

Configurar capturas de pacote de informação em AireOS WLC

Índice

[Introdução](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Limitações](#)

[Configurar](#)

[Permita o pacote que entra o WLC](#)

[Verificar](#)

[Converta saídas de registro do pacote a um arquivo .pcap](#)

[Troubleshooting](#)

Introdução

Este original descreve como executar uma descarga do pacote em um Wireless LAN Controller(WLC) de AireOS. Este método indica os pacotes enviados e/ou recebido a nível CPU do WLC encantar dentro o formato, que seja traduzido então a um arquivo .pcap com o Wireshark.

É útil nos casos onde uma comunicação entre um WLC e um server do Remote Authentication Dial-In User Service (RADIUS), um Access Point (AP) ou outros controladores precisa de ser verificada em uma maneira rápida com uma captura de pacote de informação a nível WLC mas um porta-período é duro de executar.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso do comando line interface(cli) ao WLC, preferivelmente SSH desde que a saída é mais rápida do que o console.
- O PC com Wireshark instalou

Componentes Utilizados

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

- WLC v8.3
- Wireshark v2 ou mais tarde

Note: Esta característica está disponível desde a versão 4 de AireOS.

Limitações

O registro do pacote capturará somente o plano bidirecional do controle (CP) aos pacotes do plano dos dados (DP) no WLC. Aqueles pacotes que não são enviados dos dados WLC aplanam para/desde o plano do controle (isto é estrangeiro para ancorar e assim por diante o tráfego em túnel, as gotas DP-CP) não serão capturados.

Os exemplos dos tipos de tráfego para/desde o WLC processados no CP são:

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

O tráfego para/desde o cliente é processado no plano dos dados (DP) à exceção de: Gerenciamento do 802.11, 802.1X/EAPOL, ARP, DHCP e autenticação da Web.

Configurar

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Permita o pacote que entra o WLC

Etapa 1. Início de uma sessão ao CLI do WLC.

Devido à quantidade e à velocidade dos logs que estas exibições de recursos é recomendado entrar ao WLC pelo SSH e não pelo console.

Etapa 2. Aplique um Access Control List (ACL) para limitar que tráfego é capturado.

No exemplo dado a captação mostra o tráfego para/desde a interface de gerenciamento do 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
```

Dica: Para capturar todo o tráfego para/desde o WLC recomenda-se aplicar um ACL que

rejeite o tráfego SSH para/desde o host que iniciou a sessão SSH. Estes são os comandos que você pode usar para construir o ACL:

```
>debugar o pacote que registra acl IP 1 negam o <host-IP> tcp 22 <WLC-IP>
>debugar o pacote que registra acl IP 2 negam ao <host-IP> <WLC-IP> tcp quaisquer 22
>debugar o pacote registrando a licença acl IP 3 alguma
```

Etapa 3. Configurar o formato legível por Wireshark.

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

Etapa 4. Permita recursos de registro do pacote.

Este exemplo mostra como capturar 100 recebidos/pacotes transmitido (apoiar 1 - 65535 pacotes):

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

Nota: À revelia, registra somente 25 pacotes recebidos com o comando debug o **registro do pacote que permite**.

Note: Em vez de **tudo** você pode usar o **RX** ou o **TX** para capturar tráfego somente recebido ou transmitido.

Para uns detalhes mais adicionais sobre configurar recursos de registro do pacote consulte este link:

[Guia de configuração de controle do Cisco Wireless, liberação 8.3, usando a facilidade debugar](#)

Verificar

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

Use o comando dado verificar a configuração atual do registro do pacote.

```
> 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 similar a esta aparece:

```
> 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

```

Remove os ACL do registro do pacote

A fim desabilitar os filtros aplicados pelos ACL use estes comandos:

```
> 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

```

Desabilite o registro do pacote

A fim desabilitar o pacote que registra sem remover os ACL use simplesmente este comando:

```
> 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

```

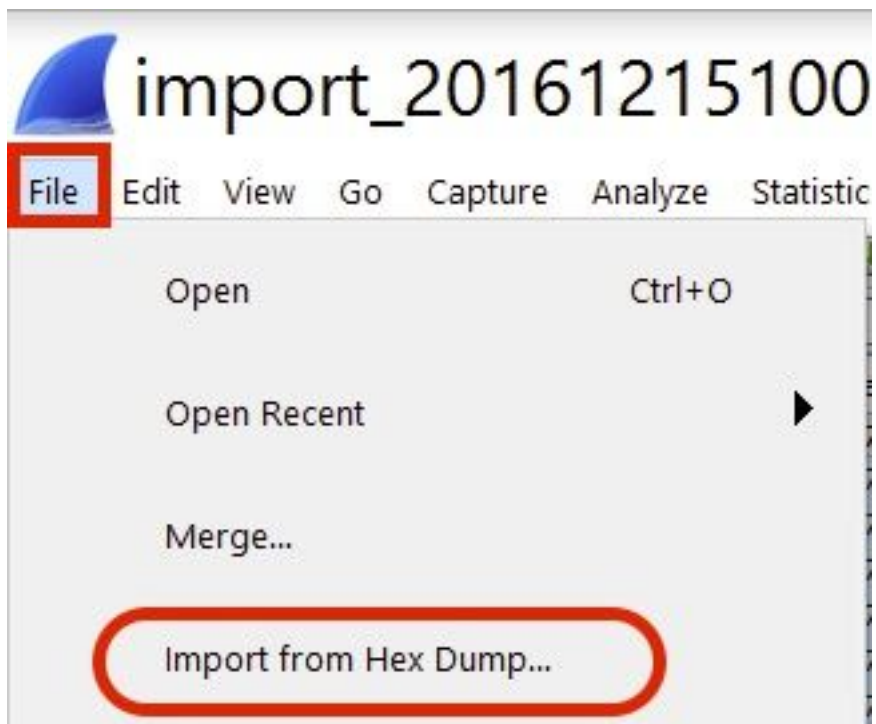
```
[4]: disabled
[5]: disabled
[6]: disabled
Ethernet ACL:
[1]: disabled
[2]: disabled
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled
IP ACL:
[1]: permit s=172.16.0.34 d=172.16.56.153 any
[2]: permit s=172.16.56.153 d=172.16.0.34 any
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled
EoIP-Ethernet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

Converta saídas de registro do pacote a um arquivo .pcap

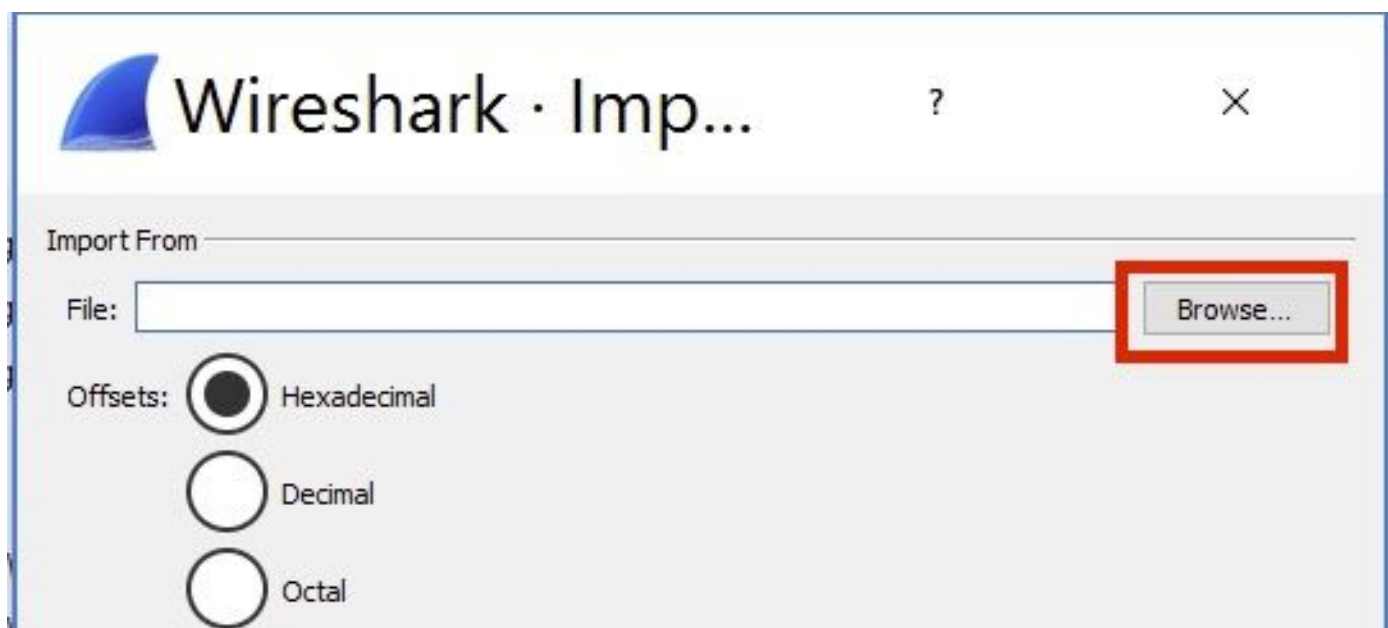
Etapa 1. Uma vez que a saída termina, recolha-a e salvar à um arquivo de texto.

Assegure que você recolhe um log limpo, se não Wireshark pôde mostrar pacotes corrupto.

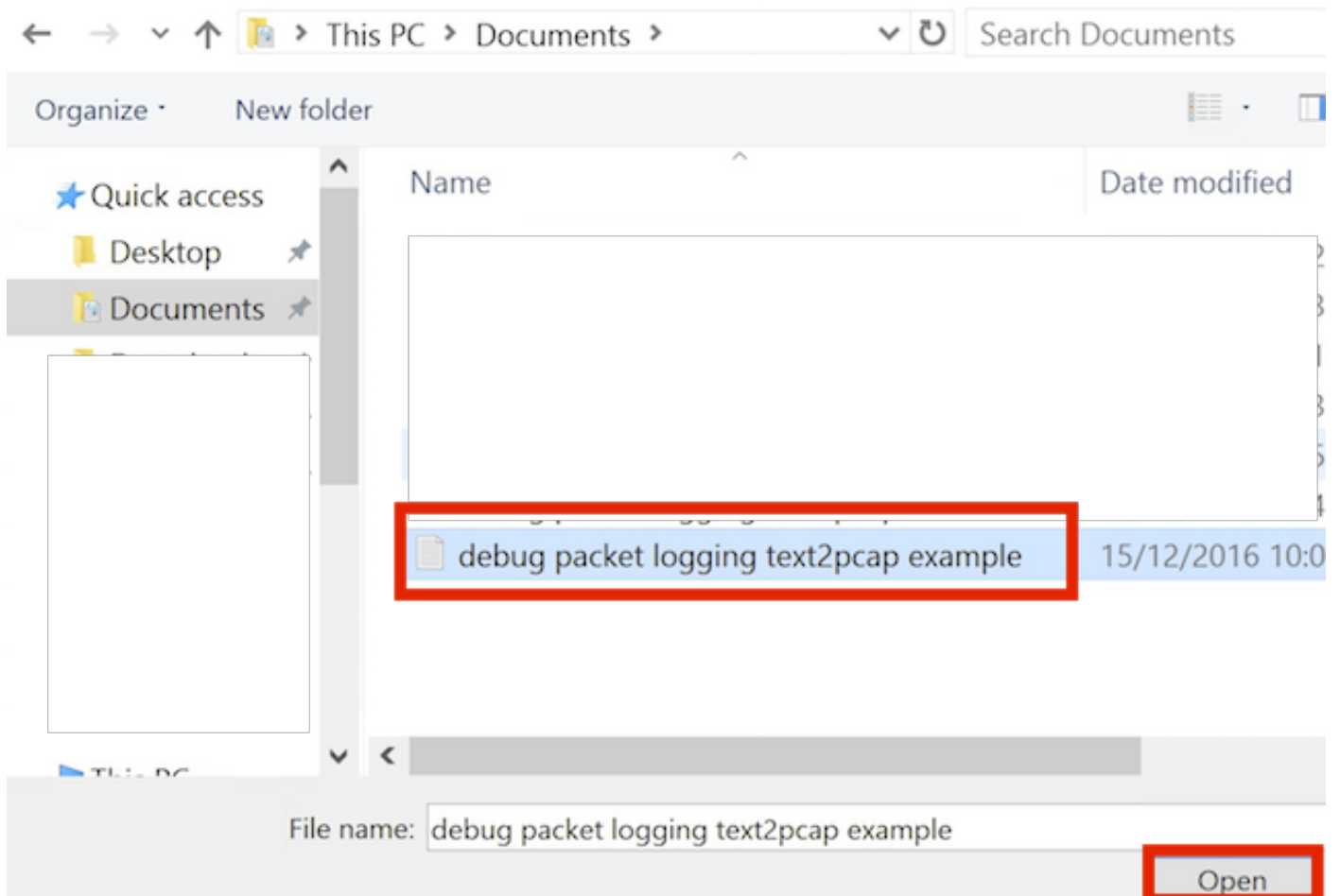
Etapa 2. Abra Wireshark e navegue para arquivar o >Import da cópia parcial da memória de HEX...



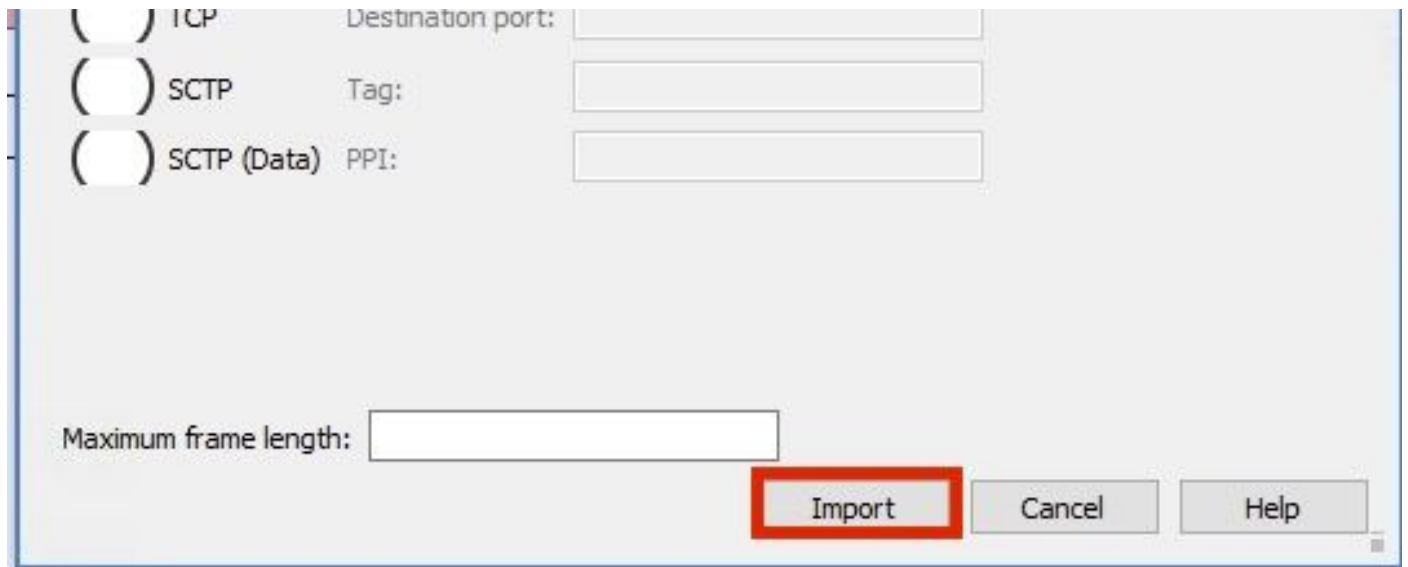
Etapa 3. O clique **consulta**.



Etapa 4. Selecione o arquivo de texto onde você salvar as saídas de registro do pacote.



Etapa 5. **Importação do clique.**



Wireshark mostra o arquivo como .pcap.

import_20161215103351_a12316.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Frame length on the wire	Info
1	0.000000	172.16.0.34	172.16.56.153	RADIUS	310	310	Access-Request(1) (id=10, l=264)
2	0.000001	172.16.56.153	172.16.0.34	RADIUS	169	169	Access-Challenge(11) (id=10, l=123)
3	0.000002	172.16.0.34	172.16.56.153	RADIUS	385	385	Access-Request(1) (id=11, l=339)
4	0.000003	172.16.56.153	172.16.0.34	RADIUS	169	169	Access-Challenge(11) (id=11, l=123)
5	0.000004	172.16.0.34	172.16.56.153	RADIUS	504	504	Access-Request(1) (id=12, l=458)
6	0.000005	172.16.56.153	172.16.0.34	RADIUS	1181	1181	Access-Challenge(11) (id=12, l=1135)
7	0.000006	172.16.0.34	172.16.56.153	RADIUS	383	383	Access-Request(1) (id=13, l=337)
8	0.000007	172.16.56.153	172.16.0.34	RADIUS	355	355	Access-Challenge(11) (id=13, l=308)
9	0.000008	172.16.0.34	172.16.56.153	RADIUS	973	973	Access-Request(1) (id=14, l=927)
10	0.000009	172.16.56.153	172.16.0.34	RADIUS	228	228	Access-Challenge(11) (id=14, l=182)
11	0.000010	172.16.0.34	172.16.56.153	RADIUS	383	383	Access-Request(1) (id=15, l=337)
12	0.000011	172.16.56.153	172.16.0.34	RADIUS	206	206	Access-Challenge(11) (id=15, l=160)
13	0.000012	172.16.0.34	172.16.56.153	RADIUS	420	420	Access-Request(1) (id=16, l=374)
14	0.000013	172.16.56.153	172.16.0.34	RADIUS	238	238	Access-Challenge(11) (id=16, l=192)
15	0.000014	172.16.0.34	172.16.56.153	RADIUS	484	484	Access-Request(1) (id=17, l=438)
16	0.000015	172.16.56.153	172.16.0.34	RADIUS	254	254	Access-Challenge(11) (id=17, l=208)
17	0.000016	172.16.0.34	172.16.56.153	RADIUS	420	420	Access-Request(1) (id=18, l=374)
18	0.000017	172.16.56.153	172.16.0.34	RADIUS	206	206	Access-Challenge(11) (id=18, l=160)
19	0.000018	172.16.0.34	172.16.56.153	RADIUS	383	383	Access-Request(1) (id=19, l=337)
20	0.000019	172.16.56.153	172.16.0.34	RADIUS	307	307	Access-Accept(2) (id=19, l=261)
21	0.000020	172.16.0.34	172.16.56.153	RADIUS	375	375	Accounting-Request(4) (id=154, l=329)
22	0.000021	172.16.56.153	172.16.0.34	RADIUS	66	66	Accounting-Response(5) (id=154, l=20)

Frame 1: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits)
Ethernet II, Src: CiscoInc_43:ef:40 (e0:89:9d:43:ef:40), Dst: CiscoInc_3f:80:f1 (78:da:6e:3f:80:f1)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 2401
Internet Protocol Version 4, Src: 172.16.0.34, Dst: 172.16.56.153
User Datagram Protocol, Src Port: 32774, Dst Port: 1812
RADIUS Protocol

```
0000 78 da 6e 3f 80 f1 e0 89 9d 43 ef 40 81 00 09 61  x.n?... .C.@...a
0010 08 00 45 00 01 24 fd 02 00 00 40 11 eb ea ac 10  ..E..$. .@.....
0020 00 22 ac 10 38 99 80 06 07 14 01 10 5a b8 01 0a  ."..8... ..Z...
0030 01 08 da 53 0e b1 50 0a 84 b9 16 8a b3 3b 79 53  ...S..P. ....;yS
0040 aa 67 01 07 75 73 65 72 34 59 03 00 83 06 00 00  .g..user 4Y.....
0050 00 01 1f 13 30 38 2d 37 34 2d 30 32 2d 37 37 2d  ...08-7 4-02-77-
0060 31 33 2d 34 35 1e 1d 30 30 2d 66 65 2d 63 38 2d  13-45..0 0-fe-c8-
0070 32 65 2d 33 62 2d 65 30 3a 63 61 70 74 75 72 65  2e-3b-e0 :capture
0080 31 78 05 06 00 00 00 02 1a 31 00 00 00 09 01 2b  1x..... .l.....+
0090 61 75 64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64  audit-se ssion-id
00a0 3d 61 63 31 30 30 30 32 32 30 30 30 30 30 30 33  =ac10002 20000003
00b0 31 35 38 35 32 62 64 62 35 2c 20 35 38 35 32 62  15852bdb 5, 5852b
```

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

Troubleshooting

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

Informações Relacionadas

- [Descarga do pacote AP](#)
- [Fundamentos do sniffing wireless do 802.11](#)

- [Suporte Técnico e Documentação - Cisco Systems](#)