Understanding Networking Fundamentals Lab Guide

L3150C-008-3
June 2014

Global Knowledge®

Understanding Networking Fundamentals Lab Guide

L3150C-008-3
June 2014

Copyright Information

Project Team

PAUL SIMONEAU	Course Director
TORI EASTERLY	Product Director, Networking
BRAD JONES	Product Director, Networking
GEORGE STIEFELMEYER	Lab Technician

Global Knowledge®

9000 Regency Parkway
Cary, North Carolina 27518
Phone: 919-461-8600
1-800-COURSES
Fax: 919-461-8646
www.globalknowledge.com

Printed in Canada

Font Conventions Used in This Course Manual

Different fonts and font styles signify different items or tasks. The following is a key to font usage.

Font	Item or Task	Examples
Bold	• Commands, directory paths, folders, file names, Web and e-mail addresses, registry keys, icons, and anything you would see in a command line or when programming • Text that can be manipulated in windows or dialog boxes	• The **dir** command • **c:\winnt\system** • **notepad.exe** • **am.globalknowledge.com** • **YesNoDialog** is a subclass of **Object**, not **Dialog**. • Check the **Write the event to a system log** box.
ALL CAPS	• Key names • Messages	• CTRL+ALT+DELETE (Press the CTRL, ALT, and DELETE keys simultaneously) • SYN/ACK message • CALL PROCEEDING message
Courier New	• Computer-generated text	• `Input a valid user id and password.`
Courier New bold	• Code or commands not in text flow or tables that are entered by the user	• **`<h1>Global Knowledge</h1>`** • **`$ show cluster /continuous`**
Italic	• Placeholder variables	• `$` **`more [`*`file1`* **`[`*`file2...`*`]]`** • The example runs ***cmd2*** if ***cmd1*** returns success.

Global Knowledge®

Table of Contents

Global Knowledge®

L1

Lab 1: Simple Networking with Ethernet

Hands-On Lab

Lab Objectives

In this lab, you will:

- Configure a PC with a static IP address
- Test connectivity in the classroom network
- Use the **netstat** command to examine the amount of traffic in your network

Part 1: Initial Configuration

Introduction

Some presentations of this course will be done using the Global Knowledge Remote Labs environment. The remote labs have been built to mimic, as closely as possible, what you might encounter in the real world of data networking. Each class will have use of a rack of networking equipment including the following hardware:

- Two Cisco 2600 routers
- Two Cisco 2950 Ethernet switches
- One ADTRAN 1335 router/switch
- One Dell Rack server supporting 20 Windows 8 virtual workstations and one Linux server

These components will show you a diversity of hardware and software that might be found in any networking environment.

The ADTRAN router/switch has been configured with a number of virtual LANs. In the lab environment, these virtual LANs provide additional subnets to evaluate the routing needed in a large network.

The network environment in the classroom includes seven local LAN networks and one WAN (wide area network).

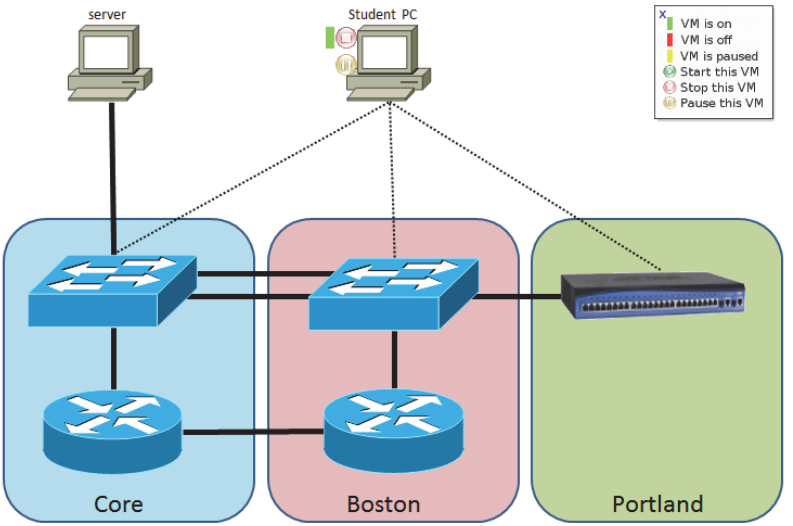

Figure 1: Logical Diagram

The logical diagram shown in Figure 1 provides a snapshot of the network environment. The Core network houses the servers used in the classroom. The instructor administers these devices. The remaining LANs contain workstations that are configured by you, the student.

Core Workgroups and Address Assignments

Core Workgroup	IP Address	Username	Password
student01	192.168.100.51		
student02	192.168.100.52		
student03	192.168.100.53		
student04	192.168.100.54		
student05	192.168.100.55		
student06	192.168.100.56		
student07	192.168.100.57		
student08	192.168.100.58		
student09	192.168.100.59		
student10	192.168.100.60		
student11	192.168.100.61		
student12	192.168.100.62		
student13	192.168.100.63		
student14	192.168.100.64		
student15	192.168.100.65		
student16	192.168.100.66		
student17	192.168.100.67		
student18	192.168.100.68		

Figure 2: Core Workgroups and Address Assignments

Exercise 1: Accessing the Virtual Lab Environment

1. Your instructor will give you a username and password that you will use to access your remote labs. Write them down below:

   Username: _____

   Password: _____

2. Open your Internet browser (such as Internet Explorer or Firefox) and navigate to the following URL:

   `http://www.remotelabs.com`

3. When the page shown in Figure 3 appears, enter your name and password; then click the **Log In** button.

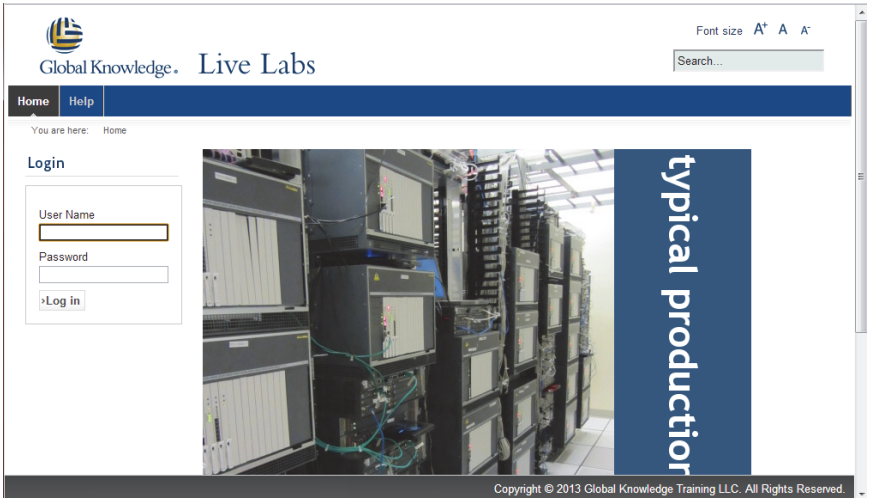

Figure 3: Connecting to the Remote Desktop

4. You will then see the main Live Labs page as shown in Figure 4.

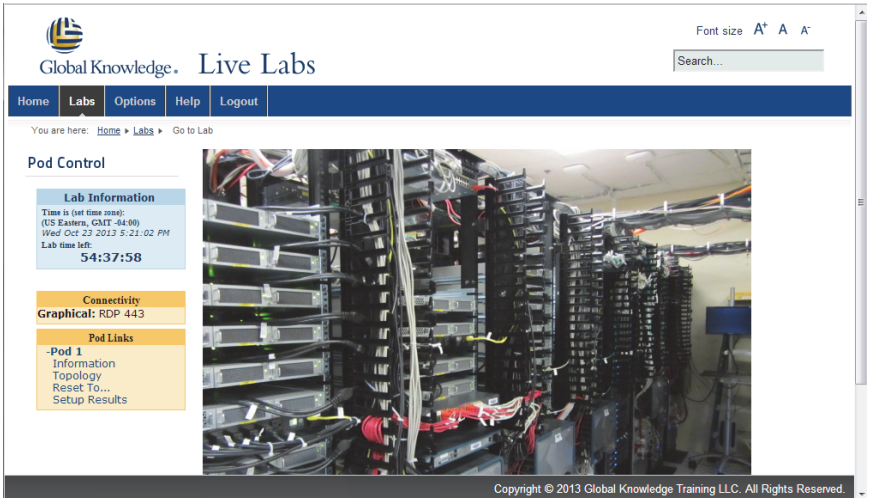

Figure 4: The Main Live Labs Page

5. To gain access to the lab equipment, click the **Topology** link on the main page. This will launch a Remote Desktop connection to the lab access server. The connection makes use of a digital certificate. The certificate in use cannot be verified using standard methods, so you must bypass the warning shown in Figure 5. Click **Connect.**

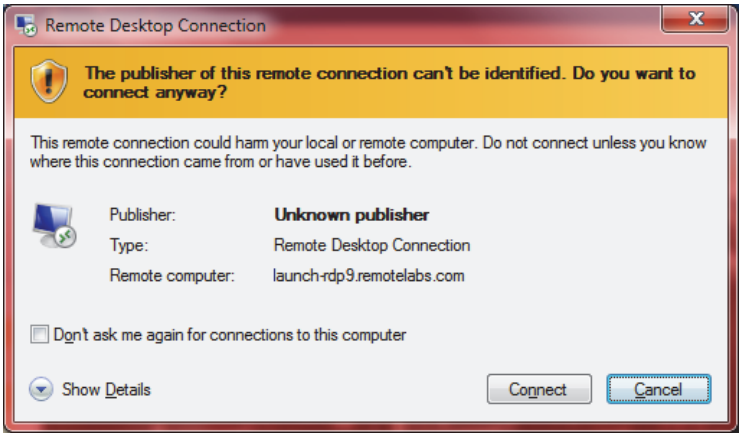

Figure 5: Remote Desktop Connection Certificate Warning

6. When the Windows Security dialog opens, you will be asked to provide your password. You will be presented with a screen similar to the one in Figure 6. Enter the password you were provided by your instructor and click **OK**.

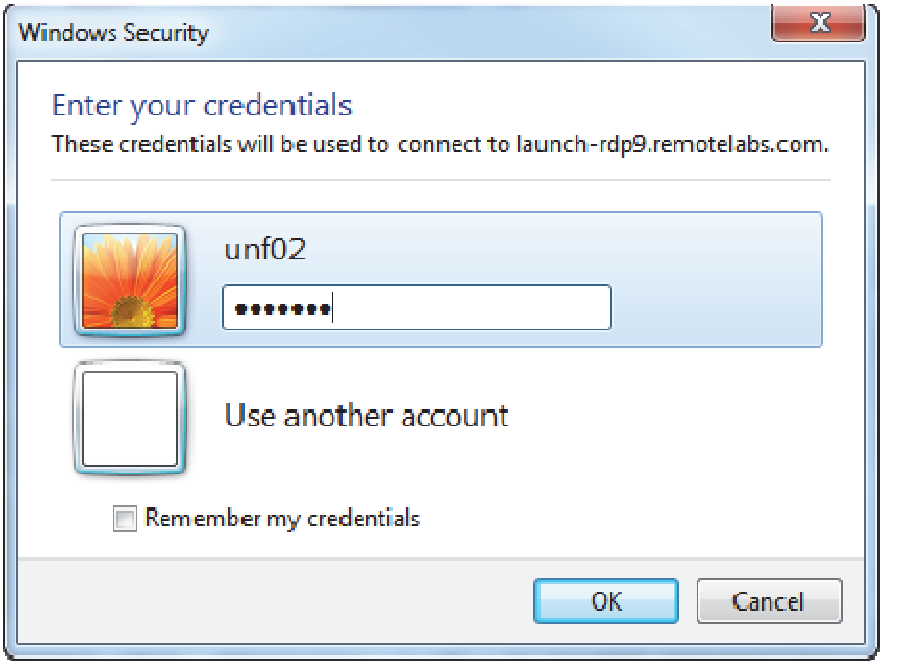

Figure 6: Enter User Credentials Using a Listed Username

7. The login will continue and you will be presented a map of the lab environment from the student perspective. The only icon you can click on to access a device in the network is the icon labeled **Student PC**. Move your mouse pointer to the **Student PC** icon and left-click.

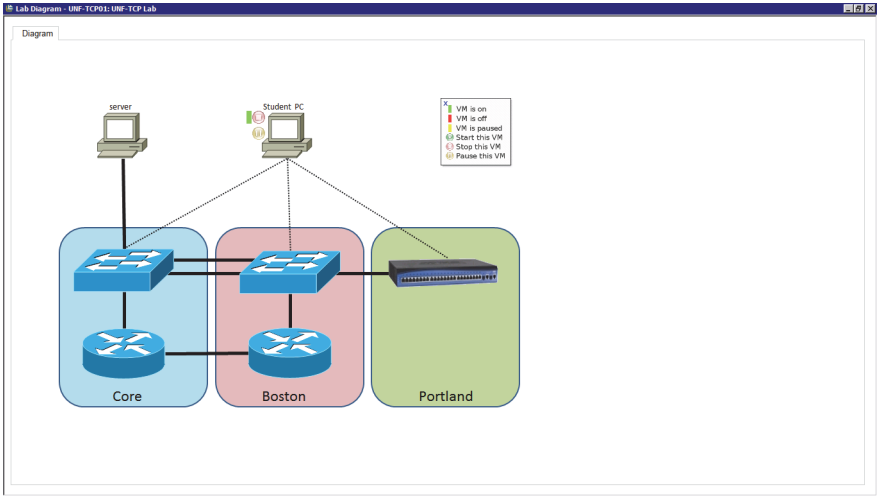

Figure 7: Map of the Lab Environment

8. As the process of accessing your student PC continues, you may see varying screen formats. The student image you are accessing is a Windows 8 operating system with the Windows 8 desktop configured to look like Windows 7. The typical Windows 8 desktop is hidden to simplify use in the lab. The right scrollbar is available if you need to relocate the screen vertically. There are three icons in the taskbar at the bottom of the desktop—Internet Explorer, File Explorer, and Control Panel. You will use these programs during lab time. You will also use the command prompt, which is accessible from the icon on the desktop.

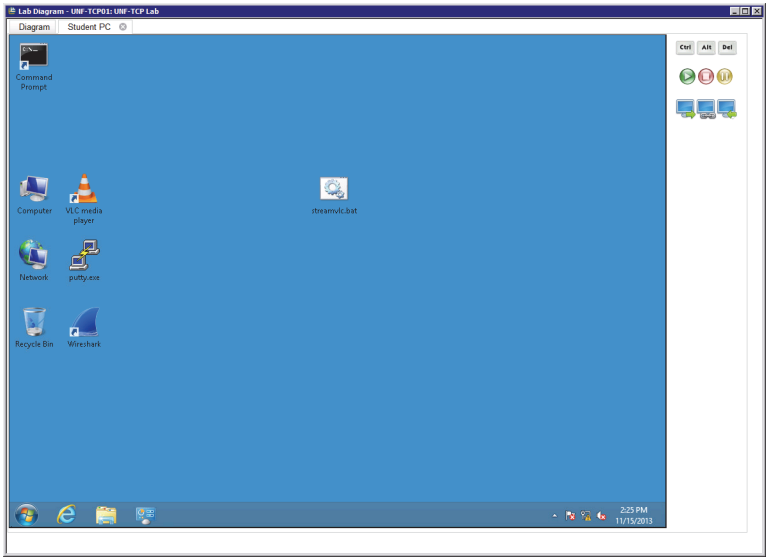

Figure 8: Remote Windows 8 Workstation Desktop

As you begin the configuration of the workstations, you will need to reference some important information:

- The subnet mask that is used on all workstations is 255.255.255.0.
- The DNS server address that is used on all workstations is 192.168.100.10.

Note
Refer to the addressing table in Figure 2 to view address assignments for your workgroup.

Exercise 2: Modifying Your System Configuration

1. Now that you have successfully logged into the system and have gained access to your student PC, it is time to configure the network connection information. Click the **Control Panel** icon at the bottom of the screen. You'll see the Control Panel dialog open as displayed in Figure 9. In the Network and Internet section, select **View network status and tasks**.

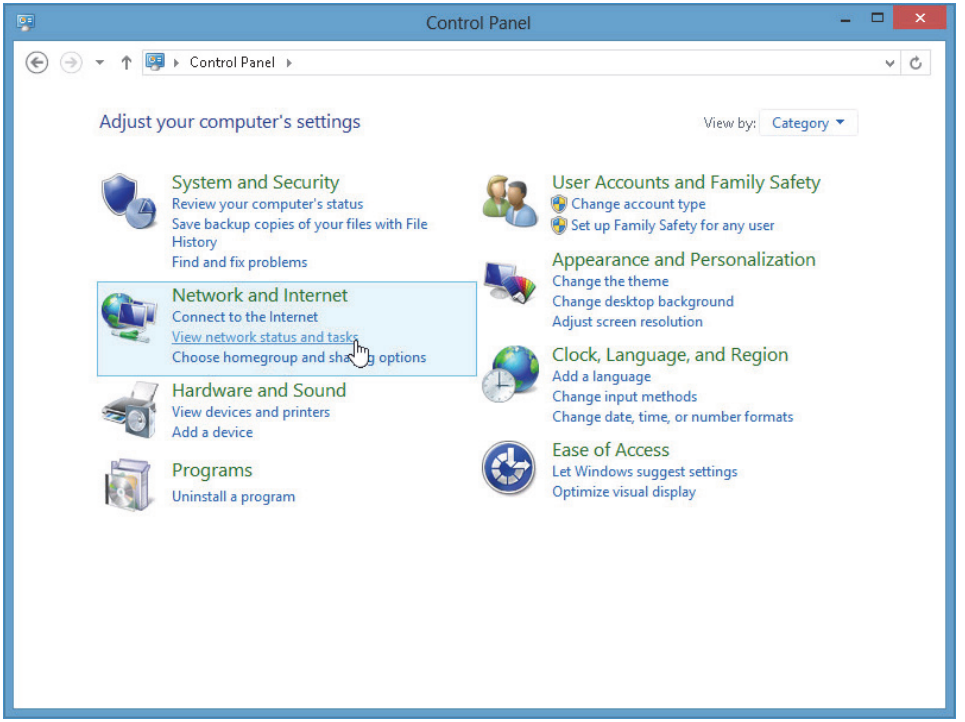

Figure 9: Select View Network Status and Tasks

2. Click the **Change adapter settings** link on the left side of this dialog.

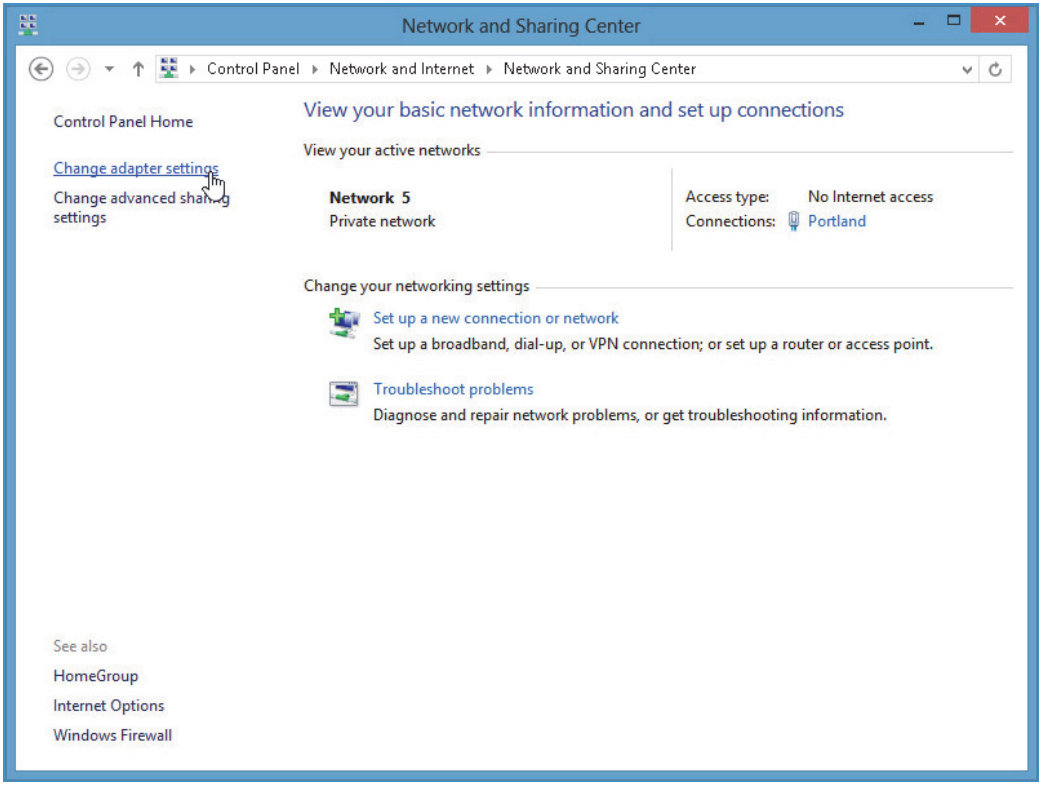

Figure 10: Click Change Adapter Settings

3. Your workstation features three virtual Ethernet interfaces. At this time, you will disable any active interfaces and enable the interface to the switch for your assigned workgroup, which should be Core. Highlight and click any enabled interfaces in your list and click **Disable this network device**.

4. When you have disabled all of the devices, click the **Core** interface and then click **Enable this network device**. You should now have one enabled network device.

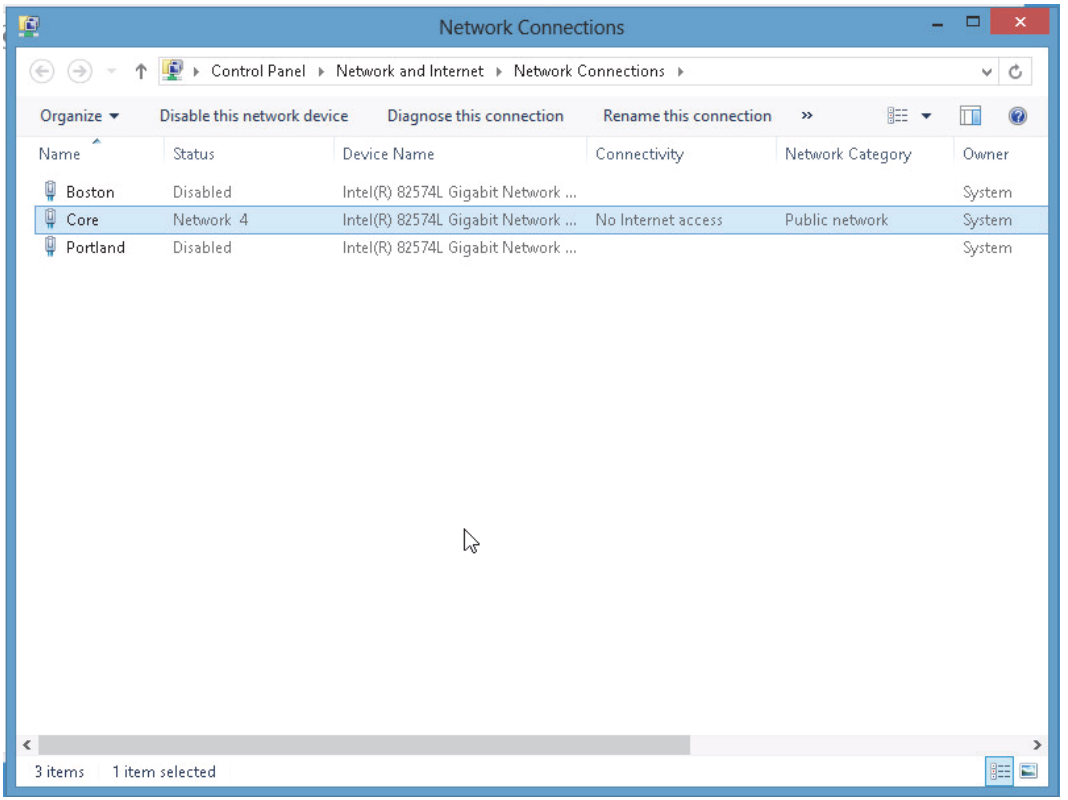

Figure 11: Enable Network Devices

5. Place your mouse pointer on the row of the enabled interface and double-click to open the configuration dialog (Figure 12).

6. Click the **Properties** button.

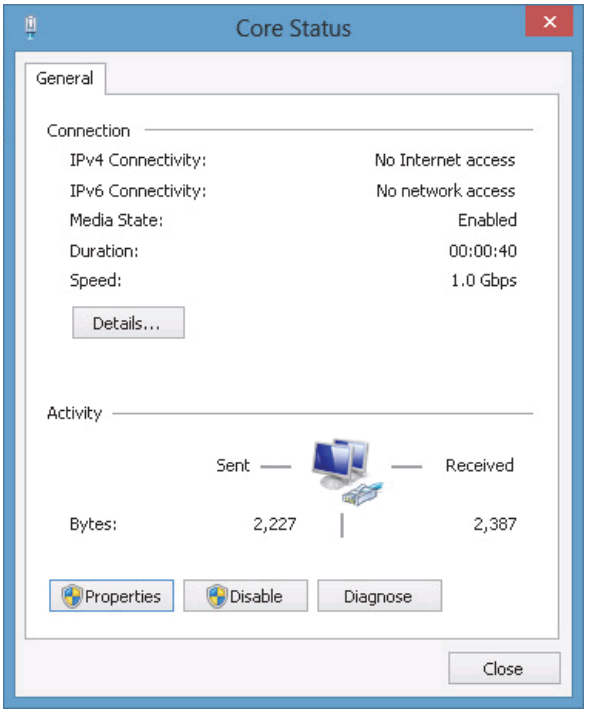

Figure 12: Core Status Dialog Box

7. When the properties dialog opens, remove the check from the **IP Version 6** check box if it is checked. We will work with that protocol later.

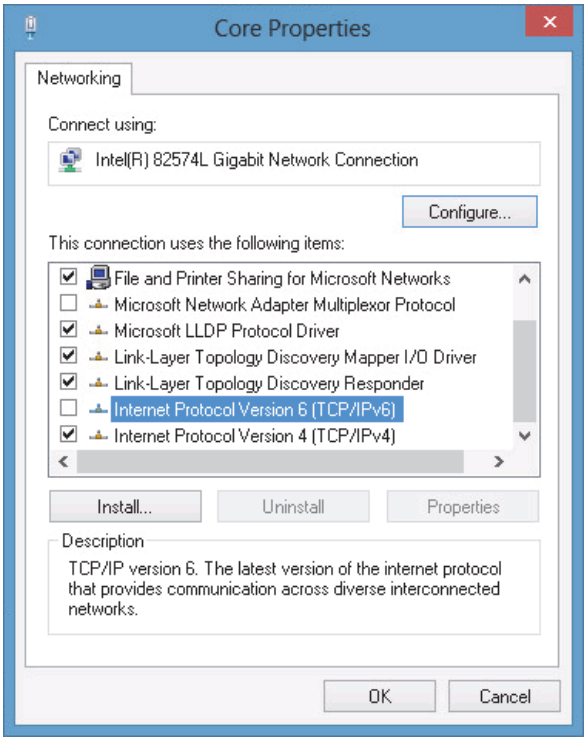

Figure 13: Deselect Internet Protocol Version 6

8. Highlight the **IP Version 4** protocol line and click the **Properties** button.

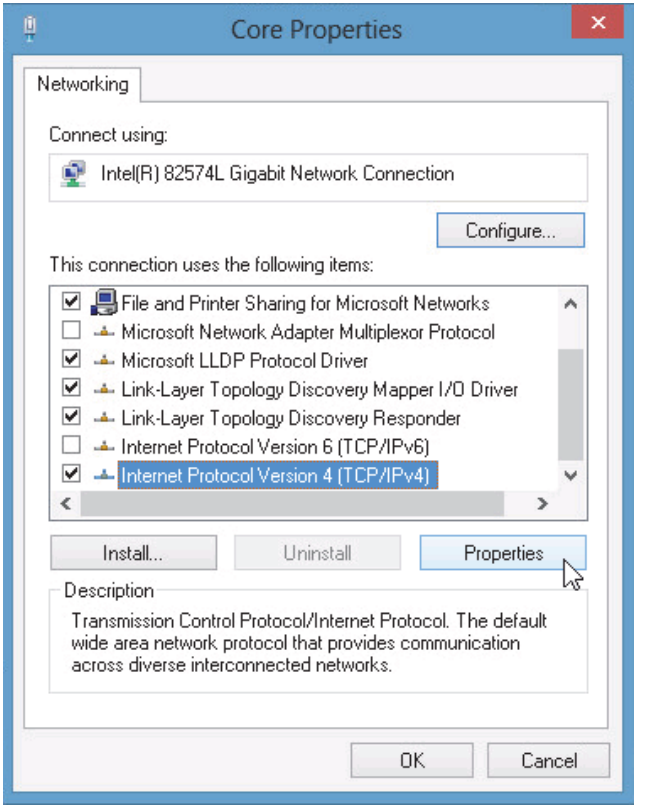

Figure 14: Select IPv4 and Click Properties

9. Click the **Use the following IP address** radio button. Change the **IP address** to match the one assigned by your instructor. Use the following values for the subnet mask and default gateway:
    - Subnet mask: 255.255.255.0
    - Default gateway: 192.168.100.2
10. Click the **Use the following DNS server addresses** radio button and fill in the following address as the preferred DNS server: **192.168.100.10**. Then click the **Advanced** button.

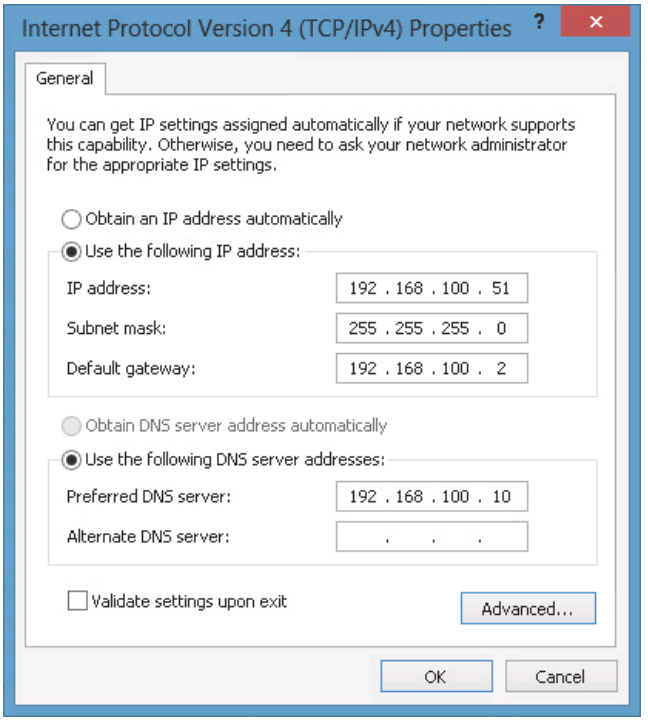

Figure 15: Configure IP Address, Subnet Mask, and Default Gateway

11. Click the **DNS** tab at the top of the Advanced dialog. Ensure that your entries include selecting the **Append primary and connection specific DNS suffixes** radio button and checking the **Append parent suffixes of the primary DNS suffix** check box. Enter **gklabs.com** in the DNS suffix for this connection space. Finally, check the last two boxes in the dialog as seen in Figure 16. Click **OK**, then **OK** again. Click **Close** until you return to the main desktop screen.

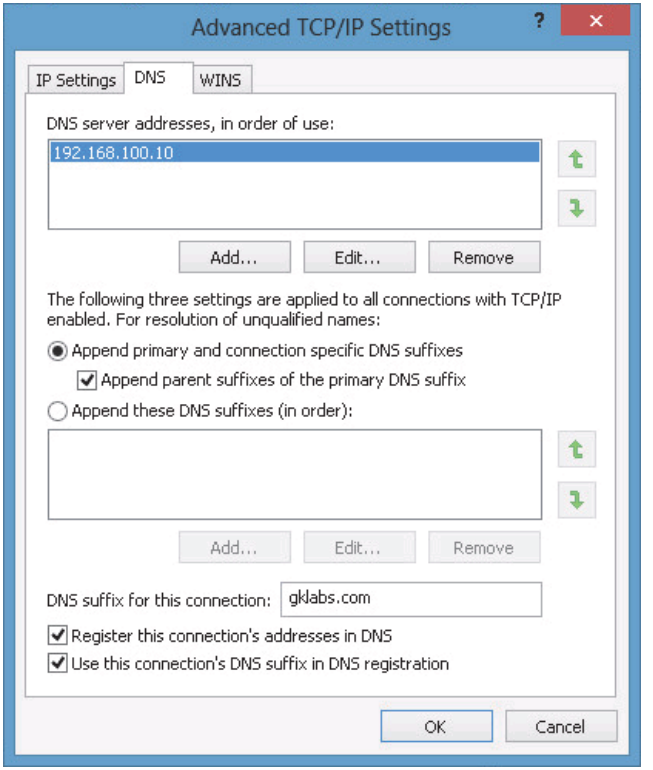

Figure 16: Configure DNS

12. The final configuration step is changing the device name of your workstation. Open the Control Panel by clicking the icon on the bottom menu bar. Click the **System and Security** link in the Control Panel. When the dialog opens, click the **See the name of this computer** link under the **System** label.

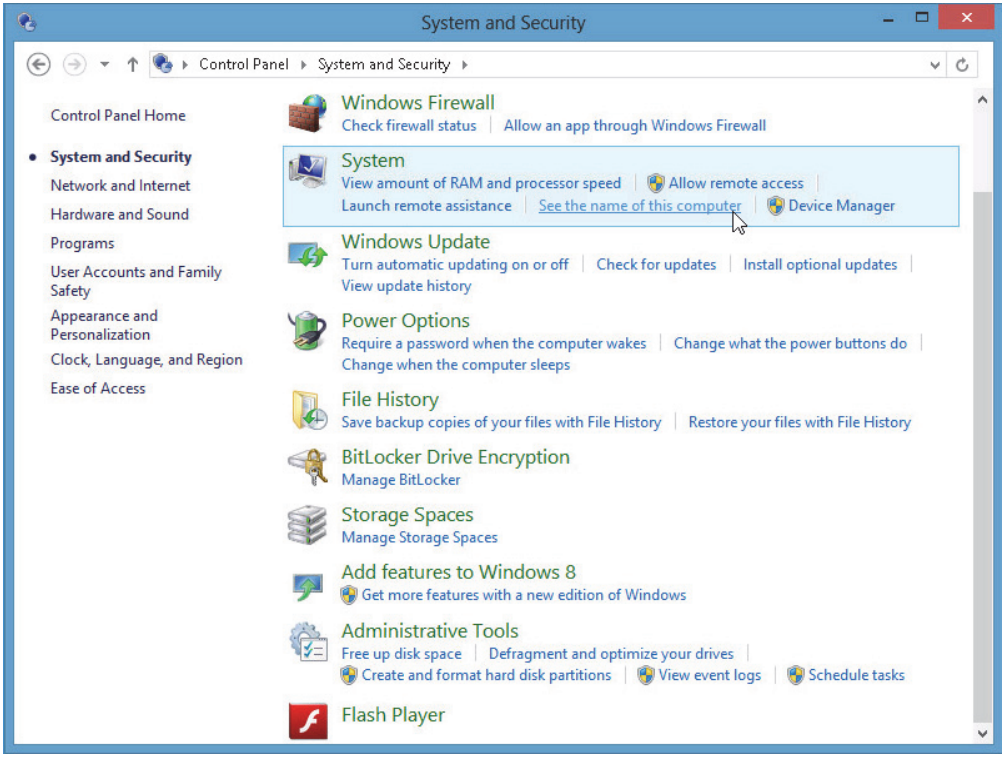

Figure 17: Click See the Name of This Computer

13. Near the bottom right side of the new dialog, click **Change settings**.

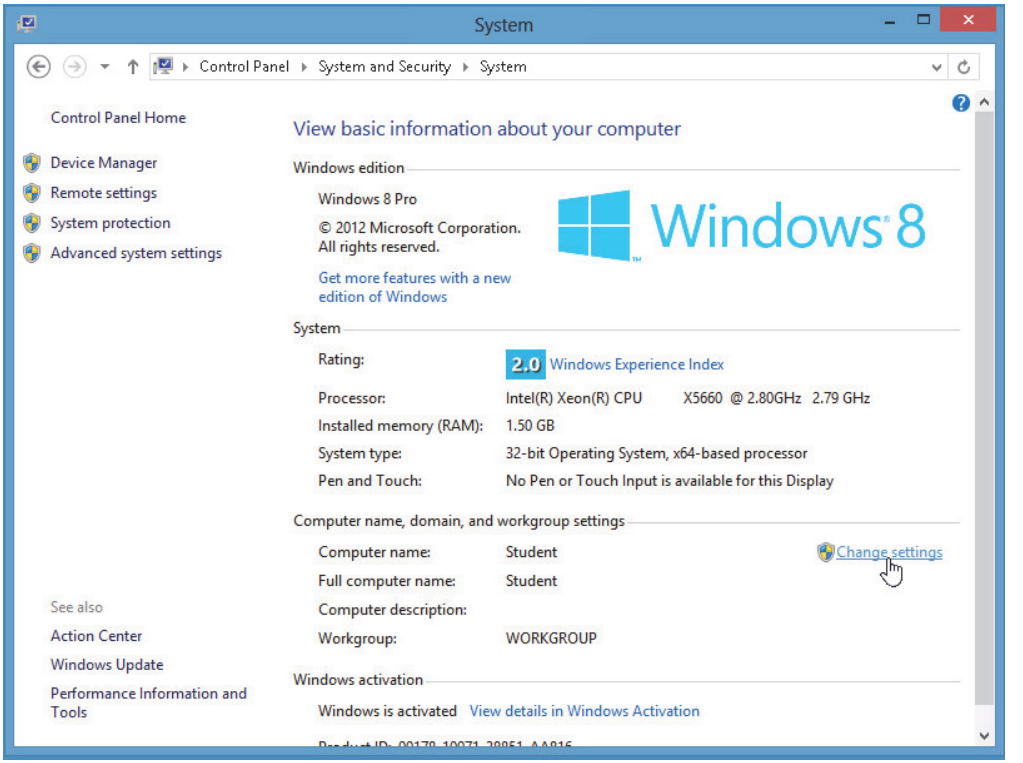

Figure 18: Click Change Settings

14. In the System Properties dialog, click the **Change** button.

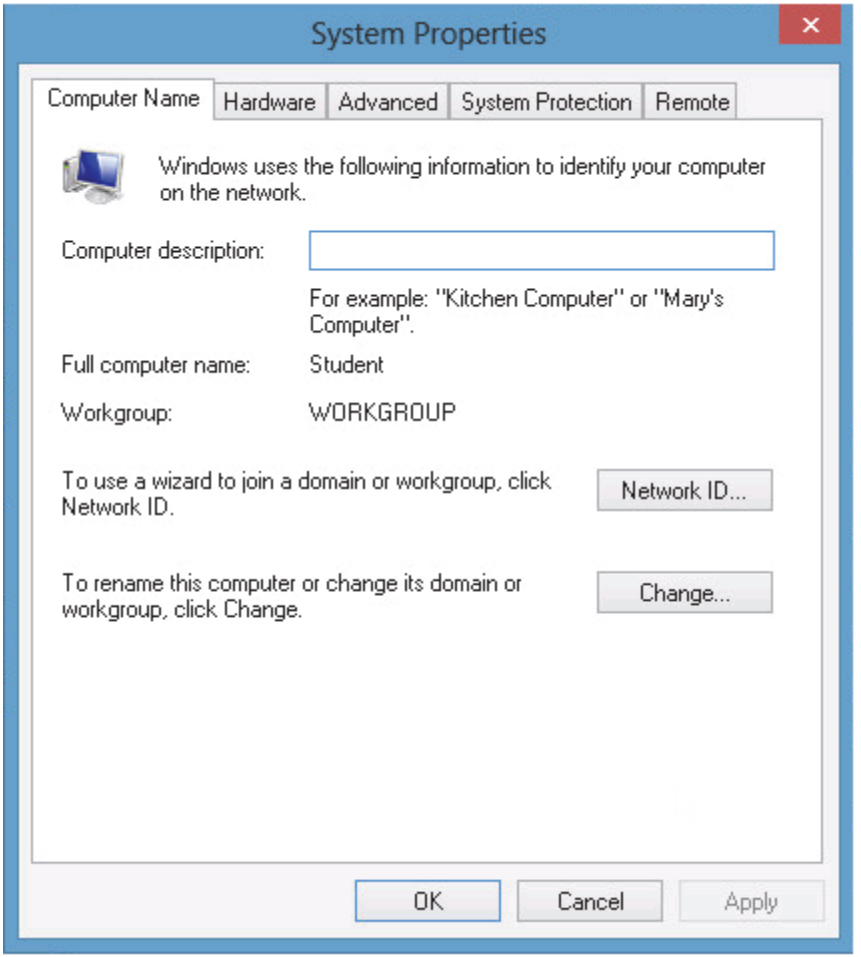

Figure 19: System Properties Dialog Box

15. In the **Computer name** space, enter your assigned workstation name (student01, student02, etc.). Do not change any other information on this dialog. Click **OK**.

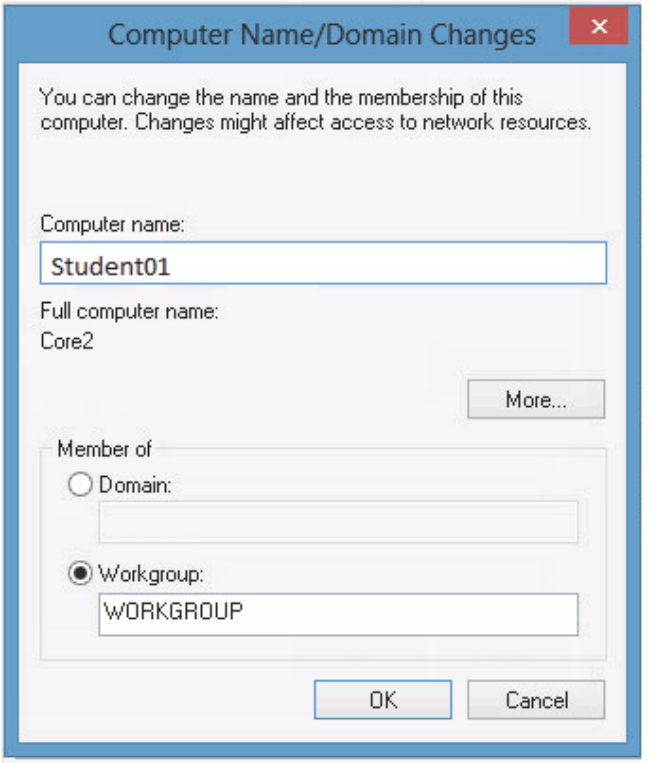

Figure 20: Click Change Settings

16. Click **OK** to save the change you just made. You will be prompted to restart to apply this change. Click **OK**. Then close the dialog and click the **Restart Now** button. Your machine will restart.

17. Once the workstation is restarted, your configuration is complete.

18. Verify your configuration using the **ipconfig** program.
    18.1 Click the **Command Prompt** shortcut to open the Command Prompt window.
    18.2 At the command line prompt, enter **ipconfig /all**.

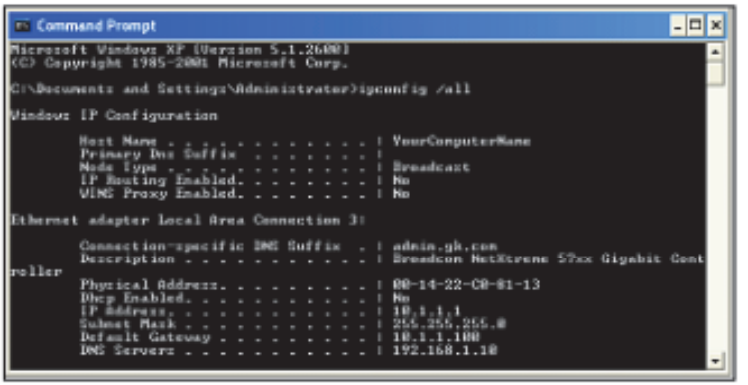

Figure 21: IP Configuration

    18.3 Record the physical address of your workstation here:

_____

    18.4 Verify your IP Address, Subnet Mask, Default Gateway, and DNS Server Address before you continue.

19. Close the Command Prompt window and return to the lab that referred you to this appendix.

Exercise 3: Using Netstat

1. Netstat is a tool that may be useful in understanding how much Ethernet traffic you experience at your workstation. One function of **netstat** is to show the amount of Ethernet traffic that has gone through the interface.

2. In your command line window, type the following command and press ENTER:

```
netstat –e
```

3. Record your results in Figure 22.

Counter Name	Received	Sent
Bytes		
Unicast packets		
Non-unicast packets		
Discards		
Errors		
Unknown protocols		

Figure 22: Ethernet Traffic Table

4. During the time that you were recording the information in the table, the Ethernet traffic continued in the network. In your command line window, type the following command and press ENTER:

```
netstat –e
```

5. Compare your new information to the information recorded in Figure 22. Note what has changed and what has remained the same.

You have successfully completed this lab.

Global Knowledge®

L2

Lab 2: Elementary Protocol Analysis

Hands-On Lab

Lab Objectives

In this lab you will:

- Learn the basic capabilities of a protocol analyzer
- Observe Ethernet traffic in a switched environment
- Determine the Ethernet error reporting capabilities of Windows

Lab Procedures

Exercise 1: Ethernet Header Analysis

During the labs, you will be using a protocol analyzer called Wireshark. The purpose of the protocol analyzer in the lab environment is to allow you to view and understand the contents of the protocols you are investigating. You will not be fully exploring the capabilities of Wireshark.

Figure 23: Wireshark Icon

1. Click the Wireshark icon to launch the protocol analyzer.

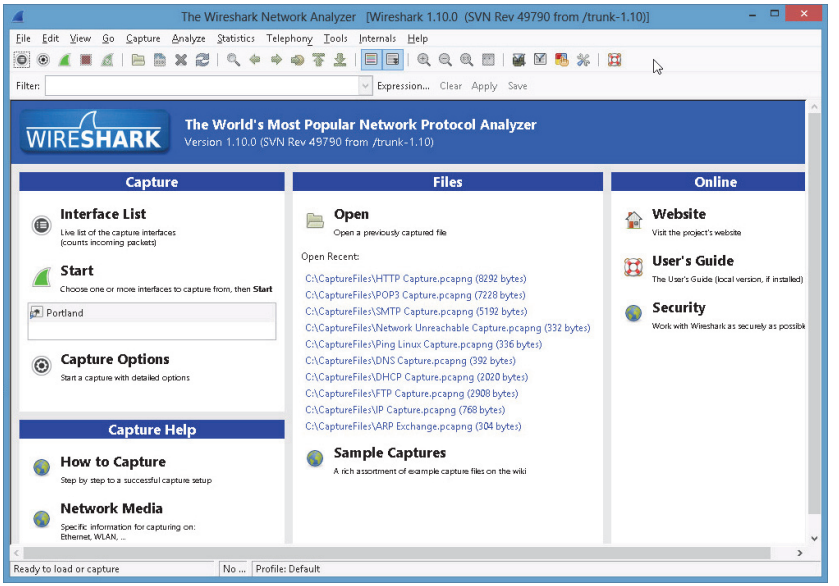

Figure 24: Wireshark Window

2. The top menu will be used for these labs. The toolbar contains shortcuts to the menus that will be explored later.

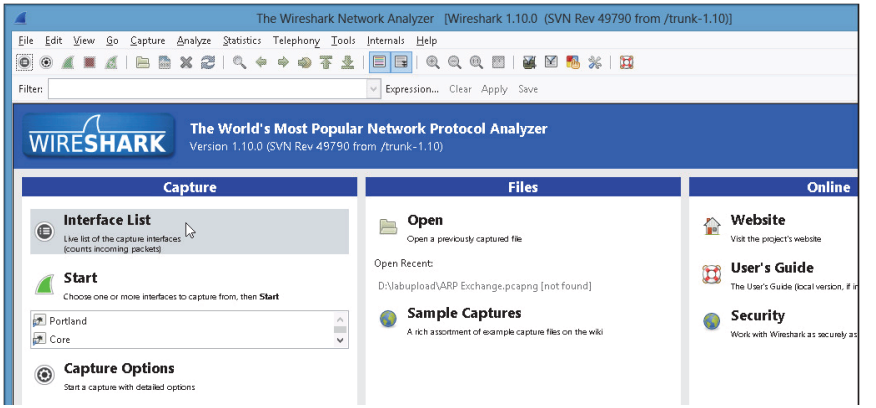

Figure 25: Initial Wireshark screen

3. The process of obtaining packets from the network is called capturing. To begin capturing packets, click the **Interface List** option under Capture on the left side of the Wireshark interface and check the interface row containing your IP address. Click **Start**.

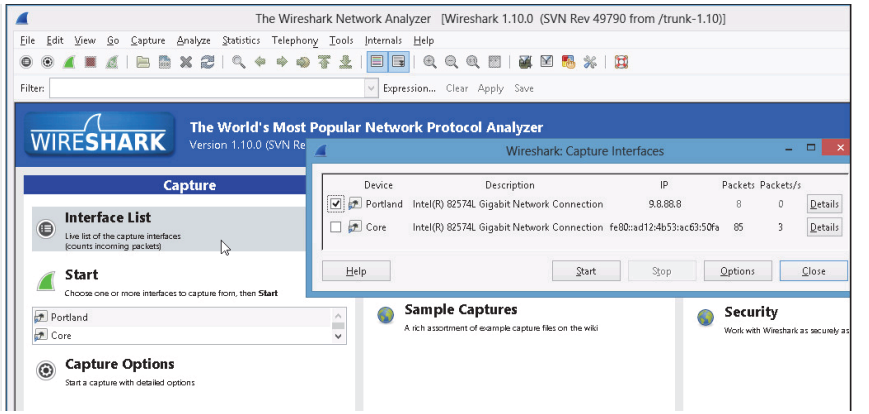

Figure 26: Capture Options

4. At this point, you are viewing the capture buffer display. The program is now capturing packets. Packets should begin being displayed in the central region of the screen. Each packet is assigned a number, and additional information (for example, Time, Source, Destination, Protocol, etc.) is displayed. Of particular interest are the source and destination addresses, size, and protocol information, which will be important as you continue to use this tool in later labs.

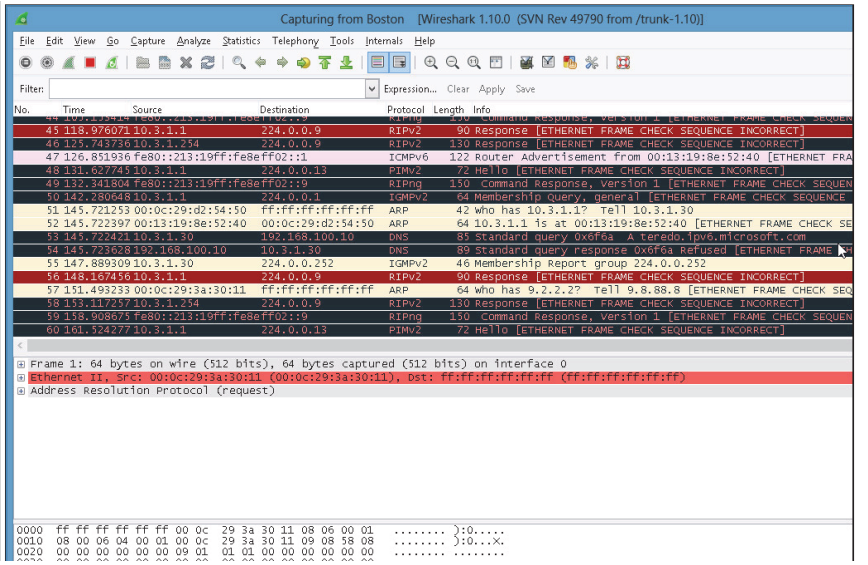

Figure 27: Packet List

5. To stop the capture process and begin reviewing a packet, click **Capture** from the menu at the top of the Wireshark window; then click **Stop**.

6. Place your mouse pointer on any line (packet) in your capture buffer, and double-click. Your display will now change to show you the contents of the selected packet. You are looking at a packet you captured in real time.

7. Using your local information, fill in the following information:

   Source Ethernet address: _____

   Destination Ethernet address: _____

Exercise 2: Error Messages

1. Close Wireshark by clicking the large **Close** button in the upper-right corner of the display. If asked, do not save any of the captured frames.
2. Open your command-line prompt. Enter the following command:

```
netstat –e
```

3. How many errors are recorded in the display?

You have successfully completed this lab.

L3

Lab 3: Exploring Layer 2 Switching

Hands-On Lab

Lab Objectives

In this lab you will:

- Discover how a switch controls Ethernet traffic
- View a forwarding table in a single switch
- Interconnect switches using copper wiring
- Create a loop in the network
- Watch STP control the traffic levels
- Examine the forwarding tables in switches from different vendors
- Discover how VLANs limit traffic and provide security

Lab Procedures

Exercise 1: Using a Single Workgroup Switch

1. Test connectivity to the other students in the classroom. The assigned IP (Internet Protocol) addresses are listed in Figure 28.

Command	Successful
ping linux.gklabs.com	
ping 192.168.100.51	
ping 192.168.100.52	
ping 192.168.100.53	
ping 192.168.100.54	
ping 192.168.100.55	
ping 192.168.100.56	
ping 192.168.100.57	
ping 192.168.100.58	
ping 192.168.100.59	
ping 192.168.100.60	
ping 192.168.100.61	
ping 192.168.100.62	
ping 192.168.100.63	
ping 192.168.100.64	

Command	Successful
ping 192.168.100.65	
ping 192.168.100.66	
ping 192.168.100.67	
ping 192.168.100.68	

Figure 28: Ping Results Using Single Workgroup Switch

2. The switch provides the same type of connectivity that you found in the hub. What is different?

Exercise 2: Viewing the Switch Forwarding Table

1. In this exercise, you will use a Telnet session to view the forwarding table on the switch you are attached to. Open your command line window by double-clicking the **Command Prompt** icon on the desktop.

2. Enter the following command:

   `telnet 192.168.100.21`

   2.1 A Telnet session begins. You will be prompted by the Telnet session on the switch to enter a password. Enter the following password:

   `telnet`

   2.2 When you are logged in to the switch, you will see the following prompt:

   `CoreSwitch>`

3. At the Core prompt, enter the following command:

   `show mac-address`

   This command tells the switch to display the current contents of the MAC (media access control) address forwarding table.

4. Locate the MAC address of your NIC (network interface card) in the table and answer the following questions.

   4.1 What port does the switch say you are plugged in to?

   _____

   4.2 If you move your cable from one switch port to another, how does the switch know that you have moved to a new port?

   _____

4.3 When does the switch learn that your MAC address is now at a new port location?

5. Type **Exit** to end the Telnet session.
   Wait until your instructor tells you to continue.

Exercise 3: Using Multiple Switches

1. Enter the following command:

   telnet 192.168.100.21

   1.1 A Telnet session begins. You are prompted by the Telnet session on the switch to enter a password. Enter the following password:

   telnet

   1.2 When you are logged in to the switch, you will see the following prompt:

   CoreSwitch>

2. At the Core prompt, enter the following command:

   show mac-address

   This command tells the switch to display the current contents of the MAC address forwarding table.

3. Locate the MAC address of your NIC in the table. On what port does the switch say your MAC address is found?

   _____

   You are directly connected to the Core switch. Your port number should match your student number.

4. Type **Exit** to end the Telnet session.

5. Enter the following command:

   telnet 192.168.100.22

   5.1 A Telnet session begins. You are prompted by the Telnet session on the switch to enter a password. Enter the following password:

   telnet

   5.2 When you are logged in to the switch, you see the following prompt:

   BostonSwitch>

6. At the Boston prompt, enter the following command:

```
show mac-address
```

This command tells the switch to display the current contents of the MAC address forwarding table.

7. Locate the MAC address of your NIC in the table. On what port does the switch say your MAC address is found?

_____

8. Type **Exit** to end the Telnet session.

   You should clearly see how the switch finds your workstation by using the MAC address table.

   Wait until your instructor tells you to continue.

Exercise 4: Controlling Traffic with the Spanning Tree Protocol

1. Your instructor will now connect the Core switch to the Boston switch using another crossover cable connecting port 24 on both switches.

2. STP is now controlling the flow of the traffic, eliminating the loop by forwarding on some interfaces and blocking on others.

3. Enter the following command:

   `telnet 192.168.100.21`

   3.1 A Telnet session begins. You are prompted by the Telnet session on the switch to enter a password. Enter the following password:

   `telnet`

   3.2 When you are logged in to the switch, you will see the following prompt:

   `CoreSwitch>`

4. At the Core prompt, enter the following command:

   `show spanning-tree`

   From the spanning tree display, answer the following questions:

   4.1 Is this the root bridge? (The display will clearly indicate if this device is the root bridge.)

4.2 What is the MAC address of the root bridge?

_____

4.3 What ports are forwarding?

_____

4.4 What ports are blocking?

_____

5. Type **Exit** to end the Telnet session.

6. Now we will look at the STP operation on the second switch. Enter the following command:

```
telnet 192.168.100.22
```

6.1 A Telnet session begins. You are prompted by the Telnet session on the switch to enter a password. Enter the following password:

```
telnet
```

6.2 When you are logged in to the switch, you will see the following prompt:

```
BostonSwitch>
```

7. At the Boston prompt, enter the following command:

```
show spanning-tree
```

From the STP display, answer the following questions:

7.1 Is this the root bridge? (The display will clearly state if this device is the root bridge.)

7.2 What is the MAC address of the root bridge?

7.3 What ports are forwarding?

7.4 What ports are blocking?

8. Your instructor will now connect to the Portland switch into the network and issue the show spanning-tree.

8.1 What is the MAC address of the root bridge?

8.2 What does STA (Spanning Tree Algorithm) use to determine which device is the root bridge?

9. Type **Exit** to end the Telnet session.

You have successfully completed this lab.

L4

Lab 4: Logical Addressing

Hands-On Lab

Lab Objectives

In this lab, you will:

- Identify addresses according to traditional class
- Identify addresses as private or public
- Identify properly formatted masks and prefixes
- Label diagrams with proper IP addresses

Lab Procedures

Exercise 1: Identifying Classes of Addresses

Label each of the following addresses with the correct address class (A, B, C, or D):

___ 1. 204.238.7.99

___ 2. 99.66.55.11

___ 3. 173.98.1.198

___ 4. 229.42.111.2

___ 5. 10.1.1.9

___ 6. 172.38.9.101

___ 7. 192.168.100.22

___ 8. 127.0.0.1

Exercise 2: Identifying Public and Private Addresses

Label the private addresses below with the letter “P”. Do not label the public addresses.

___ 1. 10.99.1.4

___ 2. 192.168.255.98

___ 3. 172.88.198.22

___ 4. 178.168.1.55

___ 5. 172.16.0.255

___ 6. 191.28.155.240

___ 7. 55.198.224.1

___ 8. 11.11.11.11

Exercise 3: Identifying Properly Formatted Masks

Label each of the following masks. Enter "C" for correct or "I" for incorrect.

___ 1. 255.255.255.0

___ 2. 255.248.0.255

___ 3. 256.255.0.0

___ 4. 255.255.255.179

___ 5. 255.255.255.255

___ 6. 192.255.255.255

___ 7. 255.254.0.0

Exercise 4: Identifying Masks and Prefixes

For each of the following masks, enter the correct prefix representation.
For example, 255.255.255.0 = /24.

Mask	Prefix
255.255.255.192	
255.255.0.0	
255.255.224.0	
255.255.255.248	
255.0.0.0	
255.240.0.0	
255.255.254.0	

Figure 29: Identifying Masks and Prefixes

Exercise 5: IP Network Address Selection

You have been asked to assist in determining which IP (Internet Protocol) addresses would be best to use for three different corporations.

- X Corp is a moderately sized corporation with a need for about 25,000 IP addresses.
- Y Corp is very small and has only 50 IP devices in their entire network.
- Z Corp is very large with many locations and many devices in each location. The last device inventory showed over 70,000 IP devices.

Figure 30: IP Network Address Selection

Label each corporate location with an appropriate IP network address that would be useful for the company. Choose from the following list by entering the letter corresponding to the address in the space below each location in Figure 30.

a. 10.0.0.0
b. 172.30.6.0
c. 192.168.100.0
d. 127.0.0.0
e. 224.238.100.0
f. 172.32.99.0
g. 192.196.224.0
h. 126.0.0.0

Exercise 6: Labeling an IP Network with Correct Addresses

Two routers are used to interconnect two different networks. The network between the two routers will always require very few addresses. The other two networks are much larger. The network on the left will require a lot of addresses. The network on the right will require fewer. From the addresses provided in Figure 31, correctly assign IP addresses to the devices in the diagram. Enter the letter corresponding to the address in the space next to the devices.

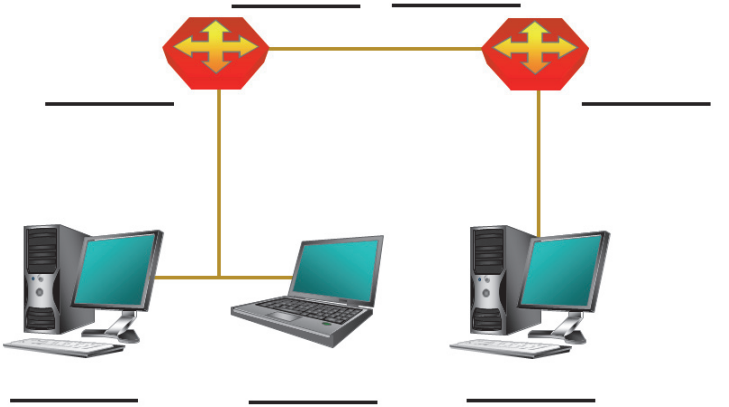

Figure 31: Labeling an IP Network with Correct Addresses

a. 172.16.0.1
b. 192.168.1.1
c. 10.0.0.1
d. 172.16.0.55
e. 10.0.0.129
f. 192.168.1.2
g. 10.0.0.5

You have successfully completed this lab.

L5

Lab 5: ARP Processing

Hands-On Lab

Lab Objectives

In this lab, you will:

- View the contents of your ARP cache
- Generate entries for your ARP cache
- Use the protocol analyzer to view ARP packets

Lab Procedures

Exercise 1: View the ARP Cache

1. Open your command line window by double-clicking the **Command Prompt** icon on the desktop.
2. In the command line window, enter the command **arp -a**.
3. Enter the contents of your ARP (Address Resolution Protocol) cache in Figure 32.

Helpful Hint
You may not find any ARP cache entries. That is not an error.

IP Address	MAC Address	Type of Entry

Figure 32: ARP Cache Entries

4. Ping Server1 by entering the following command:

```
ping linux.gklabs.com
```

5. Enter the command **arp –a**.

6. Locate the ARP cache entry for Server1 and enter it in Figure 33.

IP Address	MAC Address	Type of Entry

Figure 33: ARP Cache Entry for Server1

7. Ping the Core router by entering the following command:

```
ping core.gklabs.com
```

8. Enter the command **arp –a**.

9. Locate the ARP cache entry for Core router and enter it in Figure 34.

IP Address	MAC Address	Type of Entry

Figure 34: ARP Cache Entry for Server2

10. Clear your ARP cache by entering the following command:

```
arp -d
```

11. Now check to see if the ARP cache is empty. Enter the following command:

```
arp -a
```

Exercise 2: Verify the ARP Cache Entries for the Classroom

While you may not be required to do this in an actual network, it is often good to have documentation containing the MAC (media access control) addresses for each device in the network. One way to get this information is to use the ARP cache.

1. Select three or four of the addresses in Figure 35. Ping each of the devices you selected. Record the MAC address found in your ARP cache after you have completed the ping. You may wish to ping a number of devices before you view the ARP cache to speed up the process. Remember, however, that Windows automatically removes ARP cache entries after about two minutes.

Command	ARP Entry
ping linux.gklabs.com	
ping 192.168.100.51	
ping 192.168.100.52	
ping 192.168.100.53	
ping 192.168.100.54	
ping 192.168.100.55	
ping 192.168.100.56	
ping 192.168.100.57	
ping 192.168.100.58	
ping 192.168.100.59	
ping 192.168.100.60	
ping 192.168.100.61	
ping 192.168.100.62	

Command	ARP Entry
ping 192.168.100.63	
ping 192.168.100.64	
ping 192.168.100.65	
ping 192.168.100.66	
ping 192.168.100.67	
ping 192.168.100.68	

Figure 35: MAC Addresses from the ARP Cache

2. In the command line window, enter the command **arp -a** to view the ARP cache.

Exercise 3: View an ARP Exchange Using the Protocol Analyzer

1. If Wireshark is not currently running, launch the program by double-clicking the desktop icon.

2. Once the program has started, click **File** in the menu bar and select **Open** to display the Open dialog box. From the list of available files, click **ARP Exchange.pcapng** and then click the **Open** button in the lower right corner.

3. Your display will contain a pre-captured ARP Exchange. You will use this exchange to observe ARP request and response frames.

4. Locate the ARP request frame in the capture buffer and click the line to decode it. This frame should be the first frame in the capture buffer. When you open the frame, you will see three lines, each with a box containing a plus (+) inside. This indicates that additional information can be found by clicking on the plus (+). Click the two plus (+) boxes labeled **Ethernet II** and **Address Resolution Protocol** to open and inspect the contents of the ARP frame.

5. Record the contents of the ARP request in the table in Figure 36.

Field	Value
Ethernet destination	
Ethernet source	
Type	
ARP hardware type	
ARP protocol	
ARP hardware size	
ARP protocol size	
ARP opcode	
ARP sender MAC address	
ARP sender IP address	
ARP target MAC address	
ARP target IP address	

Figure 36: ARP Request Contents

6. Move to the second packet in the capture buffer by clicking the left green arrow icon next to the magnifying glass on the toolbar of the decode window. This is the ARP response frame.

7. Record the contents of the ARP response in the table in Figure 37.

Field	Value
Ethernet destination	
Ethernet source	
Type	
ARP hardware type	
ARP protocol	
ARP hardware size	
ARP protocol size	
ARP opcode	
ARP sender MAC address	
ARP sender IP address	
ARP target MAC address	
ARP target IP address	

Figure 37: ARP Response Contents

8. Close the Wireshark application by clicking **File** and then **Quit** in the menu bar.

You have successfully completed this lab.

L6

Lab 6: Subnetting

Hands-On Lab

Lab Objectives

In this lab, you will:

- Determine the proper masks to address particular problems
- Create a subnet plan for a simple network
- Label a network drawing with addresses from your subnet plan
- Implement a subnet plan for the local classroom network and assign IP addresses to local devices with no default gateway

Lab Procedures

Exercise 1: Selecting Masks for Various Problems

Using the subnet mask tables at the end of this lab, select the correct mask for each of the following problems.

Network Number	Number of Subnets	Number of Hosts per Subnet	Mask
171.99.0.0	265	99	
121.0.0.0	21988	190	
199.33.2.0	10	8	
201.3.99.0	3	22	
138.21.0.0	653	50	
128.193.0.0	1088	190	

Figure 38: Subnet Mask Entries

Exercise 2: Creating a Subnet Plan

You are responsible for creating a subnet plan for a small corporate network. The network designer has provided you with information about the network to help you in your planning process. Using the information provided, select a subnet mask that meets the needs of the network design. Then create an addressing plan that includes addresses for each of the subnets you need. Populate the addressing matrix (Figure 40) with the addresses you have decided to use.

The network that requires an address plan is as follows:

- The corporate headquarters network in Chicago has 193 devices in one large subnet.
- The branch office network in Atlanta has 113 devices.
- Another branch office in London has 22 devices.
- The third branch office in Hong Kong has 57 devices.
- The fourth branch office in Los Angeles has 129 devices.

The connection between the branch offices and Chicago is done using point-to-point leased line services. Each of these point-to-point circuits requires two IP addresses. In addition, the Los Angeles and Atlanta networks are also connected together for redundancy.

Figure 39: Small Corporate Network

1. How many total subnets are required to complete this plan?

2. Which is the largest subnet in terms of devices?

3. Someone has suggested that you use the address 192.168.100.0 for your network plan. Explain why this address is not appropriate.

4. The network address you are to use is 172.18.0.0. Using this address, what mask would be most useful in completing this exercise?

5. Now that you have selected your mask and know the network address to use, create the address plan for the network. Complete the matrix in Figure 40.

Network Name	Subnet Address	First IP Address	Last IP Address	Subnet Broadcast Address
Chicago				
Atlanta				
Los Angeles				
Hong Kong				
London				
Chicago to London				
Chicago to Atlanta				
Chicago to Los Angeles				
Chicago to Hong Kong				
Chicago to London				
Atlanta to Los Angeles				

Figure 40: Subnet Address Matrix

Exercise 3: Labeling the Network Diagram

In the network diagram in Figure 41, label each network with the network number from your matrix in Figure 40. Place the network number on the bold line near the network location or link.

Figure 41: Network Diagram

Subnet Mask Tables

Class A Subnet Mask Table

Subnets	Hosts	Mask	Subnet Bits	Host Bits	Prefix
2	8388608	255.128.0.0	1	23	/9
4	4194304	255.192.0.0	2	22	/10
8	2097152	255.224.0.0	3	21	/11
16	1048576	255.240.0.0	4	20	/12
32	524288	255.248.0.0	5	19	/13
64	262144	255.252.0.0	6	18	/14
128	131072	255.254.0.0	7	17	/15
256	65536	255.255.0.0	8	16	/16
512	32768	255.255.128.0	9	15	/17
1024	16384	255.255.192.0	10	14	/18
2048	8192	255.255.224.0	11	13	/19
4096	4096	255.255.240.0	12	12	/20
8192	2048	255.255.248.0	13	11	/21
16384	1024	255.255.252.0	14	10	/22
32768	512	255.255.254.0	15	9	/23
65536	256	255.255.255.0	16	8	/24

Subnets	Hosts	Mask	Subnet Bits	Host Bits	Prefix
131072	128	255.255.255.128	17	7	/25
262144	64	255.255.255.192	18	6	/26
524288	32	255.255.255.224	19	5	/27
1048576	16	255.255.255.240	20	4	/28
2097152	8	255.255.255.248	21	3	/29
4194304	4	255.255.255.252	22	2	/30
8388608	2	255.255.255.254	23	1	/31

Figure 42: Class A Subnet Mask Table

Class B Subnet Mask Table

Subnets	Hosts	Mask	Subnet Bits	Host Bits	Prefix
2	32768	255.255.128.0	1	15	/17
4	16384	255.255.192.0	2	14	/18
8	8192	255.255.224.0	3	13	/19
16	4096	255.255.240.0	4	12	/20
32	2048	255.255.248.0	5	11	/21
64	1024	255.255.252.0	6	10	/22
128	512	255.255.254.0	7	9	/23
256	256	255.255.255.0	8	8	/24
512	128	255.255.255.128	9	7	/25
1024	64	255.255.255.192	10	6	/26
2048	32	255.255.255.224	11	5	/27
4096	16	255.255.255.240	12	4	/28
8192	8	255.255.255.248	13	3	/29
16384	4	255.255.255.252	14	2	/30
32768	2	255.255.255.254	15	1	/31

Figure 43: Class B Subnet Mask Table

Class C Subnet Mask Table

Subnets	Hosts	Mask	Subnet Bits	Host Bits	Prefix
2	128	255.255.255.128	1	7	/25
4	64	255.255.255.192	2	6	/26
8	32	255.255.255.224	3	5	/27
16	16	255.255.255.240	4	4	/28
32	8	255.255.255.248	5	3	/29
64	4	255.255.255.252	6	2	/30
128	2	255.255.255.254	7	1	/31

Figure 44: Class C Subnet Mask Table

You have successfully completed this lab.

Global Knowledge®

L7

Lab 7: Routing

Hands-On Lab

Lab Objectives

In this lab, you will:

- Add routers to the network configuration
- Convert your workstation to DHCP for address assignment
- Use sample router commands
- View interface information on the various routers
- View the routing tables
- View the ARP caches
- Compare router functionality
- As an option, discuss the router configuration files

Lab Procedures

Exercise 1: Add Routers to the Network

The purpose of this exercise is to extend the network by adding routers.

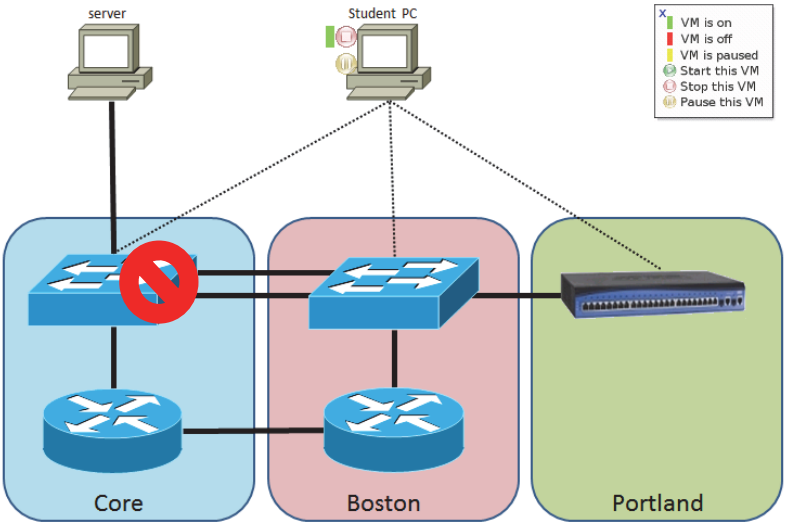

Figure 45: Network Routing Diagram

Note
Your instructor will now disable the layer 2 connections between the Core and Boston switches (ports 23 and 24).

Exercise 2: Convert Your Workstation to DHCP for Address Assignment

1. Click the **Control Panel** icon on the lower left of the screen.
2. From the Network and Internet selections, click **View network status and tasks**.
3. Click **Change adapter settings**.
4. Click on the Core switch icon, and click on **Disable this network device**. Use the following table to move to one of the switches.

Workstation	Workgroup
student01	Core
student02	Boston
student03	Portland
student04	Core
student05	Boston
student06	Portland
student07	Core
student08	Boston
student09	Portland
student10	Core
student11	Boston
student12	Portland
student13	Core
student14	Boston
student15	Portland
student16	Core
student17	Boston
student18	Portland

Figure 46: Workstations and Workgroups

5. Click on your assigned switch (Core, Boston, or Portland), then click on **Enable this network device**.
6. After your switch shows a network number, then double-click on it to access the Ethernet network properties dialog box.
7. Double-click on the **Properties** box.
8. Scroll down and click **IP Version 4**, then click **Properties**.
9. Select the **Obtain IP address automatically** radio button and **Obtain DNS server address automatically** radio button. Click **OK**. Click **OK** again and close the control panel window.
10. To verify your configuration, double-click on the **Command Prompt** shortcut on the desktop to open the command line interface window.
11. At the command line prompt, type **ipconfig /all** and press the ENTER key.
12. Record your DHCP assigned address information below:

    Connection-specific DNS suffix:

    _____

    Description:

    _____

    Physical address:

    _____

    DHCP enabled:

    _____

    Autoconfiguration enabled:

    _____

IP address:

Subnet mask:

Default gateway:

DHCP server:

DNS servers:

Lease obtained:

Lease expires:

Exercise 3: Core Router Information

1. If it is not already open, double-click the **Command Prompt** icon on the desktop to open the Command Prompt window.
2. Telnet to the Core router by entering the following command:

   ```
   telnet core.gklabs.com
   ```

3. Log in to the router using the following password:

   ```
   telnet
   ```

4. When the router responds, you will see a prompt as indicated below:

   ```
   CoreRouter>
   ```

5. Enter the following command to find out the version of the operating system on the router:

   ```
   show ver
   ```

6. What version did you find?

   _____

7. Enter the following command to view the router IP address configuration:

   ```
   show ip int brief
   ```

8. What IP addresses are found on this router? Using the display resulting from the previous router command, locate the requested information and enter it in the table in Figure 47.

Interface	IP Address	Status	Protocol

Figure 47: Core IP Addresses

9. Enter the following command to view the routing table:

```
show ip route
```

10. What routes are listed in the routing table? List only those entries with a letter in front of the network address line. Using the display resulting from the previous router command, locate the requested information and enter it in the table in Figure 48.

Code	Network	Next Hop/Connected	Interface

Figure 48: Core Routes

11. Enter the following command to view the ARP (Address Resolution Protocol) cache:

```
show ip arp
```

12. What entries are in the ARP cache? There are additional fields in the display, but enter only those requested in Figure 49. Using the display resulting from the previous router command, locate the requested information and enter it in the table in Figure 49.

Address	Age	Hardware Address	Interface

Figure 49: Core ARP Cache Entries

13. Enter the following command to end the Telnet session:

```
exit
```

14. You may need to press the ENTER key one extra time to return to the command prompt following the end of the Telnet session.

Exercise 4: Boston Router Information

1. If it is not already open, double-click the **Command Prompt** icon on the desktop to open the Command Prompt window.
2. Telnet to the Boston router by entering the following command:

   ```
   telnet boston.gklabs.com
   ```

3. Log in to the router using the following password:

   ```
   telnet
   ```

4. When the router responds you will see a prompt as indicated below:

   ```
   BostonRouter>
   ```

5. Enter the following command to view the router IP address configuration:

   ```
   show ip int brief
   ```

6. What IP addresses are found on this router? Using the display resulting from the **show** command you entered in step 5, locate the requested information and enter it in the table in Figure 50.

Interface	IP-Address	Status	Protocol

Figure 50: Boston IP Addresses

7. Enter the following command to view the routing table:

```
show ip route
```

8. What routes are listed in the routing table? List only those entries with a letter in front of the network address line. Using the display resulting from the previous router command, locate the requested information and enter it in the table in Figure 51.

Code	Network	Next Hop/Connected	Interface

Figure 51: Boston Routes

Exercise 5: Configurations

If time permits, your instructor may review the configuration files for the routers and switches found in Appendix A.

You have successfully completed this lab.

L8

Lab 8: IP Header Analysis

Hands-On Lab

Lab Objectives

In this lab, you will:

- Use the analyzer to view IP header information

Lab Procedures

Exercise 1: IP Header Information

1. Open the Wireshark application by double-clicking the desktop icon.
2. When Wireshark opens, select **File**, **Open** on the menu bar. From the files presented, select **IP Capture**. Then click the **Open** button in the lower right corner of the Open dialog box.
3. Click the first IP frame in the capture buffer to open the decode display. From the decode display, enter the information into the table in Figure 52.

IP Header Field	Value
Version	
Header length	
Differentiated services	
Total length	
Identification	
Flag bit 1	
Flag bit 2	
Flag bit 3	
Fragment offset	
Time to live	
Protocol	
Header checksum	
Source	
Destination	

Figure 52: First IP Frame Values

4. Move to the second frame in the capture buffer by clicking the second packet in the capture buffer area. From the decode display, enter the information into the table in Figure 53.

IP Header Field	Value
Version	
Header length	
Differentiated services	
Total length	
Identification	
Flag bit 1	
Flag bit 2	
Flag bit 3	
Fragment offset	
Time to live	
Protocol	
Header checksum	
Source	
Destination	

Figure 53: Second IP Frame Values

5. The first frame is an IP datagram containing a ping request sent to a Cisco router from a Microsoft XP device. The second frame is an IP datagram containing a ping reply sent from the Cisco router back to the Microsoft XP device. Answer the following questions about the two packets that you viewed:

   5.1 Is either datagram fragmented?

   5.2 Why are the two time-to-live values different?

   5.3 Why are the source and destination addresses swapped in the two datagrams?

You have successfully completed this lab.

Global Knowledge®

L9

Lab 9: TCP Operation

Hands-On Lab

Lab Objectives

In this lab, you will:

- View a TCP session using the protocol analyzer
- Locate and document the three-step startup process
- Locate and document the application login process
- Locate and document the logout process
- Locate and document the TCP session termination

Lab Procedures

Exercise 1: Viewing a TCP Session

In this lab, you will use a pre-captured protocol analyzer session. This session captured an FTP (File Transfer Protocol) login and logout process between the two servers in the network. During the lab, you will study the TCP process to see how it is implemented in the classroom software.

1. Open the Wireshark application by double-clicking the desktop icon.
2. When Wireshark opens, select **File, Open** on the menu bar. From the files presented, select **FTP Capture** and click the **Open** button in the lower right corner of the Open dialog box.

Exercise 2: Locating and Documenting the Three-Step Startup Process

1. The first three frames of the capture buffer contain the three steps of the TCP startup. In the capture buffer, locate frames 1, 2, and 3.
2. What is the IP address of the device starting the FTP process (the client)? This is the source IP address of the first frame.

_____

3. What is the IP address of the FTP server? This is the destination IP address of the first frame.

_____

4. What is the source port number used by the client? Look in the Info area of the first frame. The source port number is the number before the greater than (>) sign.

   _____

5. What is the destination port number used to indicate the service to be used on the server? The destination port number is the number following the greater than (>) sign in the Info area.

   _____

6. The Info area of the capture buffer contains flag information as well as the port numbers you recorded in steps 4 and 5. Locate frame 1 in the capture buffer. Circle the flags that are indicated in the Info area within the brackets [ ].

   Acknowledge Synchronize Reset Final Data

7. Locate frame 2. Circle the flags that are indicated in the Info area.

   Acknowledge Synchronize Reset Final Data

8. Locate frame 3. Circle the flags that are indicated in the Info area.

   Acknowledge Synchronize Reset Final Data

Exercise 3: Locating and Documenting the Application Login Process

Following the three-step startup process, the FTP server provides identification information to the client. The analyzer marks each client request with the word "Request:" at the beginning of the Info area. Server responses are labeled "Response:".

1. Locate frame 4. Does this frame come from the client or the server?

2. What type of server is being used?

3. Continue scanning the Info area. What user ID is being used to log in to the server?

4. Continue scanning the Info area. What password is being used to log in to the server?

5. Since you can clearly see the user ID and password in the capture buffer, does this represent a security risk in the network?

Exercise 4: Locating and Documenting the Logout Process

1. Locate frame 20. What command is being sent from the client to the server to indicate that the user wishes to end the FTP session?

2. Locate frame 21. A message is being sent from the server to the client. Answer the following questions about the message:
   2.1 What message number is being sent?

   2.2 What does this message mean?

   2.3 Where might you look to get clarification about the purpose of the message?

Exercise 5: Locating and Documenting TCP Session Termination

1. Frames 22 through 25 are the four steps of the shutdown process used by TCP. Which device, the client or the server, starts the shutdown process?

2. Locate frame 22. Circle the flags that are indicated in the Info area.

   Acknowledge Synchronize Reset Final Data

3. Locate frame 23. Circle the flags that are indicated in the Info area.

   Acknowledge Synchronize Reset Final Data

4. Locate frame 24. Circle the flags that are indicated in the Info area.

   Acknowledge Synchronize Reset Final Data

5. Locate frame 25. Circle the flags that are indicated in the Info area.

   Acknowledge Synchronize Reset Final Data

You have successfully completed this lab.

Global Knowledge®

L10

Lab 10: DHCP Operation and Analysis

Hands-On Lab

Lab Objectives

In this lab, you will:

- View the result of DHCP failure
- View your DHCP configuration
- View a UDP header
- View the four-step DHCP process

Lab Procedures

Exercise 1: Viewing the Result of DHCP Failure

Your instructor will temporarily disable the DHCP (Dynamic Host Configuration Protocol) server in the classroom. Without the DHCP server, you will not receive an IP address from the server. In this exercise, you will learn what happens when the DHCP server is not available.

1. Open a command line window by double clicking the **Command Prompt** icon on the desktop.
2. Enter the following command:

   ```
   ipconfig /release
   ```

3. Enter the following command:

   ```
   ipconfig /renew
   ```

   After a brief period of time, you will receive an error message indicating that an IP address was not obtained from DHCP.

4. In your command line window, enter the following command:

   ```
   ipconfig /all
   ```

5. Though DHCP did not assign you an IP address, you can see that you have an address assigned to your device. Record the IP address information below:

   5.1 IP address:

   _____

   5.2 Subnet mask:

   _____

   5.3 Default gateway:

   _____

6. Where did this address come from?

_____

_____

7. Your instructor will now enable the DHCP server. Wait until your instructor tells you it is okay to proceed.

Exercise 2: Viewing Your DHCP Configuration

1. Your command line window should already be open. If not, open a command line window by double-clicking the **Command Prompt** icon on the desktop.
2. Enter the following command:

   ```
   ipconfig /release
   ```

3. Enter the following command:

   ```
   ipconfig /renew
   ```

   After a brief period of time, you will be assigned an IP address from the DHCP server.

4. In your command line window, enter the following command:

   ```
   ipconfig /all
   ```

5. DHCP has assigned you an IP address and other configuration information. Record the information in the space below:

   5.1 Connection-specific DNS suffix:

   _____

   5.2 Description:

   _____

   5.3 Physical address:

   _____

5.4 DHCP enabled:

5.5 Autoconfiguration enabled:

5.6 IP address:

5.7 Subnet mask:

5.8 Default gateway:

5.9 DHCP server:

5.10 DNS servers:

5.11 Primary WINS server:

5.12 Lease obtained:

5.13 Lease expires:

Exercise 3: Viewing a UDP Header

1. Open the Wireshark application by double-clicking the desktop icon.
2. When Wireshark opens, select **File, Open** on the menu bar. From the files presented, select **DHCP Capture** and click the **Open** button in the lower right corner of the Open dialog box.
3. Locate frame 1. This frame is a DHCP release message sent from a client to the DHCP server. In this frame, you will be looking at the UDP (User Datagram Protocol) header.
4. Double-click the line for frame 1 to open the decode window. Locate and record the following information from frame 1:
   - 4.1 From the IP header:
     - 4.1.1 Protocol:

     - 4.1.2 Source IP address:

     - 4.1.3 Destination IP address:

4.2 From the UDP header:

4.2.1 Source port:

4.2.2 Destination port:

4.2.3 Length:

4.2.4 UDP checksum:

---

5. You should now be viewing the capture buffer, which contains five frames.

Exercise 4: Viewing the Four-Step DHCP Process

1. Frames 2 through 5 are the four steps of the DHCP lease process. For each of the frames listed in Figure 54, record the information from the capture buffer display.

Frame Number	Source IP Address	Destination IP Address	DHCP Packet Type (from the Info area)
2			
3			
4			
5			

Figure 54: DHCP Frame Information

2. The last frame, frame 5, contains all of the information necessary to configure the IP device. Double-click frame 5 in the capture buffer to view the decode window. Record the following information from the capture buffer:
   2.1 From the IP header:
      2.1.1 Source IP address:

      _____

      2.1.2 Destination IP address:

      _____

2.2 From the BOOTP header:

2.2.1 Message type:

2.2.2 Transaction ID:

2.2.3 Client IP address:

2.2.4 Next server IP address:

2.2.5 Relay agent IP address:

2.2.6 Client MAC address:

2.3 From the DHCP header (below the magic cookie):

2.3.1 DHCP message type:

2.3.2 Renewal time value:

2.3.3 Rebinding time value:

2.3.4 IP address lease time:

2.3.5 Subnet mask:

2.3.6 Domain name:

2.3.7 Router address:

2.3.8 Domain Name Server address:

---

3. Close the capture buffer window by selecting **File, Close** from the menu bar.

You have successfully completed this lab.

Global Knowledge®

L11

Lab 11: DNS

Hands-On Lab

Lab Objectives

In this lab, you will:

- Use the **nslookup** command to query a DNS server
- View a DNS request using the protocol analyzer
- View the DNS response using the protocol analyzer

Lab Procedures

Exercise 1: Querying a DNS Server with nslookup

1. Open a command line window by double-clicking the **Command Prompt** icon on the desktop.

2. When the command prompt opens, enter the following command:

   ```
   nslookup linux.gklabs.com
   ```

   2.1 What IP address is returned in response to your **nslookup** request?

   _____

   This form of **nslookup** request is used to query one address at a time.

3. The **nslookup** command is also an application program that performs many different functions. In the next few steps, you will be using **nslookup** in the multifunction application mode. Enter the following command in the command line window:

   ```
   nslookup
   ```

   The display now contains the name and IP address of the DNS (Domain Name System) server that **nslookup** will be using. Enter the server name and IP address below:

   3.1 Server name:

   _____

   3.2 IP address:

   _____

4. Below the server name and address, you will see a greater than (>) symbol. This is the command prompt for **nslookup**. People often confuse this for the DOS prompt.

5. Next to the ">" prompt for **nslookup**, enter the following request:

```
boston.gklabs.com
```

5.1 What address is returned by **nslookup**?

_____

6. Enter the following request to exit **nslookup**:

```
exit
```

You will return to the command prompt.

Exercise 2: Viewing a DNS Request

1. If Wireshark is not open, open the Wireshark application by double-clicking the desktop icon.

2. When Wireshark opens, select **File, Open** on the menu bar. From the files presented, select **DNS Capture** and click the **Open** button in the lower right corner of the Open dialog box.

3. Locate frame 1. This frame is a DNS request message sent from a client to the DNS server. In this frame, you will be looking at the UDP (User Datagram Protocol) header and the DNS request information.

4. Double-click the line for frame 1 to open the decode window. Locate and record the following information from frame 1:

   4.1 From the IP header:

   4.1.1 Protocol:

   _____

   4.1.2 Source IP address:

   _____

   4.1.3 Destination IP address:

   _____

4.2 From the UDP header:

4.2.1 Source port:

4.2.2 Destination port:

4.2.3 Length:

4.2.4 UDP checksum:

4.3 From the DNS header:

4.3.1 Questions:

4.3.2 Answers:

4.4 Queries: (Click the Queries "+" box to see the question asked in the DNS request.)

4.4.1 Domain name:

4.4.2 Type:

4.4.3 Class:

Exercise 3: Viewing a DNS Response

1. Locate frame 2 in the capture buffer. Double-click the line for frame 2 to open the decode window.
2. Locate and record the following information from frame 2:
   - 2.1 From the IP header:
     - 2.1.1 Protocol:

     - 2.1.2 Source IP address:

     - 2.1.3 Destination IP address:

   - 2.2 From the UDP header:
     - 2.2.1 Source port:

     - 2.2.2 Destination port:

     - 2.2.3 Length:

2.2.4 UDP checksum:

2.3 From the DNS header:

2.3.1 Questions:

2.3.2 Answers:

2.4 Queries:

2.4.1 Domain name:

2.4.2 Type:

2.4.3 Class:

2.5 Answers: (Click the "+" box next to the domain name in the answers area to see the information needed to fill in this part of the lab.)

2.5.1 Domain name:

2.5.2 Type:

2.5.3 Class:

2.5.4 Time to live:

2.5.5 Data length:

2.5.6 IP address:

---

3. Look at the DNS flags in the current frame, frame 2. Is this answer an "authoritative" answer?

---

4. Close the decode window by clicking the **X** in the upper right corner. You should now be viewing the capture buffer, which contains two frames.

5. Close the capture buffer window by selecting **File, Close** from the menu bar.

You have successfully completed this lab.

Global Knowledge®

L12

Lab 12: Internet Control Message Protocol

Hands-On Lab

Lab Objectives

In this lab, you will:

- Examine an **Echo Request**/**Echo Response** message pair
- Examine a **Destination Unreachable** message

Lab Procedures

Exercise 1: Examining an Echo Request/Echo Response Message Pair

1. Open the Wireshark application by double-clicking the desktop icon.
2. When Wireshark opens, click **File, Open** on the menu bar. From the files presented, select **Ping Linux Capture** and click the **Open** button in the lower right corner of the Open dialog box.
3. Double-click the first IP frame in the capture buffer to open the decode window. From the decode display, enter the information indicated in Figure 55.

IP Header Field	Value
Time to live	
Protocol	
Source IP address	
Destination IP address	

ICMP Header Field	Value
ICMP type	
ICMP code	
ICMP checksum	
Identifier	
Sequence number	

Figure 55: First IP Frame of Echo Message Pair

4. Double-click the second frame in the capture buffer to open the decode window. From the decode display, enter the information indicated in Figure 56.

IP Header Field	Value
Time to live	
Protocol	
Source IP address	
Destination IP address	

ICMP Header Field	Value
ICMP type	
ICMP code	
ICMP checksum	
Identifier	
Sequence number	

Figure 56: Second IP Frame of Echo Message Pair

5. Click the ICMP **Data** area tag in the decode window to highlight the ICMP (Internet Control Message Protocol) data in the hexadecimal and ASCII areas. Look at the contents of the ASCII display.

   5.1 Move to the first frame in the capture buffer. Move back and forth between frames 1 and 2 by clicking the lines.

      5.1.1 Do the contents of the data area change when being returned from the ICMP target device?

6. Compare the time-to-live values in the two frames. Why are the time-to-live values different?

Exercise 2: Examining a Network Unreachable Message

1. In the open Wireshark application, click **File, Open** on the menu bar. From the files presented, select **Network Unreachable Capture** and click the **Open** button in the lower right corner of the Open dialog box.

2. Click the first IP frame in the capture buffer. From the decode display, enter the information indicated in Figure 57.

IP Header Field	Value
Time to live	
Protocol	
Source IP address	
Destination IP address	

Figure 57: First IP Frame of Network Unreachable Message

3. Move to the second frame in the capture buffer. From the decode display, enter the information indicated in Figure 58.

IP Header Field	Value
Time to live	
Protocol	
Source IP address	
Destination IP address	

ICMP Header Field	Value
ICMP type	
ICMP code	
ICMP checksum	

Figure 58: Second IP Frame of Network Unreachable Message

4. Scroll down below the ICMP header field to find the next IP header in the ICMP message frame. This is the header of the message that caused the error. Record the information indicated in Figure 59.

IP Header Field	Value
Time to live	
Protocol	
Source IP address	
Destination IP address	

Figure 59: IP Header of the Network Unreachable Message

5. This is a **Destination Unreachable**, **Network Unreachable** message. Answer the following questions:

   5.1 What was the original destination address?

   _____

   5.2 What router could not forward the frame correctly?

   _____

You have successfully completed this lab.

L13

Lab 13: Network Security

Hands-On Lab

Lab Objectives

In this lab, you will;

- Implement the Windows 7/8 firewall function
- Test the Windows 7/8 firewall function
- View the configuration of the firewall implementation in the network
- Test the network firewall function

Lab Procedures

Exercise 1: Implementing the Windows 7/8 Firewall Function

You can customize four settings for each type of network location in Windows Firewall. To find these settings, follow these steps:

1. Open Windows Firewall by clicking the **Start** button. In the search box, type **firewall**, and then click **Windows Firewall**.

2. In the left pane, click **Turn Windows Firewall on or off**. Under both private and public network settings, click **Turn on Windows Firewall**. Click **OK**. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.

Exercise 2: Testing the Windows 7/8 Firewall Function

1. Your device is now protected. Test your protection and that of your fellow classmates by issuing several ping requests. Ask students from the four different workgroups for their IP addresses. Enter them in the table in Figure 60 and then attempt to ping them.

Workgroup	IP Address	Successful
1		
2		
3		
4		

Figure 60: Workgroup IP Addresses and Ping Results

2. Ping the network devices listed in the table in Figure 61.

IP Address	Successful
192.168.100.10	
192.168.100.2	
192.168.100.6	

Figure 61: Addresses for Network Devices and Ping Results

3. Why might you be able to ping some devices but not others?

4. Using the procedures in Exercise 1, turn off the Windows Firewall function. Remember to set the firewall to **Off**.

Note
At this point in the lab, your instructor will be modifying the configuration of one of the routers to include firewall protection for the network. Please wait to continue until your instructor tells you to do so.

Exercise 3: Viewing the Configuration of the Firewall Implementation in the Network

Your instructor will review with you the configuration of the firewall in the router.

Exercise 4: Testing the Network Firewall Function

1. The network now has a firewall function installed. Depending on where you are in the network, you will be able to connect to some devices, but not others.

2. Ping each of the IP addresses listed in Figure 62. Note which addresses you can successfully ping and which you cannot.

IP Address	Successful
192.168.100.10	
10.3.1.1	
172.16.1.1	

Figure 62: Network Firewall Test Results

3. The Windows firewall has been disabled. Ask students from the three different workgroups for their IP addresses. Enter them in the table below and then attempt to ping them.

Workgroup	IP Address	Successful
Core		
Boston		
Portland		

Figure 63: Network Test Results with Firewall Disabled

4. The Windows 7/8 Firewall is not protecting the devices. What device is protecting these devices from your device?

You have successfully completed this lab.

Global Knowledge®

L14

Lab 14: User Processes

Hands-On Lab

Lab Objectives

In this lab, you will:

- Examine how e-mail is transmitted and received

Lab Procedures

Exercise 1: Viewing an SMTP Session

1. If Wireshark is not open, open the Wireshark application by double-clicking the desktop icon.
2. When Wireshark opens, select **File, Open** on the menu bar. From the files presented, select **SMTP Capture** and click **Open** in the lower right corner of the Open dialog box.
3. SMTP (Simple Mail Transfer Protocol) is a TCP-based application. The first three frames are the three steps of the TCP startup. The remaining frames between frame 4 and frame 20 are the frames containing the e-mail process and the e-mail message. The last four frames contain the four steps of the TCP shutdown.

   3.1 What port number is being used by the client?

   _____

   3.2 What port number is used to connect to the server?

   _____

4. Locate frame 13 and double-click to open the decode window. Scroll down in the windows until you find the SMTP part of the frame. Answer the following questions from the e-mail message:

   4.1 What is the name of the person sending the e-mail message?

   _____

   4.2 When was she born?

   _____

   4.3 What is her social security number?

   _____

   4.4 In viewing this message, would you be concerned about Internet security?

   _____

5. Close the decode window by clicking the **X** in the upper right corner.

Exercise 2: Viewing a POP3 Session

1. In the open Wireshark application, select **File, Open** on the menu bar. From the files presented, select **POP3 Capture**. Click the **Open** button in the lower right corner of the Open dialog box.

2. POP3 (Post Office Protocol version 3) is a TCP-based application. The first three frames are the three steps of the TCP startup. The remaining frames between frame 4 and frame 30 are the frames containing the e-mail retrieval and the e-mail message. The last four frames contain the four steps of the TCP shutdown.

   2.1 What port number is being used by the client?

   _____

   2.2 What port number is used to connect to the server?

   _____

3. Locate frames 4 through 18 in the capture buffer. These frames are used to process the user ID and password required by the POP3 (Post Office Protocol 3) security process. Notice that some of the information is encrypted.

   3.1 From what you see, can you determine the user ID and password of the user?

   _____

   3.2 Does encrypting the user ID and password assure the security of the information in the e-mail message?

   _____

4. Locate frame 24 and double-click to open the decode window. Scroll down to the POP (Post Office Protocol) part of the display and answer the following questions:

   4.1 Can you read the contents of the message?

   _____

   4.2 Are you concerned about Internet security after reading this message, even though access to the message is password protected?

   _____

5. Close Wireshark by clicking **File** and then **Close**.

Exercise 3: Viewing an HTTP Session

1. In Wireshark, select **File, Open** on the menu bar. From the files presented, select **HTTP Capture**. Click the **Open** button in the lower right corner of the Open dialog box.

2. There are three HTTP Get request messages in the capture buffer. In the Info area, locate each of them and write in the spaces below the contents of each Get.

   Get 1 = _____

   Get 2 = _____

   Get 3 = _____

3. What was the name of the first file returned by the first get request?

   _____

4. What was the second file?

   _____

5. Was the third file found? _____ How can you tell?

   _____

You have successfully completed this lab.

Global Knowledge®

A

Appendix A: Router/Switch Configurations

Core Switch Configuration

```
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname CoreSwitch
!
no logging console
enable secret 5 $1$YTrQ$NibLUx.EfamGiA8oKKJdZ.
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
vtp domain qos
vtp mode transparent
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
vlan 2
 name test2
!
interface FastEthernet0/1
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/2
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/3
 switchport mode access
 spanning-tree portfast
!
```

```
interface FastEthernet0/4
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/5
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/6
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/7
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/8
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/9
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/10
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/11
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/12
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/13
 switchport mode access
 spanning-tree portfast
!
```

```
interface FastEthernet0/14
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/15
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/16
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/17
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/18
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/19
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/20
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/21
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/22
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/23
 switchport mode trunk
 no shutdown
!
```

```
interface FastEthernet0/24
 switchport mode trunk
 no shutdown
!
interface Vlan1
 ip address 192.168.100.21 255.255.255.0
 no ip route-cache
 no shutdown
!
ip default-gateway 192.168.100.2
ip http server
!
line con 0
line vty 0 4
 password telnet
 login
line vty 5 15
 password telnet
 login
!
!
end
```

Core Router Configuration

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CoreRouter
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$GKKi$yMyW/oOCp11cX3JYJiK0j1
!
no aaa new-model
!
resource policy
!
no network-clock-participate slot 1
no network-clock-participate wic 0
ip cef
!
!
ip multicast-routing
!
ipv6 unicast-routing
!
!
archive
 log config
  hidekeys
!
!
interface FastEthernet0/0
 ip address 192.168.100.2 255.255.255.0
 ip pim dense-mode
 duplex auto
 speed auto
 ipv6 address 2019:0:0:1::2/64
```

```
 ipv6 enable
 ipv6 rip gkn enable
 ipv6 rip one enable
 no cdp enable
 no shutdown
!
interface FastEthernet0/1
 ip address 192.168.1.1 255.255.255.248
 ip pim dense-mode
 duplex auto
 speed auto
 ipv6 address 2020:0:0:1::1/64
 ipv6 address 2FFB:2222:3333:4400::/64 eui-64
 ipv6 enable
 ipv6 rip gkn enable
 ipv6 rip one enable
 no shutdown
!
interface Serial1/0
 no ip address
 shutdown
 no fair-queue
 no dce-terminal-timing-enable
!
interface Serial1/1
 no ip address
 shutdown
 no dce-terminal-timing-enable
!
interface Serial1/2
 no ip address
 shutdown
 no dce-terminal-timing-enable
!
interface Serial1/3
 no ip address
 shutdown
 no dce-terminal-timing-enable
!
router rip
```

```
 version 2
 network 172.20.0.0
 network 192.168.1.0
 network 192.168.2.0
 network 192.168.100.0
!
!
ip http server
no ip http secure-server
!
ipv6 router rip one
!
ipv6 router rip gkn
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 password telnet
 login
line vty 5 15
 password telnet
 login
!
!
end
```

Boston Switch Configuration

```
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname BostonSwitch
!
no logging console
enable secret 5 $1$a5LV$gRg5AxwmEFl8745LAENJS/
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
vtp domain qos
vtp mode transparent
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
interface FastEthernet0/1
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/2
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/3
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/4
 switchport mode access
```

```
 spanning-tree portfast
!
interface FastEthernet0/5
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/6
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/7
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/8
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/9
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/10
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/11
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/12
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/13
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/14
 switchport mode access
```

```
 spanning-tree portfast
!
interface FastEthernet0/15
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/16
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/17
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/18
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/19
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/20
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/21
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/22
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/23
 switchport mode trunk
!
interface FastEthernet0/24
 switchport mode trunk
!
```

```
interface Vlan1
 ip address 192.168.100.22 255.255.255.0
 no ip route-cache
 no shutdown
!
interface Vlan2
 no ip address
 no ip route-cache
 no shutdown
!
ip default-gateway 10.3.1.1
ip http server
!
line con 0
line vty 0 4
 password telnet
 login
line vty 5 15
 password telnet
 login
!
!
end
```

Boston Router Configuration

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BostonRouter
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$69D8$.gRPlrPBTdtprwkL8H5jD.
!
no aaa new-model
!
resource policy
!
no network-clock-participate slot 1
no network-clock-participate wic 0
ip cef
!
!
ip name-server 192.168.100.10
ip multicast-routing
!
ipv6 unicast-routing
!
!
archive
 log config
  hidekey
!
!
interface FastEthernet0/0
 ip address 10.3.1.1 255.255.255.0
 ip helper-address 192.168.100.10
 ip pim dense-mode
 duplex auto
```

```
 speed auto
 ipv6 address 2021:0:0:1::1/64
 ipv6 rip one enable
 no shutdown
!
interface FastEthernet0/1
 ip address 192.168.1.2 255.255.255.248
 ip pim dense-mode
 duplex auto
 speed auto
 ipv6 address 2020:0:0:1::2/64
 ipv6 rip one enable
 no shutdown
!
interface Serial1/0
 no ip address
 shutdown
 no fair-queue
 no dce-terminal-timing-enable
!
interface Serial1/1
 no ip address
 shutdown
 no dce-terminal-timing-enable
!
interface Serial1/2
 no ip address
 shutdown
 no dce-terminal-timing-enable
!
interface Serial1/3
 no ip address
 shutdown
 no dce-terminal-timing-enable
!
router rip
 version 2
 network 10.0.0.0
 network 172.20.0.0
 network 192.168.1.0
```

```
 network 192.168.100.0
!
!
ip http server
no ip http secure-server
!
ipv6 router rip one
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 password telnet
 login
line vty 5 15
 password telnet
 login
!
!
end
```

Portland Switch/Router Configuration

```
!
! ADTRAN, Inc. OS version R10.8.0.E
! Boot ROM version 15.01.B1
! Platform: NetVanta 1335, part number 1700515E2
! Serial number LBADTN1303AH432
!
!
hostname "PortlandRouter"
enable password encrypted 2a23c888f5accc03f20ac97256a0314f5bbb
!
clock timezone -11
!
ip subnet-zero
ip classless
ip routing
!
!
name-server 192.168.100.10
!
ip multicast-routing
ip mcast-stub helper-address 192.168.100.10
!
no ip route-cache express
!
no auto-config
auto-config authname adtran encrypted password 4046f0ba5cdf72bf460b8f2203161619f745
!
event-history on
no logging forwarding
no logging email
!
service password-encryption
!
portal-list "console" ssh telnet
portal-list "web" http-admin
!
username "admin" password encrypted "3b3345936452022l3b4261202185124bef3f"
username "user" portal-list "console" password encrypted "2127ecd408c12c0dfa2262b5796c652c338a"
```

```
username "webuser" portal-list "web" password encrypted "2a23d2ef07715b9ccedb3a133f07d353344f"
ip forward-protocol udp bootps
!
!
no ip firewall alg msn
no ip firewall alg mszone
no ip firewall alg h323
!
!
no dot11ap access-point-control
!
!
vlan 1
  name "Default"
!
vlan 2
  name "coredevices"
!
vlan 3
  name "Chicago"
!
vlan 4
  name "Paris"
!
vlan 5
  name "HongKong"
!
!
interface switchport 0/1
  no shutdown
!
interface switchport 0/2
  no shutdown
!
interface switchport 0/3
  no shutdown
!
interface switchport 0/4
  no shutdown
!
```

```
interface switchport 0/5
  no shutdown
!
interface switchport 0/6
  no shutdown
!
interface switchport 0/7
  no shutdown
!
interface switchport 0/8
  no shutdown
!
interface switchport 0/9
  no shutdown
!
interface switchport 0/10
  no shutdown
!
interface switchport 0/11
  no shutdown
!
interface switchport 0/12
  no shutdown
!
interface switchport 0/13
  no shutdown
!
interface switchport 0/14
  no shutdown
!
interface switchport 0/15
  no shutdown
!
interface switchport 0/16
  no shutdown
!
interface switchport 0/17
  no shutdown
!
interface switchport 0/18
```

```
  no shutdown
!
interface switchport 0/19
  no shutdown
!
interface switchport 0/20
  no shutdown
!
interface switchport 0/21
  no shutdown
  switchport access vlan 2
!
interface switchport 0/22
  no shutdown
!
interface switchport 0/23
  no shutdown
!
interface switchport 0/24
  no shutdown
!
!
interface gigabit-switchport 0/1
  no shutdown
!
interface gigabit-switchport 0/2
  no shutdown
!
!
interface vlan 1
  ip address   172.20.1.1   255.255.255.0
  ip mcast-stub downstream
  ip mcast-stub helper-enable
  ip helper-address   192.168.100.10
  ip route-cache express
  no shutdown
!
interface vlan 2
  ip address   10.3.1.254   255.255.255.0
  ip mcast-stub upstream
```

```
  ip route-cache express
  no shutdown
!
interface vlan 3
  ip address   172.18.4.1   255.255.255.0
  ip route-cache express
  no shutdown
!
interface vlan 4
  ip address   172.16.5.1   255.255.255.0
  ip route-cache express
  no shutdown
!
interface vlan 5
  ip address   172.31.1.1   255.255.255.0
  ip route-cache express
  no shutdown
!
!
router rip
  version 2
  network 172.20.1.0 255.255.255.0
  network 10.3.1.0 255.255.255.0
  network 172.16.5.0 255.255.255.0
  network 172.18.4.0 255.255.255.0
  network 172.31.1.0 255.255.255.0
!
!
router pim-sparse
!
!
tftp server
no tftp server overwrite
http server
no http secure-server
no snmp agent
no ip ftp server
ip ftp server default-filesystem flash
no ip scp server
no ip sntp server
```

```
!
!
sip udp 5060
sip tcp 5060
!
!
line con 0
  login
!
line telnet 0 4
  login
  password encrypted 1f199cf3af3fa800762180a3f6d45720e408
  no shutdown
line ssh 0 4
  login local-userlist
  no shutdown
!
!
end
```