Configuración de Capturas de Paquetes en AireOS WLC

Contenido

Introducción

Este documento describe cómo ejecutar un vaciado de paquetes en un controlador de LAN inalámbrica AireOS (WLC). Este método muestra los paquetes enviados y/o recibidos en el nivel de CPU del WLC en formato hexadecimal, que luego se traduce a un archivo .pcap con Wireshark.

Es útil en los casos en que la comunicación entre un WLC y un servidor de servicio de usuario de acceso telefónico de autenticación remota (RADIUS), un punto de acceso (AP) u otros controladores necesita verificarse de manera rápida con una captura de paquetes en el nivel WLC pero un tramo de puerto es difícil de realizar.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso de la interfaz de línea de comandos (CLI) al WLC, preferiblemente SSH, ya que la salida es más rápida que la consola.
- PC con Wireshark instalado

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC v8.3
- Wireshark v2 o posterior

Nota: Esta función está disponible desde la versión 4 de AireOS.

Limitaciones

El registro de paquetes capturará solamente los paquetes del plano de control bidireccional (CP) a los paquetes del plano de datos (DP) en el WLC. No se capturarán los paquetes que no se envían desde el plano de datos del WLC hacia/desde el plano de control (es decir, el tráfico tunelizado externo para anclar, las caídas de DP-CP, etc.).

Ejemplos de tipos de tráfico hacia/desde el WLC procesado en el CP son:

- TELNET
- SSH
- HTTP
- HTTPS
- SNMP (Protocolo de administración de red simple)
- NTP
- RADIUS
- TACACS+
- Mensajes de movilidad
- control CAPWAP
- NMSP
- TFTP/FTP/SFTP
- Syslog
- IAPP

El tráfico hacia/desde el cliente se procesa en el plano de datos (DP) excepto por: Administración 802.11, 802.1X/EAPOL, ARP, DHCP y autenticación web.

Configurar

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Activar el registro de paquetes en WLC

Paso 1. Inicie sesión en la CLI del WLC.

Debido a la cantidad y velocidad de los registros que muestra esta función, se recomienda iniciar sesión en el WLC por SSH y no por consola.

Paso 2. Aplique una lista de control de acceso (ACL) para limitar el tráfico capturado.

En el ejemplo dado, la captura muestra el tráfico hacia/desde la interfaz de administración del WLC (dirección IP 172.16.0.34) y el servidor RADIUS (172.16.56.153).

```
> debug packet logging acl ip 1 permit 172.16.0.34 172.16.56.153
> debug packet logging acl ip 2 permit 172.16.56.153 172.16.0.34
```

> **Consejo:** Para capturar todo el tráfico hacia/desde el WLC se recomienda aplicar una ACL que descarte el tráfico SSH hacia/desde el host que inició la sesión SSH. Estos son los

comandos que puede utilizar para generar la ACL:

>debug packet logging acl ip 1 deny <WLC-IP> <host-IP> tcp 22 any
>debug packet logging acl ip 2 deny <host-IP> <WLC-IP> tcp any 22
>debug packet logging acl ip 3 permit any

Paso 3. Configure el formato legible por Wireshark.

```
> debug packet logging format text2pcap
```

Paso 4. Habilite la función de registro de paquetes.

Este ejemplo muestra cómo capturar 100 paquetes recibidos/transmitidos (soporta 1 - 65535 paquetes):

```
> debug packet logging enable all 100
```

Paso 5. Registre el resultado en un archivo de texto.

Nota: De forma predeterminada, sólo registra 25 paquetes recibidos con el comando **debug packet logging enable**.

Nota: En lugar de **todo** puede utilizar **rx** o **tx** para capturar solamente el tráfico recibido o transmitido.

Para obtener más información sobre la configuración de la función de registro de paquetes, consulte este enlace:

Guía de Configuración del Controlador Inalámbrico de Cisco, Versión 8.3, Uso de la Función Debug

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Utilice el comando dado para verificar la configuración actual del registro de paquetes.

```
> show debug packet

Status..................................... rx/tx            !!! This means the capture is
active
Number of packets to display..................... 100
Bytes/packet to display.......................... 0
Packet display format............................ text2pcap

   Driver ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
```

```
      [4]: disabled
      [5]: disabled
      [6]: disabled
   Ethernet ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   IP ACL:
      [1]: permit s=172.16.0.34 d=172.16.56.153 any
      [2]: permit s=172.16.56.153 d=172.16.0.34 any
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   EoIP-Ethernet ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   EoIP-IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   LWAPP-Dot11 ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   LWAPP-IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
```

Reproduzca el comportamiento necesario para generar el tráfico.

Aparece una salida similar a esta:

```
rx len=108, encap=unknown, port=2
0000 E0 89 9D 43 EF 40 C8 5B 76 1D AB 51 81 00 09 61 `..Co@H[v.+Q...a
0010 08 00 45 00 00 5A 69 81 00 00 80 01 78 A7 AC 10 ..E..Zi.....x',.
0020 00 38 AC 10 00 22 03 03 55 B3 00 00 00 00 45 00 .8,.."..U3....E.
0030 00 3E 0B 71 00 00 FE 11 58 C3 AC 10 00 22 AC 10 .>.q..~.XC,.."",.
0040 00 38 15 B3 13 88 00 2A 8E DF A8 a1 00 0E 00 0E .8.3...*._(!....
0050 01 00 00 00 00 22 F1 FC 8B E0 18 24 07 00 C4 00 ....."q|.`.$..D.
0060 F4 00 50 1C BF B5 F9 DF EF 59 F7 15 t.P.?5y_oYw.
rx len=58, encap=ip, port=2
0000 E0 89 9D 43 EF 40 C8 5B 76 1D AB 51 81 00 09 61 `..Co@H[v.+Q...a
0010 08 00 45 00 00 28 69 82 40 00 80 06 38 D3 AC 10 ..E..(i.@...8S,.
```

```
0020 00 38 AC 10 00 22 F6 3A 00 16 AF 52 FE F5 1F 0C .8,.."v:../R~u..
0030 40 29 50 10 01 01 52 8A 00 00 @)P...R...
rx len=58, encap=ip, port=2
0000 E0 89 9D 43 EF 40 C8 5B 76 1D AB 51 81 00 09 61 `..Co@H[v.+Q...a
0010 08 00 45 00 00 28 69 83 40 00 80 06 38 D2 AC 10 ..E..(i.@...8R,.
0020 00 38 AC 10 00 22 F6 3A 00 16 AF 52 FE F5 1F 0C .8,.."v:../R~u..
0030 41 59 50 10 01 00 51 5B 00 00 AYP...Q[..
rx len=58, encap=ip, port=2
0000 E0 89 9D 43 EF 40 C8 5B 76 1D AB 51 81 00 09 61 `..Co@H[v.+Q...a
0010 08 00 45 00 00 28 69 84 40 00 80 06 38 D1 AC 10 ..E..(i.@...8Q,.
0020 00 38 AC 10 00 22 F6 3A 00 16 AF 52 FE F5 1F 0C .8,.."v:../R~u..
0030 43 19 50 10 01 05 4F 96 00 00 C.P...O...
```

Eliminar ACL del registro de paquetes

Para inhabilitar los filtros aplicados por las ACL, utilice estos comandos:

```
> debug packet logging acl ip 1 disable
>debug packet logging acl ip 2 disable
```

Deshabilitar el registro de paquetes

Para inhabilitar el registro de paquetes sin quitar las ACL, simplemente utilice este comando:

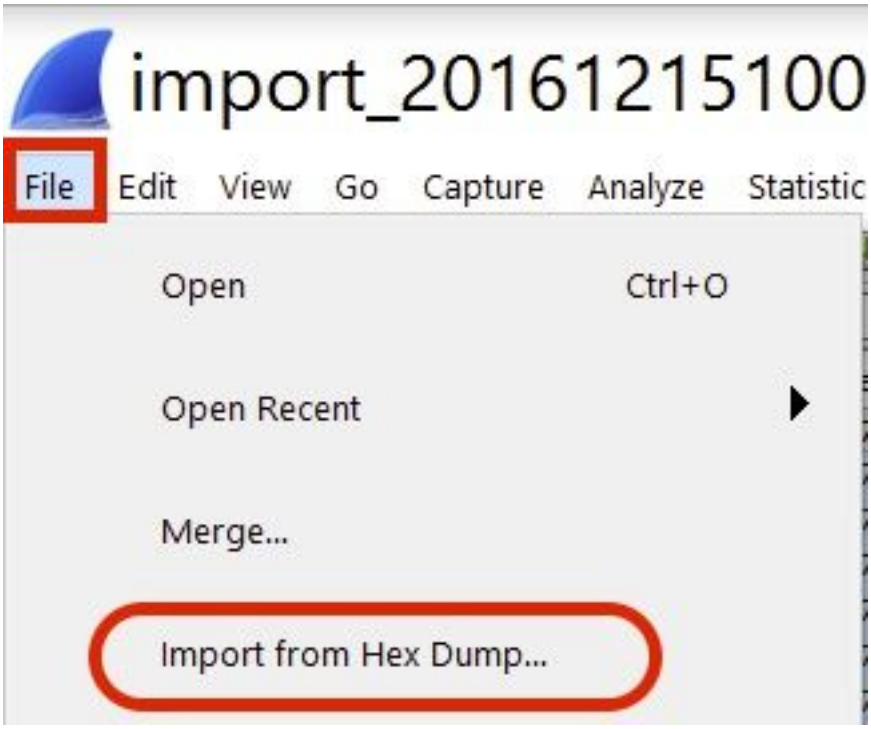
```
> debug packet logging disable
```

Convertir la salida de registro de paquetes en un archivo .pcap

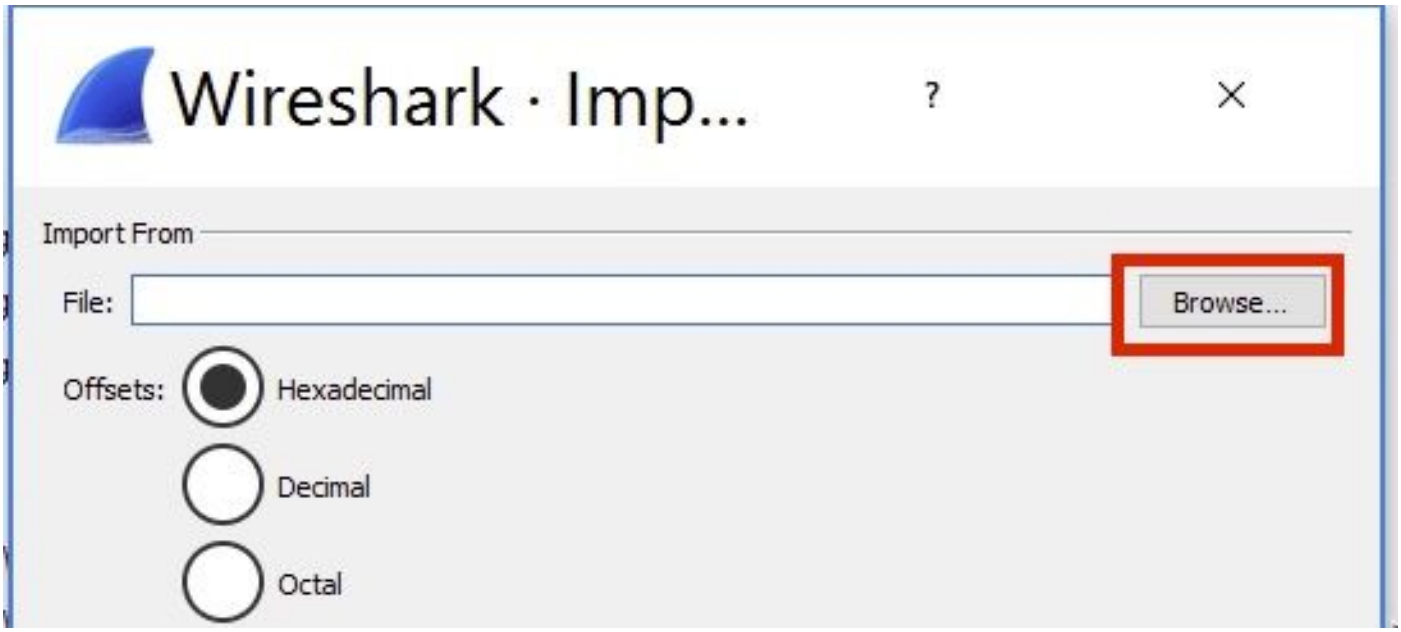
Paso 1. Una vez que el resultado haya terminado, recopile el resultado y guárdelo en un archivo de texto.

Asegúrese de recopilar un registro limpio; de lo contrario, Wireshark podría mostrar los paquetes dañados.

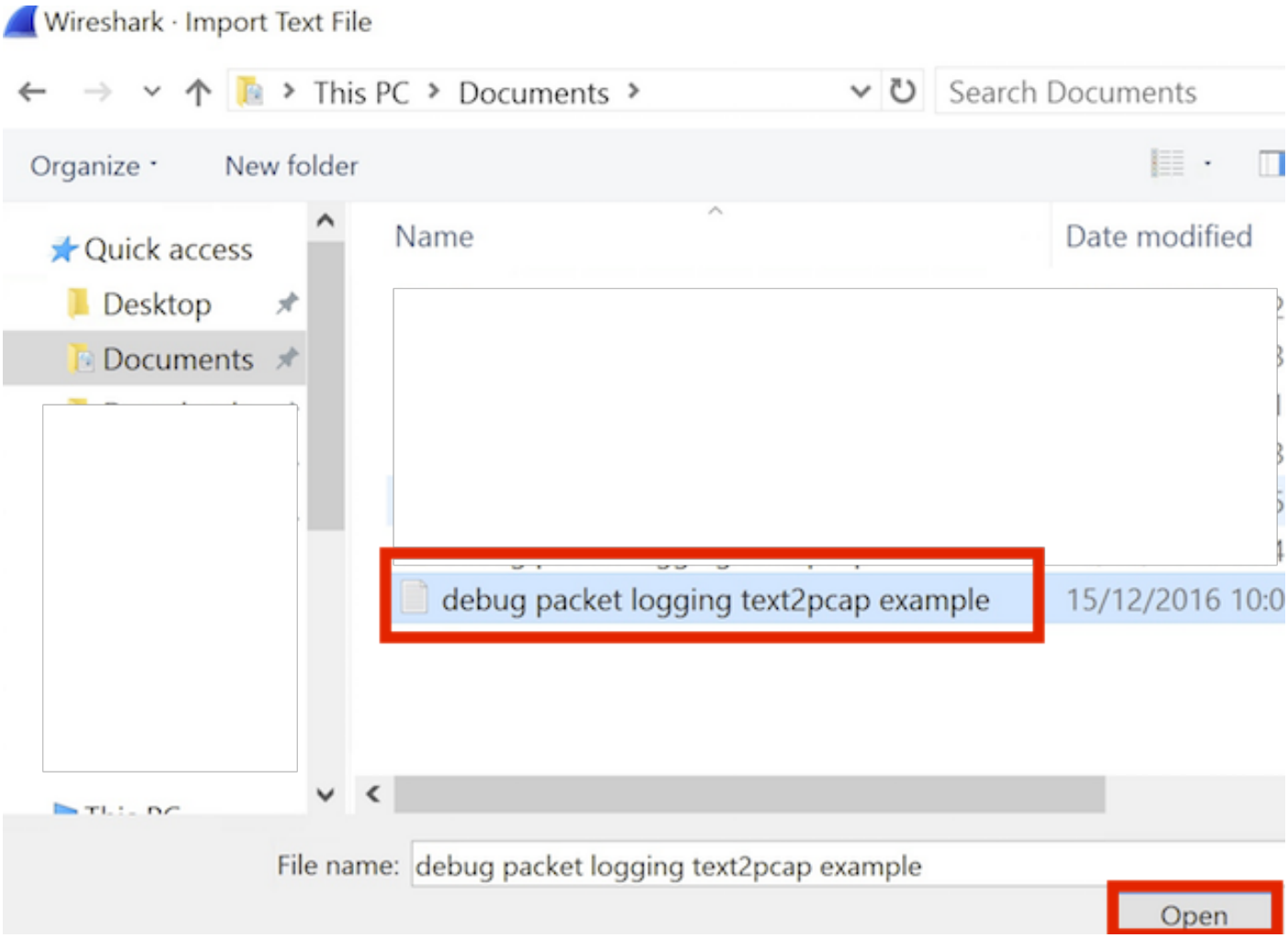
Paso 2. Abra Wireshark y navegue hasta **Archivo>Importar de volcado hexadecimal...**



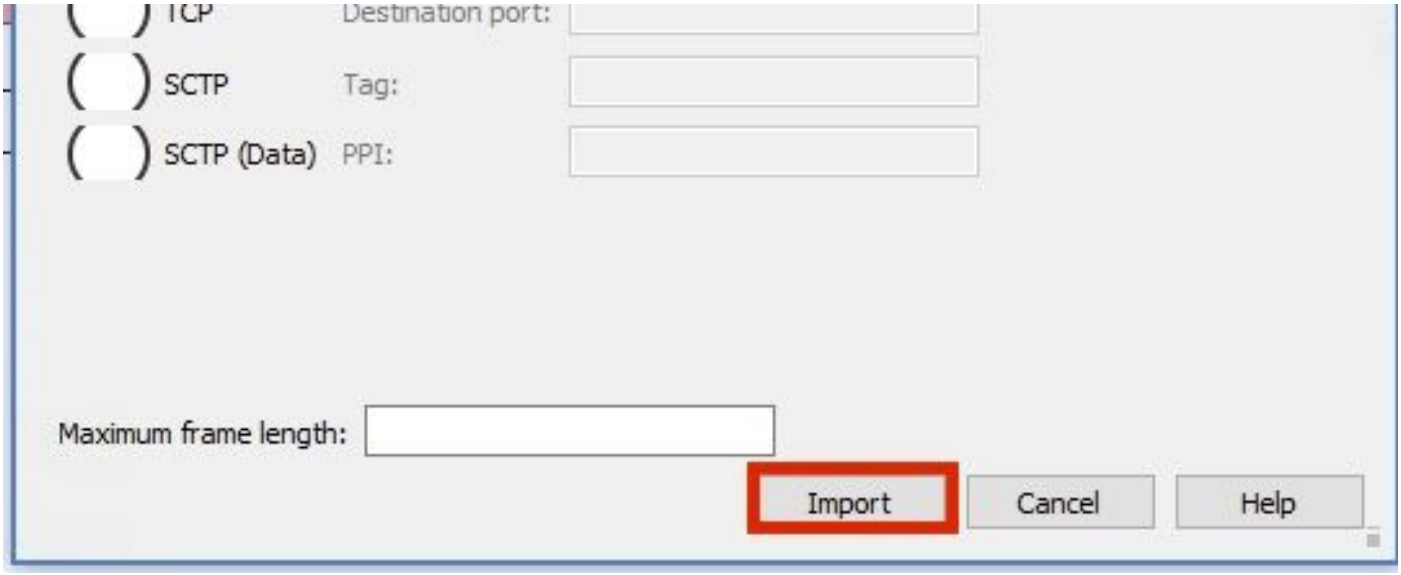
Paso 3. Haga clic en **Examinar.**



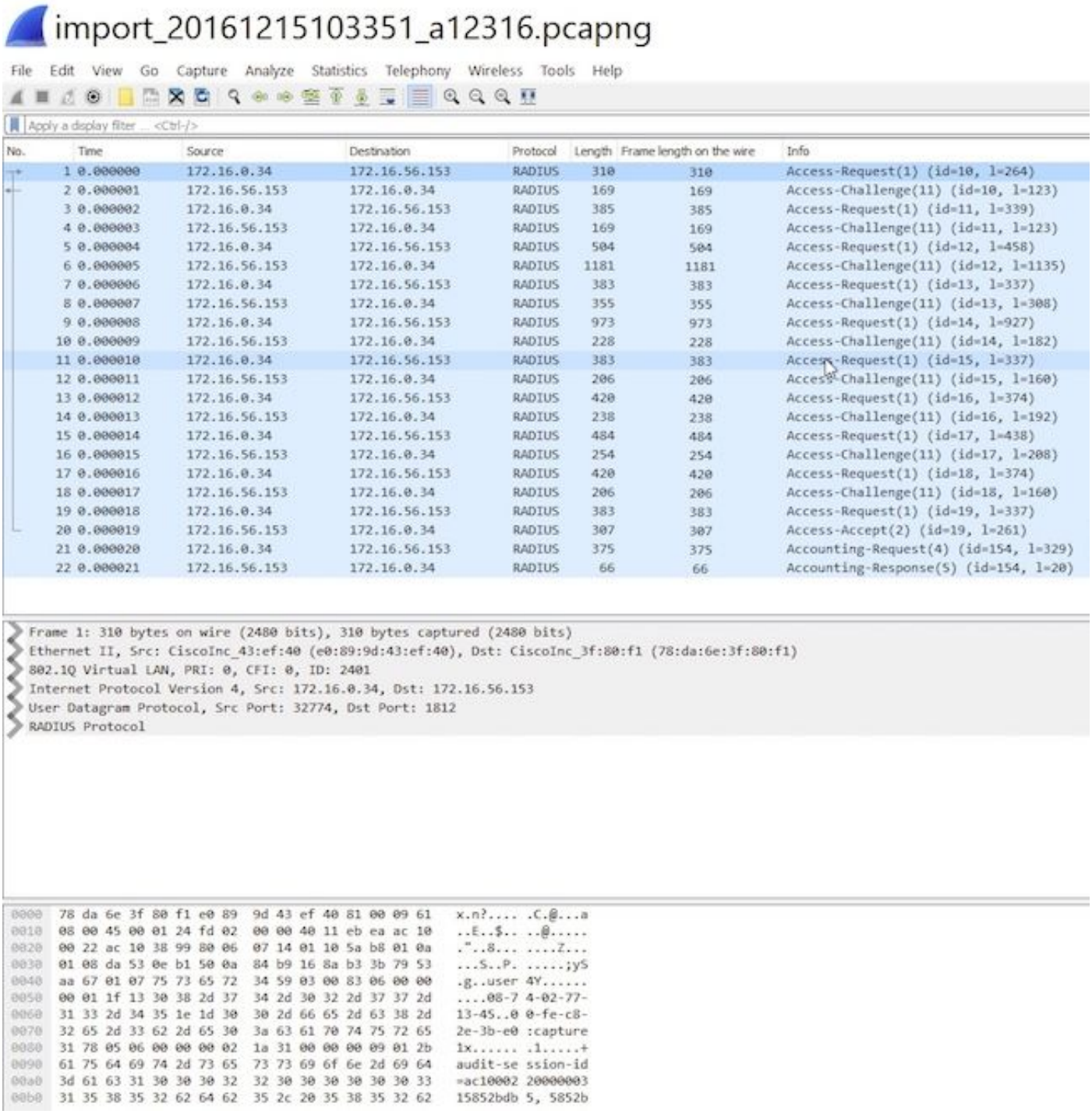
Paso 4. Seleccione el archivo de texto en el que guardó la salida de registro de paquetes.



Paso 5. Haga clic en **Importar.**



Wireshark muestra el archivo como .pcap.



Nota: Tenga en cuenta que las marcas de tiempo no son precisas ni el tiempo delta entre las tramas.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Volcado de paquetes AP
- Aspectos básicos de la manipulación inalámbrica 802.11
- Soporte Técnico y Documentación - Cisco Systems