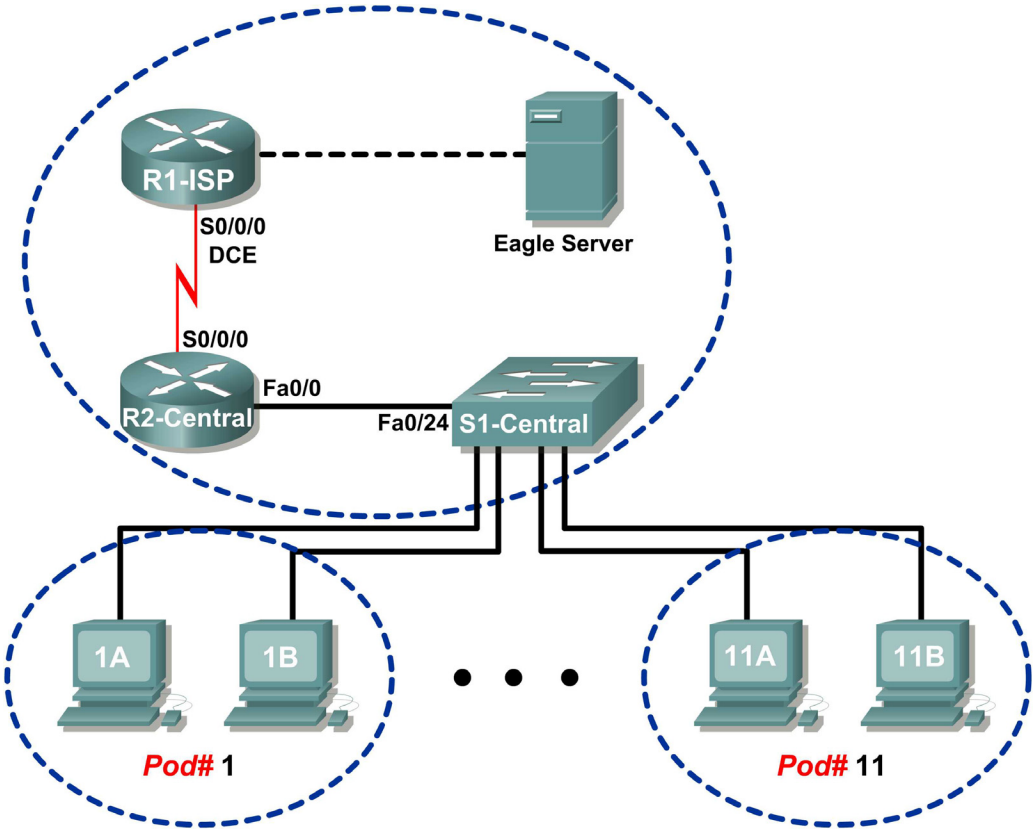
## Solución

Cisco | Networking Academy®
Mind Wide Open™

# Laboratorio 4.5.3: Examen de protocolos de las capas de aplicación y de transporte

## 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 la computadora host para capturar protocolos de la capa de aplicación.
- Capturar y analizar la comunicación HTTP entre la computadora host del módulo y un servidor Web.
- Capturar y analizar la comunicación FTP entre la computadora host del módulo y un servidor FTP.
- Observar los canales TCP para establecer y administrar la comunicación con conexiones HTTP y FTP.

## Información básica

La función principal de la capa de transporte es mantener un registro de las conversaciones de múltiples aplicaciones en el mismo host. Sin embargo, cada aplicación tiene determinados requisitos para sus datos y, por lo tanto, se han desarrollado diferentes protocolos de transporte para que cumplan con estos requisitos. Los protocolos de la capa de aplicación definen la comunicación entre servicios de red, como un servidor Web y un cliente y un servidor FTP y un cliente. Los clientes inician la comunicación con el servidor adecuado y el servidor responde al cliente. Para cada servicio de red existe un servidor determinado que escucha, en un puerto determinado, las conexiones del cliente. Puede haber diversos servidores en el mismo dispositivo final. Un usuario puede abrir diferentes aplicaciones del cliente para el mismo servidor, pero cada cliente se comunica, en forma exclusiva, con una sesión establecida entre el cliente y el servidor.

Los protocolos de la capa de aplicación se basan en los protocolos TCP/IP de menor nivel, como TCP o UDP. Esta práctica de laboratorio examina dos protocolos populares de la capa de aplicación, HTTP y FTP, y la manera en que los protocolos de la capa de transporte, TCP y UDP, administran el canal de comunicación. También se examinan las solicitudes más comunes de los clientes y las correspondientes respuestas del servidor.

## Escenario

En esta práctica de laboratorio se utilizarán las aplicaciones del cliente para conectarse a los servicios de red del eagle server. El usuario monitorea la comunicación con Wireshark y analiza los paquetes capturados.

Se utiliza un explorador Web como Internet Explorer o Firefox para conectarse al servicio de red del eagle server. Eagle server tiene varios servicios de red previamente configurados, como el HTTP, que esperan responder las solicitudes del cliente.

También se utilizará el explorador Web para examinar el protocolo FTP y el cliente de línea de comando FTP. El ejercicio demostrará que, aunque los clientes pueden diferir, la comunicación subyacente con el servidor sigue siendo la misma.

### Tarea 1: Configuración de la computadora host del módulo para capturar protocolos de la capa de aplicación.

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: Descargar e instalar wireshark.**


**Figura 1. Descarga de FTP para Wireshark**

Si Wireshark no está instalado en la computadora host del módulo, puede descargarse desde eagle-server.example.com. Vea la Figura 1. El URL de descarga es: ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter3.

1. Haga clic con el botón derecho del mouse sobre el nombre del archivo wireshark. Luego, guarde el archivo en la computadora host del módulo.
2. Cuando el archivo se haya descargado, haga doble clic en el nombre del archivo e instale Wireshark con las configuraciones predeterminadas.

**Paso 2: Iniciar Wireshark y configurar la Interfaz de captura.**

1. Inicie Wireshark desde **Inicio > Todos los programas > Wireshark > Wireshark**.
2. Cuando se muestra la ventana que se abre, establezca la Interfaz de captura correcta. La interfaz correcta es la interfaz con la dirección IP de la computadora host del módulo. Vea la Figura 2.

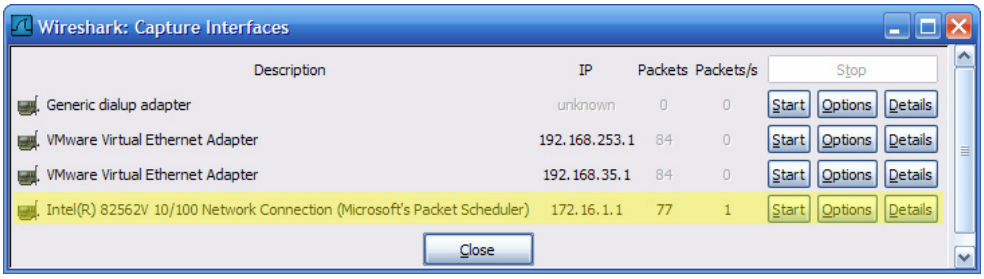



**Figura 2: Ventana de captura de interfaz de Wireshark**

Wireshark puede iniciarse haciendo clic en el botón **Inicio** de la interfaz. Después, la interfaz se utiliza como predeterminada y no se la necesita cambiar.

Wireshark debe comenzar a registrar datos.

3. Detenga Wireshark por ahora. Wireshark se utilizará en las siguientes tareas.

## Tarea 2: Captura y análisis de la comunicación HTTP entre la computadora host del módulo y un servidor Web.

HTTP es un protocolo de capa de aplicación que depende de los protocolos de menor nivel, como TCP, para establecer y administrar el canal de comunicación. HTTP versión 1.1 se define en RFC 2616, en el año 1999. Esta parte de la práctica de laboratorio demostrará cómo las sesiones entre múltiples clientes Web y el servidor Web se mantienen separadas.

### Paso 1: Iniciar las capturas de Wireshark.

Inicie una captura de Wireshark. Wireshark mostrará capturas basadas en el tipo de paquete.

### Paso 2: Iniciar el explorador Web del host del módulo. (vamos a cambiar las urls, ya que no existen)

1. Con un explorador Web, como Internet Explorer o Firefox, conéctese al URL http://futbol server.example.com. Se muestra una página Web similar a la de la Figura 3. No cierre este explorador Web hasta que se le indique. (usar esta url-> http://futboljovellanos.esp.st)

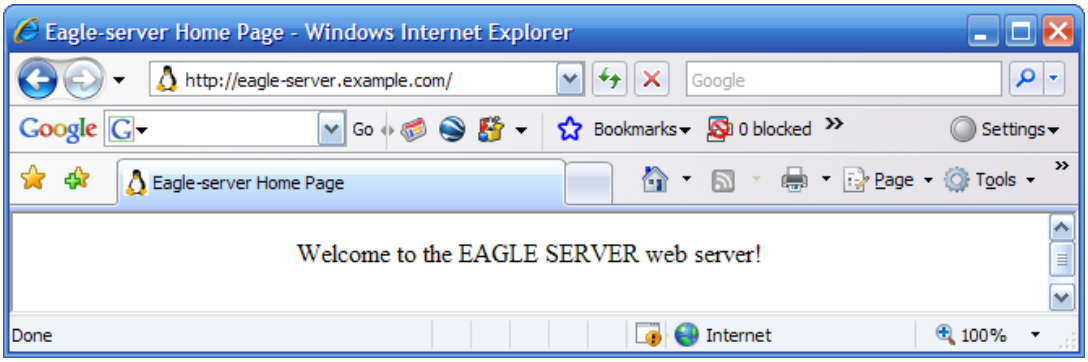



**Figura 3: Explorador Web conectado al servidor Web**

2. Haga clic en el botón **Actualizar** del explorador Web. No debe haber cambios en la pantalla del cliente Web. (usar en el paso 3 esta url-> http://lacomunidadasix.wordpress.com)
3. Abra un segundo explorador Web y conéctese al URL http://eagle-server.example.com/page2.html. En la pantalla aparece una página Web diferente.

   No cierre ningún explorador hasta que la captura de Wireshark se detenga.

### Paso 3: Detener las capturas de Wireshark y analizar los datos capturados.

1. Detenga las capturas de Wireshark.
2. Cierre los exploradores Web.

Se muestran los datos Wireshark resultantes. En el paso 2, se crearon al menos tres sesiones HTTP. La primera sesión HTTP comenzó con una conexión a http://eagle-server.example.com. La segunda sesión se produjo con una actualización. La tercera sesión se produjo cuando el segundo explorador Web entró a http://eagle-server.example.com/page2.html.

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 10 | 10.168217 | 172.16.1.2 | 192.168.254.254 | TCP | 1056 > http [SYN] Seq=0 Len=0 MSS=1460 |
| 11 | 10.170734 | 192.168.254.254 | 172.16.1.2 | TCP | http > 1056 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 12 | 10.170767 | 172.16.1.2 | 192.168.254.254 | TCP | 1056 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 13 | 10.171086 | 172.16.1.2 | 192.168.254.254 | HTTP | GET / HTTP/1.1 |
| 14 | 10.171625 | 192.168.254.254 | 172.16.1.2 | TCP | http > 1056 [ACK] Seq=1 Ack=208 Win=6432 Len=0 |
| 15 | 10.172518 | 192.168.254.254 | 172.16.1.2 | HTTP | HTTP/1.1 200 OK (text/html) |
| 16 | 10.172540 | 192.168.254.254 | 172.16.1.2 | TCP | http > 1056 [FIN, ACK] Seq=448 Ack=208 Win=6432 Len=0 |
| 17 | 10.172567 | 172.16.1.2 | 192.168.254.254 | TCP | 1056 > http [ACK] Seq=208 Ack=449 Win=63793 Len=0 |
| 18 | 10.174196 | 172.16.1.2 | 192.168.254.254 | TCP | 1056 > http [FIN, ACK] Seq=208 Ack=449 Win=63793 Len=0 |
| 19 | 10.174661 | 192.168.254.254 | 172.16.1.2 | TCP | http > 1056 [ACK] Seq=449 Ack=209 Win=6432 Len=0 |

**Figura 4: Sesión de HTTP capturada**

En la Figura 4 se muestra un ejemplo de una sesión HTTP capturada. Antes de que la HTTP pueda comenzar, se debe crear una sesión TCP. Esto se ve en las tres primeras líneas de sesión, números 10, 11 y 12. Utilice los resultados de captura de Wireshark o similares para responder las siguientes preguntas:

3. Complete la siguiente tabla con la información presentada en la sesión HTTP:

| | |
|---|---|
| Dirección IP del explorador Web | 192.168.2.101 |
| Dirección IP del servidor Web | 89.17.220.221 |
| Protocolo de la capa de transporte (UDP/TCP) | TCP |
| Número de puerto del explorador Web | 49401 |
| Número de puerto del servidor Web | 80 |

4. ¿Qué computadora inició la sesión HTTP y cómo lo hizo?

La computadora con ip 192.168.2.101, enviando un segmento TCP con el flag Syn a 1, el numero de secuencia igual a 0 y el tamaño de ventana 8192 bytes

5. ¿Qué computadora señaló inicialmente un fin a la sesión HTTP y cómo lo hizo?

La computadora con ip 192.168.2.101 enviando un segmento TCP con los flags Syn y ACK a 1

6. Resalte la primera línea del protocolo HTTP, una solicitud **GET** (Obtener) del explorador Web. En la Figura 4 de arriba, la solicitud **GET** está en la línea 13. Vaya a la segunda ventana de Wireshark (la del medio) para examinar los protocolos en capas. Si es necesario, expanda los campos.
7. ¿Qué protocolo se lleva (encapsulado) dentro del segmento TCP?

El protocolo Hypertext Transfer Protocol (HTTP)

8. Expanda el último registro de protocolo y cualquier subcampo. Ésta es la información real enviada al servidor Web. Complete la siguiente tabla utilizando la información del protocolo.

Versión del protocolo: HTTP/1.1

Método de solicitud: GET

* Solicitud URI : /index.php

Idioma :es-es, es; q=0.8, en-us;q=0.5, en;q00.8\r\n

* La solicitud URI es la ruta para el documento solicitado. En el primer explorador, la ruta es el directorio raíz del servidor Web. Aunque no se solicitó ninguna página, algunos servidores Web están configurados para mostrar un archivo predeterminado, si está disponible.

El servidor Web responde con el próximo paquete HTTP. En la Figura 4 se puede ver en la línea 15. Una respuesta para el explorador Web es posible porque el servidor Web (1) comprende el tipo de solicitud y (2) tiene que devolver un archivo. Los crackers a veces envían solicitudes desconocidas o dañadas a servidores Web para intentar detener el servidor o poder acceder a la línea de comando del servidor. Además, una solicitud para una página Web desconocida da como resultado un mensaje de error.

9. Resalte la respuesta del servidor Web y luego vaya a la segunda ventana (la del medio). Abra todos los subcampos de HTTP colapsados. Observe la información que devuelve el servidor. En esta respuesta, sólo hay unas pocas líneas de texto (las respuestas del servidor Web pueden contener miles o millones de bytes). El explorador Web comprende los datos de la ventana del explorador y los formatea correctamente. .
10. ¿Cuál es la respuesta del servidor Web para la solicitud **GET** del cliente Web?

HTTP/1.1 200 ok (text/html)

11. ¿Qué significa esta respuesta?

Que acepta la petición y nos envia texto html (contenido html de la pagina index.php)

12. Desplácese hacia abajo de la ventana superior de Wireshark hasta que se muestre la segunda sesión de HTTP, actualizada. La Figura 5 muestra una captura de muestra.

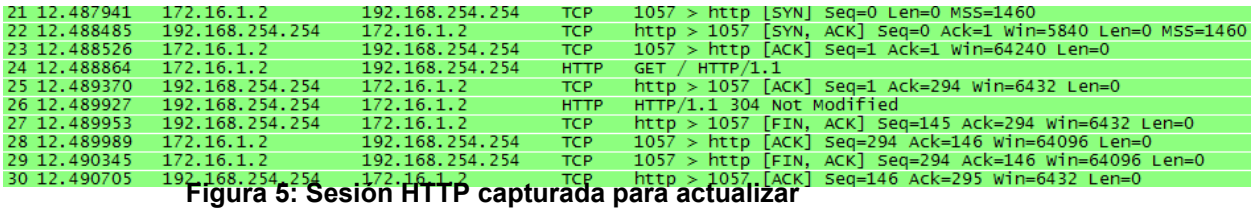



**Figura 5: Sesión HTTP capturada para actualizar**

El significado de la acción de actualización se encuentra en la respuesta del servidor, `304 Not Modified` (304 No modificado). Con un paquete simple devuelto para la solicitud inicial de **GET** y para la actualización, el ancho de banda utilizada es mínimo. Sin embargo, para una respuesta inicial que contenga millones de bytes, un simple paquete de respuesta puede generar un significativo ahorro de ancho de banda.

Debido a que esta página Web ha sido guardada en la caché del cliente Web, la solicitud **GET** contenía las siguientes instrucciones adicionales para el servidor Web.

```
If-modified-since: Fri, 26 Jan 2007 06:19:33 GMT\r\n
If-None-Match "98072-b8-82da8740"\r\n  <-
```
page tag number (ETAG)

13. ¿Cuál es la respuesta ETAG del servidor Web?

En nuestro caso no se genero, ya que la respuesta fue OK

## Tarea 3: Captura y análisis de la comunicación FTP entre la computadora host del módulo y un servidor Web.

El protocolo de la capa de aplicación FTP ha recibido una revisión significativa desde que apareció por primera vez en RFC 114, en 1971. La versión 5.1 de FTP se define en RFC 959, de octubre de 1985.

El explorador Web conocido no sólo puede usarse para comunicarse con el servidor HTTP. En esta tarea, el explorador Web y una utilidad de línea de comando FTP se utilizan para descargar datos desde un servidor FTP.

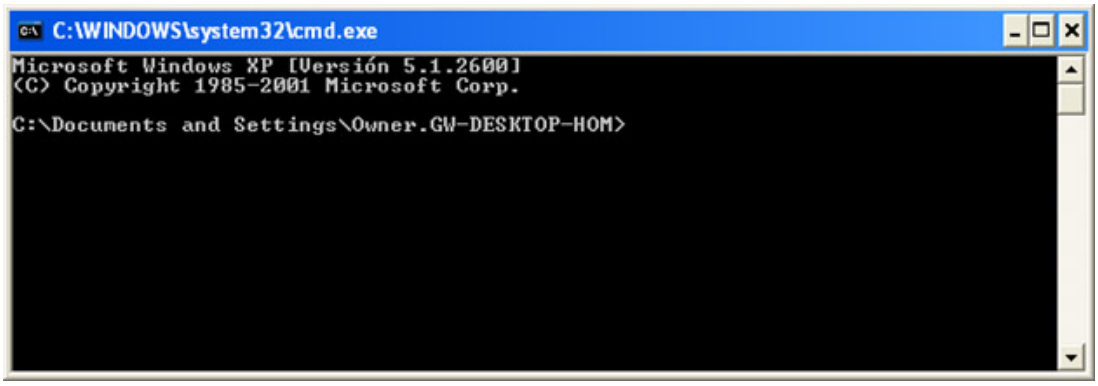



**Figura 6: Pantalla de línea de comandos de Windows**

Para prepararse para esta tarea, abra una línea de comandos en la computadora host del módulo. Esto puede lograrse haciendo clic en **Inicio > Ejecutar** y luego escribiendo **CMD** y haciendo clic en **Aceptar**. Se muestra una pantalla similar a la de la Figura 6.

**Paso 1: Iniciar las capturas de Wireshark.**

Si es necesario, consulte la Tarea 1, Paso 2, para abrir Wireshark.

**Paso 2: Iniciar el cliente FTP de la línea de comandos host del módulo.**

1. Inicie una sesión FTP de una computadora host del módulo con el servidor FTP, usando la utilidad del cliente FTP de Windows. Para autenticar, utilice la identificación de usuario **anonymous** (anónima). Como respuesta a la petición de contraseña, presione <**Intro**>.

```
> ftp eagle-server.example.com
Conectado a eagle-server.example.com.
220 Bienvenido al servicio FTP de eagle-server.
Usuario (eagle-server.example.com:(ninguno)): anonymous
331 Especifique la contraseña.
Contraseña: <INTRO>
230 Conexión exitosa.
```

2. El indicador del cliente FTP es `ftp>`. Esto significa que el cliente FTP espera un comando para enviar al servidor FTP. Para ver una lista de los comandos del cliente FTP, escriba **`help <INTRO>`** (ayuda, <aceptar>):

```
ftp> help
Los comandos se pueden abreviar.  Comandos:

!           delete      literal     prompt      send
?           debug       ls          put         status
append      dir         mdelete     pwd         trace
ascii       disconnect  mdir        quit        type
bell        get         mget        quote       user
binary      glob        mkdir       recv        verbose
bye         hash        mls         remotehelp
cd          help        mput        rename
close       lcd         open        rmdir
```

Desafortunadamente, la gran cantidad de comandos del cliente FTP dificulta el uso de la utilidad de la línea de comandos para un principiante. Sólo usaremos unos pocos comandos para la evaluación de Wireshark.

3. Escriba el comando **dir** para mostrar los contenidos actuales del directorio:

```
ftp> dir
200 Comando PORT command exitoso. Considere usar PASV.
150 Aquí aparece el listado de directorio.
drwxr-xr-x    3 0        0            4096 Jan 12 04:32 pub
```

El cliente FTP es un directorio raíz del servidor FTP. Éste no es el directorio raíz real del servidor; sólo el punto más importante al que puede acceder el usuario **anonymous.** El usuario **anonymous** ha sido ubicado en una root jail, prohibiendo el acceso fuera del directorio actual.

4. Sin embargo, los subdirectorios se pueden recorrer y los archivos se pueden transferir a la computadora host del módulo. Vaya al directorio pub/eagle_labs/eagle1/chapter2, descargue un archivo y salga.

```
ftp> cd pub/eagle_labs/eagle1/chapter2
250 Se cambió exitosamente el directorio.
ftp> dir
200 Comando PORT command exitoso. Considere usar PASV.
150 Aquí aparece el listado de directorio.
-rw-r--r--  1 0 100     5853 Jan 12 04:26 ftptoeagle-server.pcap
-rw-r--r--  1 0 100     4493 Jan 12 04:27 http to eagle-server.pcap
-rw-r--r--  1 0 100     1486 Jan 12 04:27 ping to 192.168.254.254.pcap
-rw-r--r--  1 0 100 15163750 Jan 12 04:30 wireshark-setup-0.99.4.exe
226 Se envió correctamente el directorio.
ftp: 333 bytes received in 0.04Seconds 8.12Kbytes/sec.
ftp> get "ftptoeagle-server.pcap"
200 Comando PORT command exitoso. Considere usar PASV.
150 Abriendo la conexión de datos con el modo BINARIO para ftptoeagle-
server.pcap (5853 bytes).
226 Se envió correctamente el archivo.
ftp: 5853 bytes recibidos en 0.34 segundos 17.21 Kbytes/seg.
ftp> quit
221 Adiós.
```

5. Cierre la ventana de la línea de comandos con el comando exit (salir).
6. Detenga las capturas de Wireshark y guárdelas como FTP_Command_Line_Client.

**Paso 3: Iniciar el explorador Web del host del módulo.**

1. Inicie nuevamente las capturas Wireshark.

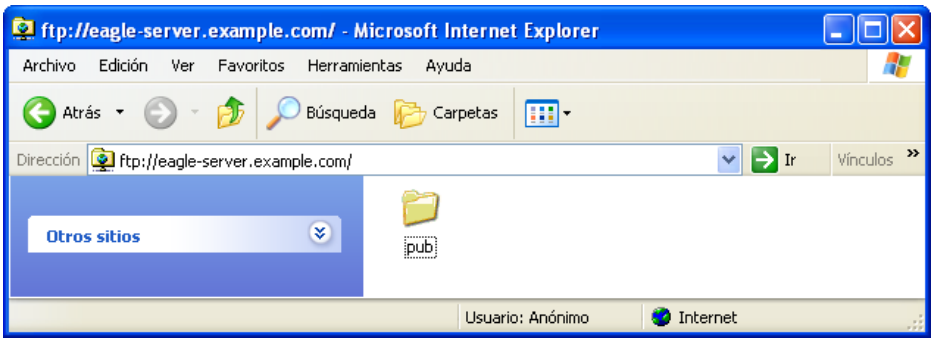



**Figura 7. Explorador Web utilizado como un cliente FTP**

2. Abra un explorador Web como lo muestra la Figura 7 y escriba el URL `ftp://eagle-server.example.com`. Se abre una ventana del explorador que muestra el directorio pub. Además, el explorador Web se registró en el servidor FTP como usuario Anonymous, como se muestra en la parte inferior de la captura de la pantalla.
3. Utilizando el explorador, vaya por los directorios hasta la ruta URL `pub/eagle-labs/eagle1/chapter2`. Haga doble clic en el archivo `ftptoeagle-server.pcap` y guarde el archivo.
4. Al finalizar, cierre el explorador Web.
5. Detenga las capturas de Wireshark y guárdelas como FTP_Web_Browser_Client.

**Paso 4: Detener las capturas de Wireshark y analizar los datos capturados.**

1. Si aún no está abierta, abra la captura de Wireshark FTP_Web_Browser_Client.
2. En la ventana superior de Wireshark, seleccione la captura FTP que es la primera transmisión del protocolo FTP. Respuesta: 220. En la Figura 8, es la línea número 23.

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 12 | 16.276555 | 172.16.1.2 | 192.168.254.254 | DNS | Standard query A eagle-server.example.com |
| 13 | 16.277284 | 192.168.254.254 | 172.16.1.2 | DNS | Standard query response A 192.168.254.254 |
| 14 | 16.278059 | 172.16.1.2 | 192.168.254.254 | TCP | 1073 > ftp [SYN] Seq=0 Len=0 MSS=1460 |
| 15 | 16.278540 | 192.168.254.254 | 172.16.1.2 | TCP | ftp > 1073 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 16 | 16.278575 | 172.16.1.2 | 192.168.254.254 | TCP | 1073 > ftp [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 23 | 26.281472 | 192.168.254.254 | 172.16.1.2 | FTP | Response: 220 Welcome to the eagle-server FTP service. |
| 24 | 26.281672 | 172.16.1.2 | 192.168.254.254 | FTP | Request: USER anonymous |
| 25 | 26.282120 | 192.168.254.254 | 172.16.1.2 | TCP | ftp > 1073 [ACK] Seq=47 Ack=17 Win=5840 Len=0 |
| 26 | 26.282137 | 192.168.254.254 | 172.16.1.2 | FTP | Response: 331 Please specify the password. |
| 27 | 26.282201 | 172.16.1.2 | 192.168.254.254 | FTP | Request: PASS IEUser@ |
| 28 | 26.283451 | 192.168.254.254 | 172.16.1.2 | FTP | Response: 230 Login successful. |
| 29 | 26.313423 | 172.16.1.2 | 192.168.254.254 | FTP | Request: opts utf8 on |
| 30 | 26.313959 | 192.168.254.254 | 172.16.1.2 | FTP | Response: 501 Option not understood. |
| 31 | 26.314042 | 172.16.1.2 | 192.168.254.254 | FTP | Request: syst |
| 32 | 26.314493 | 192.168.254.254 | 172.16.1.2 | FTP | Response: 215 UNIX Type: L8 |
| 33 | 26.314595 | 172.16.1.2 | 192.168.254.254 | FTP | Request: site help |
| 34 | 26.315028 | 192.168.254.254 | 172.16.1.2 | FTP | Response: 550 Permission denied. |
| 35 | 26.315113 | 172.16.1.2 | 192.168.254.254 | FTP | Request: PWD |
| 36 | 26.315566 | 192.168.254.254 | 172.16.1.2 | FTP | Response: 257 "/" |
| 37 | 26.352350 | 172.16.1.2 | 192.168.254.254 | FTP | Request: noop |
| 38 | 26.352821 | 192.168.254.254 | 172.16.1.2 | FTP | Response: 200 NOOP ok. |
| 39 | 26.482680 | 172.16.1.2 | 192.168.254.254 | FTP | Request: CWD / |
| 40 | 26.483243 | 192.168.254.254 | 172.16.1.2 | FTP | Response: 250 Directory successfully changed. |
| 41 | 26.484334 | 172.16.1.2 | 192.168.254.254 | FTP | Request: TYPE A |
| 42 | 26.484824 | 192.168.254.254 | 172.16.1.2 | FTP | Response: 200 Switching to ASCII mode. |
| 43 | 26.485292 | 172.16.1.2 | 192.168.254.254 | FTP | Request: PORT 172,16,1,2,4,50 |
| 44 | 26.485800 | 192.168.254.254 | 172.16.1.2 | FTP | Response: 200 PORT command successful. Consider using PASV. |
| 45 | 26.485892 | 172.16.1.2 | 192.168.254.254 | FTP | Request: LIST |
| 46 | 26.486503 | 192.168.254.254 | 172.16.1.2 | TCP | ftp-data > 1074 [SYN] Seq=0 Len=0 MSS=1460 TSV=12998374 TSER=0 WS=2 |
| 47 | 26.486558 | 172.16.1.2 | 192.168.254.254 | TCP | 1074 > ftp-data [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=0 TSV=0 TSER= |
| 48 | 26.486948 | 192.168.254.254 | 172.16.1.2 | TCP | ftp-data > 1074 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=12998375 TSER=0 |
| 49 | 26.487052 | 192.168.254.254 | 172.16.1.2 | FTP | Response: 150 Here comes the directory listing. |
| 50 | 26.487252 | 192.168.254.254 | 172.16.1.2 | FTP-DA | FTP Data: 61 bytes |
| 51 | 26.487267 | 192.168.254.254 | 172.16.1.2 | FTP | Response: 226 Directory send OK. |

**Figura 8: Captura de Wireshark de una sesión FTP con un explorador Web**

3. Vaya a la ventana de Wireshark del medio y expanda el protocolo FTP. FTP se comunica usando códigos, como HTTP.

¿Cuál es la respuesta 220 del servidor FTP?

Response: 200 Welcome to the eagle-server FTP service (nos da la bienvenida)

Cuando el servidor FTP emitió una Respuesta: 331. Especifique la contraseña. ¿Cuál fue la respuesta del explorador Web?
Envia la contraseña

¿Qué número de puerto utiliza el cliente FTP para conectarse al puerto 21 del servidor FTP?
el puerto 1073

Cuando se transfieren datos, o con listados simples de directorios, se abre un nuevo puerto. Esto se llama modo de transferencia. El modo de transferencia puede ser activo o pasivo. En modo activo, el servidor abre una sesión TCP para el cliente FTP y transfiere datos por ese puerto. El número de puerto de origen del servidor FTP es 20 y el número de puerto del cliente FTP es un número mayor a 1023. Si embargo, en el modo pasivo, el cliente abre un nuevo puerto para el servidor para la transferencia de datos. Ambos números de puerto son mayores a 1023.

¿Cuál es el número de puerto de Datos FTP utilizado por el servidor FTP? el puerto 20

4. Abra la captura de Wireshark FTP_Web_Browser_Client y observe la comunicación FTP. Aunque los clientes sean diferentes, los comandos son similares.

**Paso 5: Modos de transferencia FTP activo y pasivo**

Las implicaciones entre los dos modos son muy importantes desde el punto de vista de seguridad de la información. El modo de transferencia establece cómo se configura el puerto de datos.

En el modo de transferencia activo, un cliente inicia una sesión FTP con el servidor del puerto TCP 21 bien conocido. Para transferir datos, el servidor inicia una conexión desde el puerto bien conocido TCP 20 para un puerto alto del cliente, un número de puerto mayor a 1023. Vea la figura 9.

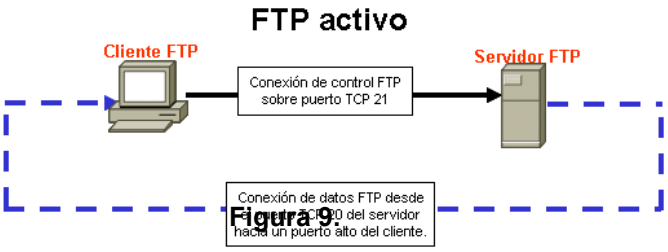



**Figura 9:**

A menos que el firewall del cliente FTP esté configurado para permitir conexiones desde afuera, la transferencia de datos puede fallar. Para establecer conectividad para la transferencia de datos, el cliente FTP debe permitir las conexiones relacionadas al FTP (que implican un filtrado de paquetes con estado) o deshabilitar el bloqueo.

En el modo de transferencia pasivo, un cliente inicia una sesión FTP con el servidor del puerto 21 TCP bien conocido, la misma conexión usada en el modo de transferencia activo. Sin embargo, para transferir datos existen dos cambios importantes. Primero, el cliente inicia la conexión de datos con el servidor. Segundo, los puertos altos se utilizan en ambos extremos de la conexión. Vea la Figura 10.

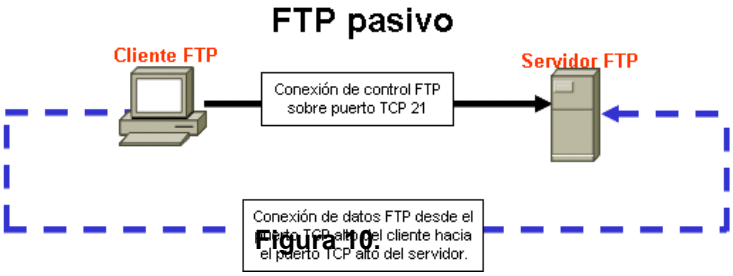



**Figura 10:**

A menos que el servidor FTP esté configurado para permitir una conexión a un puerto alto aleatorio, la transferencia de datos fallará. No todas las aplicaciones del cliente FTP admiten cambios para el modo de transferencia.

### Tarea 4: Reflexión

Los protocolos HTTP y FTP dependen de TCP para comunicarse. TCP administra la conexión entre el cliente y el servidor para asegurar la entrega de datagramas.

Una aplicación de cliente puede ser un explorador Web o una utilidad de línea de comando, pero cada una debe enviar y recibir mensajes que puedan ser interpretados en forma correcta. El protocolo de comunicación se define normalmente en un RFC.

El cliente FTP debe autenticarse al servidor FTP aunque la autenticación esté abierta al mundo. El usuario Anonymous tiene, normalmente, acceso restringido al servidor FTP y no puede cargar archivos.

Una sesión HTTP comienza cuando se realiza una solicitud al servidor HTTP y finaliza cuando el cliente HTTP ha acusado recibo. En cambio, una sesión FTP finaliza cuando el cliente indica que la deja, utilizando el comando **`quit`**.

HTTP utiliza un protocolo simple para comunicarse con el servidor HTTP. El servidor escucha en el puerto 80 para conexiones de clientes. En cambio, FTP utiliza dos protocolos. El servidor FTP escucha en el puerto 21 TCP, como la línea de comandos. Según el modo de transferencia, el servidor o cliente puede iniciar la conexión de datos.

Se puede acceder a los protocolos de capa de aplicación múltiple mediante un explorador Web simple. A pesar de que sólo se examinaron HTTP y FTP, el explorador también admite Telnet y Gopher. El explorador actúa como un cliente para el servidor, enviando solicitudes y procesando respuestas.

### Tarea 5: Desafío

Habilite la captura de Wireshark, utilice un explorador Web para navegar a R2 en http://172.16.255.254/level/7/exec o utilice un cliente Telnet para conectarse a un dispositivo de Cisco, como S1-Central o R2-Central. Observe el comportamiento de HTTP o protocolo Telnet. Emita algunos comandos para observar resultados.

¿Cuál es la similitud de Telnet del protocolo de la capa de aplicación con HTTP y FTP? ¿En qué difiere TELNET?

Se utiliza igual atraves del navegador es decir "protocolo.//url", y difiere con FTP ya que telnet esta

desencriptado como HTTP, y FTP esta encriptado

### Tarea 6: Limpieza

Si se instaló Wireshark en la computadora host del módulo para esta práctica de laboratorio, el instructor querrá que se elimine la aplicación. Para eliminar Wireshark, haga clic en **Inicio > Panel de control > Agregar o quitar programas**. Vaya hacia abajo en la lista, haga clic con el botón derecho del mouse en **Wireshark** y haga clic en **Quitar**.

Si se deben eliminar los archivos descargados desde la computadora host del módulo, elimine todos los archivos recuperados desde el servidor FTP.

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.