

Activity 3.4.1: Data Stream Capture

Learning Objectives

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

- Capture or download an audio stream
- Record the characteristics of the file
- Examine data transfer rates associated with the file

Background

When an application creates a file, the data that comprises that file must be stored somewhere. The data can be stored on the end device where it was created, or it can be transferred for storage on another device.

In this activity, you will use a microphone and Microsoft Sound Recorder to capture an audio stream. Microsoft Sound Recorder is a Windows accessory that can be found in Windows XP at **Start > Programs > Accessories > Entertainment > Sound Recorder**. If a microphone and Microsoft Sound Recorder are not available, you can download an audio file to use in this activity from http://newsroom.cisco.com/dlls/podcasts/audio_feeds.html.

Scenario

This activity is to be performed on a computer that has a microphone and Microsoft Sound Recorder or Internet access so that an audio file can be downloaded.

Estimated completion time, depending on network speed, is 30 minutes.

Task 1: Create a Sound File

Step 1: Open the Windows Sound Recorder application.

The application can be found in Windows XP at **Start > Programs > Accessories > Entertainment > Sound Recorder**. The Sound Recorder interface is shown in Figure 1.

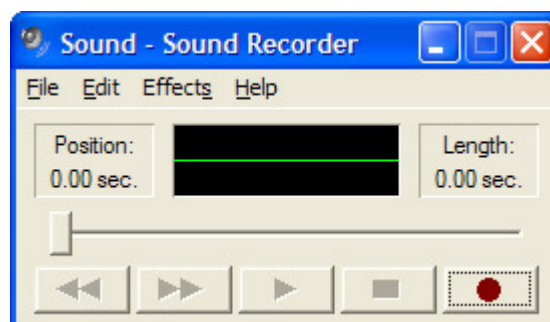


Figure 1. The Sound Recorder Interface

Step 2: Record an audio file.

1. To begin recording, click the Record button on the Sound Recorder interface.
2. Speak into the microphone, or create sounds that can be picked up by the microphone. As the audio is recorded, the waveform of the sound should appear on the Sound Recorder interface, as shown in Figure 2.



Figure 2. Recording in Progress

3. Click the Stop button when you are finished.

Step 3: Check the audio file that was recorded.

1. Press the Play button to listen to the recording. The recording that you have made should be played back, as shown in Figure 3.



Figure 3. Playback

If you are unable to hear the recording, check the configuration of the microphone, speakers, and volume settings, and attempt to create the recording again.

If you are unable to create a recording, download an audio file from News@Cisco at the following URL: http://newsroom.cisco.com/dlls/podcasts/audio_feeds.html

2. Save the audio file to the desktop and proceed to Task 2.

Step 4: Save the audio file.

1. Save the audio file that you have created to the desktop. Name the file **myaudio.wav**.
2. After the file is saved, close the Sound Recorder application.

Task 2: Observe the Properties of the Audio File

Step 1: View audio file properties.

Right-click the audio file that you saved to the desktop and click **Properties** from the popup menu.

What is the file size in kilobytes? _____

What is the file size in bytes? _____

What is the file size in bits? _____

Step 2: Open the audio file in Windows Media Player.

1. Right-click the audio file and select **Open With > Windows Media Player**.
2. When the file is open, right-click at the top of the Media Player interface and select **File > Properties** from the popup menu.

What is the length of the audio file in seconds? _____

Calculate the amount of data per second in the audio file and record the result. _____

Task 3: Reflection

Data files do not have to remain on the end devices where they are created. For example, you may want to copy the audio file that you created to another computer or a portable audio device.

If the audio file that you saved to the desktop were to be transferred at a rate of 100 megabits per second (Mbps), how long would it take for the file transfer to be completed?

Even with an Ethernet connection operating at 100 Mbps, the data that makes up a file is not transferred at this speed. All Ethernet frames contain other information, such as source and destination addresses, that is necessary for the delivery of the frame.

If 5% of the available 100 Mbps bandwidth is used up by the Ethernet overhead, and 95% of the bandwidth is left for the data payload, how long would it take for the file transfer to be completed?

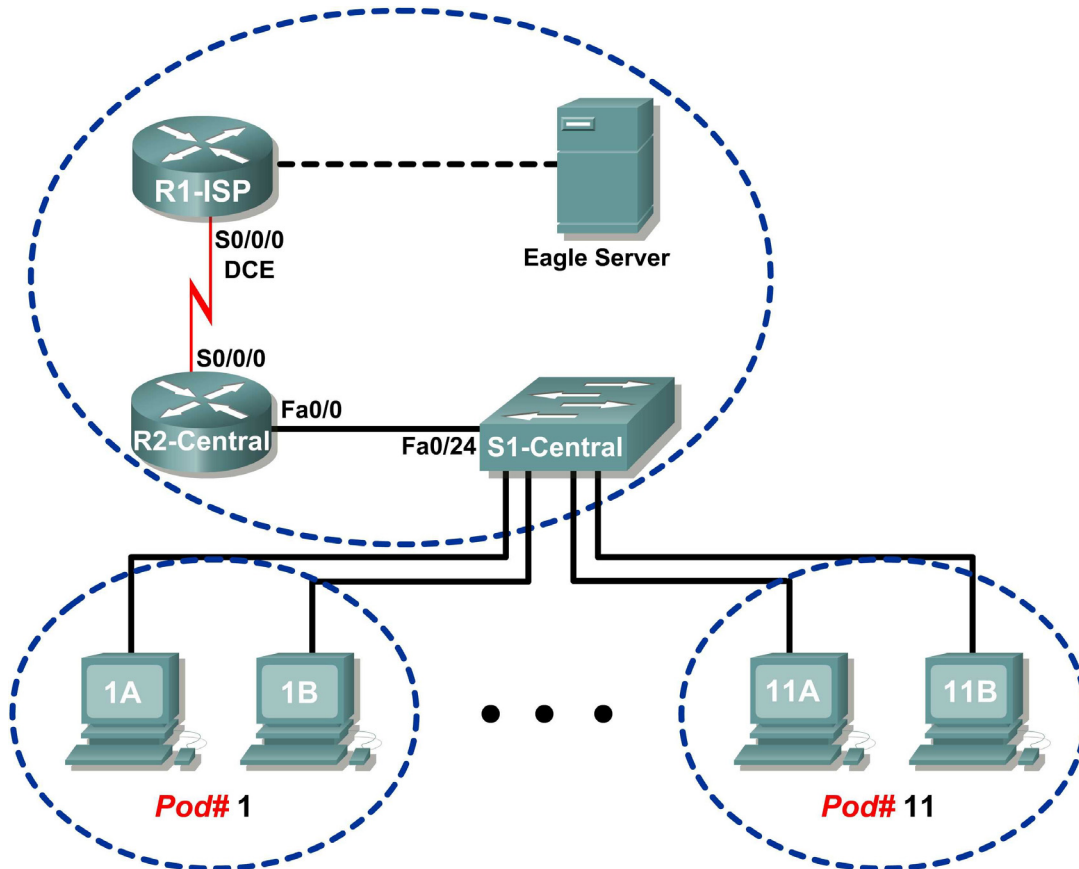
Task 4: Clean Up

You may be required to remove the audio file that you have saved from the computer. If so, delete the file from the desktop.

Unless instructed otherwise, turn off the computer.

Lab 3.4.2: Managing a Web Server

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/A
	Fa0/0	192.168.254.253	255.255.255.0	N/A
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	N/A
	Fa0/0	172.16.255.254	255.255.0.0	N/A
Eagle Server	N/A	192.168.254.254	255.255.255.0	192.168.254.253
	N/A	172.31.24.254	255.255.255.0	N/A
hostPod#A	N/A	172.16. Pod#.1	255.255.0.0	172.16.255.254
hostPod#B	N/A	172.16. Pod#.2	255.255.0.0	172.16.255.254
S1-Central	N/A	172.16.254.1	255.255.0.0	172.16.255.254

Learning Objectives

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

- Download, install, and verify a web server application
- Verify the default web server configuration file
- Capture and analyze HTTP traffic with Wireshark

Background

Web servers are an important part of the business plan for any organization with a presence on the Internet. Web browsers are used by consumers to access business web sites. However, web browsers are only half of the communication channel. The other half of the communication channel is web server support. Web server support is a valuable skill for network administrators. Based on a survey by Netcraft in January, 2007, the following table shows the top three web server applications by percent of use:

Web Server	Percent of use
Apache	60 %
Microsoft	31 %
Sun	1.6 %

Scenario

In this lab you will download, install, and configure the popular Apache web server. A web browser will be used to connect to the server, and Wireshark will be used to capture the communication. Analysis of the capture will help you understand how the HTTP protocol operates.

Task 1: Download, Install, and Verify the Apache Web Server.

The lab should be configured as shown in the Topology Diagram and logical address table. If it is not, ask the instructor for assistance before proceeding.

Step 1: Download the software from Eagle Server.

The Apache web server application is available for download from Eagle Server.

1. Use a web browser and URL ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter3 to access and download the software. See Figure 1.



Figure 1. FTP Download Screen for the Apache Web Server

2. Right-click the file and save the software on the pod host computer.

Step 2: Install the Apache web server on the pod host computer.

1. Open the folder where the software was saved, and double-click the Apache file to begin installation. Choose default values and consent to the licensing agreement. The next installation step requires customized configuration of the web server, shown in Figure 2.

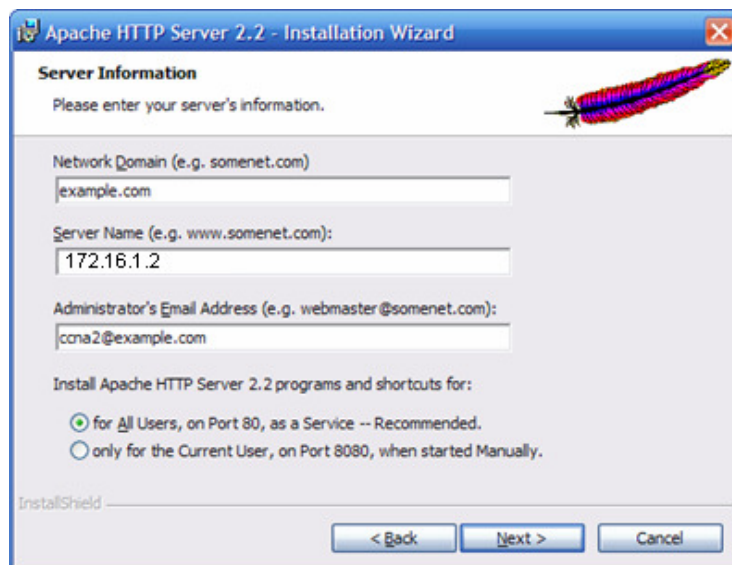


Figure 2. Customized Configuration Screen

Use the following values:

Information	Value
Network Domain	example.com
Server Name	IP address of computer
Administrator's E-mail Address	ccna*@example.com

* For example, for users 1 through 22, if the computer is on Pod 5, Host B, the administrator's e-mail number is ccna10@example.com

2. Accept the recommended port and service status. Click **Next**.
3. Accept the default typical installation, and click **Next**.

What is the default installation folder?

4. Accept the default installation folder, click **Next**, and then **Install**. When the installation has finished, close the screen.

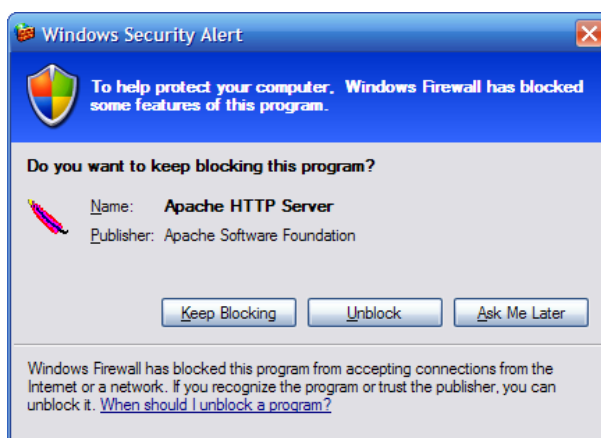


Figure 3. Windows Security Alert

Note: If a Windows Security Alert is displayed, select unblock. See Figure 3. This will permit connections to the web server.

Step 3: Verify the web server.

The **netstat** command will display protocol statistics and connection information for this lab computer.


1. Choose **Start > Run** and open a command line window. Type **cmd**, and then click **OK**. Use the **netstat -a** command to discover open and connected ports on your computer:

```
C:\>netstat -a
Active Connections
```

Proto	Local Address	Foreign Address	State
TCP	GW-desktop-hom:http	GW-desktop-hom:0	LISTENING
TCP	GW-desktop-hom:epmap	GW-desktop-hom:0	LISTENING
TCP	GW-desktop-hom:microsoft-ds	GW-desktop-hom:0	LISTENING
TCP	GW-desktop-hom:3389	GW-desktop-hom:0	LISTENING

<output omitted>
C:\>

2. Using the command **netstat -a**, verify that the web server is operating properly on the pod host computer.

The Apache web server monitor icon  should be visible on the lower right side of the screen, close to the time.

3. Open a web browser, and connect to the URL of your computer. A web page similar to Figure 4 will be displayed if the web server is working properly.

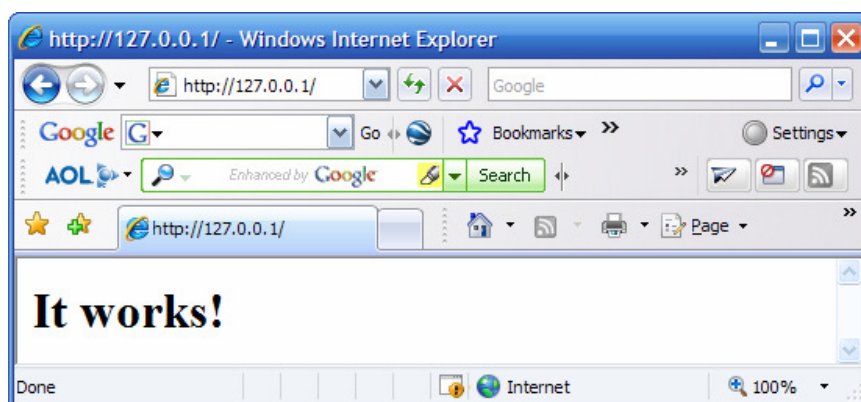


Figure 4. Web Server Default Page

The 127.0.0.0 / 8 network address is reserved and is used for local IP addresses. The same page should be displayed if the URL is changed to the IP address on the Ethernet interface or to any host IP address in the 127.0.0.0 / 8 network range.

4. Test the web server on several different IP addresses from the 127.0.0.0 / 8 network range. Fill in the following table with the results:

IP Address	Status	Explanation
127.0.0.1		
127.255.255.254		
127.255.255.255		
127.0.0.0		

Task 2: Verify the Default Web Server Configuration File.

Step 1: Access the `httpd.conf` file.

A system administrator may find the need to verify or modify the default configuration file.

Open the Apache web server configuration file, `C:\Program Files\Apache Software Foundation\Apache2.2\conf\httpd.conf`. See Figure 5.

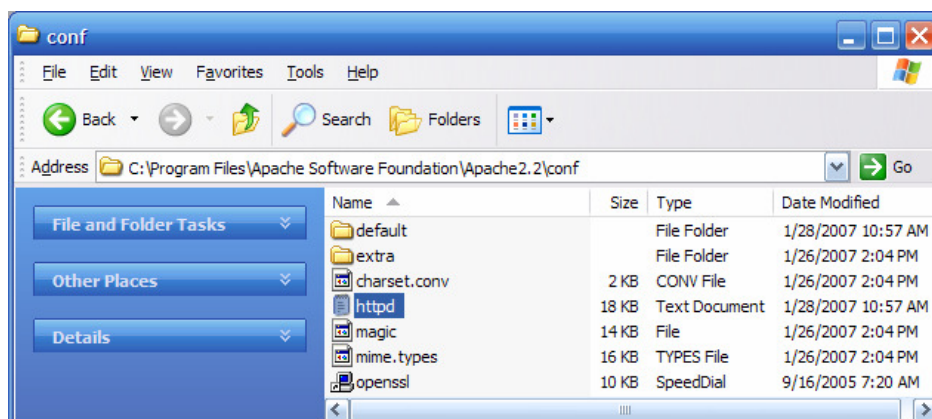


Figure 5. Apache Web Server Configuration File

Step 2: Review the `httpd.conf` file.

Numerous configuration parameters allow the Apache web server to be fully customizable. The “#” character indicates a comment for system administrators, exempt from access by the web server. Scroll down the configuration file, and verify the following settings:

Value	Meaning
<code>#Listen 12.34.56.78:80</code> <code>Listen 80</code>	Listen on TCP port 80 for all incoming connections. To accept connections from only this host, change the line to <code>Listen 127.0.0.1 80</code> .
<code>ServerAdmin ccna2@example.com</code>	If there are problems, e-mail the web server at this e-mail address.
<code>ServerName 172.16.1.2:80</code>	For servers without DNS names, use the IP address:port number.
<code>DocumentRoot "C:/Program Files/Apache Software Foundation/Apache2.2/htdocs"</code>	This is the root directory for the web server.
<code><IfModule dir_module></code> <code> DirectoryIndex index.html</code> <code></IfModule></code>	<code>DirectoryIndex</code> sets the file that Apache will serve if a directory is requested. If no page is requested from that directory, display <code>index.html</code> if it is present.

Step 3: Modify the web server default page.

Figure 4 shows the default web page from file `index.html`. Although this page is sufficient for testing, something more personal should be displayed.

1. Open folder `C:\Program Files\Apache Software Foundation\Apache2.2\htdocs`. The file `index.html` should be present. Right-click the file, and choose **Open With**. From the pull-down list, choose **notepad**. Change the file content to something similar to the following example:

```
<html><body><h1>Welcome to the Pod1HostB Web Server!!!</h1>
<center><b>
Operated by me!
</center></b>
Contact web administrator: ccna2@example.com
</body></html>
```

2. Save the file, and refresh the web browser. Or, open URL <http://127.0.0.1>. The new default page should be displayed. As changes to `index.html` are made and saved, simply refresh the web browser to view the new content.

Task 3: Capture and Analyze HTTP Traffic with Wireshark.

Wireshark will not capture packets sent from or to the 127.0.0.0 network on a Windows computer. The interface will not display. To complete this task, connect to either a student's computer or Eagle Server and analyze the data exchange.

Step 1: Analyze HTTP traffic.

1. Start Wireshark, and set the capture interface to the interface bound to the 172.16 network. Open a web browser, and connect to another computer with an active web server.

Why does `index.html` *not* have to be entered in the URL for the file contents to be displayed?

2. Deliberately enter a web page that is not on the web server, as shown in Figure 6. Note that an error message is displayed in the web browser.



Figure 6. 404 Not Found Error

Figure 7 contains a captured HTTP session. File index.htm was requested from the web server, but the server did not have the file. Instead, the server sent a **404** error. The web browser simply displayed the server response “The page cannot be found”.

No. -	Time	Source	Destination	Protocol	Info
20	14.384747	172.16.1.2	172.16.1.1	TCP	1149 > http [SYN] Seq=0 Len=0 MSS=1460
21	14.384993	172.16.1.1	172.16.1.2	TCP	http > 1149 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460
22	14.385030	172.16.1.2	172.16.1.1	TCP	1149 > http [ACK] Seq=1 Ack=1 win=64240 Len=0
23	14.388292	172.16.1.2	172.16.1.1	HTTP	GET /index.htm HTTP/1.1
24	14.389299	172.16.1.1	172.16.1.2	HTTP	HTTP/1.1 404 Not Found (text/html)
25	14.541723	172.16.1.2	172.16.1.1	TCP	1149 > http [ACK] Seq=256 Ack=423 win=63818 Len=0

Figure 7. Wireshark Capture of HTTP Traffic

3. Highlight the capture line with the 404 error, and move into the second (middle) Wireshark window. Expand the line-based text-data record.

What are the contents?

Task 4: Challenge

Modify the default web server configuration file `httpd.conf` and change the `Listen 80` line to `Listen 8080`. Open a web browser and access URL <http://127.0.0.1:8080>. Verify with the `netstat` command that the new web server TCP port is 8080.

Task 5: Reflection

Web servers are an important component of e-commerce. Depending on the organization, the network or web administrator has the responsibility of maintaining the corporate web server. This lab demonstrated how to install and configure the Apache web server, test for proper operation, and identify several key configuration parameters.

The student modified the default web page `index.html` and observed the effect on the web browser output.

Finally, Wireshark was used to capture an HTTP session of a file not found. The web server responded with an HTTP 1.1 error 404 and returned a file not found message to the web browser.

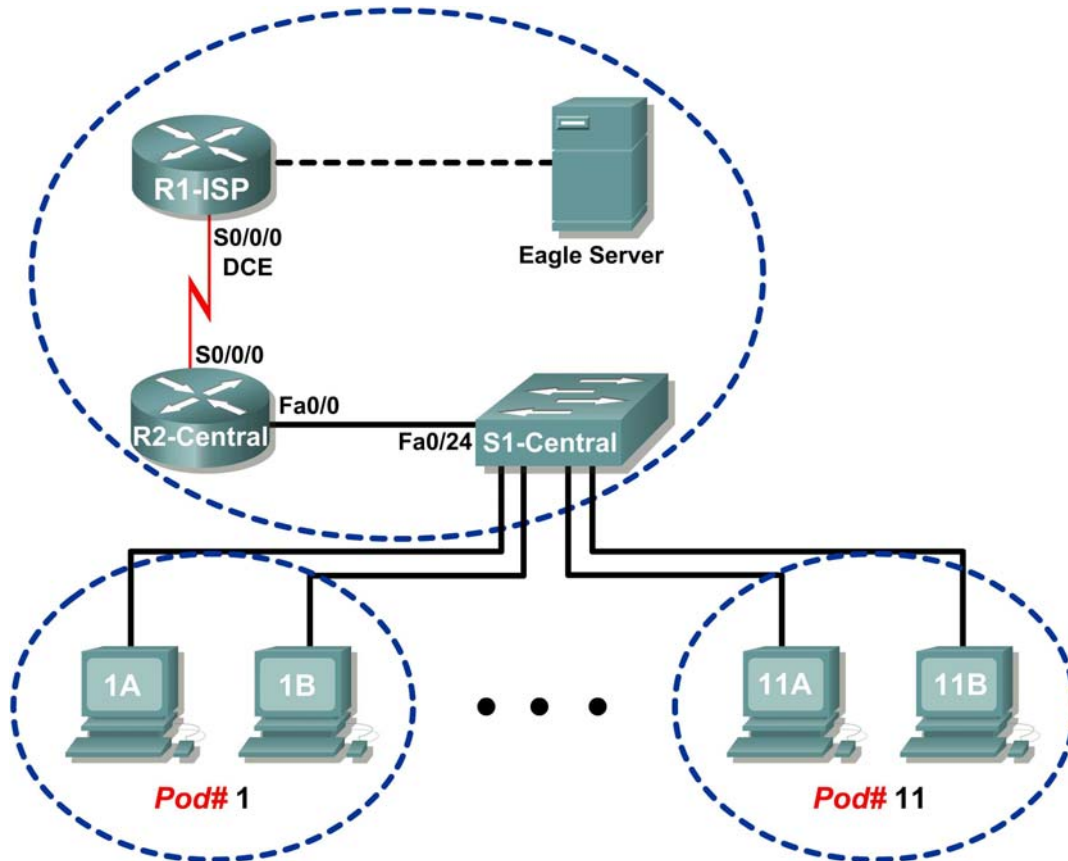
Task 6: Clean Up

During this lab the Apache web server was installed on the pod host computer. It should be uninstalled. To uninstall the web server, click **Start > Control Panel > Add or Remove Programs**. Click **Apache Web Server**, and then click **Remove**.

Unless directed otherwise by the instructor, turn off power to the host computers. Remove anything that was brought into the lab, and leave the room ready for the next class.

Lab 3.4.3: E-mail Services and Protocols

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/A
	Fa0/0	192.168.254.253	255.255.255.0	N/A
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	10.10.10.6
	Fa0/0	172.16.255.254	255.255.0.0	N/A
Eagle Server	N/A	192.168.254.254	255.255.255.0	192.168.254.253
	N/A	172.31.24.254	255.255.255.0	N/A
hostPod#A	N/A	172.16. Pod#.1	255.255.0.0	172.16.255.254
hostPod#B	N/A	172.16. Pod#.2	255.255.0.0	172.16.255.254
S1-Central	N/A	172.16.254.1	255.255.0.0	172.16.255.254

Learning Objectives

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

- Configure the pod host computer for e-mail service
- Capture and analyze e-mail communication between the pod host computer and a mail server

Background

E-mail is one of the most popular network services that uses a client/server model. The e-mail client is configured on a user's computer, and configured to connect to an e-mail server. Most Internet service providers (ISPs) provide step-by-step instructions for using e-mail services; consequently, the typical user may be unaware of the complexities of e-mail or the protocols used.

In network environments where the MUA client must connect to an e-mail server on another network to send and receive e-mail, the following two protocols are used:

- Simple Mail Transfer Protocol (SMTP) was originally defined in RFC 821, August, 1982, and has undergone many modifications and enhancements. RFC 2821, April, 2001, consolidates and updates previous e-mail -related RFCs. The SMTP server listens on well-known TCP port 25. SMTP is used to send e-mail messages from the external e-mail client to the e-mail server, deliver e-mail to local accounts, and relay e-mail between SMTP servers.
- Post Office Protocol version 3 (POPv3) — is used when an external e-mail client wishes to receive e-mail messages from the e-mail server. POPv3 servers listen on well-known TCP port 110.
- **Internet Message Access Protocol (IMAP)**—An Internet protocol that allows a central server to provide remote access to e-mail messages. IMAP servers listen on well-known TCP port 143.

In this lab, you will use IMAP instead of POP for e-mail delivery to the client.

Earlier versions of both protocols should not be used. Also, there are secure versions of both protocols that employ secure socket layers/Transport layer security (SSL/TSL) for communication.

E-mail is subject to multiple computer security vulnerabilities. Spam attacks flood networks with useless, unsolicited e-mail, consuming bandwidth and network resources. E-mail servers have had numerous vulnerabilities, which left the computer open to compromise.

Scenario

In this lab, you will configure and use an e-mail client application to connect to eagle-server network services. You will monitor the communication with Wireshark and analyze the captured packets.

An e-mail client such as Outlook Express or Mozilla Thunderbird will be used to connect to the eagle-server network service. Eagle-server has SMTP mail services preconfigured, with user accounts capable of sending and receiving external e-mail messages.

Task 1: Configure the Pod Host Computer for E-mail Service.

The lab should be configured as shown in the Topology Diagram and logical address table. If it is not, ask the instructor for assistance before proceeding.

Step 1: Download and install Mozilla Thunderbird.

If Thunderbird is not installed on the pod host computer, it can be downloaded from eagle-server.example.com. See Figure 1. The download URL is ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter3/.

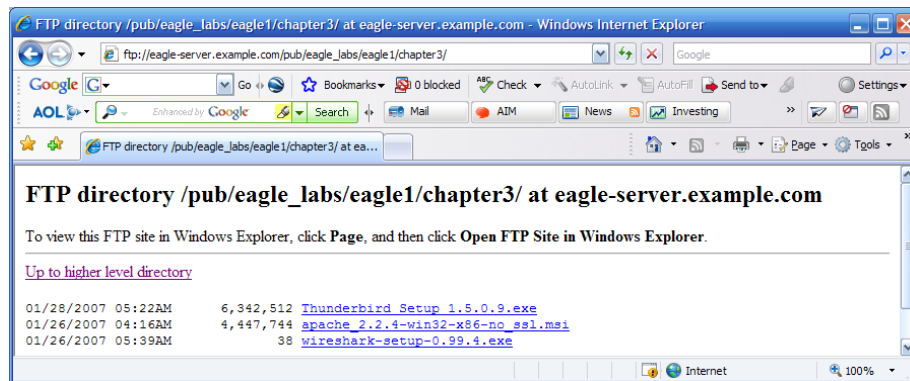


Figure 1. FTP Download for Wireshark

1. Double click the Thunderbird filename, and then select Save to save the file to the host pod computer.

Note: Depending on the connection speed of the link between the two routers and the number of students downloading the file, this download may be slow.

2. When the file has downloaded, double-click the filename, accept the software license, and install Thunderbird with the default settings.
3. When installation is complete, start Thunderbird.

Step 2: Configure Thunderbird to receive and send e-mail messages.

1. If prompted for Import Options, select “Don’t import anything” and select Next
2. When Thunderbird starts, e-mail account settings must be configured. In the New Account Setup, select “**Email account**” and select **Next**.
3. As prompted, fill in the Account information as follows:

Field	Value
Account Name	The account name is based on the pod and host computer. There are a total of 22 accounts configured on Eagle Server, labeled ccna[1..22]. If this pod host is on Pod1, Host A, then the account name is ccna1. If the pod host is on Pod 3, Host B, then the account name is ccna6. And so on.
Your Name	Use the same name as above.
E-mail address	Your_name@example.com
Type of incoming server you are using	IMAP
Incoming Server (IMAP)	Eagle-server.example.com
Outgoing Server (SMTP)	Eagle-server.example.com
Incoming User Name	Use the same name as above.
Account Name	Your_name@eagle-server.example.com

4. When Thunderbird starts, you may be prompted for a password for your email account. At this screen select **"Cancel"**

The Thunderbird client needs to have SMTP server login disabled. To do this, select **Tools > Account Settings>Outgoing Server (SMTP)**. Then from the Outgoing server screen, select **Edit**. See figure 2.

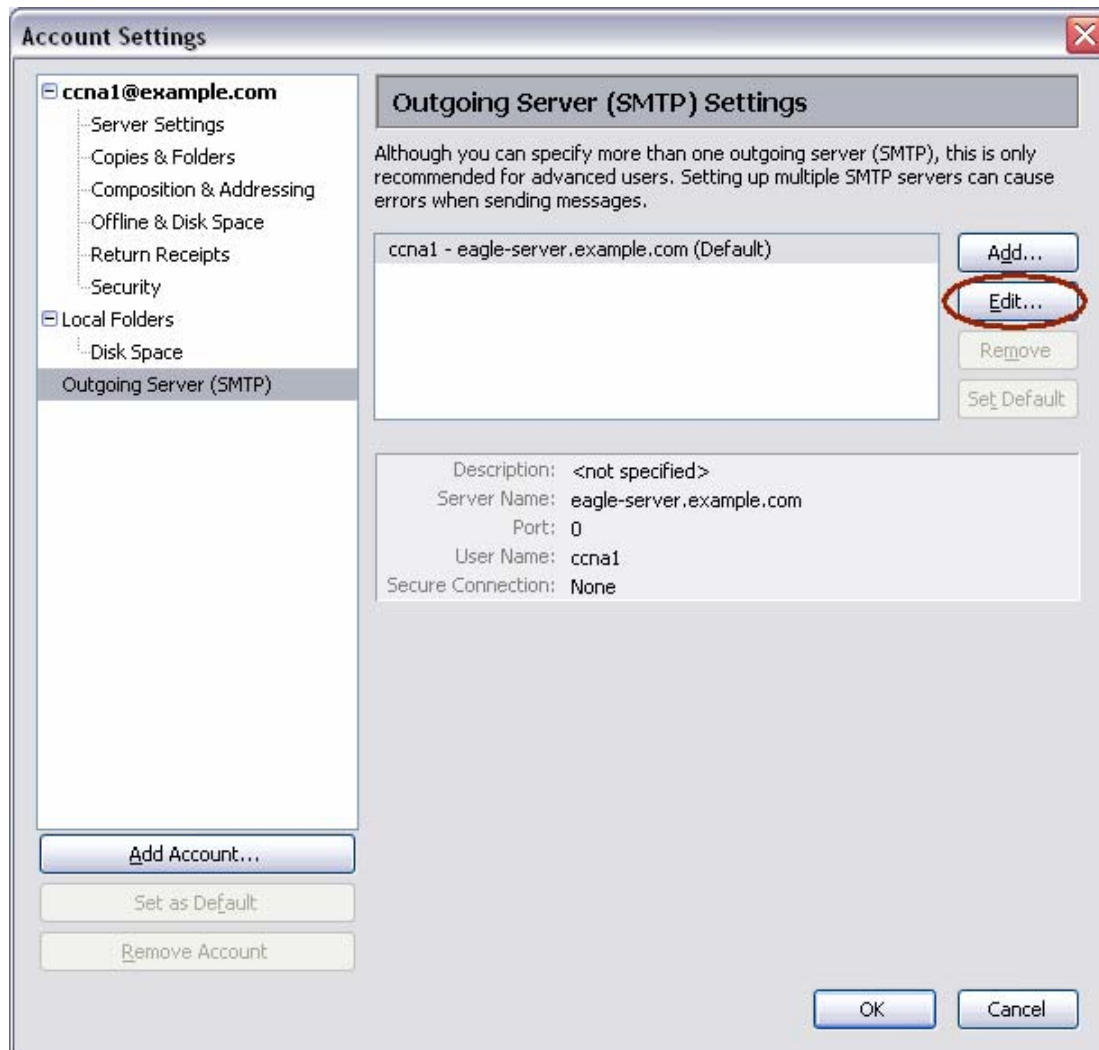


Figure 2. Thunderbird SMTP server settings

At the SMTP Server screen, uncheck the **"Use name and password"** box and select **OK** at the two screens. See Figure 3.

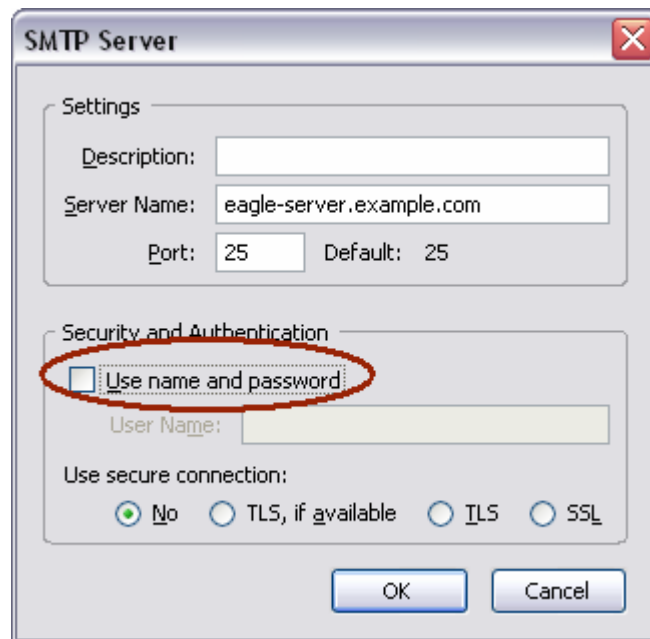


Figure 3. SMTP server edit

5. You may also want to verify account settings from **Tools > Account Settings**. See Figure 4.

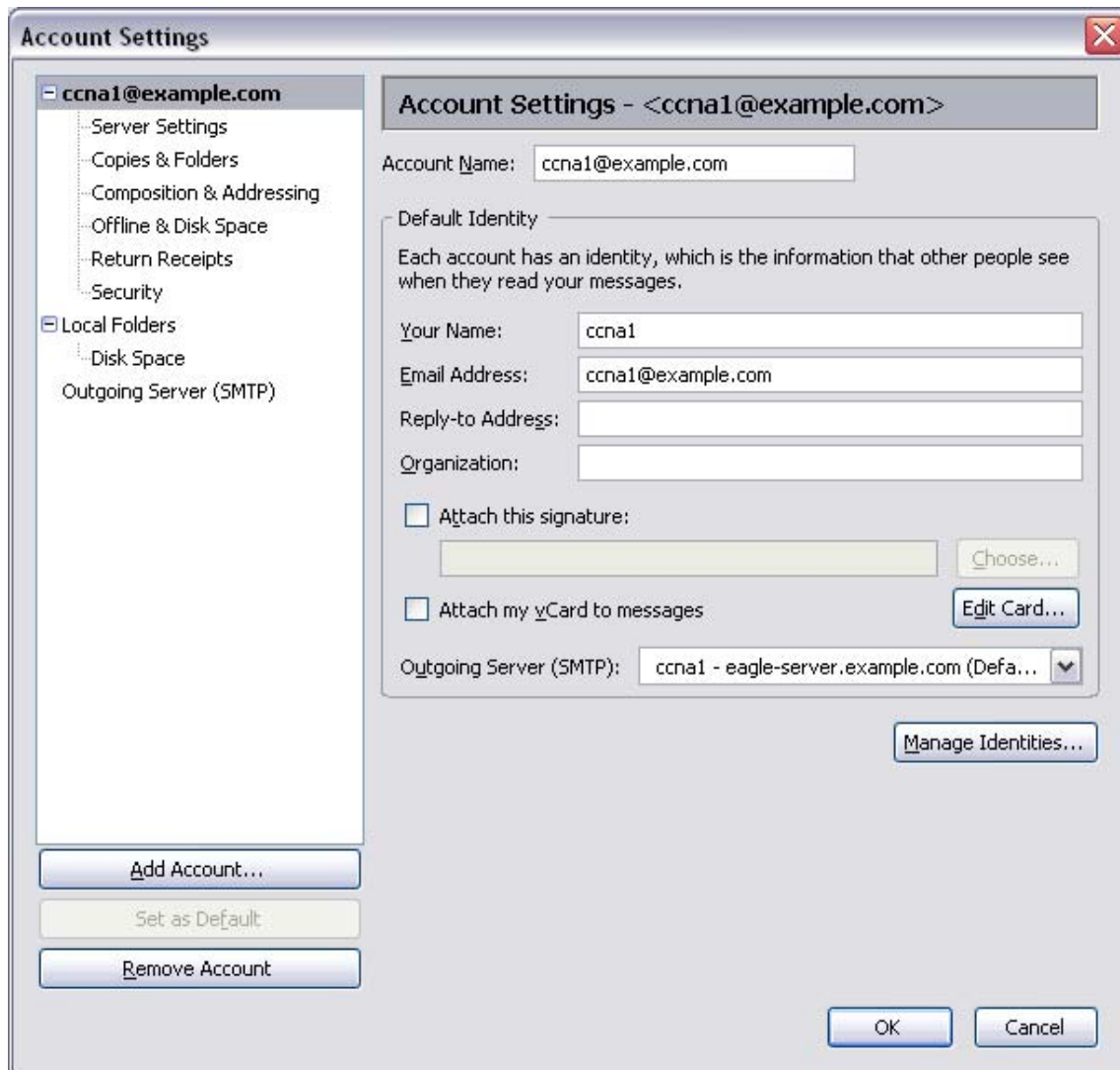


Figure 4. Thunderbird Account Settings

6. In the left pane of the Account Settings screen, click **Server Settings**. A screen similar to the one shown in Figure 5 will be displayed.

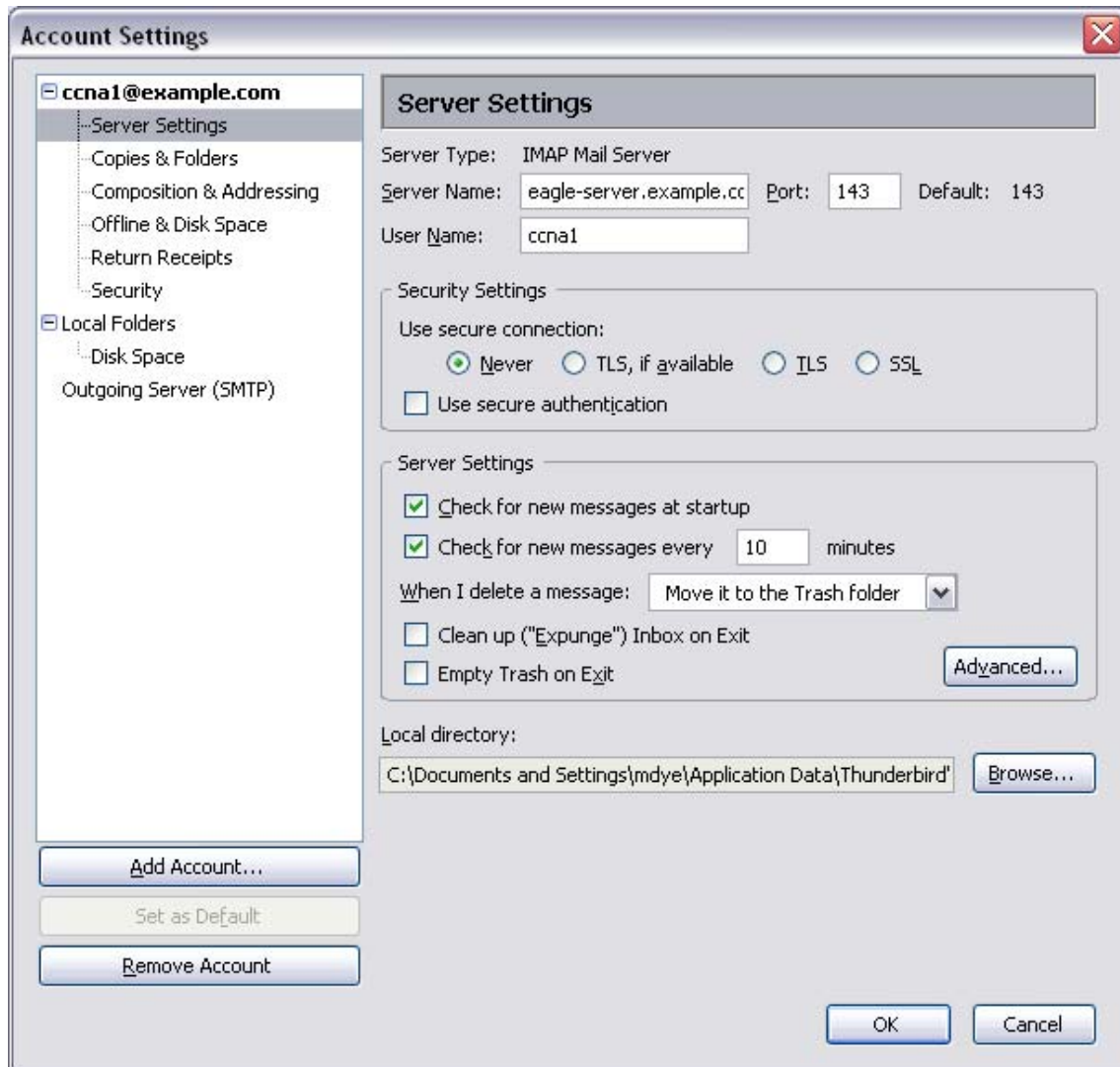


Figure 5. Thunderbird Server Settings Screen

What is the purpose of the SMTP protocol, and what is the well-known TCP port number?

Task 2: Capture and Analyze E-mail Communication between the Pod Host Computer and an E-mail Server.

Step 1: Send an e-mail.

1. Ask another student in the class for his or her e-mail name.
2. To create and send an email, select the "Write" icon. Using this name, each of you should compose and send an e-mail message to each other.
3. When the emails have been sent, check your email. In order to check your email, you must be logged in. If you have not previously logged in, enter **cisco** as the password. Please note that this is the default password which is embedded within the Eagle server.

Step 2: Start Wireshark captures.

When you are certain that the e-mail operation is working properly for both sending and receiving, start a Wireshark capture. Wireshark will display captures based on packet type.

Step 3: Analyze a Wireshark capture session of SMTP.

1. Using the e-mail client, again send and receive e-mail to a classmate. This time, however, the e-mail transactions will be captured.
2. After sending and receiving one e-mail message, stop the Wireshark capture. A partial Wireshark capture of an outgoing e-mail message using SMTP is shown in Figure 6.

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.1	172.16.255.255	NBNS	Name query NB WORKGROUP<1b>
2	0.741371	172.16.1.1	172.16.255.255	NBNS	Name query NB WORKGROUP<1b>
3	1.492443	172.16.1.1	172.16.255.255	NBNS	Name query NB WORKGROUP<1b>
4	3.306445	172.16.1.1	192.168.254.254	TCP	1250 > smtp [SYN] Seq=0 Len=0 MSS=1460
5	3.306968	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
6	3.307012	172.16.1.1	192.168.254.254	TCP	1250 > smtp [ACK] Seq=1 Ack=1 Win=64240 Len=0
7	3.313519	192.168.254.254	172.16.1.1	SMTP	Response: 220 localhost.localdomain ESMTP Sendmail 8.13.1/8.13
8	3.353004	172.16.1.1	192.168.254.254	SMTP	Command: EHLO [172.16.1.1]
9	3.353436	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [ACK] Seq=90 Ack=20 Win=5840 Len=0
10	3.353657	192.168.254.254	172.16.1.1	SMTP	Response: 250-localhost.localdomain Hello host-1.example.com [172.16.1.1]
11	3.356823	172.16.1.1	192.168.254.254	SMTP	Command: MAIL FROM:<ccna1@example.com> SIZE=398
12	3.359743	192.168.254.254	172.16.1.1	SMTP	Response: 250 2.1.0 <ccna1@example.com>... Sender ok
13	3.363127	172.16.1.1	192.168.254.254	SMTP	Command: RCPT TO:<ccna2@example.com>
14	3.365007	192.168.254.254	172.16.1.1	SMTP	Response: 250 2.1.5 <ccna2@example.com>... Recipient ok
15	3.367680	172.16.1.1	192.168.254.254	SMTP	Command: DATA
16	3.368230	192.168.254.254	172.16.1.1	SMTP	Response: 354 Enter mail, end with "." on a line by itself
17	3.376881	172.16.1.1	192.168.254.254	SMTP	Message Body
18	3.387830	192.168.254.254	172.16.1.1	SMTP	Response: 250 2.0.0 l0S8dIOY005299 Message accepted for delivery
19	3.395347	172.16.1.1	192.168.254.254	SMTP	Message Body
20	3.395855	192.168.254.254	172.16.1.1	SMTP	Response: 221 2.0.0 localhost.localdomain closing connection
21	3.395897	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [FIN, ACK] Seq=564 Ack=502 Win=6432 Len=0
22	3.395929	172.16.1.1	192.168.254.254	TCP	1250 > smtp [ACK] Seq=502 Ack=565 Win=63677 Len=0
23	3.405772	172.16.1.1	192.168.254.254	TCP	1250 > smtp [FIN, ACK] Seq=502 Ack=565 Win=63677 Len=0
24	3.406204	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [ACK] Seq=565 Ack=503 Win=6432 Len=0

Figure 6. SMTP Capture

3. Highlight the first SMTP capture in the top Wireshark window. In Figure 6, this is line number 7.
4. In the second Wireshark window, expand the Simple Mail Transfer Protocol record.

There are many different types of SMTP servers. Malicious attackers can gain valuable knowledge simply by learning the SMTP server type and version.

What is the SMTP server name and version?

E-mail client applications send commands to e-mail servers, and e-mail servers send responses. In every first SMTP exchange, the e-mail client sends the command **EHLO**. The syntax may vary between clients, however, and the command may also be **HELO** or **HELLO**. The e-mail server must respond to the command.

What is the SMTP server response to the EHLO command?

The next exchanges between the e-mail client and server contain e-mail information. Using your Wireshark capture, fill in the e-mail server responses to the e-mail client commands:

E-mail Client	E-mail Server
MAIL FROM: ,ccna1@example.com>	
RCPT TO: <ccna2@example.com>	
DATA	
(message body is sent)	

What are the contents of the last message body from the e-mail client?

How does the e-mail server respond?

Task 3: Challenge

Access a computer that has Internet access. Look up the SMTP server name and version for known weaknesses or compromises. Are there any newer versions available?

Task 4: Reflection

E-mail is probably the most common network service used. Understanding the flow of traffic with the SMTP protocol will help you understand how the protocol manages the client/server data connection. E-mail can also experience configuration issues. Is the problem with the e-mail client or e-mail server? One simple way to test SMTP server operation is to use the Windows command line Telnet utility to telnet into the SMTP server.

1. To test SMTP operation, open the Windows command line window and begin a Telnet session with the SMTP server.

```
C:\>telnet eagle-server.example.com 25
220 localhost.localdomain ESMTP Sendmail 8.13.1/8.13.1; Sun, 28 Jan
2007 20:41:0
3 +1000
HELO eagle-server.example.com
250 localhost.localdomain Hello [172.16.1.2], pleased to meet you
MAIL From: ccna2@example.com
250 2.1.0 ccna2@example.com... Sender ok
RCPT To: instructor@example.com
250 2.1.5 instructor@example.com... Recipient ok
DATA
354 Please start mail input.
e-mail SMTP server test...
.
250 Mail queued for delivery.
QUIT
221 Closing connection. Good bye.
Connection to host lost.
C:\ >
```

Task 5: Clean Up

If Thunderbird was installed on the pod host computer for this lab, the instructor may want the application removed. To remove Thunderbird, click **Start > Control Panel > Add or Remove Programs**. Scroll to and click **Thunderbird**, and then click **Remove**.

Unless directed otherwise by the instructor, turn off power to the host computers. Remove anything that was brought into the lab, and leave the room ready for the next class.