Configurar capturas de pacotes no AireOS WLC

Contents

Introduction

Este documento descreve como executar um despejo de pacote em um AireOS Wireless LAN Controller(WLC). Esse método exibe os pacotes enviados e/ou recebidos no nível da CPU da WLC em formato hexadecimal, que são convertidos em um arquivo .pcap com o Wireshark.

Éútil nos casos em que a comunicação entre uma WLC e um servidor RADIUS (Remote Authentication Dial-In User Service), um AP (Access Point, ponto de acesso) ou outros controladores precisa ser verificada de forma rápida com uma captura de pacote no nível da WLC, mas é difícil realizar um intervalo de portas.

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso à Interface de Linha de Comando (CLI - Command Line Interface) para a WLC, preferencialmente SSH, já que a saída é mais rápida que o console.
- PC com Wireshark instalado

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- WLC v8.3
- Wireshark v2 ou posterior

Observação: este recurso está disponível desde a versão 4 do AireOS.

Limitações

O registro de pacotes capturará somente pacotes de plano de controle bidirecional (CP) para plano de dados (DP) na WLC. Os pacotes que não são enviados do plano de dados da WLC

para/do plano de controle (ou seja, tráfego de túnel de âncora, descartes de DP-CP e assim por diante) não serão capturados.

Exemplos de tipos de tráfego de/para a WLC processada no CP são:

- Telnet
- SSH
- HTTP
- HTTPS
- SNMP
- NTP
- RADIUS
- TACACS+
- Mensagens de mobilidade
- controle CAPWAP
- NMSP
- TFTP/FTP/SFTP
- Syslog
- IAPP

O tráfego de/para o cliente é processado no plano de dados (DP), exceto: Gerenciamento 802.11, 802.1X/EAPOL, ARP, DHCP e Autenticação da 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Ativar o registro de pacotes na WLC

Etapa 1. Faça login na CLI da WLC.

Devido à quantidade e velocidade de registros que este recurso exibe, é recomendável fazer login na WLC pelo SSH e não pelo console.

Etapa 2. Aplique uma ACL (Access Control List, lista de controle de acesso) para limitar qual tráfego é capturado.

No exemplo fornecido, a captura mostra o tráfego de/para a interface de gerenciamento da WLC (endereço IP 172.16.0.34) e o 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
```

> **Tip**: Para capturar todo o tráfego de/para a WLC, é recomendável aplicar uma ACL que descarta o tráfego SSH de/para o host que iniciou a sessão SSH. Estes são os comandos que você pode usar para criar a 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 any

Etapa 3. Configure o formato legível pelo Wireshark.

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

Etapa 4. Ativar recurso de registro de pacotes.

Este exemplo mostra como capturar 100 pacotes recebidos/transmitidos (ele suporta 1 - 65535 pacotes):

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

Etapa 5. Registre a saída em um arquivo de texto.

Note: Por padrão, ele registra apenas 25 pacotes recebidos com o comando **debug packet logging enable**.

Note: Em vez de **tudo,** você pode usar **rx** ou **tx** para capturar apenas o tráfego recebido ou transmitido.

Para obter mais detalhes sobre como configurar o recurso de registro de pacotes, consulte este link:

Guia de configuração do Cisco Wireless Controller, Versão 8.3, usando o recurso de depuração

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Use o comando fornecido para verificar a configuração atual do registro de pacotes.

```
> 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
```

Reproduza o comportamento necessário para gerar o tráfego.

Uma saída semelhante a esta é exibida:

```
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...
```

Remover ACLs do registro de pacotes

Para desabilitar os filtros aplicados pelas ACLs, use estes comandos:

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

Desativar registro de pacotes

Para desabilitar o registro de pacotes sem remover as ACLs, basta usar este comando:

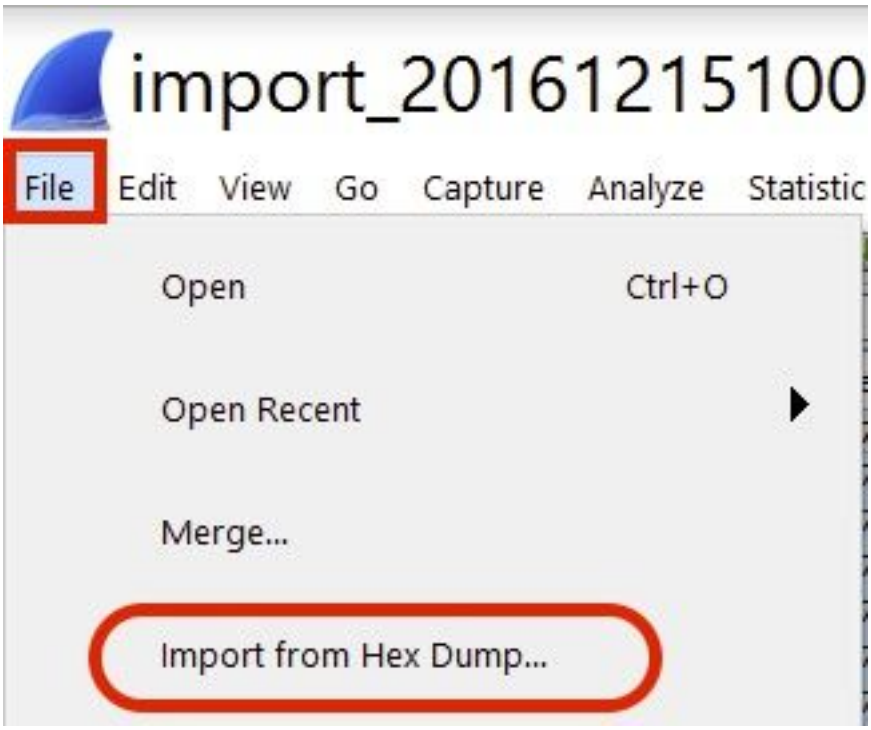
```
> debug packet logging disable
```

Converta a saída de registro de pacote em um arquivo .pcap

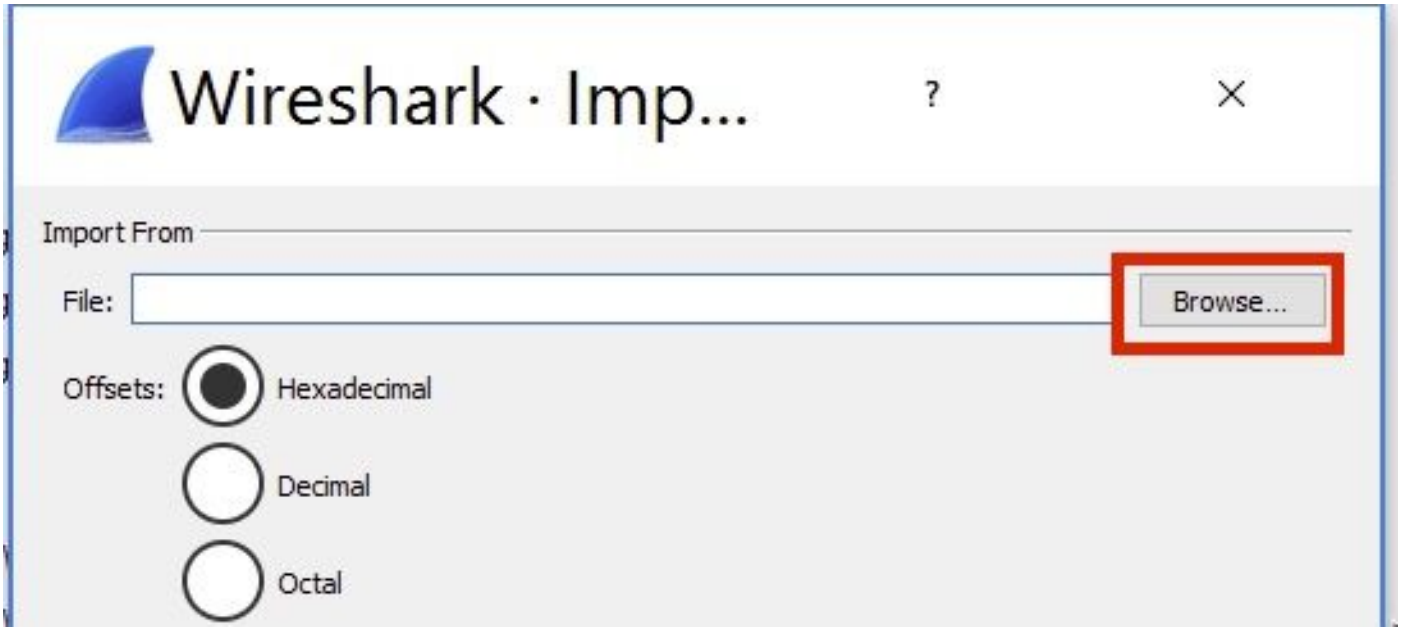
Etapa 1. Quando a saída terminar, colete-a e salve-a em um arquivo de texto.

Certifique-se de coletar um log limpo, caso contrário o Wireshark poderá mostrar pacotes corrompidos.

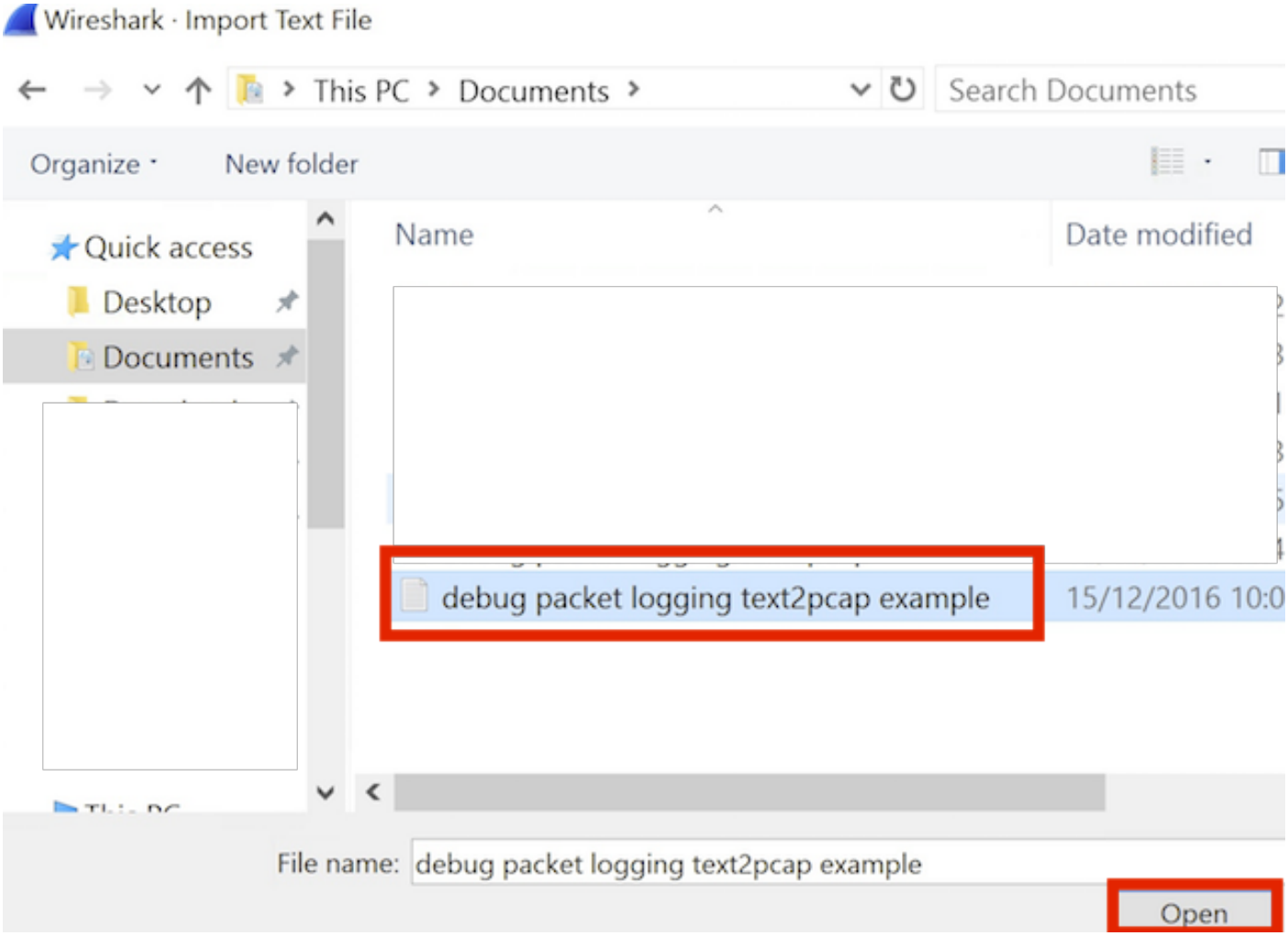
Etapa 2. Abra o Wireshark e navegue para **Arquivo>Importar de despejo hexadecimal...**



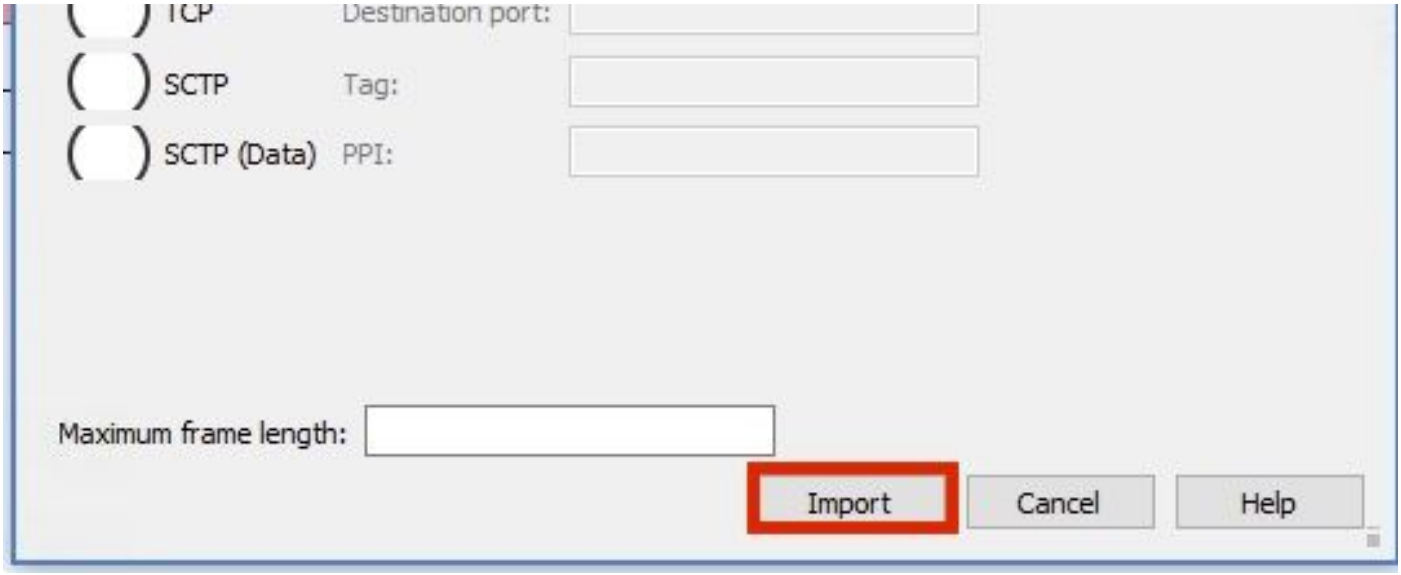
Etapa 3. Clique em **Procurar.**



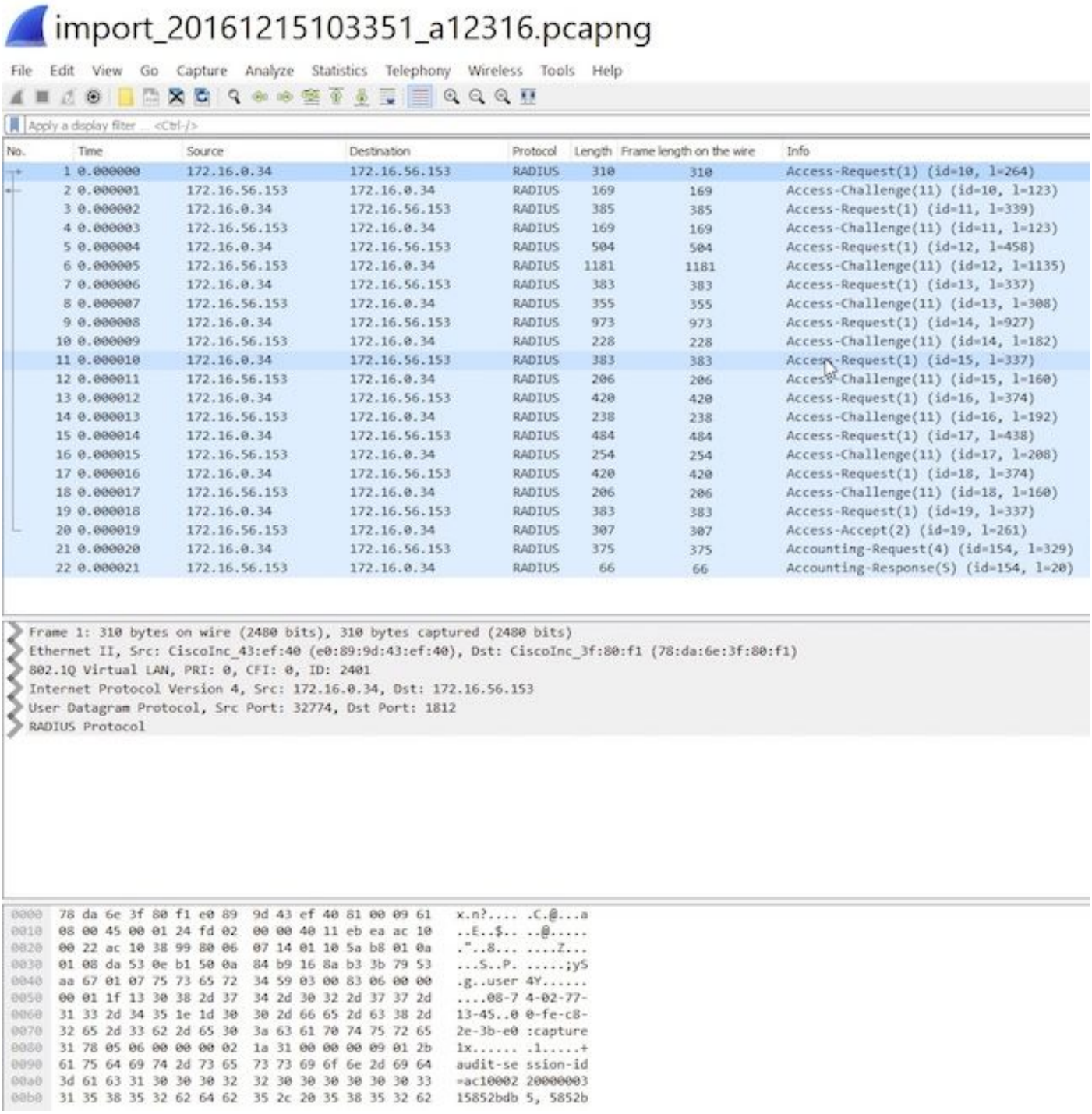
Etapa 4. Selecione o arquivo de texto em que você salvou a saída de registro do pacote.



Etapa 5. Clique em **Importar.**



O Wireshark mostra o arquivo como .pcap.



Note: Esteja ciente de que os datadores não são precisos nem o tempo delta entre os quadros.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Despejo de pacote AP
- Fundamentos do 802.11 Wireless Sniffing

- Suporte Técnico e Documentação - Cisco Systems