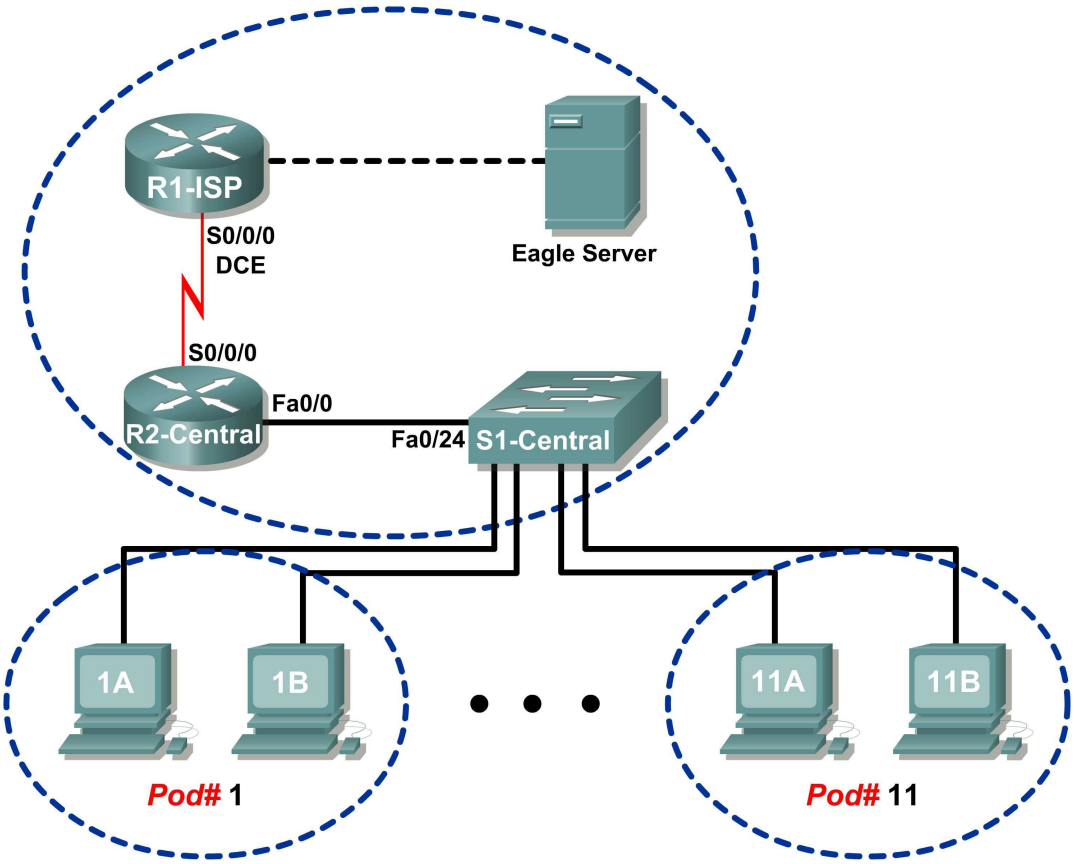
Lab 3.4.3: E-mail Services and Protocols

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
host*Pod#***A**	N/A	172.16. *Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#***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. The POPv3 server listens on well-known TCP port 110 .

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.

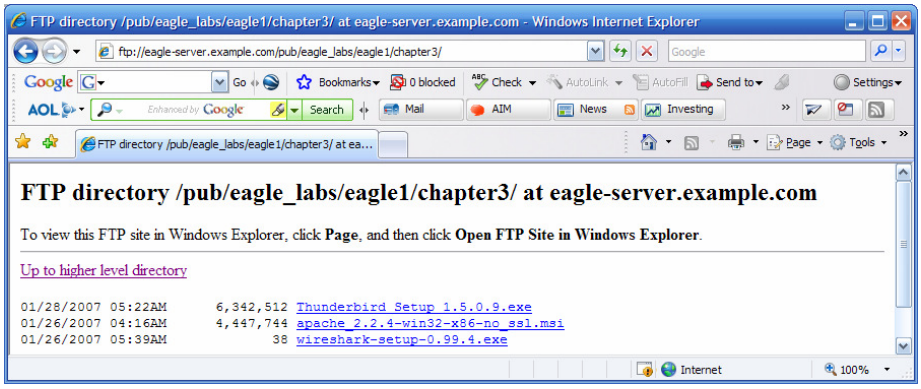


Figure 1. FTP Download for Wireshark

1. Right-click the Thunderbird filename, and then save the file to the host pod computer.
2. When the file has downloaded, double-click the filename and install Thunderbird with the default settings.
3. When finished, start Thunderbird.

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

1. When Thunderbird starts, e-mail account settings must be configured. 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`*`@eagle-server.example.com`
Type of incoming server you are using	`POP`
Incoming Server (SMTP)	`eagle-server.example.com`
Outgoing Server (SMTP)	`eagle-server.example.com`

2. Verify account settings from **Tools > Account Settings**. See Figure 2.

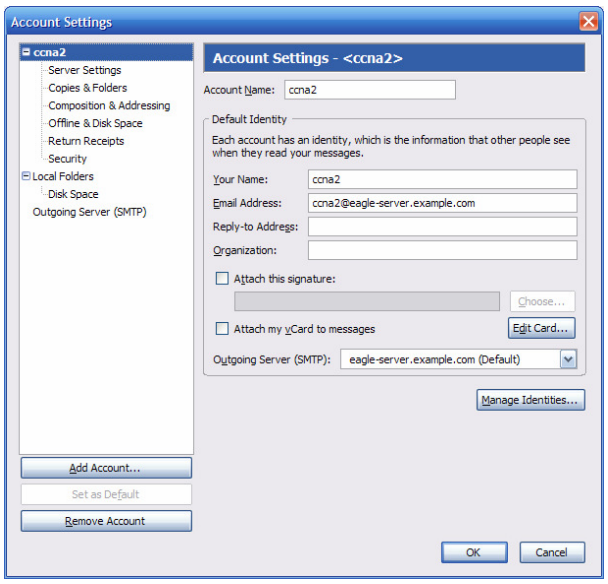


Figure 2. Thunderbird Account Settings

3. In the left pane of the Account Settings screen, click **Server Settings**. A screen similar to the one shown in Figure 3 will displayed.

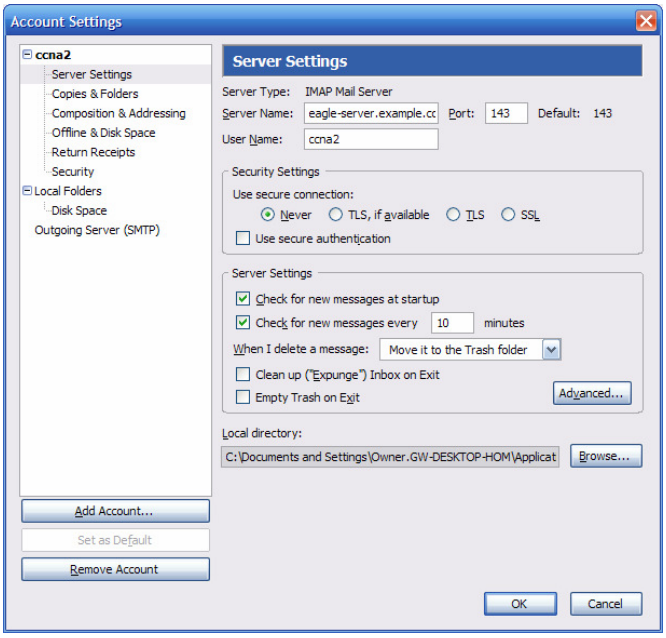


Figure 3. Thunderbird Server Settings Screen

Figure 4 shows the proper configuration for the Outgoing Server (SMTP).

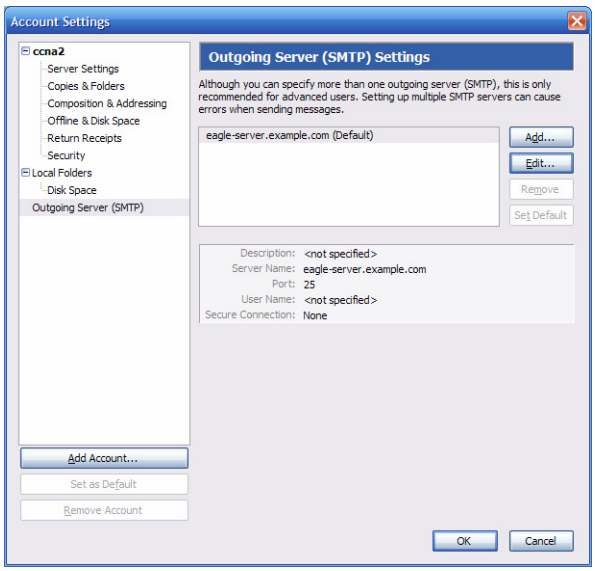


Figure 4. Outgoing Server (SMTP) Settings Screen

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 uncaptured e-mail.

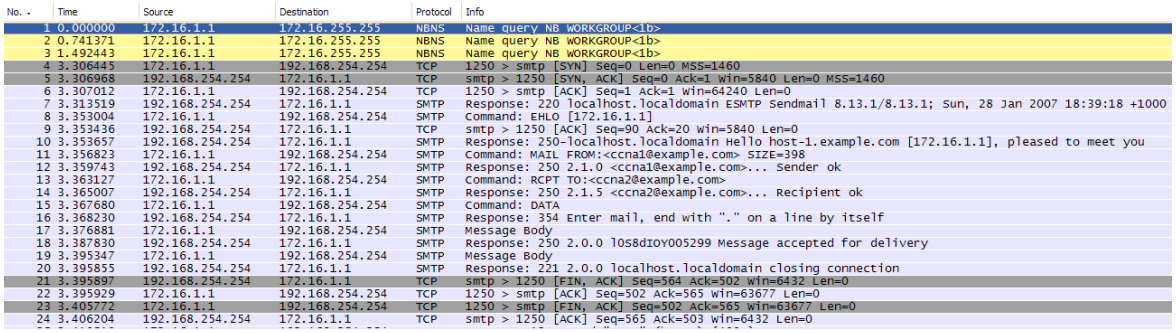
1. Ask another student in the class for his or her e-mail name.
2. Using this name, compose and send a friendly message to the student.

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 5.



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 8.13.1/8.13.1; Sun, 28 Jan 2007 18:39:18 +1000
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], pleased to meet you
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 5. SMTP Capture

3. Highlight the first SMTP capture in the top Wireshark window. In Figure 5, 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@excmaple.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.

