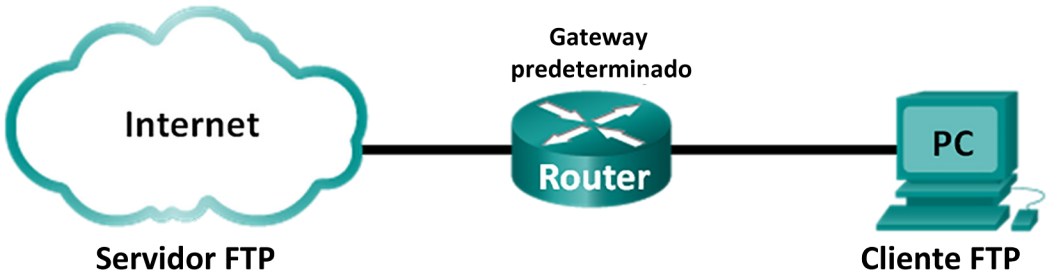
Práctica de laboratorio: Uso de Wireshark para examinar capturas de TCP y UDP

Topología: Parte 1 (FTP)

La parte 1 destacará una captura de TCP de una sesión FTP. Esta topología consta de una PC con acceso a Internet.



Topología: Parte 2 (TFTP)

La parte 2 destacará una captura de UDP de una sesión TFTP. La PC debe tener una conexión Ethernet y una conexión de consola al switch S1.

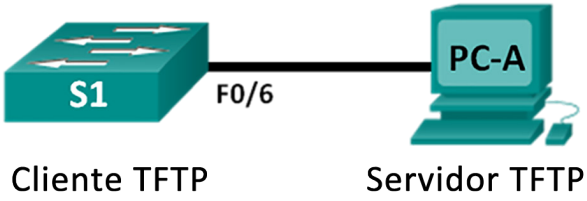


Tabla de direccionamiento (parte 2)

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 1	192.168.1.1	255.255.255.0	N/D
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objetivos

Parte 1: Identificar campos de encabezado y operación TCP mediante una captura de sesión FTP de Wireshark

Parte 2: Identificar campos de encabezado y operación UDP mediante una captura de sesión TFTP de Wireshark

Antecedentes/Escenario

Dos de los protocolos de la capa de transporte de TCP/IP son TCP (definido en RFC 761) y UDP (definido en RFC 768). Los dos protocolos admiten la comunicación de protocolos de capa superior. Por ejemplo, TCP se utiliza para proporcionar soporte de capa de transporte para el protocolo de transferencia de hipertexto (HTTP) y FTP, entre otros. UDP proporciona soporte de capa de transporte para el sistema de nombres de dominio (DNS) y TFTP, entre otros.

© 2018 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Nota: Comprender las partes de los encabezados y de la operación de TCP y UDP es una habilidad fundamental para los ingenieros de red.

En la parte 1 de esta práctica de laboratorio, utilizará la herramienta de código abierto Wireshark para capturar y analizar campos de encabezado del protocolo TCP para las transferencias de archivos FTP entre el equipo host y un servidor FTP anónimo. Para conectarse a un servidor FTP anónimo y descargar un archivo, se emplea la utilidad de línea de comandos de Windows. En la parte 2 de esta práctica de laboratorio, utilizará Wireshark para capturar y analizar campos de encabezado UDP para las transferencias de archivos TFTP entre el equipo host y S1.

Nota: El switch que se utiliza es un Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen lanbasek9). Se pueden utilizar otros switches y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio.

Nota: Asegúrese de que el switch se haya borrado y que no tenga configuraciones de inicio. Si no está seguro, consulte al instructor.

Nota: En la parte 1, se asume que la PC tiene acceso a Internet y no puede realizarse utilizando Netlab. La parte 2 es compatible con Netlab.

Recursos necesarios: Parte 1 (FTP)

1 PC (Windows 7, 8 o 10 con acceso a la petición de ingreso de comando, acceso a Internet y Wireshark instalado)

Recursos necesarios: Parte 2 (TFTP)

- 1 switch (Cisco 2960 con Cisco IOS versión 15.0(2), imagen lanbasek9 o comparable)
- 1 PC (Windows 7, 8 o 10 con Wireshark y un servidor TFTP, como tftpd32, instalados)
- Cable de consola para configurar los dispositivos con Cisco IOS mediante los puertos de consola
- Cable Ethernet, como se muestra en la topología

Parte 1: Identificar campos de encabezado y operación TCP mediante una captura de sesión FTP de Wireshark

En la parte 1, utilizará Wireshark para capturar una sesión FTP e inspeccionar los campos de encabezado de TCP.

Paso 1: Iniciar una captura de Wireshark

a. Cierre todo el tráfico de red innecesario, como el navegador web, para limitar la cantidad de tráfico durante la captura de Wireshark.

b. Inicie la captura de Wireshark.

Paso 2: Descargar el archivo Léame

a. En el símbolo del sistema, introduzca **ftp ftp.cdc.gov**.

b. Conéctese al sitio FTP de los Centros para el Control y la Prevención de Enfermedades (CDC) con el usuario **anonymous** y sin contraseña.

© 2018 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

```
C:\> ftp ftp.cdc.gov
Connected to ftp.cdc.gov.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (ftp.cdc.gov:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
```

c. Localice y descargue el archivo Léame usando el comando **ls** para mostrar los archivos.

```
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection.
.change.dir
.message
pub
Readme
Siteinfo
up.htm
w3c
welcome.msg
226 Transfer complete.
ftp: 75 bytes received in 0.00Seconds 75000.00Kbytes/sec.
```

d. Introduzca el comando **get Readme** para descargar el archivo. Cuando finalice la descarga, introduzca el comando **quit** para salir.

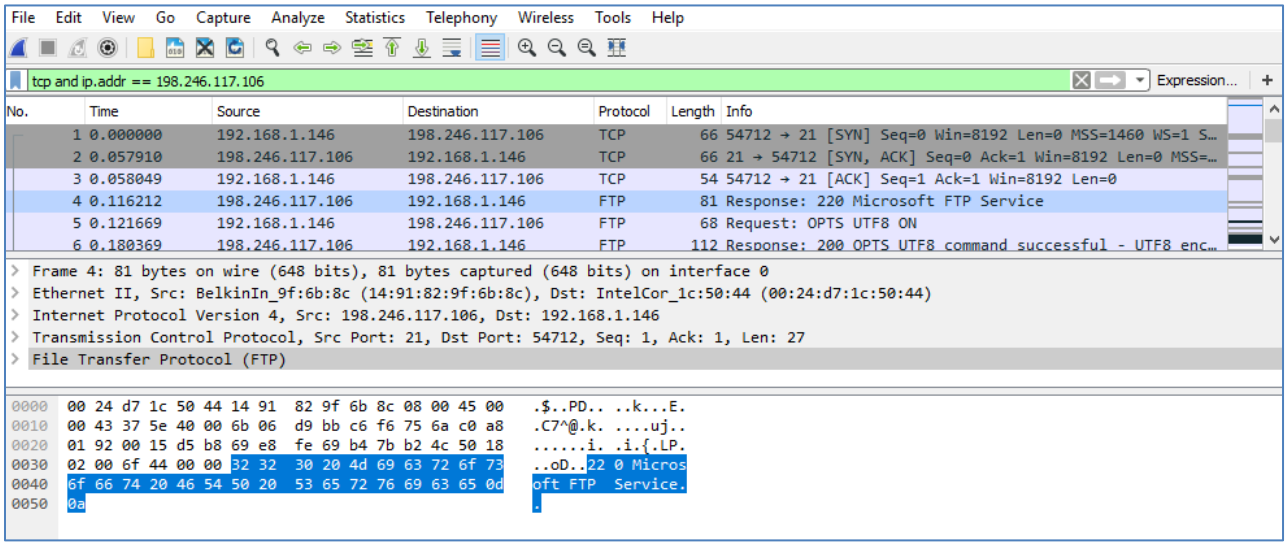
```
ftp> get Readme
200 PORT command successful.
150 Opening ASCII mode data connection.
226 Transfer complete.
ftp: 1428 bytes received in 0.08Seconds 18.08Kbytes/sec.
```

Paso 3: Detener la captura Wireshark

© 2018 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

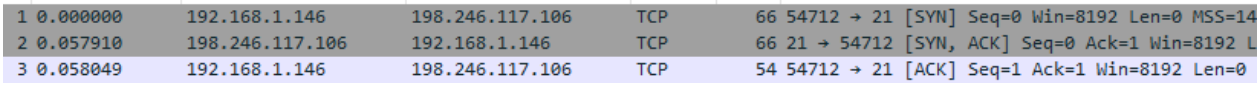
Paso 4: Ver la ventana principal de Wireshark

Wireshark capturó muchos paquetes durante la sesión FTP para ftp.cdc.gov. Para limitar la cantidad de datos para el análisis, escriba **tcp and ip.addr == 198.246.117.106** en el área de entrada **Filter:** (Filtrar:) y presione **Enter** (Introducir). La dirección IP, 198.246.117.106, es la dirección para ftp.cdc.gov en este momento.



Paso 5: Analizar los campos TCP

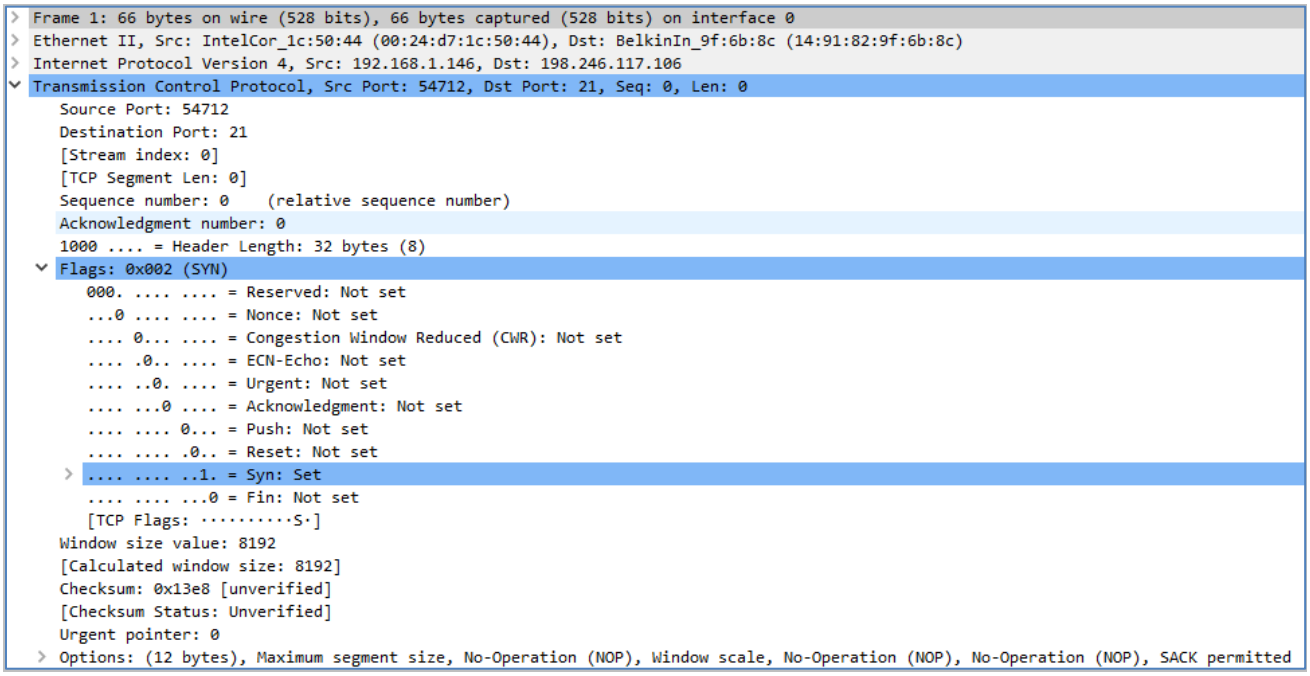
Una vez aplicado el filtro TCP, las primeras tres tramas en el panel de la lista de paquetes (sección superior) muestran el protocolo de la capa de transporte TCP que crea una sesión confiable. La secuencia de [SYN], [SYN, ACK] y [ACK] ilustra el protocolo de enlace de tres vías.

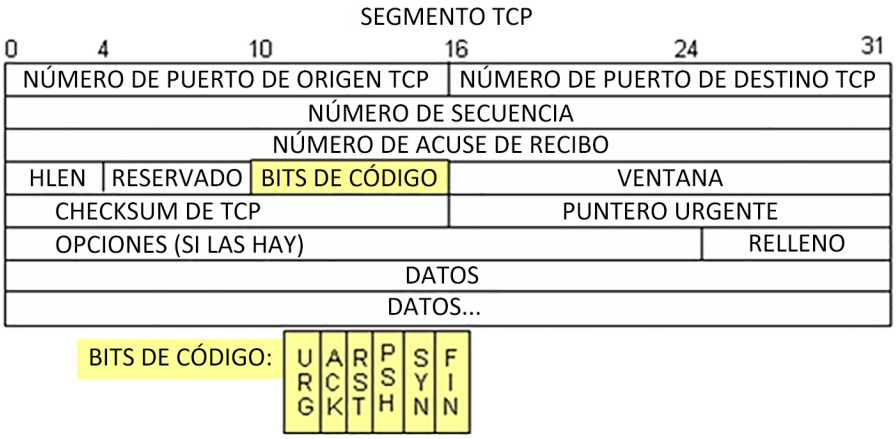


TCP se utiliza en forma continua durante una sesión para controlar la entrega de datagramas, verificar la llegada de datagramas y administrar el tamaño de la ventana. Para cada intercambio de datos entre el cliente FTP y el servidor FTP, se inicia una nueva sesión TCP. Al término de la transferencia de datos, se cierra la sesión TCP. Cuando finaliza la sesión FTP, TCP realiza un cierre y un apagado ordenados.

© 2018 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

En Wireshark, se encuentra disponible información detallada sobre TCP en el panel de detalles del paquete (sección media). Resalte el primer datagrama TCP del equipo host y expanda el datagrama TCP. El datagrama TCP expandido se muestra de manera similar al panel de detalles de paquetes que se muestra a continuación.





La imagen anterior es un diagrama del datagrama TCP. Se proporciona una explicación de cada campo para referencia:

- El **TCP Source Port Number** (Número de puerto de origen TCP) pertenece al host de la sesión TCP que abrió una conexión. Generalmente el valor es un valor aleatorio superior a 1.023.
- El **TCP Destination Port Number** (Número de puerto de destino TCP) se utiliza para identificar el protocolo o la aplicación de capa superior en el sitio remoto. Los valores en el intervalo de 0 a 1023 representan los “puertos bien conocidos” y están asociados a servicios y aplicaciones populares (como se describe en la RFC 1700); por ejemplo, Telnet, FTP y HTTP. La combinación de la dirección IP de origen, el puerto de origen, la dirección IP de destino y el puerto de destino identifica de manera exclusiva la sesión para el remitente y para el destinatario.

© 2018 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Nota: En la siguiente captura de Wireshark, el puerto de destino es 21, que es FTP. Los servidores FTP escuchan las conexiones de cliente FTP en el puerto 21.

- El **Sequence Number** (Número de secuencia) especifica el número del último octeto en un segmento.
- El **Acknowledgment Number** (Número de reconocimiento) especifica el siguiente octeto que espera el destinatario.
- **Code bits** (bits de código) tiene un significado especial en la administración de sesiones y en el tratamiento de los segmentos. Entre los valores interesantes se encuentran:
  - ACK: reconocimiento de la recepción de un segmento.
  - SYN: sincronizar, solo se configura cuando se negocia una nueva sesión TCP durante el protocolo de enlace de tres vías TCP.
  - FIN: finalizar, la solicitud para cerrar la sesión TCP.
- **Window size** (Tamaño de la ventana) es el valor de la ventana deslizante. Determina cuántos octetos pueden enviarse antes de esperar un reconocimiento.
- **Urgent pointer** (Puntero urgente) solo se utiliza con un marcador urgente (URG) cuando el remitente necesita enviar datos urgentes al destinatario.
- En **Options** (Opciones), hay una sola opción actualmente, y se define como el tamaño máximo del segmento TCP (valor opcional).

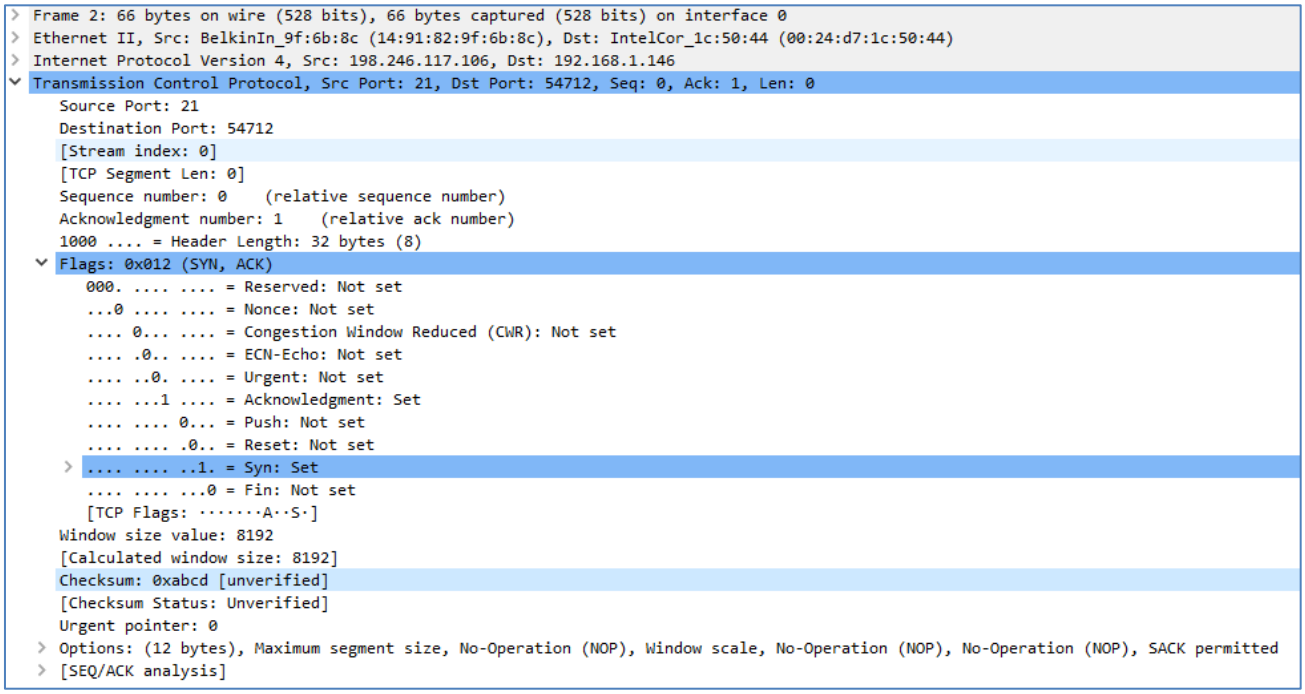
Utilice la captura Wireshark del inicio de la primera sesión TCP (bit SYN fijado en 1) para completar la información acerca del encabezado TCP.

De la PC al servidor CDC (solo el bit de SYN está configurado en 1):

Dirección IP de origen	192.168.1.4
Dirección IP de destino	198.246.117.106
Número de puerto de origen	59221
Número de puerto de destino	21
Número de secuencia	0 (relative sequence number)
Número de reconocimiento	0 (relative sequence number)
Longitud del encabezado	32
Tamaño de la ventana	8192

© 2018 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

En la segunda captura filtrada de Wireshark, el servidor FTP de CDC reconoce la solicitud de la PC. Observe los valores de los bits de SYN y ACK.

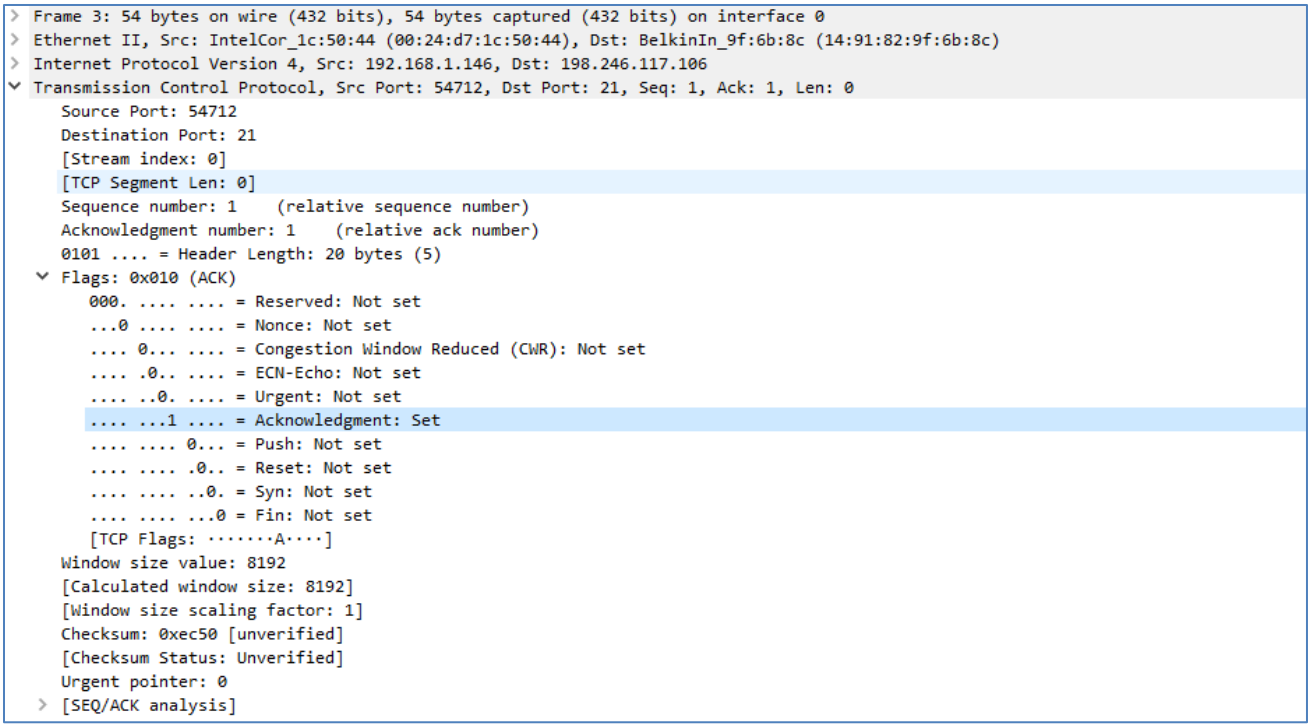


Complete la siguiente información sobre el mensaje de SYN-ACK.

Dirección IP de origen	198.246.117.106
Dirección IP de destino	192.168.1.4
Número de puerto de origen	21
Número de puerto de destino	59221
Número de secuencia	0 (relative sequence number)
Número de reconocimiento	1 (relative ack number)
Longitud del encabezado	32
Tamaño de la ventana	8192

© 2018 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

En la etapa final de la negociación para establecer las comunicaciones, la PC envía un mensaje de reconocimiento al servidor. Observe que solo el bit ACK está establecido en 1, y el número de secuencia se incrementó a 1.



Complete la siguiente información sobre el mensaje de ACK.

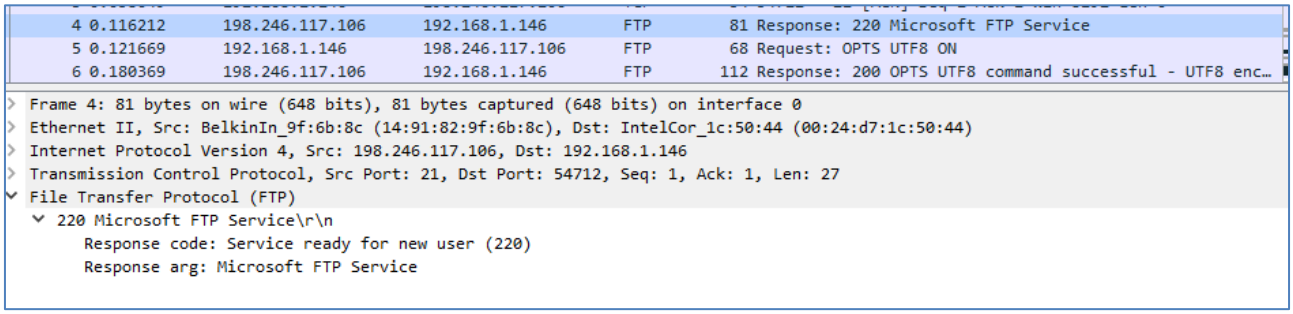
Dirección IP de origen	192.168.1.4
Dirección IP de destino	198.246.117.106
Número de puerto de origen	59221
Número de puerto de destino	21
Número de secuencia	1 (relative sequence number)
Número de reconocimiento	1 (relative ack number)
Longitud del encabezado	20 bytes
Tamaño de la ventana	8192

¿Cuántos otros datagramas TCP contenían un bit SYN?

1, porque fue el primer paquete que envió el host al principio de una sesión TCP.

© 2018 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

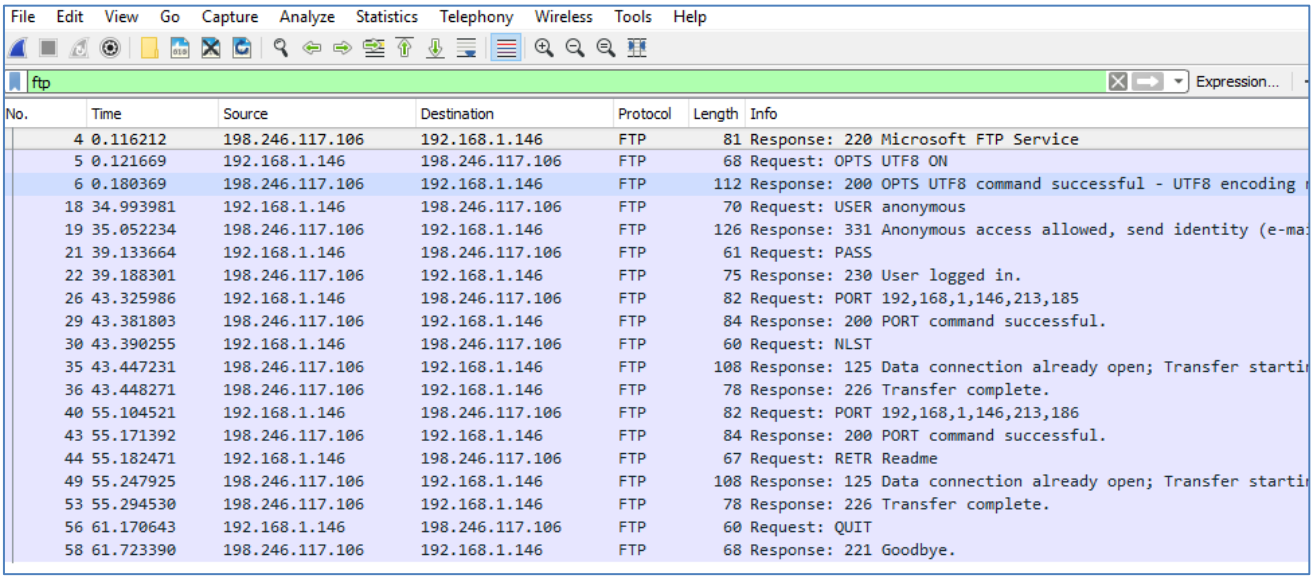
Una vez establecida una sesión TCP, puede haber tráfico FTP entre la PC y el servidor FTP. El cliente y el servidor FTP se comunican entre ellos, sin saber que TCP controla y administra la sesión. Cuando el servidor FTP envía el mensaje *Response: 220* (Respuesta:220) al cliente FTP, la sesión TCP en el cliente FTP envía un reconocimiento a la sesión TCP en el servidor. Esta secuencia es visible en la siguiente captura de Wireshark.



Cuando termina la sesión FTP, el cliente FTP envía un comando para “salir”. El servidor FTP reconoce la terminación de FTP con un mensaje *Response: 221 Goodbye* (Adiós). En este momento, la sesión TCP del servidor FTP envía un datagrama TCP al cliente FTP que anuncia la terminación de la sesión TCP. La sesión TCP del cliente FTP reconoce la recepción del datagrama de terminación y luego envía su propia terminación de sesión TCP. Cuando quien originó la terminación TCP (servidor FTP) recibe una terminación duplicada, se envía un datagrama ACK para reconocer la terminación y se cierra la sesión TCP. Esta secuencia es visible en la captura y el diagrama siguientes.

© 2018 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

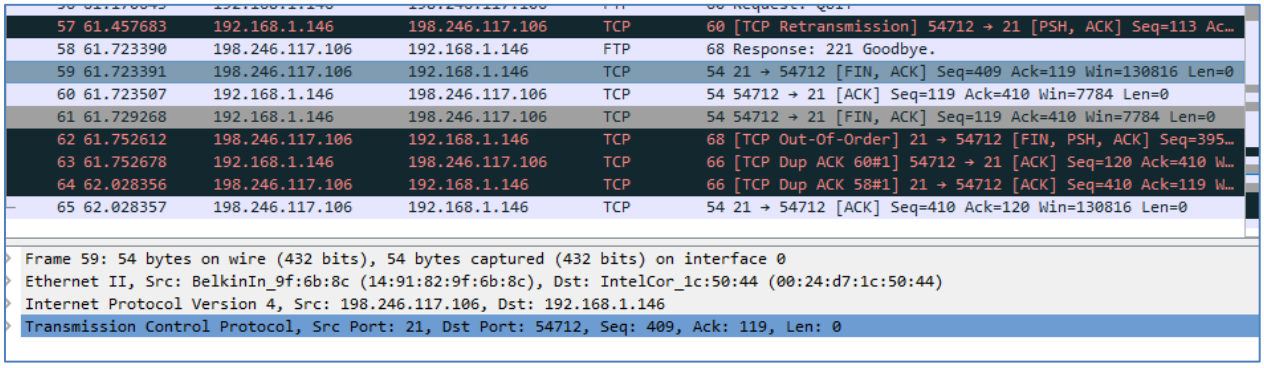
Si se aplica un filtro **ftp**, puede examinarse la secuencia completa del tráfico FTP en Wireshark. Observe la secuencia de los eventos durante esta sesión FTP. Para recuperar el archivo Léame, se utilizó el nombre de usuario **anonymous** (anónimo). Una vez que se completó la transferencia de archivos, el usuario finalizó la sesión FTP.



Vuelva a aplicar el filtro TCP en Wireshark para examinar la terminación de la sesión TCP. Se transmiten cuatro paquetes para la terminación de la sesión TCP. Dado que la conexión TCP es de dúplex completo, cada dirección debe terminar independientemente. Examine las direcciones de origen y destino.

En este ejemplo, el servidor FTP no tiene más datos para enviar en la secuencia. Envía un segmento con el marcador FIN en la trama 59. La PC envía un mensaje ACK para reconocer la recepción del mensaje FIN y terminar la sesión del servidor al cliente en la trama 60.

En la trama 61, la PC envía un mensaje FIN al servidor FTP para terminar la sesión TCP. El servidor FTP responde con un mensaje ACK para reconocer el mensaje FIN de la PC en la trama 65. Ahora, la sesión TCP terminó entre el servidor FTP y la PC.

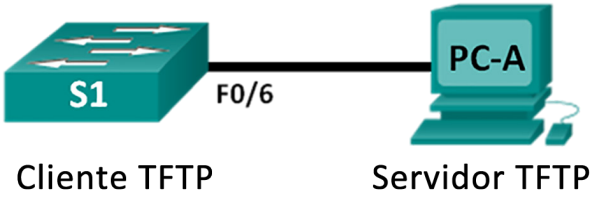


Parte 2: Identificar campos de encabezado y operación UDP mediante una captura de sesión TFTP de Wireshark

En la parte 2, utilizará Wireshark para capturar una sesión TFTP e inspeccionar los campos de encabezado de UDP.

© 2018 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Paso 1: Configurar esta topología física y prepararse para la captura de TFTP



a. Establezca una conexión de consola y Ethernet entre PC-A y S1.

b. Configure manualmente la dirección IP en la PC a 192.168.1.3. No se requiere configurar el gateway predeterminado.

c. Configure el switch. Asigne la dirección IP 192.168.1.1 a VLAN 1. Verifique la conectividad con la PC haciendo ping a 192.168.1.3. Resuelva cualquier problema que se presente.

```
Switch> enable
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# host S1
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.1 255.255.255.0
S1(config-if)# no shut
*Mar  1 00:37:50.166: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Mar  1 0:37:50.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed state to up
S1(config-if)# end
S1# ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/203/1007 ms
```

d. Guarde la configuración en ejecución en la NVRAM.

```
S1# copy run start
```

Paso 2: Preparar el servidor TFTP en la PC

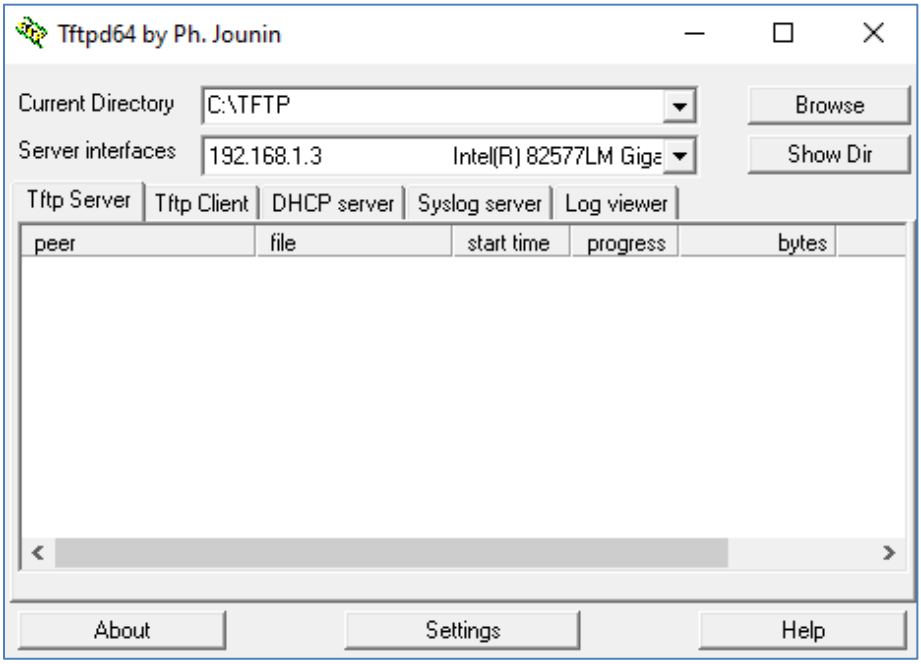
a. Si aún no existe, cree una carpeta en el disco C de la PC con el nombre **TFTP**. Los archivos del switch se copiarán en esta ubicación.

b. Inicie **tftpd32** o **Tftpd64**en la PC.

c. Haga clic en **Browse** (Examinar) y cambie el directorio actual a **C:\TFTP**.

© 2018 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

El servidor TFTP debería verse así:



Observe que, en **Current Directory** (Directorio actual), se indica la interfaz de servidor TFTP (PC-A) con la dirección IP **192.168.1.3**.

d. Pruebe la capacidad de copiar un archivo del switch a la PC con TFTP. Resuelva cualquier problema que se presente.

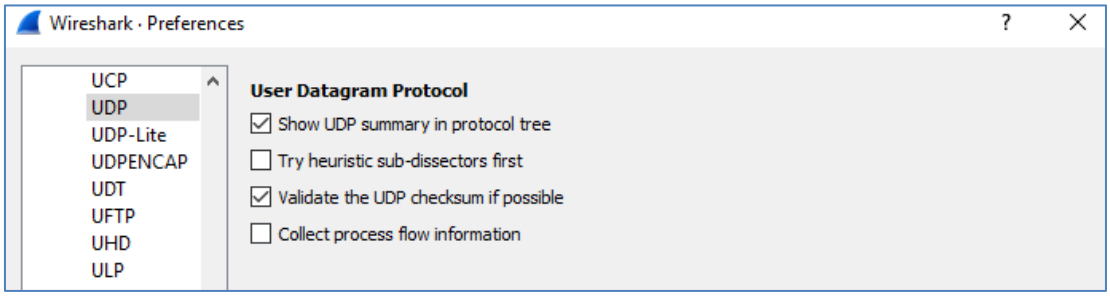
```
S1# copy start tftp
Address or name of remote host []? 192.168.1.3
Destination filename [s1-confg]?
!!
1083 bytes copied in 0,84 secs
```

Si ve que se copió el archivo, está listo para ir al paso siguiente. Si el archivo no se copió, resuelva los problemas que se presenten. Si recibe el mensaje de error **`%Error opening tftp (Permission denied)`** (Error al abrir tftp [permiso denegado]), determine si el firewall está bloqueando el protocolo TFTP y si está copiando a una ubicación donde su nombre de usuario tiene el permiso adecuado, como el escritorio.

© 2018 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Paso 3: Capturar una sesión de TFTP en Wireshark

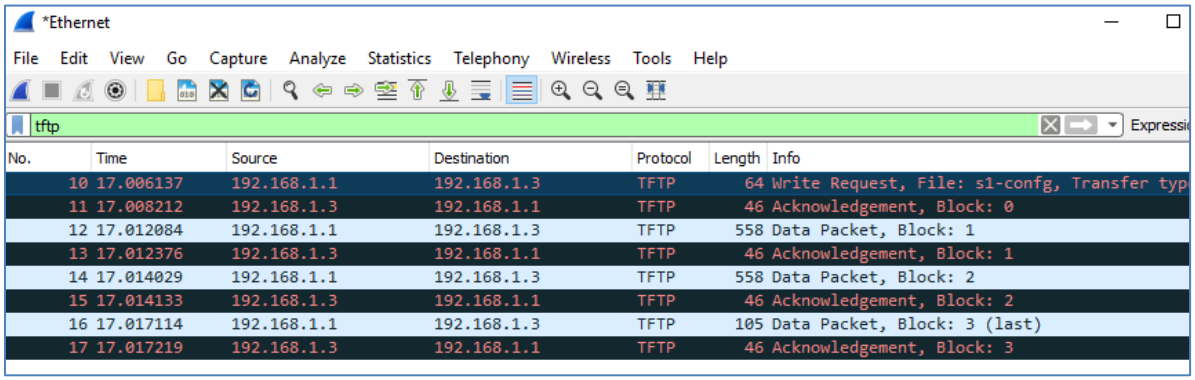
a. Abra Wireshark. En el menú **Edit** (Editar), seleccione **Preferences** (Preferencias) y haga clic en el signo (+) para expandir **Protocols** (Protocolos). Desplácese hacia abajo y seleccione **UDP**. Haga clic en la casilla de verificación **Validate the UDP checksum if possible** (Validar checksum UDP si es posible) y luego en **OK** (Aceptar).



b. Inicie una captura de Wireshark.

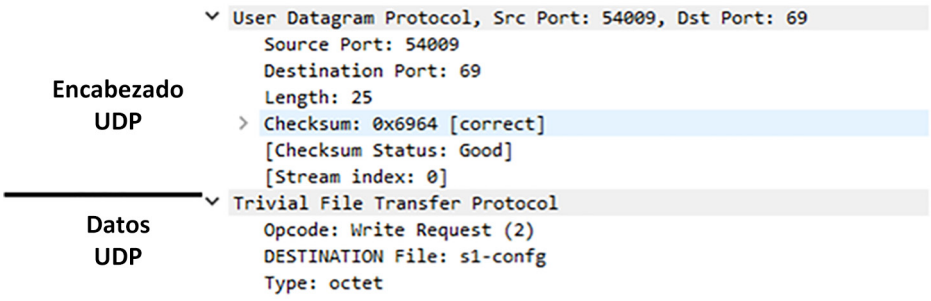
c. Ejecute el comando **copy start tftp** en el switch.

d. Detenga la captura de Wireshark.



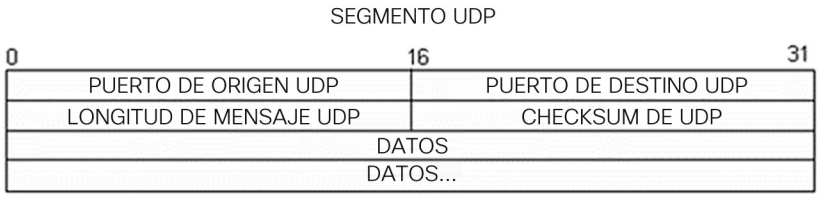
e. Configure el filtro en **tftp**. El resultado debe ser similar al que se muestra más arriba. Esta transferencia de TFTP se utiliza para analizar las operaciones de UDP de la capa de transporte.

El panel de detalles de paquetes de Wireshark muestra información detallada sobre UDP. Resalte el primer datagrama UDP del equipo host y mueva el puntero del mouse al panel de detalles de paquetes. Puede ser necesario ajustar el panel de detalles del paquete y expandir el registro UDP haciendo clic en la casilla de expansión de protocolo. El datagrama UDP expandido debe ser similar al siguiente diagrama.



© 2018 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

En la siguiente ilustración, se muestra un diagrama de datagrama UDP. La información del encabezado está dispersa comparada con la del datagrama TCP. Al igual que TCP, cada datagrama UDP se identifica mediante el puerto de origen de UDP y el puerto de destino UDP.



Utilice la captura de Wireshark del primer datagrama UDP para completar la información acerca del encabezado UDP. El valor de checksum es un valor hexadecimal (base 16) indicado por el código anterior 0x:

Dirección IP de origen	
Dirección IP de destino	
Número de puerto de origen	
Número de puerto de destino	
Longitud del mensaje UDP	
Checksum de UDP	

¿Cómo verifica UDP la integridad del datagrama?

Examine la primera trama que devuelve el servidor tftpd. Complete la información acerca del encabezado UDP:

Dirección IP de origen	
Dirección IP de destino	
Número de puerto de origen	
Número de puerto de destino	
Longitud del mensaje UDP	
Checksum de UDP	

```
User Datagram Protocol, Src Port: 65001, Dst Port: 54009
    Source Port: 65001
    Destination Port: 54009
    Length: 12
  > Checksum: 0x8372 incorrect, should be 0xab99 (maybe caused by "UDP checksum offload"?)
    [Checksum Status: Bad]
    [Stream index: 1]
Trivial File Transfer Protocol
    Opcode: Acknowledgement (4)
    [DESTINATION File: s1-confg]
    Block: 0
```

© 2018 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Observe que el datagrama UDP devuelto tiene un puerto de origen UDP diferente, pero este puerto de origen se utiliza para el resto de la transferencia TFTP. Dado que no hay una conexión confiable, para mantener la transferencia TFTP, sólo se utiliza el puerto de origen usado para comenzar la sesión TFTP.

También observe que el valor de checksum UDP es incorrecto. Lo más probable es que se deba a la descarga de checksum UDP. Para obtener más información acerca del motivo por el cual sucede esto, realice una búsqueda de “UDP checksum offload”.

Reflexión

Esta práctica de laboratorio brindó la oportunidad de analizar las operaciones de protocolo UDP y TCP de sesiones TFTP y FTP capturadas. ¿En qué se diferencia la manera de administrar la comunicación de TCP con respecto a UDP?

Desafío

Debido a que ni FTP ni TFTP son protocolos seguros, todos los datos transferidos se envían en texto no cifrado. Esto incluye cualquier ID de usuario, contraseña o contenido de archivos de texto no cifrado. Si analiza la sesión FTP de capa superior identificará rápidamente el ID de usuario, la contraseña y las contraseñas de archivo de configuración. El examen de datos TFTP de capa superior es más complicado, pero se puede examinar el campo de datos y extraer información de configuración de ID de usuario y contraseña.

Limpieza

Salvo que el instructor indique lo contrario:

1) Elimine los archivos que se copiaron en su PC.
2) Borre las configuraciones de S1.
3) Elimine la dirección IP manual de la PC y restaure la conectividad a Internet.

© 2018 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.