ← 344 | 27.151011 | 192.168.20.1 | 192.168.20.2 | ICMP     | 74     | Echo (ping) reply id   |
| 356   | 28.166370 | 192.168.20.2 | 192.168.20.1 | ICMP     | 74     | Echo (ping) request id |
| 357   | 28.166735 | 192.168.20.1 | 192.168.20.2 | ICMP     | 74     | Echo (ping) reply id   |
| 369   | 29.167411 | 192.168.20.2 | 192.168.20.1 | ICMP     | 74     | Echo (ping) request id |
| 370   | 29.167824 | 192.168.20.1 | 192.168.20.2 | ICMP     | 74     | Echo (ping) reply id   |
| 379   | 30.168457 | 192.168.20.2 | 192.168.20.1 | ICMP     | 74     | Echo (ping) request id |
| 380   | 30.168833 | 192.168.20.1 | 192.168.20.2 | ICMP     | 74     | Echo (ping) reply id   |

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



| No.   | Time      | Source       | Destination  | Protocol | Length | Info                   |
|-------|-----------|--------------|--------------|----------|--------|------------------------|
| → 343 | 27.150582 | 192.168.20.2 | 192.168.20.1 | ICMP     | 74     | Echo (ping) request id |
| ← 344 | 27.151011 | 192.168.20.1 | 192.168.20.2 | ICMP     | 74     | Echo (ping) reply id   |
| 356   | 28.166370 | 192.168.20.2 | 192.168.20.1 | ICMP     | 74     | Echo (ping) request id |
| 357   | 28.166735 | 192.168.20.1 | 192.168.20.2 | ICMP     | 74     | Echo (ping) reply id   |
| 369   | 29.167411 | 192.168.20.2 | 192.168.20.1 | ICMP     | 74     | Echo (ping) request id |
| 370   | 29.167824 | 192.168.20.1 | 192.168.20.2 | ICMP     | 74     | Echo (ping) reply id   |
| 379   | 30.168457 | 192.168.20.2 | 192.168.20.1 | ICMP     | 74     | Echo (ping) request id |
| 380   | 30.168833 | 192.168.20.1 | 192.168.20.2 | ICMP     | 74     | Echo (ping) reply id   |

| Frame 343: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0 |                                                                                                     |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| ✓                                                                                   | Ethernet II, Src: SamsungE_1f:0a:51 (e8:03:9a:1f:0a:51), Dst: NetcommW_8f:de:b5 (18:f1:45:8f:de:b5) |
| Destination: NetcommW_8f:de:b5 (18:f1:45:8f:de:b5)                                  |                                                                                                     |
| Address: NetcommW_8f:de:b5 (18:f1:45:8f:de:b5)                                      |                                                                                                     |
| ... .. = LG bit: Globally unique address (factory default)                          |                                                                                                     |
| ... .. = IG bit: Individual address (unicast)                                       |                                                                                                     |
| Source: SamsungE_1f:0a:51 (e8:03:9a:1f:0a:51)                                       |                                                                                                     |
| Address: SamsungE_1f:0a:51 (e8:03:9a:1f:0a:51)                                      |                                                                                                     |
| ... .. = LG bit: Globally unique address (factory default)                          |                                                                                                     |
| ... .. = IG bit: Individual address (unicast)                                       |                                                                                                     |
| Type: IPv4 (0x0800)                                                                 |                                                                                                     |
| Internet Protocol Version 4, Src: 192.168.20.2, Dst: 192.168.20.1                   |                                                                                                     |

Does the Source MAC address match your PC's MAC address that you recorded in Part 1 Step 1b?

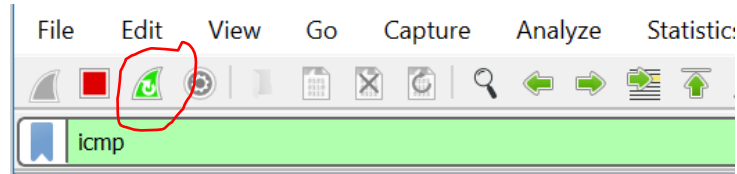
**Note:** In the preceding example of a captured ICMP request, ICMP data is encapsulated inside an IPv4 packet PDU (IPv4 packet) which is then encapsulated in an Ethernet II frame PDU (Ethernet II frame) for transmission on the LAN.

### Part 2: Capture and Analyze Remote ICMP Data in Wireshark

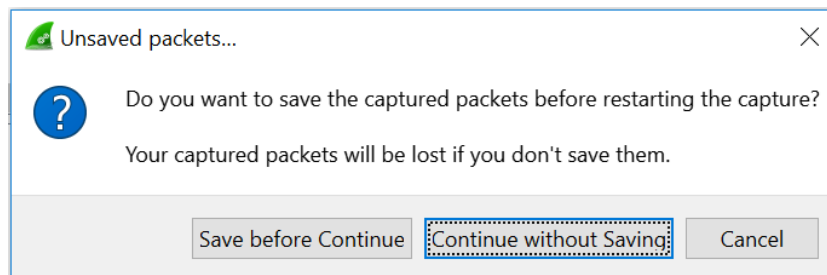
In Part 2, you will ping remote hosts (hosts not on the LAN) and examine the generated data from those pings. You will then determine what is different about this data from the data examined in Part 1.

#### Step 1: Capture remote ICMP data.

- Start capturing data on interface



- 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**.



- With the capture active, ping the following three website URLs:

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

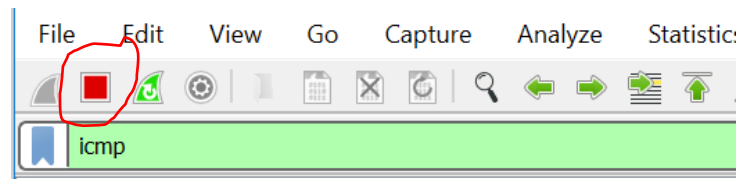
```
C:\Windows\system32\cmd.exe
C:\>ping www.yahoo.com
Pinging www.yahoo.com [72.30.38.140] with 32 bytes of data:
Reply from 72.30.38.140: bytes=32 time<1ms TTL=255
Reply from 72.30.38.140: bytes=32 time<1ms TTL=255
Reply from 72.30.38.140: bytes=32 time<1ms TTL=255
Reply from 72.30.38.140: bytes=32 time<1ms TTL=255
Ping statistics for 72.30.38.140:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping www.cisco.com
Pinging www.cisco.com [198.133.219.25] with 32 bytes of data:
Reply from 198.133.219.25: bytes=32 time<1ms TTL=255
Reply from 198.133.219.25: bytes=32 time<1ms TTL=255
Reply from 198.133.219.25: bytes=32 time<1ms TTL=255
Reply from 198.133.219.25: bytes=32 time<1ms TTL=255
Ping statistics for 198.133.219.25:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping www.google.com
Pinging www.google.com [74.125.129.99] with 32 bytes of data:
Reply from 74.125.129.99: bytes=32 time<1ms TTL=255
Reply from 74.125.129.99: bytes=32 time<1ms TTL=255
Reply from 74.125.129.99: bytes=32 time<1ms TTL=255
Reply from 74.125.129.99: bytes=32 time<1ms TTL=255
Ping statistics for 74.125.129.99:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>_
```

**Note:** When you ping the URLs listed, notice that the Domain Name Server (DNS) translates the URL to an IP address. **Note and write down the IP address received for each URL. Do not use the addresses shown in the above diagram – you must do your own pings.**



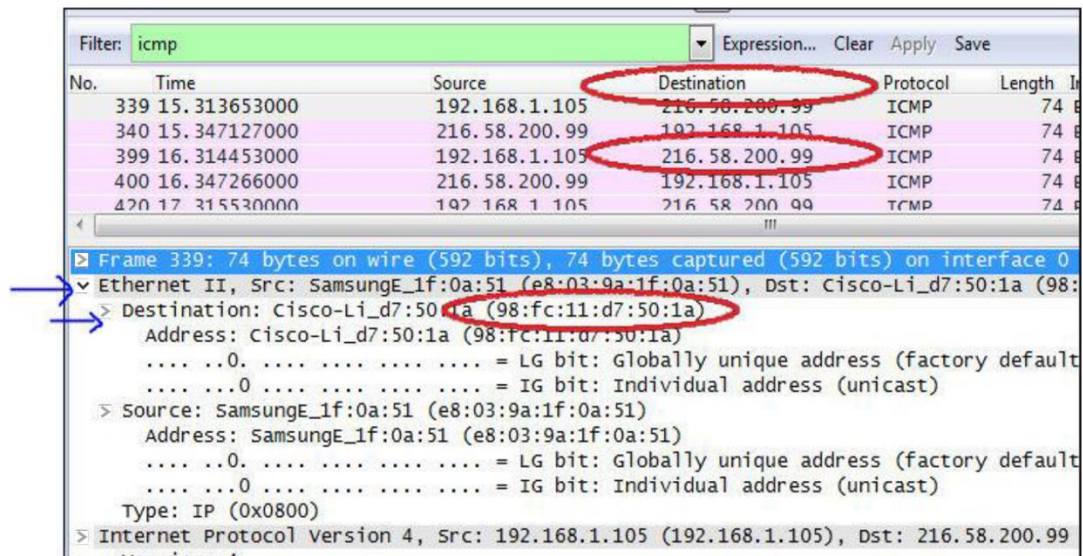
## Using Wireshark to View Network Traffic

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



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

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 you pinged. Use the addresses in your own Wireshark capture, not the example shown above.

Yahoo: IP: \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_ MAC: \_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_\_

Cisco: IP: \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_ MAC: \_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_\_

Google: IP: \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_ MAC: \_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_\_

Compare the addresses, and answer the following questions:

Are the IP addresses the same? (Yes/No)

Are the MAC addresses the same? (Yes/No)

Why do you think this is the case? \_\_\_\_\_