

## Activity 2.2.5: Using NeoTrace™ to View Internetworks

### Learning Objectives

- Explain the use of route tracing programs, such as tracert and NeoTrace.
- Use tracert and NeoTrace to trace a route from its PC to a distant server.
- Describe the interconnected and global nature of the Internet with respect to data flow.

### 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>
```

(Unix and similar systems)

or

```
tracert <destination network name or end device address>
```

(MS Windows systems)

and determines the route taken by packets across an IP network.

The **tracert** (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 the packet was forwarded through. 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 file of data, one can trace each mirror to get a good idea of which mirror would be the fastest to use.

However, it should be noted that because of the "meshed" nature of the interconnected networks that make up the Internet and the Internet Protocol's ability to select different pathways over which to send packets, two trace routes between the same source and destination conducted some time apart may produce different results.

Tools such as these are usually embedded with the operating system of the end device.

Others such as NeoTrace™ are proprietary programs that provide extra information. NeoTrace uses available online information to display graphically the route traced on a global map, for example.

### Scenario

Using an Internet connection, you will use two routing tracing programs to examine the Internet pathway to destination networks.

This activity should be preformed on a computer that has Internet access and access to a command line. First, you will use the Windows embedded **tracert** utility and then the more enhanced NeoTrace program. This lab assumes the installation of NeoTrace. If the computer you are using does not have NeoTrace installed, you can download the program using the following link:

<http://www.softpedia.com/get/Network-Tools/Traceroute-Whois-Tools/McAfee-NeoTrace-Professional.shtml>

If you have any trouble downloading or installing NeoTrace, ask your instructor for assistance.

## Task 1: Trace Route to Remote Server.

### Step 1: Trace the route to a distant network.

To trace the route to a distant network, the PC being used must have a working connection to the class/lab network.

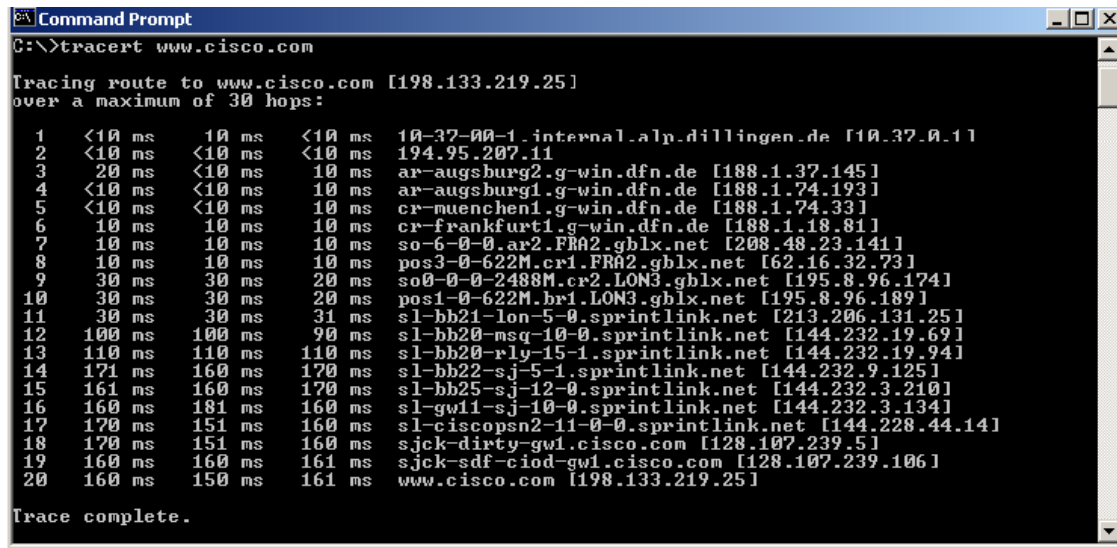
1. At the command line prompt, type: `tracert www.cisco.com`

The first output line should show the Fully Qualified Domain Name (FQDN) followed by the IP address. The Lab Domain Name Service (DNS) server was able to resolve the name to an IP address. Without this name resolution, the `tracert` would have failed, because this tool operates at the TCP/IP layers that only understand valid IP addresses.

If DNS is not available, the IP address of the destination device has to be entered after the `tracert` command instead of the server name.

2. Examine the output displayed.

How many hops between the source and destination? \_\_\_\_\_



```
Command Prompt
C:\>tracert www.cisco.com

Tracing route to www.cisco.com [198.133.219.25]
over a maximum of 30 hops:
  0  <10 ms    <10 ms    <10 ms    10-37-00-1.internal.alp.dillingen.de [10.37.0.1]
  1  <10 ms    <10 ms    <10 ms    194.95.207.11
  2  <10 ms    <10 ms    <10 ms    ar-augsburg2.g-win.dfn.de [188.1.37.145]
  3  <10 ms    <10 ms    <10 ms    ar-augsburg1.g-win.dfn.de [188.1.74.193]
  4  <10 ms    <10 ms    <10 ms    cr-muenchen1.g-win.dfn.de [188.1.74.33]
  5  <10 ms    <10 ms    <10 ms    cr-frankfurt1.g-win.dfn.de [188.1.18.81]
  6  <10 ms    <10 ms    <10 ms    so-6-0-0.ar2.FRA2.gblx.net [208.48.23.141]
  7  <10 ms    <10 ms    <10 ms    pos3-0-622M.cr1.FRA2.gblx.net [62.16.32.73]
  8  <10 ms    <10 ms    <10 ms    so0-0-0-2488M.cr2.LON3.gblx.net [195.8.96.174]
  9  <10 ms    <10 ms    <10 ms    pos1-0-622M.br1.LON3.gblx.net [195.8.96.189]
 10  <10 ms    <10 ms    <10 ms    sl-bb21-lon-5-0.sprintlink.net [213.206.131.25]
 11  <10 ms    <10 ms    <10 ms    sl-bb20-msq-10-0.sprintlink.net [144.232.19.69]
 12  <10 ms    <10 ms    <10 ms    sl-bb20-rly-15-1.sprintlink.net [144.232.19.94]
 13  <10 ms    <10 ms    <10 ms    sl-bb22-sj-5-1.sprintlink.net [144.232.9.125]
 14  <10 ms    <10 ms    <10 ms    sl-bb25-sj-12-0.sprintlink.net [144.232.3.210]
 15  <10 ms    <10 ms    <10 ms    sl-gw11-sj-10-0.sprintlink.net [144.232.3.134]
 16  <10 ms    <10 ms    <10 ms    sl-ciscopsn2-11-0-0.sprintlink.net [144.228.44.14]
 17  <10 ms    <10 ms    <10 ms    sjck-dirty-gw1.cisco.com [128.107.239.5]
 18  <10 ms    <10 ms    <10 ms    sjck-sdf-ciod-gw1.cisco.com [128.107.239.106]
 19  <10 ms    <10 ms    <10 ms    www.cisco.com [198.133.219.25]
 20  <10 ms    <10 ms    <10 ms    www.cisco.com [198.133.219.25]

Trace complete.
```

Figure 1. tracert Command

Figure 1 shows the successful result when running:

`tracert www.cisco.com`

from a location in Bavaria, Germany.

The first output line shows the FQDN, followed by the IP address. Therefore, a DNS server was able to resolve the name to an IP address. Then there are listings of all routers through which the `tracert` requests had to pass to get to the destination.

3. Try the same trace route on a PC connected to the Internet, and examine your output.

Number of hops to www.cisco.com: \_\_\_\_\_

**Step 2: Try another trace route on the same PC, and examine your output.**

Destination URL: \_\_\_\_\_

Destination IP Address: \_\_\_\_\_

**Task 2: Trace Route using NeoTrace.**

1. Launch the NeoTrace program.
2. On the **View** menu, choose **Options**. Click the **Map** tab and in the **Home Location** section click the **Set Home Location** button.
3. Follow the instructions to select your country and location in your country.  
Alternatively, you can click the **Advanced** button, which enables you to enter the precise latitude and longitude of your location. See the Challenge section of Activity 1.2.5(1).
4. Enter "www.cisco.com" in the **Target** field and click **Go**.
5. From the **View** menu, **List View** displays the list of routers similar to `tracert`.  
**Node View** from the **View** menu displays the connections graphically with symbols.  
**Map View** on the **View** menu displays the links and routers in their geographic location on a global map.
6. Select each view in turn and note the differences and similarities.
7. Try a number of different URLs and view the routes to those destinations.

**Task 3: Reflection**

Review the purpose and usefulness of trace route programs.

Relate the displays of the output of NeoTrace to the concept of interconnected networks and the global nature of the Internet.

**Task 4: Challenge**

Consider and discuss possible network security issues that could arise from the use of programs like traceroute and NeoTrace. Consider what technical details are revealed and how perhaps this information could be misused.

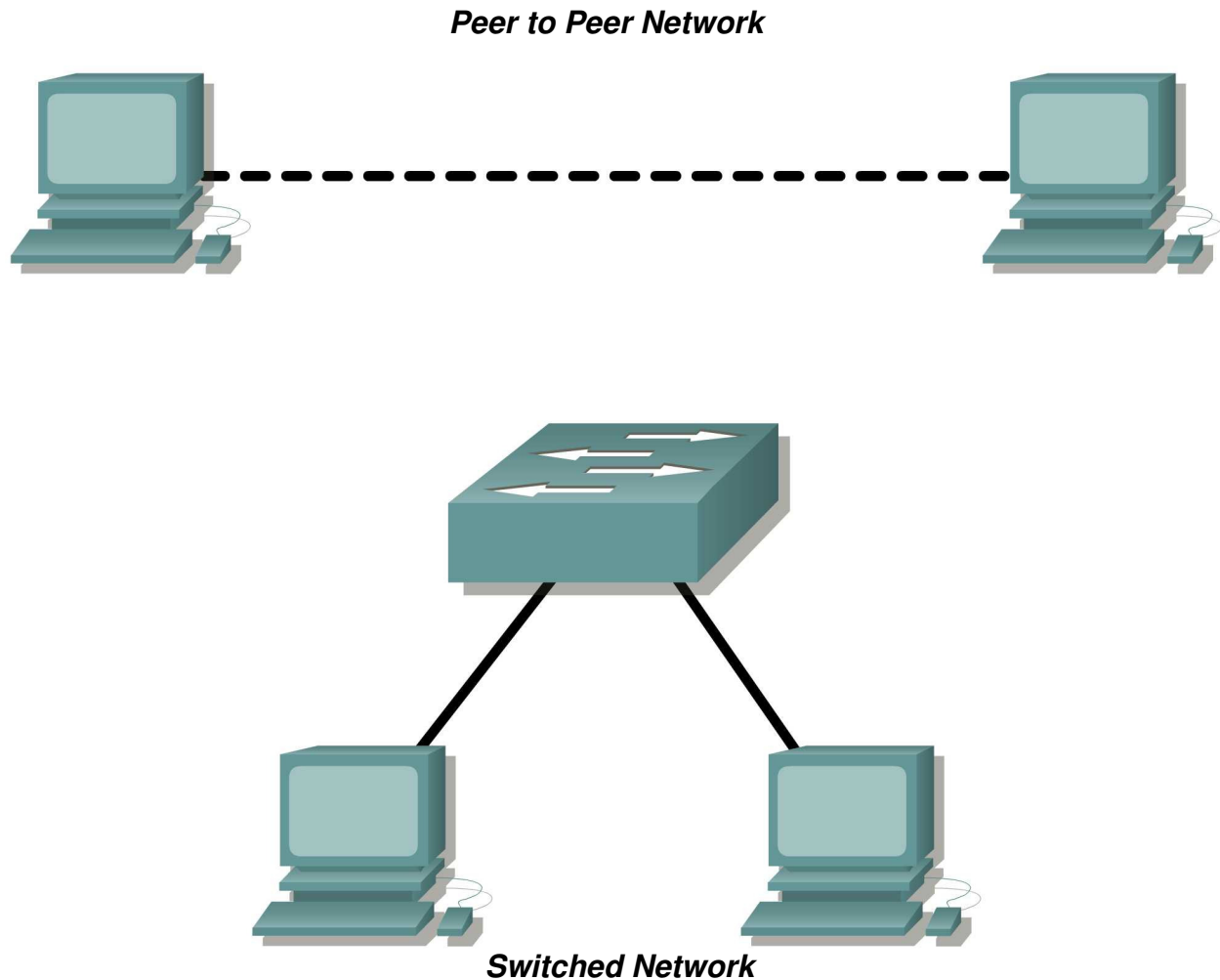
**Task 5: Clean Up**

Exit the NeoTrace program.

Unless instructed otherwise by your instructor, properly shut down the computer.

## Lab 2.6.1: Topology Orientation and Building a Small Network

### Topology Diagram



### Learning Objectives

Upon completion of this lab, you will be able to:

- Correctly identify cables for use in the network.
- Physically cable a peer-to-peer and switched network.
- Verify basic connectivity on each network.

### Background

Many network problems can be fixed at the Physical layer of a network. For this reason, it is important to have a clear understanding of which cables to use for your network connections.

At the Physical layer (Layer 1) of the OSI model, end devices must be connected by media (cables). The type of media required depends on the type of device being connected. In the basic portion of this lab, straight-through or patch—cables will be used to connect workstations and switches.

In addition, two or more devices communicate through an address. The Network layer (Layer 3) requires a unique address (also known as a logical address or IP Addresses), which allows the data to reach the appropriate destination device.

Addressing for this lab will be applied to the workstations and will be used to enable communication between the devices.

## Scenario

This lab starts with the simplest form of networking (peer-to-peer) and ends with the lab connecting through a switch.

### Task 1: Create a Peer-to-Peer Network.

**Step 1: Select a lab partner.**

**Step 2: Obtain equipment and resources for the lab.**

Equipment needed:

- 2 workstations
- 2 straight through (patch) cables
- 1 crossover cable
- 1 switch (or hub)

### Task 2: Identify the Cables used in a Network.

Before the devices can be cabled, you will need to identify the types of media you will be using. The cables used in this lab are crossover and straight-through.

Use a **crossover cable** to connect two workstations to each other through their NIC's Ethernet port. This is an Ethernet cable. When you look at the plug you will notice that the orange and green wires are in opposite positions on each end of the cable.

Use a **straight-through cable** to connect the router's Ethernet port to a switch port or a workstation to a switch port. This is also an Ethernet cable. When you look at the plug you will notice that both ends of the cable are exactly the same in each pin position.

### Task 3: Cable the Peer-to-peer Network.



**Step 1: Connect two workstations.**

Using the correct Ethernet cable, connect two workstations together. Connect one end of the cable to the NIC port on PC1 and the other end of the cable to PC2.

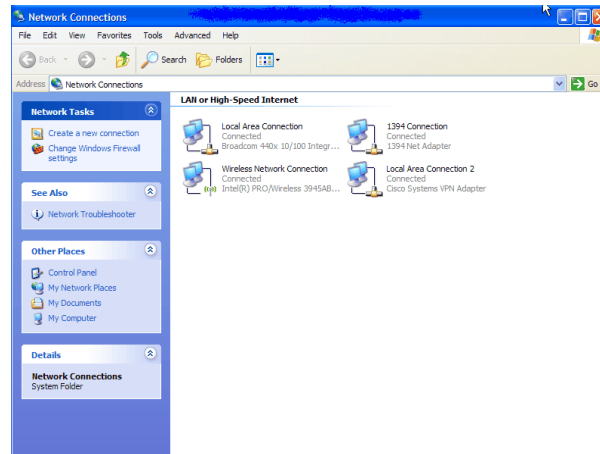
Which cable did you use? \_\_\_\_\_

## Step 2: Apply a Layer 3 address to the workstations.

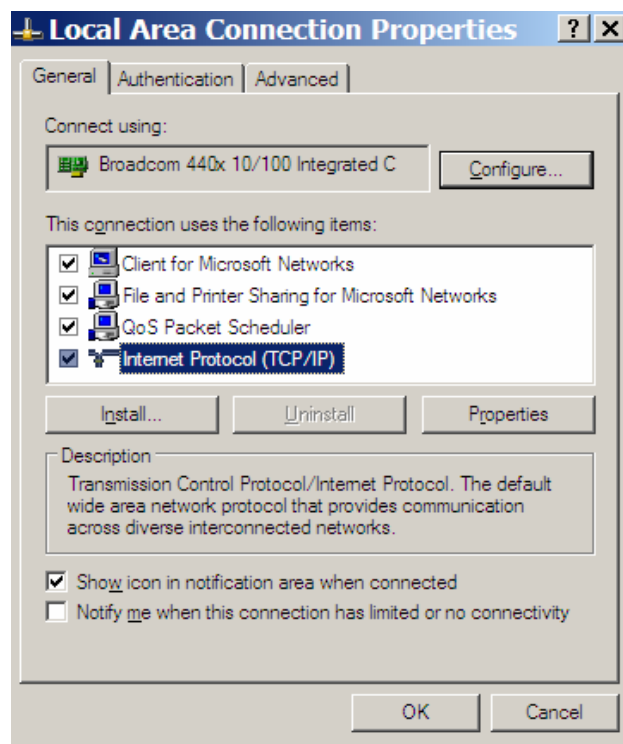
To complete this task, you will need to follow the step-by-step instructions below.

**Note:** These steps must be completed on *each* workstation. The instructions are for Windows XP—steps may differ slightly if you are using a different operating system.

1. On your computer, click **Start**, right-click **My Network Places**, and then click **Properties**. The Network Connections window should appear, with icons showing the different network connections.

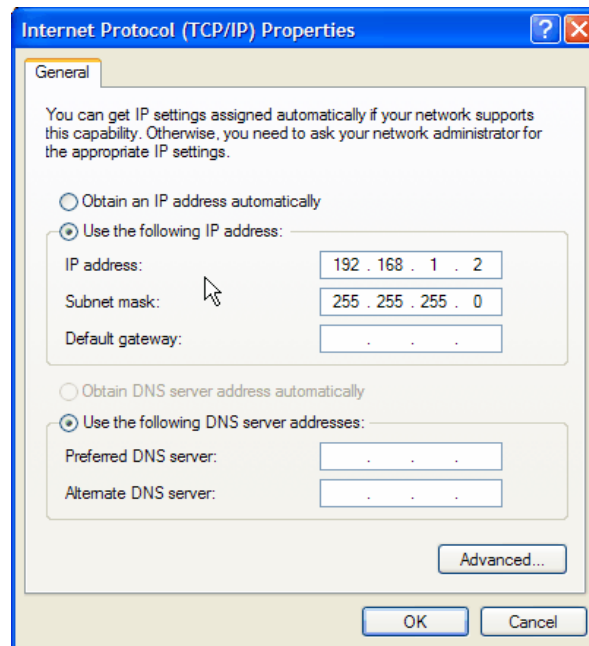


2. Right-click the **Local Area Connection** and click **Properties**.
3. Select the **Internet Protocol (TCP/IP)** item and then click the **Properties** button.



4. On the General tab of the Internet Protocol (TCP/IP) Properties window, select the **Use the following IP address** option.

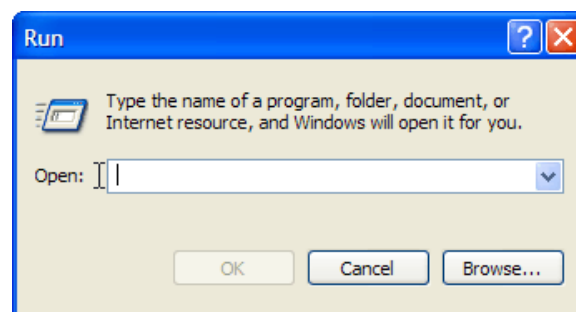
5. In the **IP address** box, enter the IP address 192.168.1.2 for PC1. (Enter the IP address 192.168.1.3 for PC2.)
6. Press the tab key and the Subnet mask is automatically entered. The subnet address should be 255.255.255.0. If this address is not automatically entered, enter this address manually.
7. Click **OK**.



8. Close the Local Area Connection Properties window.

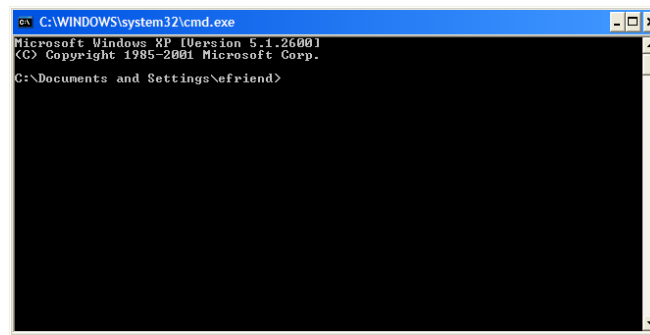
### Step 3: Verify connectivity.

1. On your computer, click **Start**, and then click **Run**.



2. Type **cmd** in the Open box and then click **OK**.

The DOS command (cmd.exe) window will appear. You can enter DOS commands using this window. For the purposes of this lab, basic network commands will be entered to allow you to test you computer connections.



The **ping** command is a computer network tool used to test whether a host (workstation, router, server, etc.) is reachable across an IP network.

3. Use the **ping** command to verify that PC1 can reach PC2 and PC2 can reach PC1. From the PC1 DOS command prompt, type **ping 192.168.1.3**. From the PC2 DOS command prompt, type **ping 192.168.1.2**.

What is the output of the **ping** command?

---

---

---

---

If the **ping** command displays an error message or doesn't receive a reply from the other workstation, troubleshoot as necessary. Possible areas to troubleshoot include:

- Verifying the correct IP addresses on both workstations
- Ensuring that the correct type of cable is used between the workstations

What is the output of the **ping** command if you unplug the network cable and ping the other workstation?

---

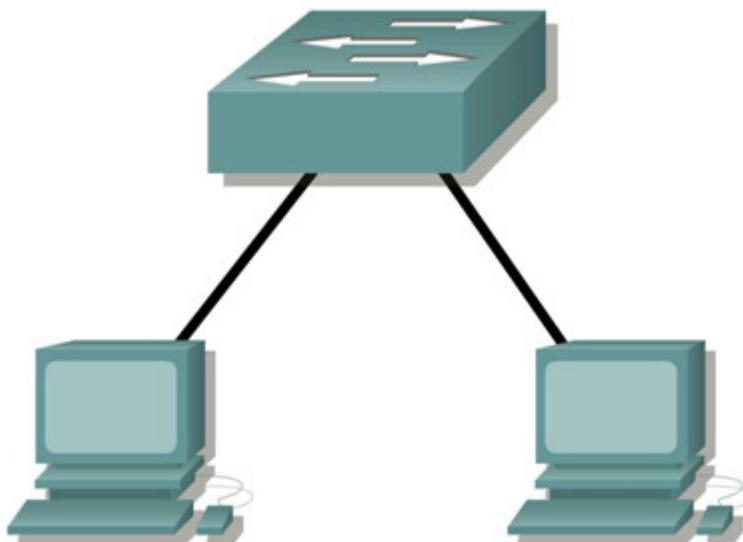
---

---

---



#### Task 4: Connect Your Workstations to the Classroom Lab Switch.



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

Using the correct cable, connect one end of the cable to the NIC port on the workstation and the other end to a port on the switch.

##### Step 2: Repeat this process for each workstation on your network.

Which cable did you use? \_\_\_\_\_

##### Step 3: Verify connectivity.

Verify network connectivity by using the **ping** command to reach the other workstations attached to the switch.

What is the output of the **ping** command?

---

---

---

---

What is the output of the **ping** command if you ping an address that is not connected to this network?

---

---

---

---

##### Step 4: Share a document between PCs.

1. On your desktop, create a new folder and name it **test**.
2. Right-click the folder and click File sharing. **Note:** A hand will be placed under the icon.

3. Place a file in the folder.
4. On the desktop, double-click **My Network Places** and then **Computers Near Me**.
5. Double-click the workstation icon. The **test** folder should appear. You will be able to access this folder across the network. Once you are able to see it and work with the file, you have access through all 7 layers of the OSI model.

### Task 5: Reflection

What could prevent a ping from being sent between the workstations when they are directly connected?

---

---

---

---

What could prevent the ping from being sent to the workstations when they are connected through the switch?

---

---

---

---

## Lab 2.6.2: Using Wireshark™ to View Protocol Data Units

### Learning Objectives

- Be able to explain the purpose of a protocol analyzer (Wireshark).
- Be able to perform basic PDU capture using Wireshark.
- Be able to perform basic PDU analysis on straightforward network data traffic.
- Experiment with Wireshark features and options such as PDU capture and display filtering.

### Background

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. Before June 2006, Wireshark was known as Ethereal.

A packet sniffer (also known as a network analyzer or protocol analyzer) is computer software that can intercept and log data traffic passing over a data network. 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 programmed to recognize the structure of different network protocols. This enables it to display the encapsulation and individual fields of a PDU and interpret their meaning.

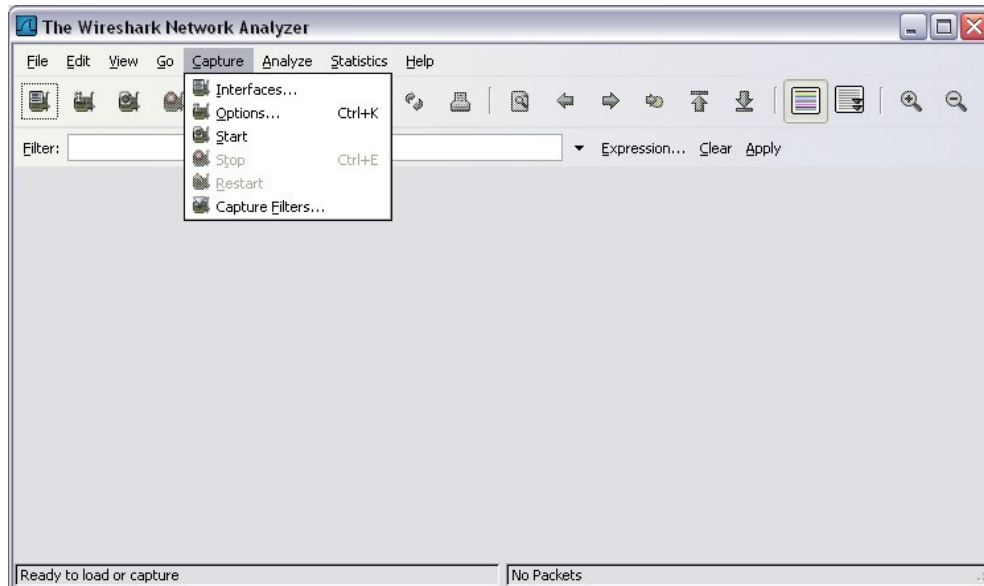
It is a useful tool for anyone working with networks and can be used with most labs in the CCNA courses for data analysis and troubleshooting.

For information and to download the program go to - <http://www.Wireshark.org>

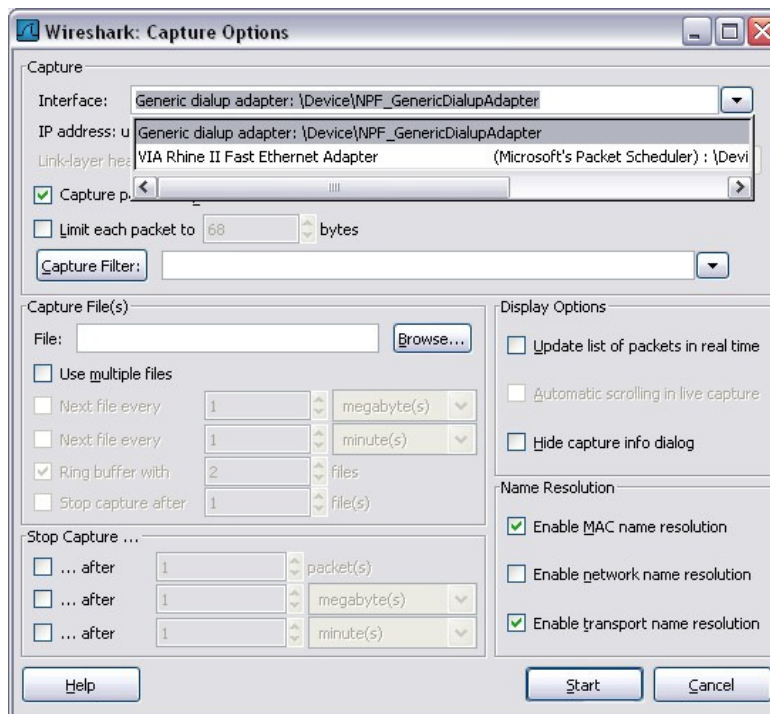
### Scenario

To capture PDUs the computer on which Wireshark is installed must have a working connection to the network and Wireshark must be running before any data can be captured.

When Wireshark is launched, the screen below is displayed.

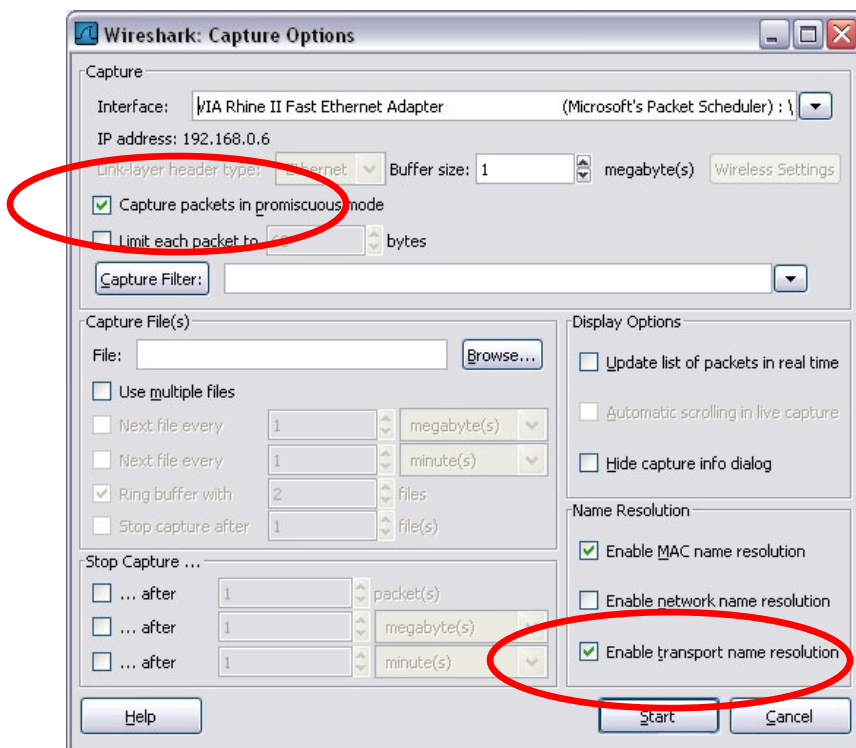


To start data capture it is first necessary to go to the **Capture** menu and select the **Options** choice. The **Options** dialog provides a range of settings and filters which determines which and how much data traffic is captured.



First, it is necessary to ensure that Wireshark is set to monitor the correct interface. From the **Interface** drop down list, select the network adapter in use. Typically, for a computer this will be the connected Ethernet Adapter.

Then other Options can be set. Among those available in **Capture Options**, the two highlighted below are worth examination.



### Setting Wireshark to capture packets in promiscuous mode

If this feature is NOT checked, only PDUs destined for this computer will be captured.

If this feature is checked, all PDUs destined for this computer AND all those detected by the computer NIC on the same network segment (i.e., those that "pass by" the NIC but are not destined for the computer) are captured.

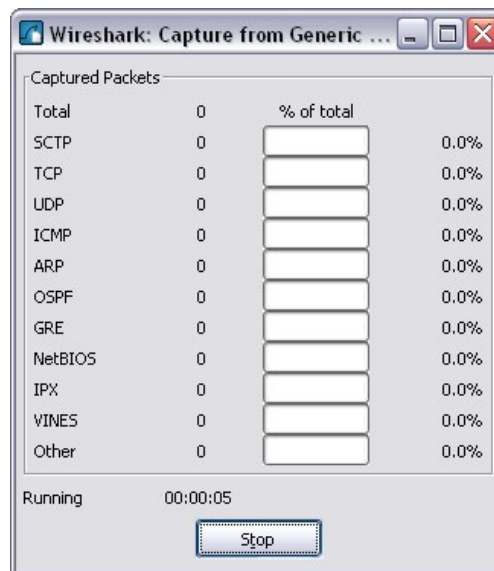
Note: The capturing of these other PDUs depends on the intermediary device connecting the end device computers on this network. As you use different intermediary devices (hubs, switches, routers) throughout these courses, you will experience the different Wireshark results.

### Setting Wireshark for network name resolution

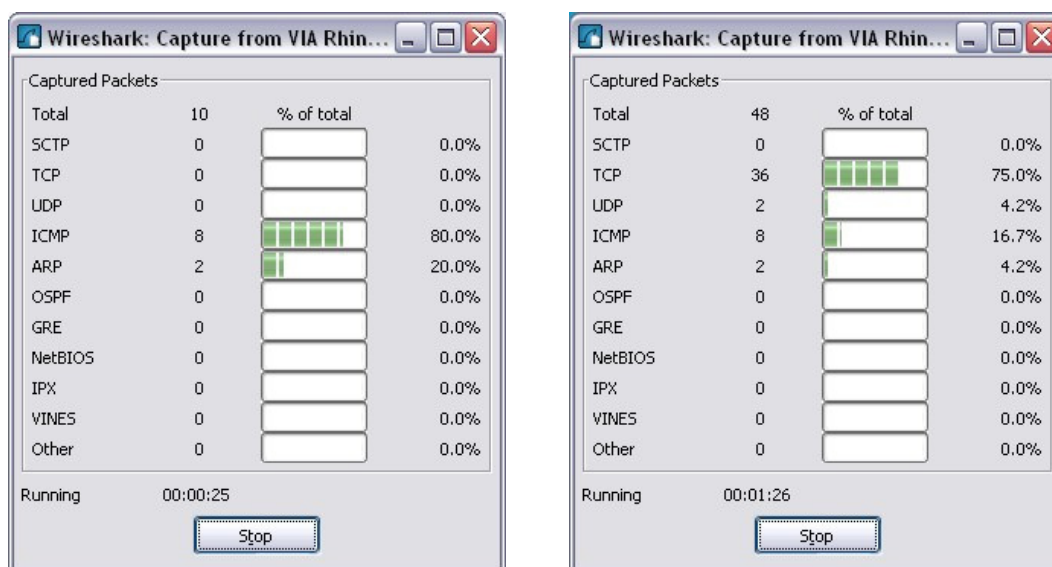
This option allows you to control whether or not Wireshark translates network addresses found in PDUs into names. Although this is a useful feature, the name resolution process may add extra PDUs to your captured data perhaps distorting the analysis.

There are also a number of other capture filtering and process settings available.

Clicking on the **Start** button starts the data capture process and a message box displays the progress of this process.



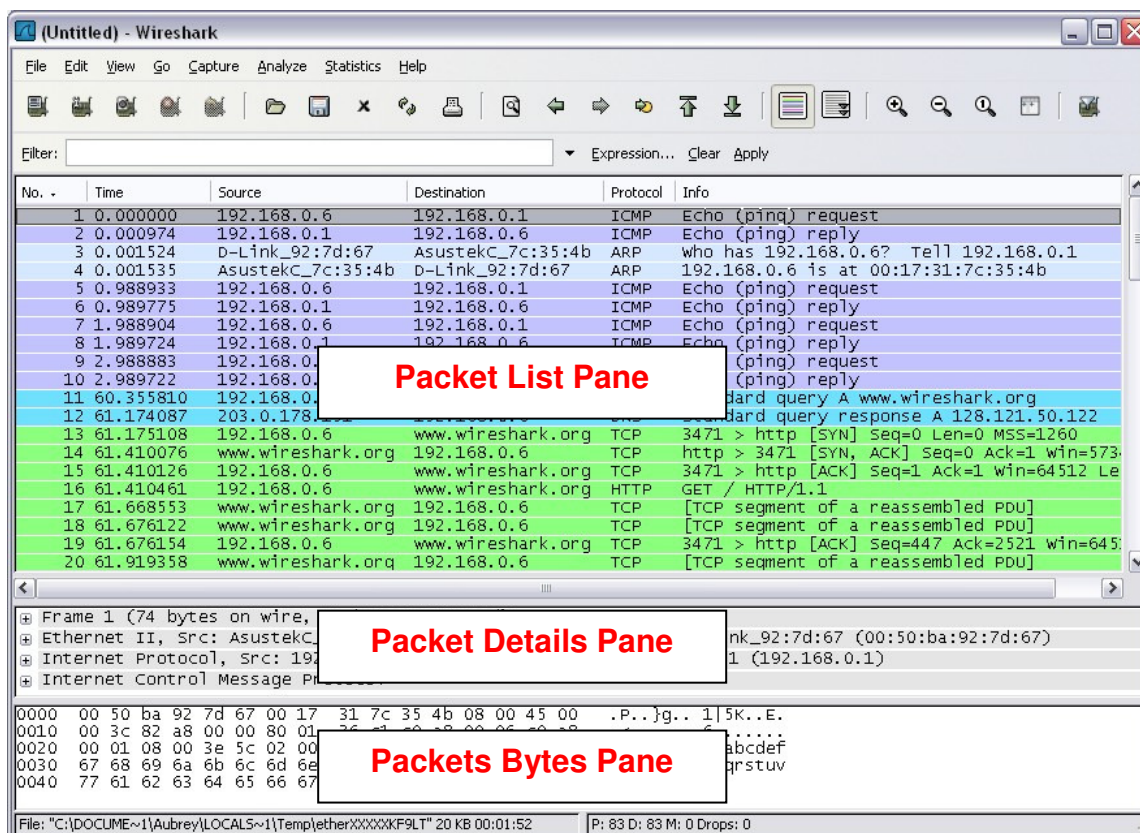
As data PDUs are captured, the types and number are indicated in the message box



The examples above show the capture of a ping process and then accessing a web page.

When the **Stop** button is clicked, the capture process is terminated and the main screen is displayed.

This main display window of Wireshark has three panes.



The PDU (or Packet) List Pane at the top of the diagram displays a summary of each packet captured. By clicking on packets in this pane, you control what is displayed in the other two panes.

The PDU (or Packet) Details Pane in the middle of the diagram displays the packet selected in the Packet List Pane in more detail.

The PDU (or Packet) Bytes Pane at the bottom of the diagram displays the actual data (in hexadecimal form representing the actual binary) from the packet selected in the Packet List Pane, and highlights the field selected in the Packet Details Pane.

Each line in the Packet List corresponds to one PDU or packet of the captured data. If you select a line in this pane, more details will be displayed in the "Packet Details" and "Packet Bytes" panes. The example above shows the PDUs captured when the ping utility was used and <http://www.Wireshark.org> was accessed. Packet number 1 is selected in this pane.

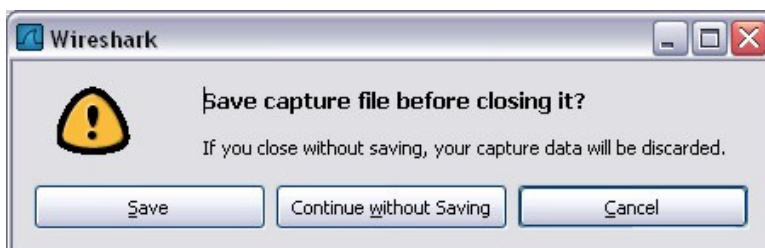
The Packet Details pane shows the current packet (selected in the "Packet List" pane) in a more detailed form. This pane shows the protocols and protocol fields of the selected packet. The protocols and fields of the packet are displayed using a tree, which can be expanded and collapsed.

The Packet Bytes pane shows the data of the current packet (selected in the "Packet List" pane) in what is known as "hexdump" style. In this lab, this pane will not be examined in detail. However, when a more in-depth analysis is required this displayed information is useful for examining the binary values and content of PDUs.



The information captured for the data PDUs can be saved in a file. This file can then be opened in Wireshark for analysis some time in the future without the need to re-capture the same data traffic again. The information displayed when a capture file is opened is the same as the original capture.

When closing a data capture screen or exiting Wireshark you are prompted to save the captured PDUs.



Clicking on **Continue without Saving** closes the file or exits Wireshark without saving the displayed captured data.

## Task 1: Ping PDU Capture

**Step 1: After ensuring that the standard lab topology and configuration is correct, launch Wireshark on a computer in a lab pod.**

Set the Capture Options as described above in the overview and start the capture process.

From the command line of the computer, ping the IP address of another network connected and powered on end device on in the lab topology. In this case, ping the Eagle Server at using the command ping **192.168.254.254**.

After receiving the successful replies to the ping in the command line window, stop the packet capture.

**Step 2: Examine the Packet List pane.**

The Packet List pane on Wireshark should now look something like this:

A screenshot of the Wireshark Packet List pane. It displays a table of captured packets with columns for No., Time, Source, Destination, Protocol, and Info. The packets are numbered 1 through 18. Packets 6, 7, 8, 9, 11, 12, 14, and 15 are highlighted in blue. The 'Info' column shows details for each packet, such as 'Spanning-tree-(for STP)', 'Broadcast', 'ARP', 'Echo (ping) request', and 'Echo (ping) reply'.

Look at the packets listed above; we are interested in packet numbers 6, 7, 8, 9, 11, 12, 14 and 15.

Locate the equivalent packets on the packet list on your computer.



If you performed Step 1A above match the messages displayed in the command line window when the ping was issued with the six packets captured by Wireshark.

From the Wireshark Packet List answer the following:

What protocol is used by ping? \_\_\_\_\_

What is the full protocol name? \_\_\_\_\_

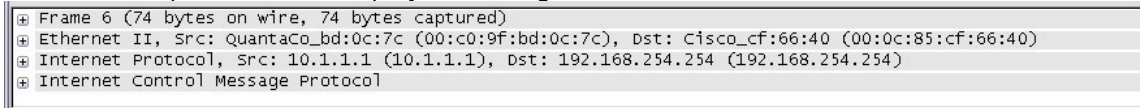
What are the names of the two ping messages? \_\_\_\_\_

Are the listed source and destination IP addresses what you expected? Yes / No

Why? \_\_\_\_\_

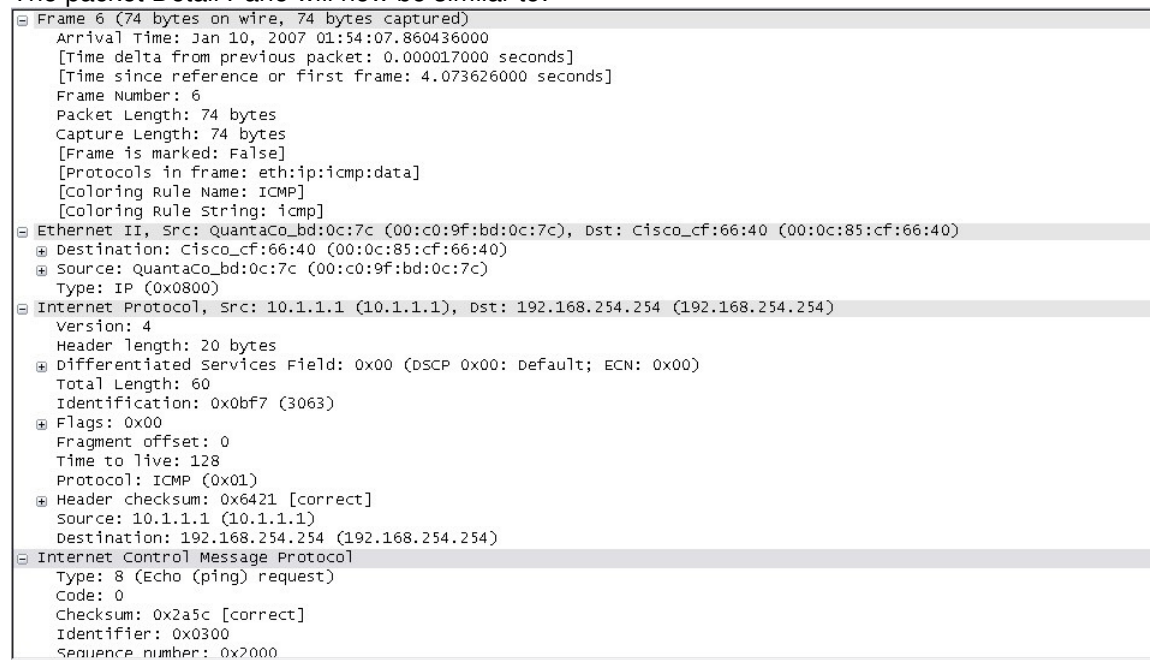
**Step 3: Select (highlight) the first echo request packet on the list with the mouse.**

The Packet Detail pane will now display something similar to:



Click on each of the four "+" to expand the information.

The packet Detail Pane will now be similar to:



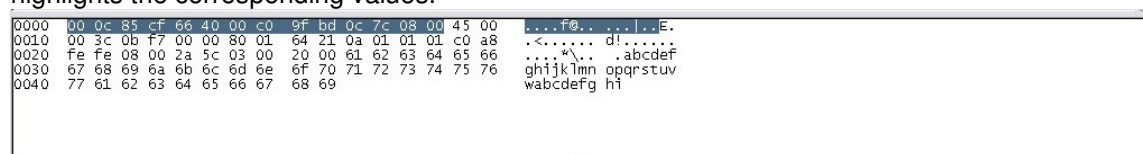
As you can see, the details for each section and protocol can be expanded further. Spend some time scrolling through this information. At this stage of the course, you may not fully understand the information displayed but make a note of the information you do recognize.

Locate the two different types of "Source" and "Destination". Why are there two types?

What protocols are in the Ethernet frame?

As you select a line in the Packets Detail pane all or part of the information in the Packet Bytes pane also becomes highlighted.

For example, if the second line (+ Ethernet II) is highlighted in the Details pane the Bytes pane now highlights the corresponding values.



This shows the particular binary values that represent that information in the PDU. At this stage of the course, it is not necessary to understand this information in detail.

#### Step 4: Go to the File menu and select Close.

Click on **Continue without Saving** when this message box appears.



## Task 2: FTP PDU Capture

### Step 1: Start packet capture.

Assuming Wireshark is still running from the previous steps, start packet capture by clicking on the **Start** option on the **Capture** menu of Wireshark.

At the command line on your computer running Wireshark, enter [ftp 192.168.254.254](ftp://192.168.254.254)

When the connection is established, enter **anonymous** as the user without a password.

Username: **anonymous**

Password: <ENTER>

You may alternatively use login with userid **cisco** and with password **cisco**.

When successfully logged in enter **get /pub/eagle\_labs/eagle1/chapter1/gaim-1.5.0.exe** and press the enter key <ENTER>. This will start downloading the file from the ftp server. The output will look similar to:

```
C:\Documents and Settings\ccna1>ftp eagle-server.example.com
Connected to eagle-server.example.com.
220 Welcome to the eagle-server FTP service.
User (eagle-server.example.com:(none)): anonymous
331 Please specify the password.
Password:<ENTER>
230 Login successful.
ftp> get /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for
pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe (6967072 bytes).
226 File send OK.
ftp: 6967072 bytes received in 0.59Seconds 11729.08Kbytes/sec.
```

When the file download is complete enter **quit**

```
ftp> quit
221 Goodbye.
C:\Documents and Settings\ccna1>
```

When the file has successfully downloaded, stop the PDU capture in Wireshark.

## Step 2: Increase the size of the Wireshark Packet List pane and scroll through the PDUs listed.

Locate and note those PDUs associated with the file download.  
These will be the PDUs from the Layer 4 protocol TCP and the Layer 7 protocol FTP.

Identify the three groups of PDUs associated with the file transfer.

| If you performed the step above, match the packets with the messages and prompts in the FTP command line window.

The first group is associated with the "connection" phase and logging into the server.  
List examples of messages exchanged in this phase.

Locate and list examples of messages exchanged in the second phase that is the actual download request and the data transfer.

The third group of PDUs relate to logging out and "breaking the connection".  
List examples of messages exchanged during this process.

Locate recurring TCP exchanges throughout the FTP process. What feature of TCP does this indicate?

---

---

### Step 3: Examine Packet Details.

Select (highlight) a packet on the list associated with the first phase of the FTP process.  
View the packet details in the Details pane.

What are the protocols encapsulated in the frame?

---

Highlight the packets containing the user name and password.  
Examine the highlighted portion in the Packet Bytes pane.

What does this say about the security of this FTP login process?

---

Highlight a packet associated with the second phase.  
From any pane, locate the packet containing the file name.

The filename is: \_\_\_\_\_

Highlight a packet containing the actual file content - note the plain text visible in the Bytes pane.

Highlight and examine, in the Details and Bytes panes, some packets exchanged in the third phase of the file download.

What features distinguish the content of these packets?

---

When finished, close the Wireshark file and continue without saving

## Task 3: HTTP PDU Capture

### Step 1: Start packet capture.

Assuming Wireshark is still running from the previous steps, start packet capture by clicking on the **Start** option on the **Capture** menu of Wireshark.

**Note:** Capture Options do not have to be set if continuing from previous steps of this lab.

Launch a web browser on the computer that is running Wireshark.  
Enter the URL of the Eagle Server of **example.com** or enter the IP address-192.168.254.254. When the webpage has fully downloaded, stop the Wireshark packet capture.

### Step 2: Increase the size of the Wireshark Packet List pane and scroll through the PDUs listed.

Locate and identify the TCP and HTTP packets associated with the webpage download.

Note the similarity between this message exchange and the FTP exchange.

**Step 3: In the Packet List pane, highlight an HTTP packet that has the notation "(text/html)" in the Info column.**

In the Packet Detail pane click on the "+" next to "**Line-based text data: html**"  
When this information expands what is displayed?

---

Examine the highlighted portion of the Byte Panel.  
This shows the HTML data carried by the packet.

When finished close the Wireshark file and continue without saving

### Task 4: Reflection

Consider the encapsulation information pertaining to captured network data Wireshark can provide. Relate this to the OSI and TCP/IP layer models. It is important that you can recognize and link both the protocols represented and the protocol layer and encapsulation types of the models with the information provided by Wireshark.

### Task 5: Challenge

Discuss how you could use a protocol analyzer such as Wireshark to:

- (1) Troubleshoot the failure of a webpage to download successfully to a browser on a computer.  
and
- (2) Identify data traffic on a network that is requested by users.

---

---

---

---

---

---

---

### Task 6: Cleanup

Unless instructed otherwise by your instructor, exit Wireshark and properly shutdown the computer.