Práctica de laboratorio 3.4.3: Protocolos y servicios de correo electrónico

Diagrama de topología

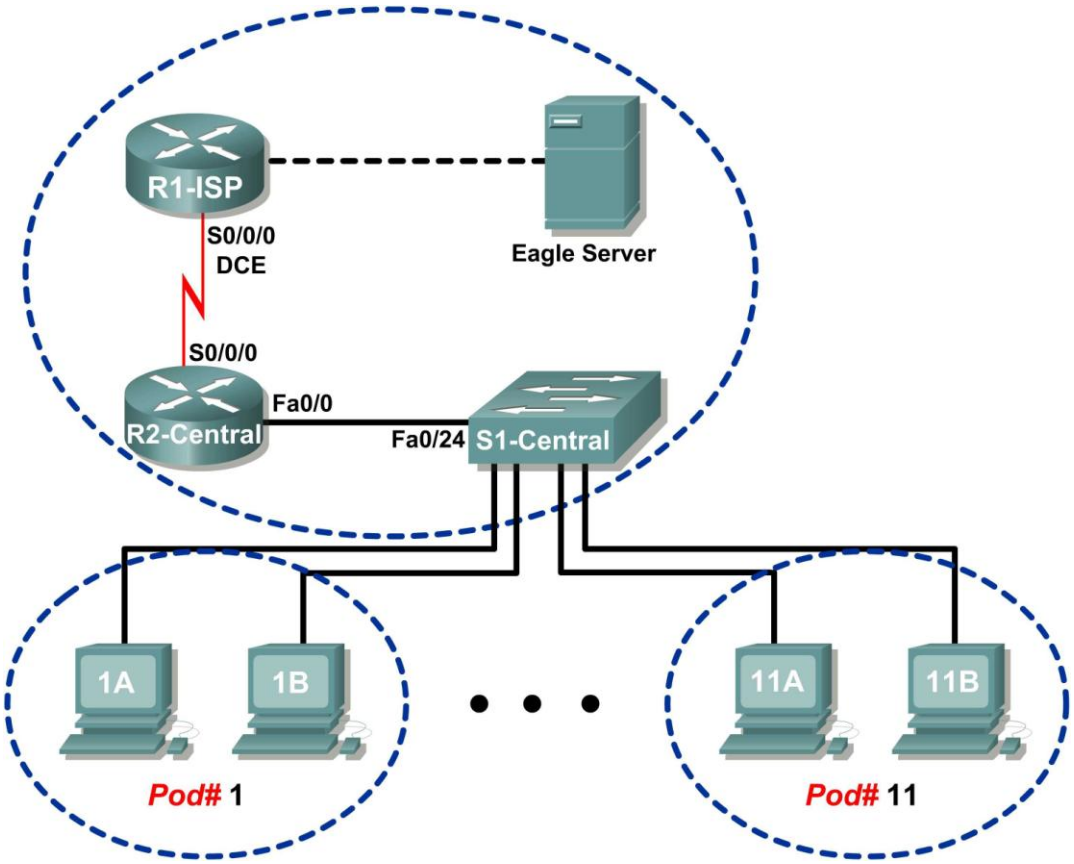


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	*No aplicable*
	Fa0/0	192.168.254.253	255.255.255.0	*No aplicable*
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	*No aplicable*
	Fa0/0	172.16.255.254	255.255.0.0	*No aplicable*
Eagle Server	*No aplicable*	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	*No aplicable*
host*Pod#***A**	*No aplicable*	172.16. *Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#***B**	*No aplicable*	172.16. *Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	*No aplicable*	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Configurar el equipo host del módulo para el servicio de correo electrónico
- Capturar y analizar comunicaciones por correo electrónico entre el equipo host del módulo y un servidor de mail

Información básica

El correo electrónico es uno de los servicios de red más populares que utiliza un modelo cliente/servidor. El cliente de correo electrónico se configura en una computadora de usuario para conectarse a un servidor de correo electrónico. La mayoría de los proveedores de servicios de Internet (ISP) provee instrucciones paso a paso para el uso de los servicios de correo electrónico. Es por eso que un usuario típico puede desconocer las complejidades del correo electrónico o de los protocolos que se utilizan.

En entornos de red donde el cliente MUA debe conectarse a un servidor de correo electrónico en otra red para enviar y recibir correos electrónicos, se utilizan los siguientes dos protocolos:

- Simple Mail Transfer Protocol (SMTP), que se definió originalmente en RFC 281, agosto de 1982, y ha pasado por varias modificaciones y mejoras. RFC 2821, abril de 2001, que consolida y actualiza RFC relacionados con correos electrónicos anteriores. El servidor SMTP escucha el puerto TCP 25 bien conocido. El SMTP se utiliza para enviar correos electrónicos del cliente externo al servidor de correos electrónico, entregar correos electrónicos a cuentas locales y relay de correos electrónicos entre servidores SMTP.
- Post Office Protocol versión 3 (POPv3) se utiliza cuando un cliente de correo electrónico externo desea recibir correos electrónicos desde el servidor de correo electrónico. El servidor POPv3 escucha el puerto TCP 110 bien conocido.

Las versiones anteriores de ambos protocolos no deben utilizarse. También existen versiones seguras de ambos protocolos que usan capas de socket seguras/seguridad de la capa de transporte (SSL/TSL) para la comunicación.

El correo electrónico está sujeto a múltiples vulnerabilidades de seguridad de equipos. Los ataques de correo no deseado invaden la red con correos electrónicos no solicitados e inútiles que consumen ancho de banda y recursos de red. Los servidores de correo electrónico han tenido numerosas vulnerabilidades que han generado peligro para los equipos.

Escenario

En esta práctica de laboratorio, el usuario configurará y utilizará una aplicación de cliente de correo electrónico para conectarse a los servicios de red de eagle-server. El usuario monitorea la comunicación con Wireshark y analiza los paquetes capturados.

Se utilizará un cliente de correo electrónico, como Outlook Express o Mozilla Thunderbird, para conectarse a un servicio de red de eagle-server. Eagle-server tiene servicios de correo SMTP previamente configurados con cuentas de usuarios que pueden enviar y recibir correos electrónicos externos.

Tarea 1: Configurar el equipo host del módulo para el servicio de correo electrónico.

La práctica de laboratorio debe estar configurada como se muestra en el Diagrama de topología y en la tabla de dirección lógica. En caso contrario, pídale ayuda al instructor antes de continuar.

Paso 1: Descargue e instale Mozilla Thunderbird.

Si Thunderbird no está instalado en el equipo host del módulo, se puede descargar de eagle- server.example.com. Ver Figura 1. El URL para descargarlo es ftp://eagle-server.example.com/pub/eagle labs/eagle1/chapter3.

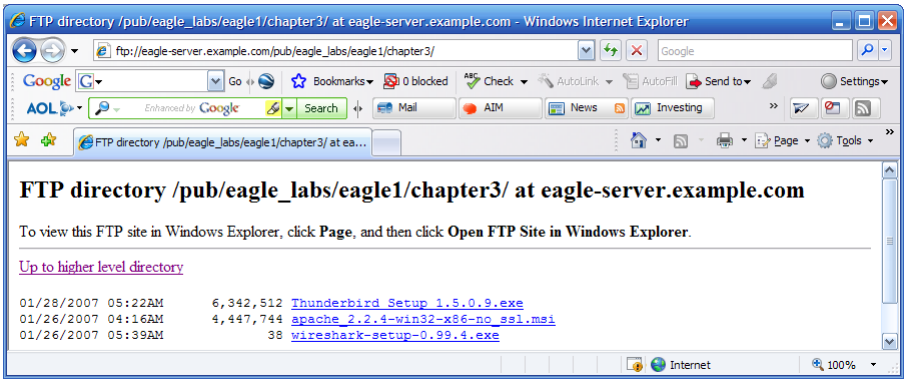


Figura 1. Descarga de FTP para Wireshark

1. Haga clic con el botón derecho en el nombre de archivo Thunderbird y luego guarde el archivo en el equipo host del módulo.
2. Una vez que se descargó el archivo, haga doble clic en el nombre de archivo e instale Thunderbird con las configuraciones predeterminadas.
3. Cuando haya finalizado, inicie Thunderbird.

Paso 2: Configurar Thunderbird para recibir y enviar correos electrónicos.

1. Cuando Thunderbird inicie, se debe configurar la cuenta de correo electrónico. Complete la información de la cuenta tal como se indica a continuación:

Campo	Valor
Nombre de la cuenta	El nombre de la cuenta está basado en el equipo host del módulo. Hay un total de 22 cuentas configuradas en Eagle Server, rotuladas ccna[1.22]. Si este host del módulo está en Pod1, Host A, entonces el nombre de la cuenta es ccna1. Si este host del módulo está en Pod3, Host B, entonces el nombre de la cuenta es ccna6. Y así sucesivamente.
Su nombre	Utilice el mismo nombre que arriba.
Dirección de correo electrónico	*Su_nombre*@eagle-server.example.com
Tipo de servidor de entrada que utiliza	POP
Servidor de entrada (SMTP)	eagle-server.example.com
Servidor de salida (SMTP)	eagle-server.example.com

2. Verifique las configuraciones de la cuenta en **Herramientas > Configuraciones de la cuenta**. Vea la Figura 2.

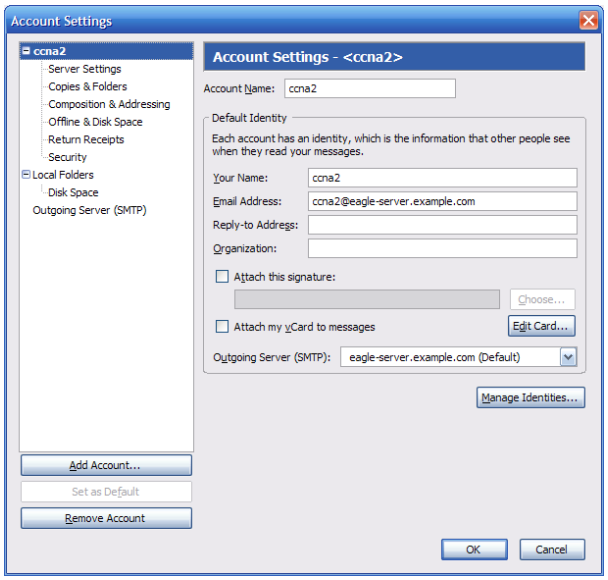


Figura 2. Configuraciones de la cuenta Thunderbird

3. En el panel izquierdo de la pantalla Configuraciones de la cuenta, haga clic en **Configuraciones del servidor**. Se verá una pantalla similar a la que se muestra en la Figura 3.

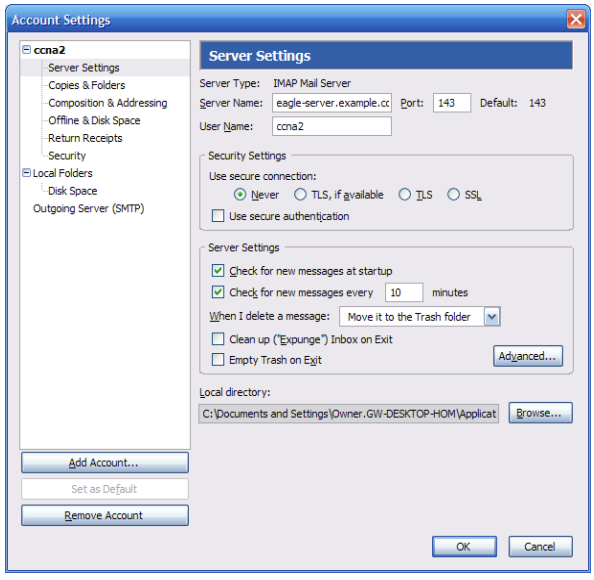


Figura 3. Pantalla Configuraciones del servidor de Thunderbird

La Figura 4 muestra la configuración correcta para el servidor de salida (SMTP).

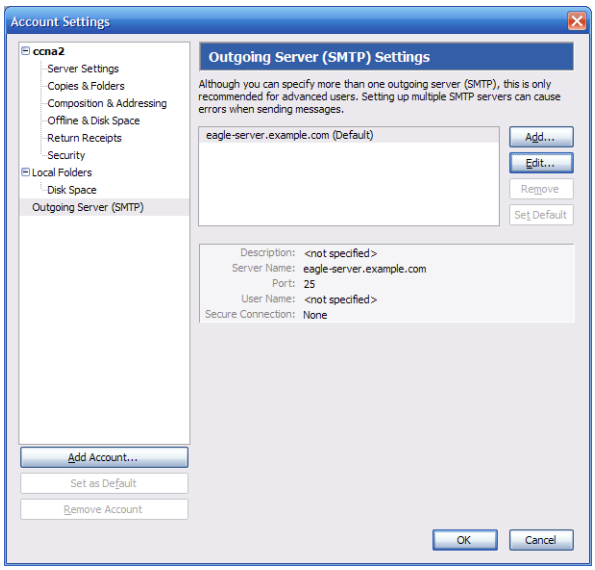


Figura 4. Pantalla Configuraciones del servidor de salida (SMTP)

¿Cuál es el propósito del protocolo SMTP y cuál es el número de puerto TCP bien conocido?

_____

_____

Tarea 2: Capturar y analizar comunicaciones por correo electrónico entre el equipo host del módulo y un servidor de correo electrónico.

Paso 1: Enviar un correo electrónico no capturado.

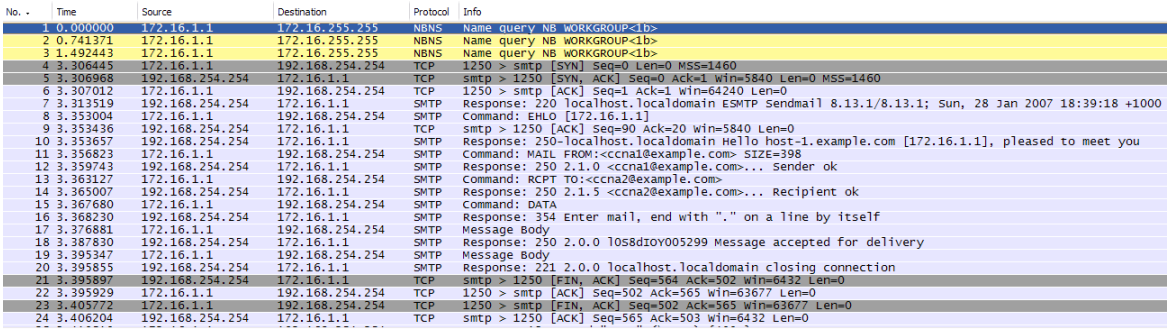
1. Pregúntele a otro estudiante de la clase cuál es su nombre de correo electrónico.
2. Utilice ese nombre para componer y enviar un mensaje amistoso a un estudiante.

Paso 2: Iniciar las capturas de Wireshark.

Una vez que esté seguro de que el funcionamiento del correo electrónico es el correcto tanto para enviar como para recibir, inicie la captura Wireshark. Wireshark mostrará capturas basadas en el tipo de paquete.

Paso 3: Analice una sesión de captura Wireshark de SMTP.

1. Utilice al cliente de correo electrónico y de nuevo, envíe un correo electrónico a un estudiante y reciba otro de él. Esta vez, no obstante, las transacciones del correo electrónico serán capturadas.
2. Después de enviar y recibir un mensaje de correo electrónico, detenga la captura Wireshark. En la Figura 5 se muestra una captura parcial Wireshark de un correo electrónico saliente utilizando SMTP.



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

Figura 5. Captura SMTP

3. Resalte la primera captura SMTP en la ventana Wireshark de arriba. En la Figura 5, es la línea número 7.
4. Expanda el registro del Simple Mail Transfer Protocol en la segunda ventana Wireshark.

   Hay varios tipos diferentes de servidores SMTP. Atacantes maliciosos pueden acceder a información valiosa simplemente aprendiendo el tipo y versión del servidor SMTP.

¿Cuál es el nombre y la versión del servidor SMTP?

_____

Las aplicaciones del cliente de correo electrónico envían comandos a los servidores de correo electrónico y los servidores de correo electrónico envían respuestas. En cada primer intercambio SMTP, el cliente de correo electrónico envía el comando **EHLO.** Sin embargo, la sintaxis puede variar entre clientes y el comando ser **HELO** o **HELLO**. El servidor de correo electrónico debe responder al comando.

¿Cuál es la respuesta del servidor SMTP al comando EHLO?

_____

Los próximos intercambios entre cliente y servidor de correo electrónico contienen información de correo electrónico. Utilice la captura Wireshark, complete las respuestas del servidor de correo electrónico a los comandos del cliente de correo electrónico:

Cliente de correo electrónico	Servidor de correo electrónico
MAIL FROM:,ccna1@excmaple.com>	
RCPT TO:<ccna2@example.com>	
DATOS	
(cuerpo de mensaje enviado)	

¿Cuáles son los contenidos del último cuerpo de mensaje de parte del cliente de correo electrónico?

_____

¿Cómo responde el servidor de correo electrónico?

_____

Tarea 3: Desafío

Acceda a un equipo que tenga acceso a Internet. Busque el nombre y la versión del servidor SMTP para conocer las debilidades o compromisos. ¿Hay versiones más nuevas disponibles?

Tarea 4: Reflexión

El correo electrónico es probablemente el servicio de red más comúnmente usado. Entender el flujo de tráfico con el protocolo SMTP lo ayudará a entender cómo el protocolo administra la conexión de datos cliente/servidor. El correo electrónico también puede tener problemas de configuración. ¿El problema es con el cliente de correo electrónico o con el servidor de correo electrónico? Una manera simple de probar el funcionamiento del servidor SMTP es usar la utilidad Telnet de la línea de comandos Windows para telnet dentro del servidor SMTP.

1. Para probar la operación SMTP, abra la ventana de línea de comandos Windows y comience una sesión Telnet con el servidor SMTP.

```
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.
correo electrónico SMTP server test...
.
250 Mail queued for delivery.
QUIT
221 Closing connection. Good bye.
Connection to host lost.
C:\>
```

Tarea 5: Limpieza

Si se instaló Thunderbird en el equipo host del módulo para esta práctica de laboratorio, seguramente el instructor va a querer que se elimine la aplicación. Para eliminar Thunderbird, haga clic en **Inicio > Panel de Control > Agregar o quitar programas.** Desplácese hasta **Thunderbird** y haga clic allí, luego haga clic en **Quitar**.

A menos que el instructor le indique lo contrario, apague las computadoras host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.