VANIER COLLEGE – Computer Engineering Technology – Autumn 2021

Network Systems Design (247-509-VA)

Leonardo Fusser (1946995)

LABORATORY EXPERIMENT 1

Email Services and Protocols

NOTE:

To be completed in one lab session of 3 hrs.

No **formal report** is required. Answer all questions, *attached necessary screen shots to show your work/result*, and include a discussion and conclusion session. To be submitted by the end of the lab session.

This exercise is to be done individually except where specified in the procedure. **Each** student must submit a lab results with original observations and conclusions.

OBJECTIVES:

After performing this experiment, the student will be able to:

1. Configure the host computer for email service
2. Capture and analyze email communication between the host computer and a mail server
3. Observe and perform simulation on operations of DNS and HTTP using packet tracer

THEORY

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, 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.

PROCEDURE
(Modified based on CCNA's labs)

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.

Part A: Install and setup Mozilla Thunderbird

1) The lab will be using the same Eagle-server Topology. If you have changed your computer, please modify your network IP address accordingly.

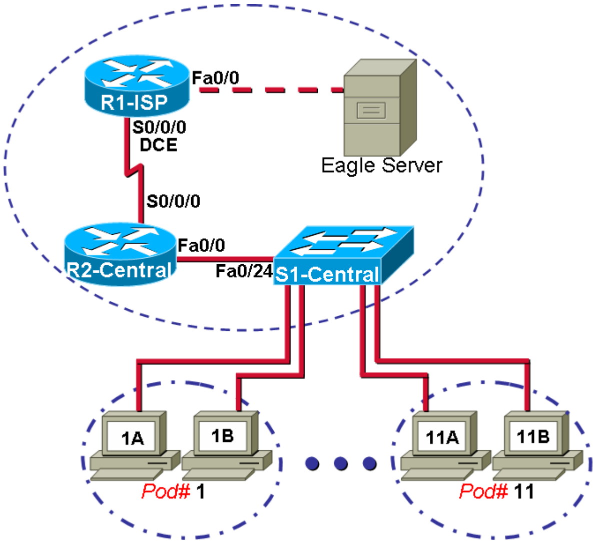


Figure 1 : ***Eagle Server Topology***

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

2) Download and install the latest Mozilla Thunderbird from internet using default settings. Note that the following procedure and screen shots are based on Thunderbird version 60.8.0.

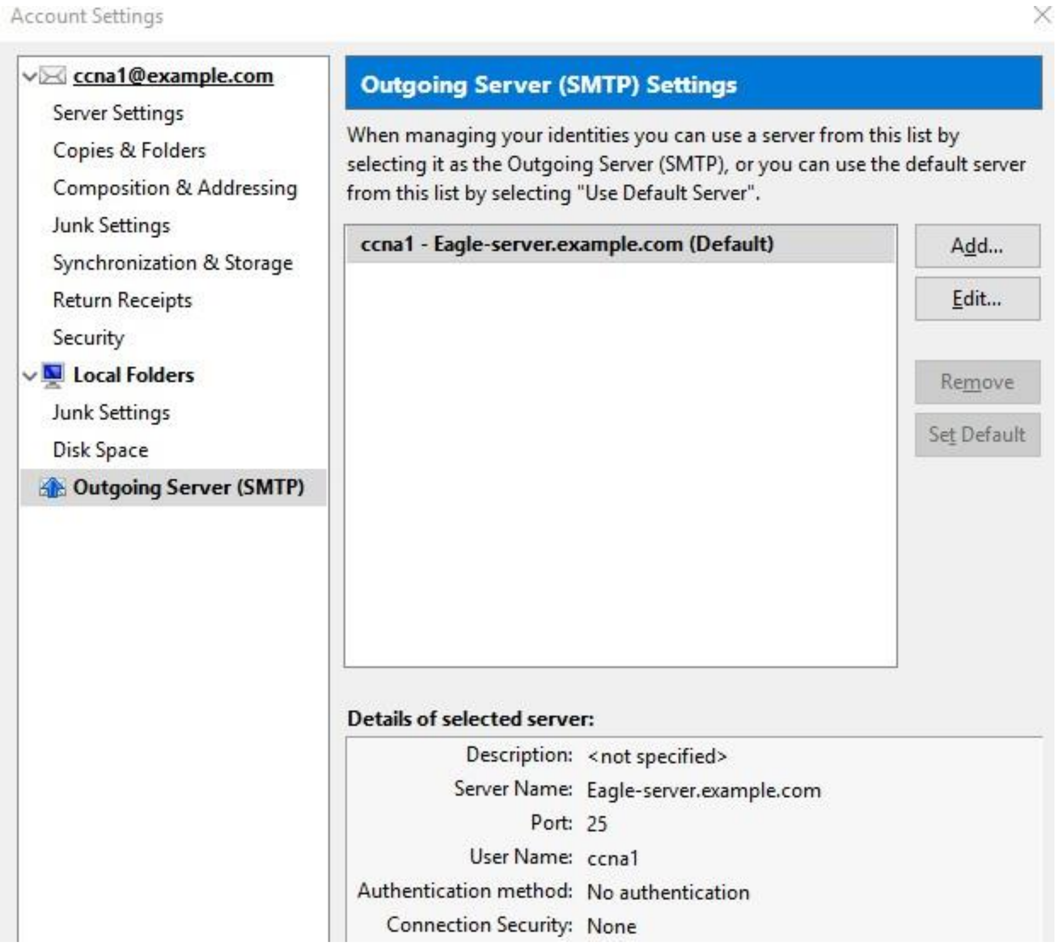
3) Set up an existing e-mail account using the following settings:

Field	Value
Your Name	*Your name* is based on the host computer. There are a total of 16 accounts configured on Eagle Server, labeled ccna[1..16]. If this host is on computer 1, then the account name is `ccna1`.
E-mail address	*`Your name@example.com`*

Do not setup any password, and uncheck "Remember password". Click "Continue", and "Done".

4) Your account should now appear at the left column of Thunderbird application. Left click on it, and select "Settings" to setup various servers.

   a) Click on **Outgoing Server (SMTP).** Setup your server as shown in Figure 2.



Outgoing Server (SMTP) Settings

When managing your identities you can use a server from this list by selecting it as the Outgoing Server (SMTP), or you can use the default server from this list by selecting "Use Default Server".

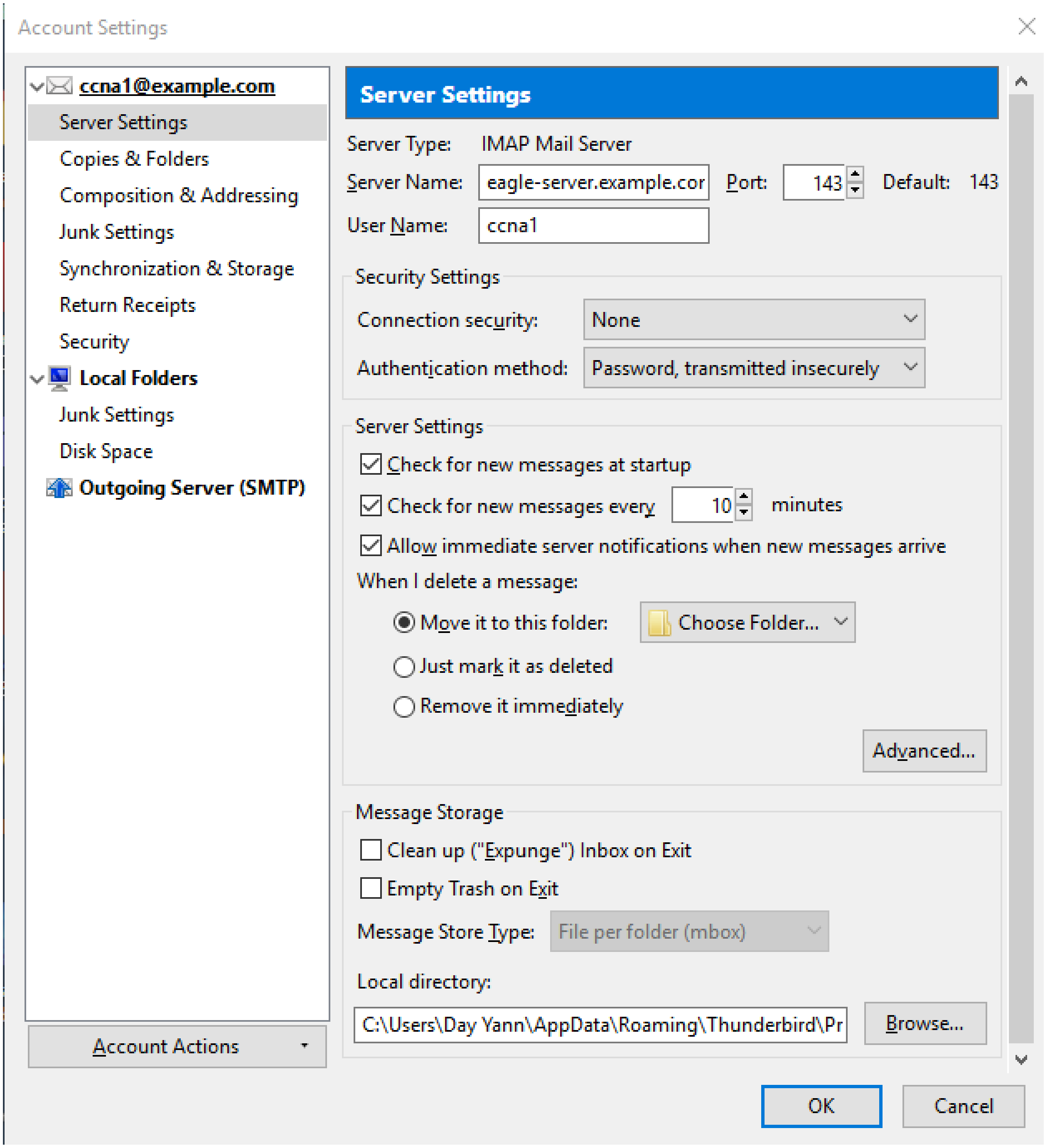
ccna1 - Eagle-server.example.com (Default)

Details of selected server:

Description:	<not specified>
Server Name:	Eagle-server.example.com
Port:	25
User Name:	ccna1
Authentication method:	No authentication
Connection Security:	None

Figure 2 : Thunderbird Outgoing Server Settings

   b) In the left pane of the Account Settings screen, click **Server Settings**. Setup the server accordingly as shown in Figure 3.



Server Settings

Server Type: IMAP Mail Server

Server Name: eagle-server.example.cor Port: 143 Default: 143

User Name: ccna1

Security Settings

Connection security: None

Authentication method: Password, transmitted insecurely

Server Settings

☑ Check for new messages at startup

☑ Check for new messages every 10 minutes

☑ Allow immediate server notifications when new messages arrive

When I delete a message:

● Move it to this folder: Choose Folder...

○ Just mark it as deleted

○ Remove it immediately

Message Storage

☐ Clean up ("Expunge") Inbox on Exit

☐ Empty Trash on Exit

Message Store Type: File per folder (mbox)

Local directory:

C:\Users\Day Yann\AppData\Roaming\Thunderbird\Pr

Figure 3 : Thunderbird server settings screen

c) Click on the Inbox. Enter "***cisco***" as password for eagle-server.example.com.

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

- SMTP stands for Simple Mail Transfer Protocol, and it's an application used by mail servers to send, receive, and/or relay outgoing mail between email senders and receivers. The well-known TCP port number for SMPT is port 25.

https://sendgrid.com/blog/what-is-an-smtp-server/

Part B: Capture and Analyze Email communication between the host computer and Email server

5) Send an email.

   a) Compose and send an email to each other.

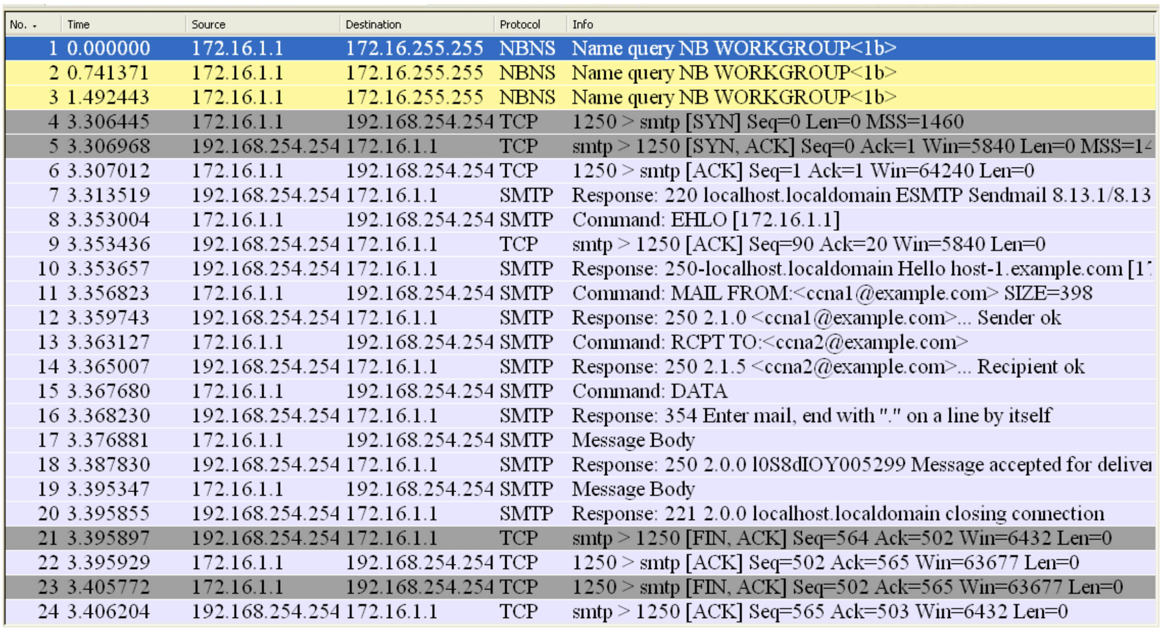
   b) When the emails have been sent, check your email. In order to check your email, you must be logged in. If you have not previously logged in, enter **cisco** as the password. Please note that this is the default password which is embedded within the Eagle server.

6) 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.

7) Analyze a Wireshark capture session of SMTP.

   a) Using the e-mail client, again send and receive e-mail to a classmate. This time, however, the e-mail transactions will be captured.

   b) 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 4.



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=1
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 [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 deliver
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

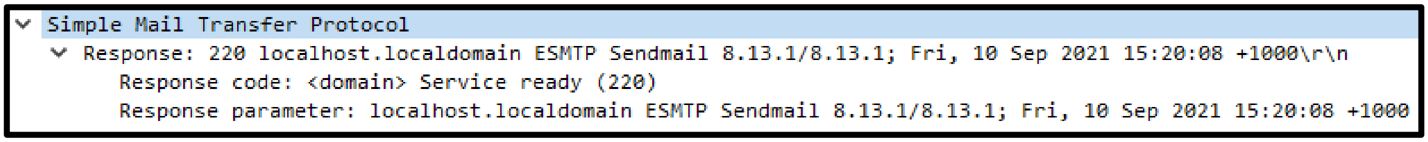
Figure 4 : SMTP Capture

   c) Highlight the first SMTP capture in the top Wireshark window.

d) 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?

- The SMTP server name is "localhost.localdomain" and the SMTP version is 8.13.1. See screenshot below.



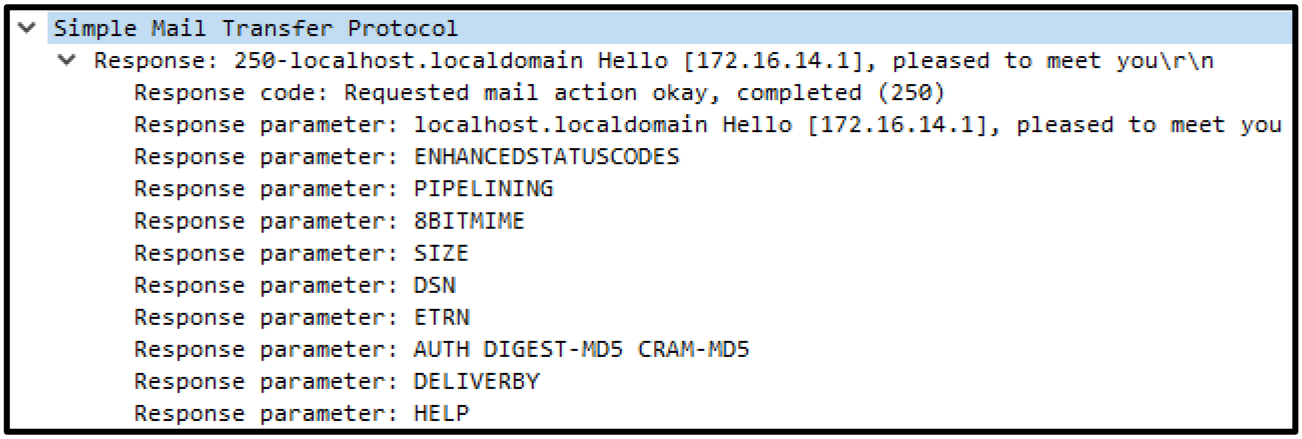
```
v Simple Mail Transfer Protocol
  v Response: 220 localhost.localdomain ESMTP Sendmail 8.13.1/8.13.1; Fri, 10 Sep 2021 15:20:08 +1000\r\n
      Response code: <domain> Service ready (220)
      Response parameter: localhost.localdomain ESMTP Sendmail 8.13.1/8.13.1; Fri, 10 Sep 2021 15:20:08 +1000
```

Screenshot from Wireshark capture. First SMTP capture is selected and the corresponding SMTP record is shown above.

e) Email 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 SMTP server response to the EHLO command sent by the client is "Hello [172.16.14.1], pleased to meet you" (172.16.14.1 is the client's IP address). See screenshot below.



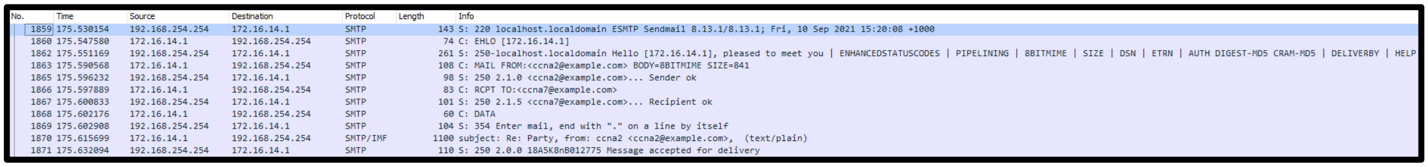
```
v Simple Mail Transfer Protocol
  v Response: 250-localhost.localdomain Hello [172.16.14.1], pleased to meet you\r\n
      Response code: Requested mail action okay, completed (250)
      Response parameter: localhost.localdomain Hello [172.16.14.1], pleased to meet you
      Response parameter: ENHANCEDSTATUSCODES
      Response parameter: PIPELINING
      Response parameter: 8BITMIME
      Response parameter: SIZE
      Response parameter: DSN
      Response parameter: ETRN
      Response parameter: AUTH DIGEST-MD5 CRAM-MD5
      Response parameter: DELIVERBY
      Response parameter: HELP
```

Screenshot from Wireshark capture. Complete SMTP server response to EHLO command sent by client shown above.

f) 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>`	`250 2.1.0 <ccna2@example.com>... Sender ok`
`RCPT TO:<ccna2@example.com>`	`250 2.1.5 <ccna7@example.com>... Recipient ok`
`DATA`	`354 Enter mail, end with ".” on a line by itself`
`(message body is sent)`	`250 2.0.0 18A5K8nB012775 Message accepted for delivery`

See screenshot below.

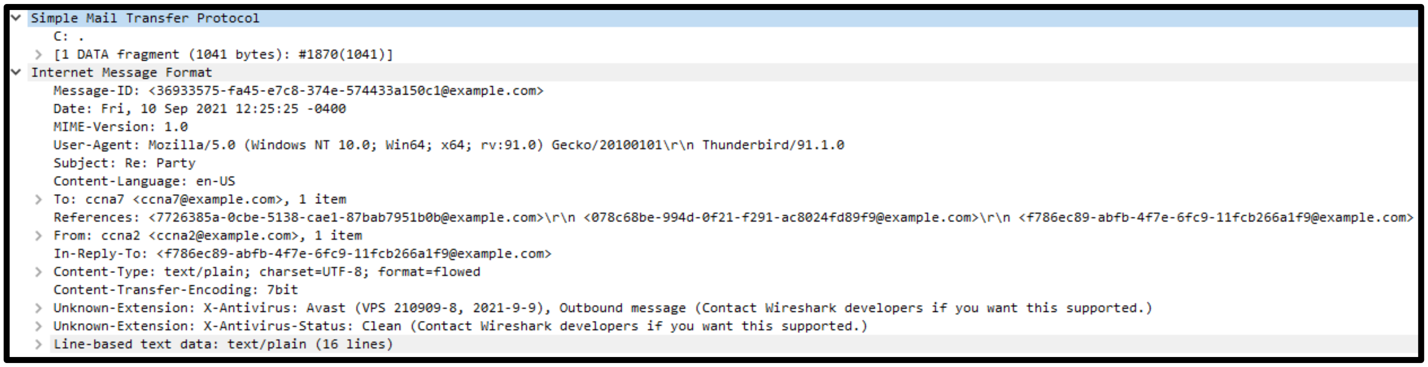


```
No.   Time       Source           Destination      Protocol  Length Info
 1859 175.530154 192.168.254.254  172.16.14.1      SMTP         143 S: 220 localhost.localdomain ESMTP Sendmail 8.13.1/8.13.1; Fri, 10 Sep 2021 15:20:08 +1000
 1860 175.547580 172.16.14.1      192.168.254.254  SMTP          74 C: EHLO [172.16.14.1]
 1862 175.551169 192.168.254.254  172.16.14.1      SMTP         261 S: 250-localhost.localdomain Hello [172.16.14.1], pleased to meet you | ENHANCEDSTATUSCODES | PIPELINING | 8BITMIME | SIZE | DSN | ETRN | AUTH DIGEST-MD5 CRAM-MD5 | DELIVERBY | HELP
 1863 175.590568 172.16.14.1      192.168.254.254  SMTP         108 C: MAIL FROM:<ccna2@example.com> BODY=8BITMIME SIZE=841
 1865 175.596232 192.168.254.254  172.16.14.1      SMTP          98 S: 250 2.1.0 <ccna2@example.com>... Sender ok
 1866 175.597889 172.16.14.1      192.168.254.254  SMTP          83 C: RCPT TO:<ccna7@example.com>
 1867 175.600833 192.168.254.254  172.16.14.1      SMTP         101 S: 250 2.1.5 <ccna7@example.com>... Recipient ok
 1868 175.602176 172.16.14.1      192.168.254.254  SMTP          60 C: DATA
 1869 175.602908 192.168.254.254  172.16.14.1      SMTP         104 S: 354 Enter mail, end with "." on a line by itself
 1870 175.615699 172.16.14.1      192.168.254.254  SMTP/IMF    1100 subject: Re: Party, from: ccna2 <ccna2@example.com>,  (text/plain)
 1871 175.632094 192.168.254.254  172.16.14.1      SMTP         110 S: 250 2.0.0 18A5K8nB012775 Message accepted for delivery
```

Screenshot from Wireshark capture. Complete summarized exchange between client and server shown above (same process repeats for each new message sent out from the client to the server).

What are the contents of the last message body from the email client?

- The contents of the last message body from the client show almost all details about the client (operating system used, email client used, time mail sent, etc…) and the mail that the client is sending out (the entire message is visible to the user who is analyzing the Wireshark capture -> not secure way for sending messages!). See screenshot below.

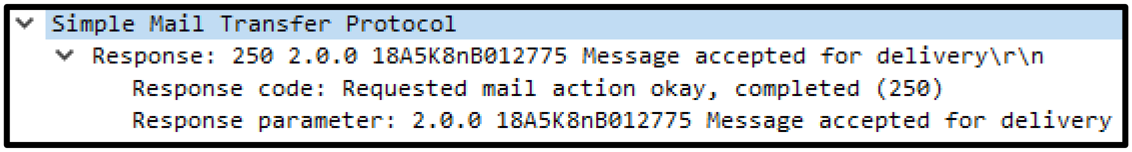


```
v Simple Mail Transfer Protocol
     C: .
   > [1 DATA fragment (1041 bytes): #1870(1041)]
v Internet Message Format
     Message-ID: <36933575-fa45-e7c8-374e-574433a150c1@example.com>
     Date: Fri, 10 Sep 2021 12:25:25 -0400
     MIME-Version: 1.0
     User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101\r\n Thunderbird/91.1.0
     Subject: Re: Party
     Content-Language: en-US
   > To: ccna7 <ccna7@example.com>, 1 item
     References: <7726385a-0cbe-5138-cae1-87bab7951b0b@example.com>\r\n <078c68be-994d-0f21-f291-ac8024fd89f9@example.com>\r\n <f786ec89-abfb-4f7e-6fc9-11fcb266a1f9@example.com>
   > From: ccna2 <ccna2@example.com>, 1 item
     In-Reply-To: <f786ec89-abfb-4f7e-6fc9-11fcb266a1f9@example.com>
   > Content-Type: text/plain; charset=UTF-8; format=flowed
     Content-Transfer-Encoding: 7bit
   > Unknown-Extension: X-Antivirus: Avast (VPS 210909-8, 2021-9-9), Outbound message (Contact Wireshark developers if you want this supported.)
   > Unknown-Extension: X-Antivirus-Status: Clean (Contact Wireshark developers if you want this supported.)
   > Line-based text data: text/plain (16 lines)
```

Screenshot from Wireshark capture. Complete details about the contents of the last message body sent from the client to the server shown above.

How does the email server respond?

- When the mail that the client is sending out reaches the server, the server eventually responds with a statement reading "Message accepted for delivery". See screenshot below.



```
Simple Mail Transfer Protocol
  Response: 250 2.0.0 18A5K8nB012775 Message accepted for delivery\r\n
      Response code: Requested mail action okay, completed (250)
      Response parameter: 2.0.0 18A5K8nB012775 Message accepted for delivery
```

Screenshot from Wireshark capture. Complete details about the response from the email server (when client sends out mail to the server) shown above.

Discussion:

- The entire lab was successful, but without its own complications. At first, the installation of the email client (in this case, Mozilla Thunderbird) was not too difficult. The only challenge was during configuration, since the version installed did not correspond with the one used in this document, so configuration was a little difficult to configure the email client. Despite having the correct settings applied to the email client, there was a problem communicating with the email server (Eagle server). The client repeatedly stated that it "could not connect to eagle-server.example.com". Basic networking troubleshooting began, including checking for physical connection to the network, and the problem was found in the client's host IP configuration. Despite having the correct IP address set, including subnet mask and default gateway, there was no DNS server specified. The problem became clear since there was no DNS server specified, as its job is to translate host names into IP addresses, so each time the email client tried to communicate with the email server "egale-server.example.com", it would fail since the role of the DNS server was not present. Once the DNS server was specified in the client's host IP configuration, the email client was able to communicate with the email server. All messages sent to the email client (ccna2@example.com) was shown upon clicking the inbox icon in the email client. Once the email client was able to establish a connection and fetch information from the email server, a few test messages were sent out to other recipients and a response was found after a short while. At the same time the test was going on, a Wireshark packet capture was in progress. After the test stopped, so did the capture, and a thorough analysis was conducted. In the Wireshark capture, the complete exchange between the email server and the client is shown for each of the messages sent out from the client and received by the client. After some further analysis, it was revealed that private information, such as the addresses of the people sending the mail, was visible. Complete contents of the mail being sent out and received were shown as well. This shows that the communication using SMTP to send messages is not secure, since almost all private information is revealed to the user who is performing the packet capture, which leaves both sender and recipient vulnerable!

Conclusion:

- Successfully installed email client software on host computer.
- Successfully configured host computer for email service.
- Successfully sent out and received mail from other recipients.
- Successfully observed and analyzed exchange between email client (host computer) and email server (Eagle server).