Packet Capture op AireOS WLC configureren

Inhoud

Inleiding

Dit document beschrijft hoe u een pakkettransport kunt uitvoeren op een AireOS draadloze LAN-controller (WLC). Deze methode toont de pakketten die op cpu-niveau van de WLC in hex-indeling worden verzonden en/of ontvangen, die vervolgens met Wireshark worden vertaald in een .pcap-bestand.

Het is behulpzaam in gevallen waar de communicatie tussen een WLC en een RADIUS-server (Dial-In User Service), een access point (AP) of andere controllers snel moet worden geverifieerd met een pakketvastlegging op WLC-niveau, maar een poortspan is moeilijk uit te voeren.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Opdracht line Interface (CLI) toegang tot de WLC, bij voorkeur SSH omdat de uitvoer sneller is dan console.
- PC met draadloos WAN geïnstalleerd

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- WLC v8.3
- Wireshark v2 of hoger

Opmerking: Deze optie is beschikbaar sinds AireOS versie 4.

Beperkingen

De pakketvastlegging beperkt zich alleen tot bidirectionele besturingsplane (CP) voor datacommunicatie (DP)-pakketten in WLC. De pakketten die niet worden verzonden van het WLC

Data-vliegtuig naar/van het bedieningspaneel (d.w.z. vreemd voor anker getunneld verkeer, DP-CP-druppels etc.) worden niet opgenomen.

Voorbeelden van soorten verkeer naar/van de WLC die bij de CP worden verwerkt zijn:

- Telnet
- SSH
- HTTP
- HTTPS
- SNMP
- NTP
- RADIUS
- TACACS+
- Mobiliteitsberichten
- CAPWAP-controle
- NMSP
- TFTP/FTP/SFTP
- Syslog
- APP

Het verkeer naar/van de cliënt wordt verwerkt in het datacentrum (DP), behalve voor: 802.11-beheer, 802.1X/EAPOL-, ARP-, DHCP- en webverificatie.

Configureren

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Packet logging in WLC inschakelen

Stap 1. Meld u aan bij de CLI van de WLC.

Vanwege de hoeveelheid en snelheid van de logbestanden die deze functie weergeven, wordt geadviseerd om met SSH en niet met console in te loggen op de WLC.

Stap 2. Pas een toegangscontrolelijst (ACL) toe om te beperken welk verkeer wordt opgenomen.

In het gegeven voorbeeld toont de opname het verkeer naar/van de beheerinterface van de WLC (IP-adres 172.16.0.34) en de RADIUS-server (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**: Om al het verkeer naar/van de WLC op te nemen wordt het aanbevolen om ACL toe te passen dat het SSH-verkeer naar/van de host die de SSH-sessie gestart heeft, weggooit. Dit zijn de opdrachten die u kunt gebruiken om ACL te bouwen:

>1debug van pakketvastlegging doel ip 1 ontkent <WLC-IP> <host-IP> TCP 22
>debug van pakketvastlegging knop ip 2 ontkent <host-IP> <WLC-IP> TCP 22
>pakketvastlegging controleren met behulp van ip 3-licentie

Stap 3. Configureer de bestandsindeling die leesbaar is via Wireshark.

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

Stap 4. Schakel de optie pakketvastlegging in.

Dit voorbeeld toont hoe te om 100 ontvangen/verzonden pakketten op te nemen (het steunt 1 - 65535 pakketten):

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

Stap 5. Meld u aan bij de uitvoer naar een tekstbestand.

> Opmerking: Standaard logt alleen 25 ontvangen pakketten in terwijl de opdracht **pakketvastlegging debug** biedt.

> Opmerking: In plaats van **alles** kunt u **rx** of **tx** gebruiken om alleen ontvangen of verzonden verkeer op te nemen.

Zie deze link voor meer informatie over het configureren van pakketvastlegging:

[Cisco-configuratiegids voor draadloze controllers, release 8.3, met behulp van de Debug-faciliteit]

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Gebruik de gegeven opdracht om de huidige configuratie van pakketvastlegging te verifiëren.

```
> 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
```

Reproduceren het gewenste gedrag om het verkeer te genereren.

Een soortgelijke uitvoer wordt weergegeven:

```
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...
```

Verwijder ACL's uit pakketvastlegging

Om de filters die door ACL's worden toegepast uit te schakelen, gebruikt u deze opdrachten:

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

Packet-loggen uitschakelen

Om de pakketvastlegging uit te schakelen zonder de ACL's te verwijderen gebruikt u deze opdracht:

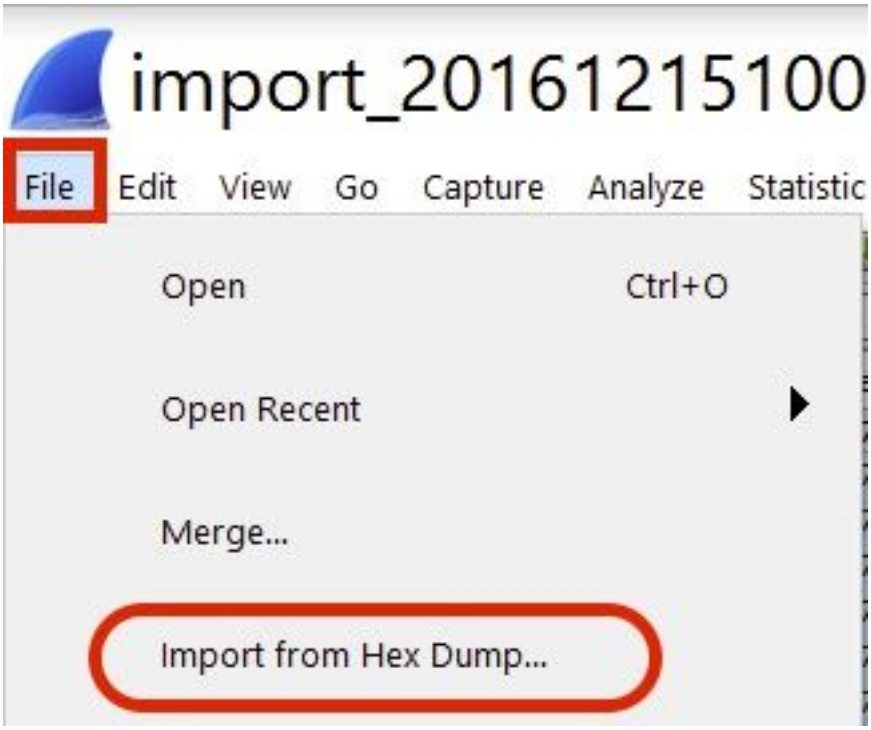
```
> debug packet logging disable
```

Packet logging uitvoer naar een .pcap-bestand converteren

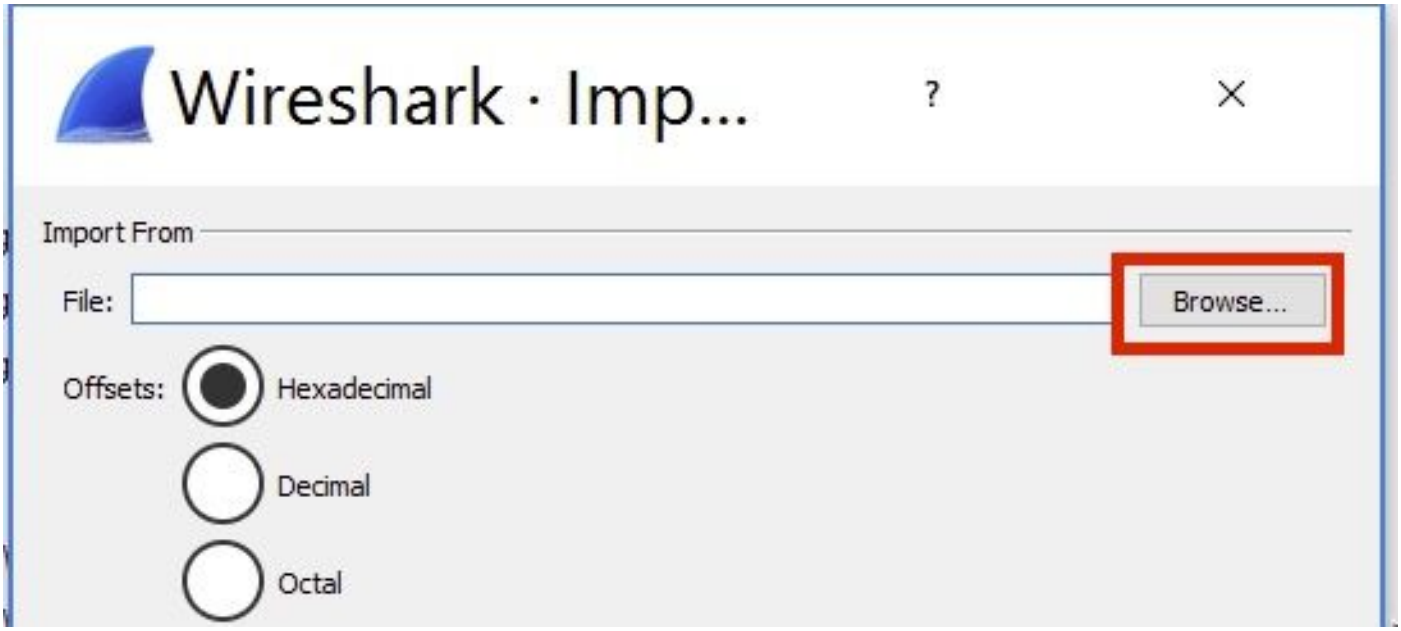
Stap 1. Zodra de uitvoer is voltooid, verzamelt u het document en slaat u het op in een tekstbestand.

Zorg ervoor dat u een schoon logbestand verzamelt, anders kan Wireshark gecorrumpeerde pakketten tonen.

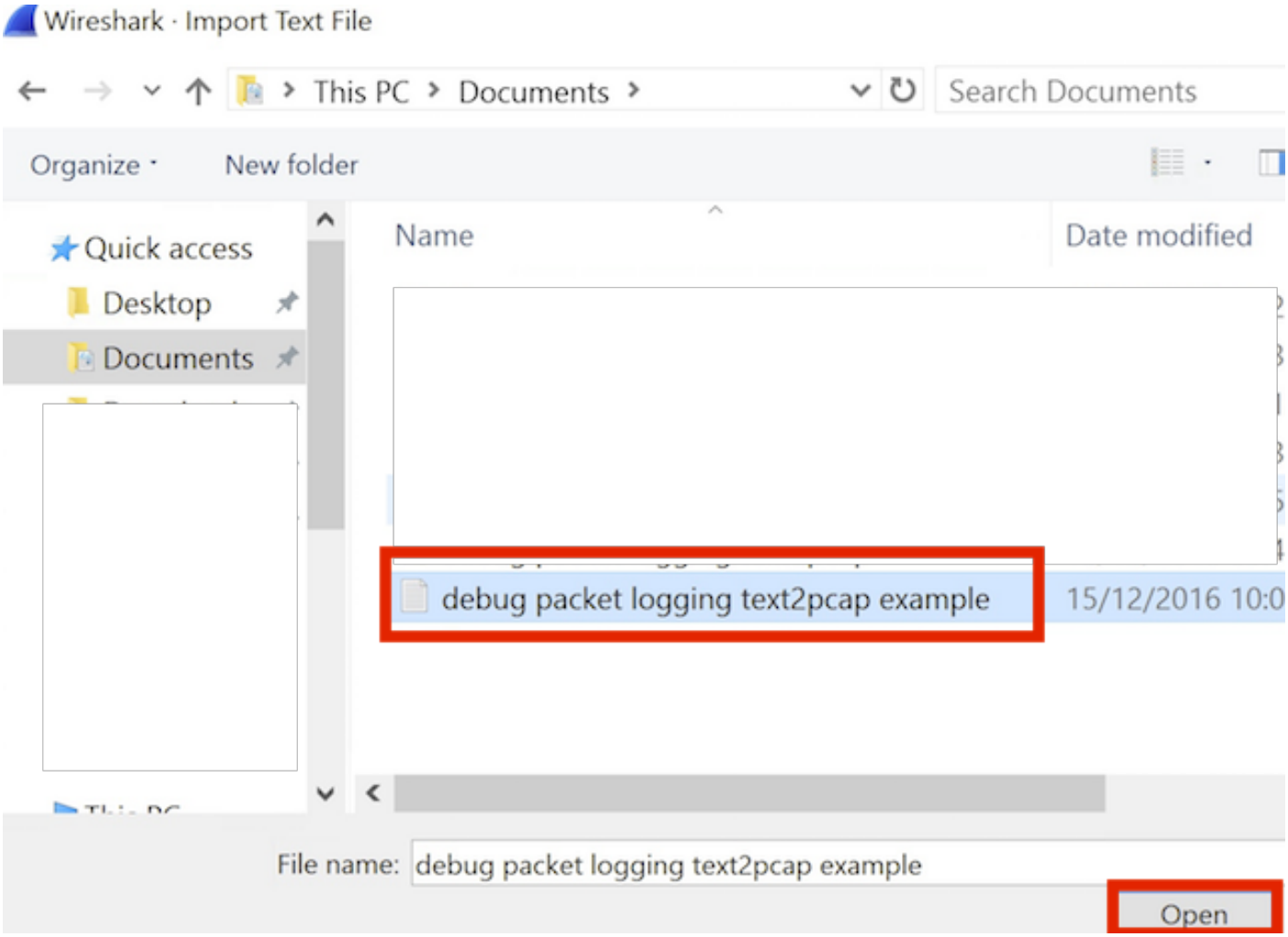
Stap 2. Open Wireshark en navigeer naar **Bestand>Importeren uit Hex Dump...**



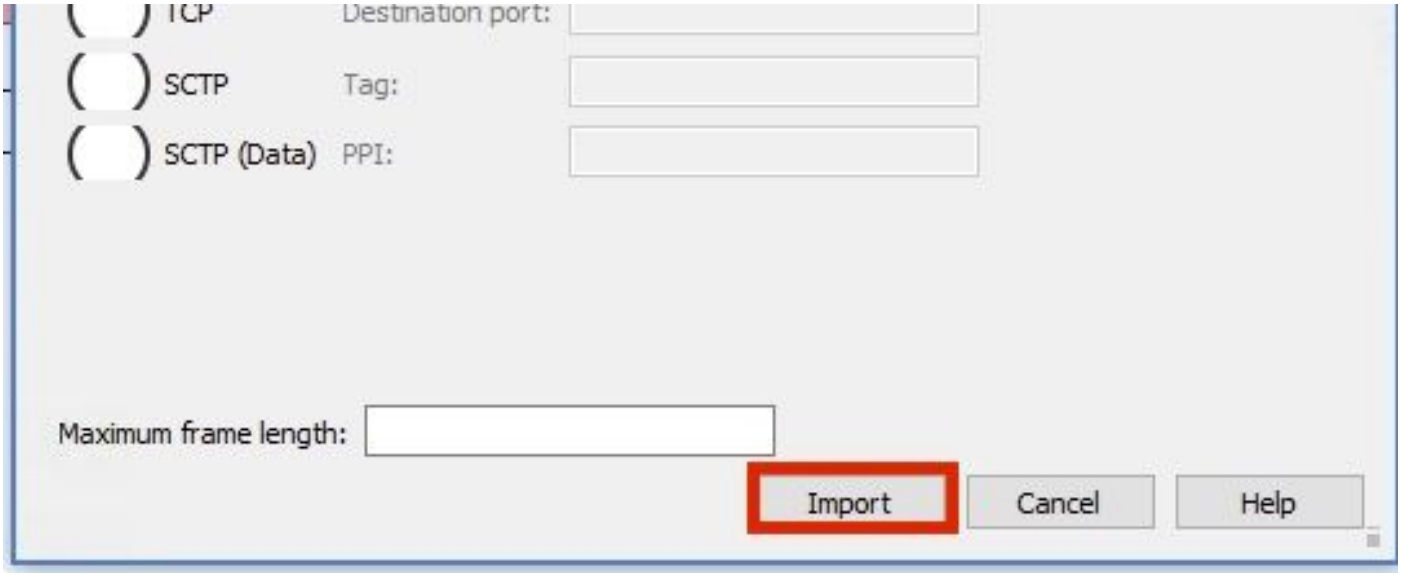
Stap 3. Klik op **Bladeren.**



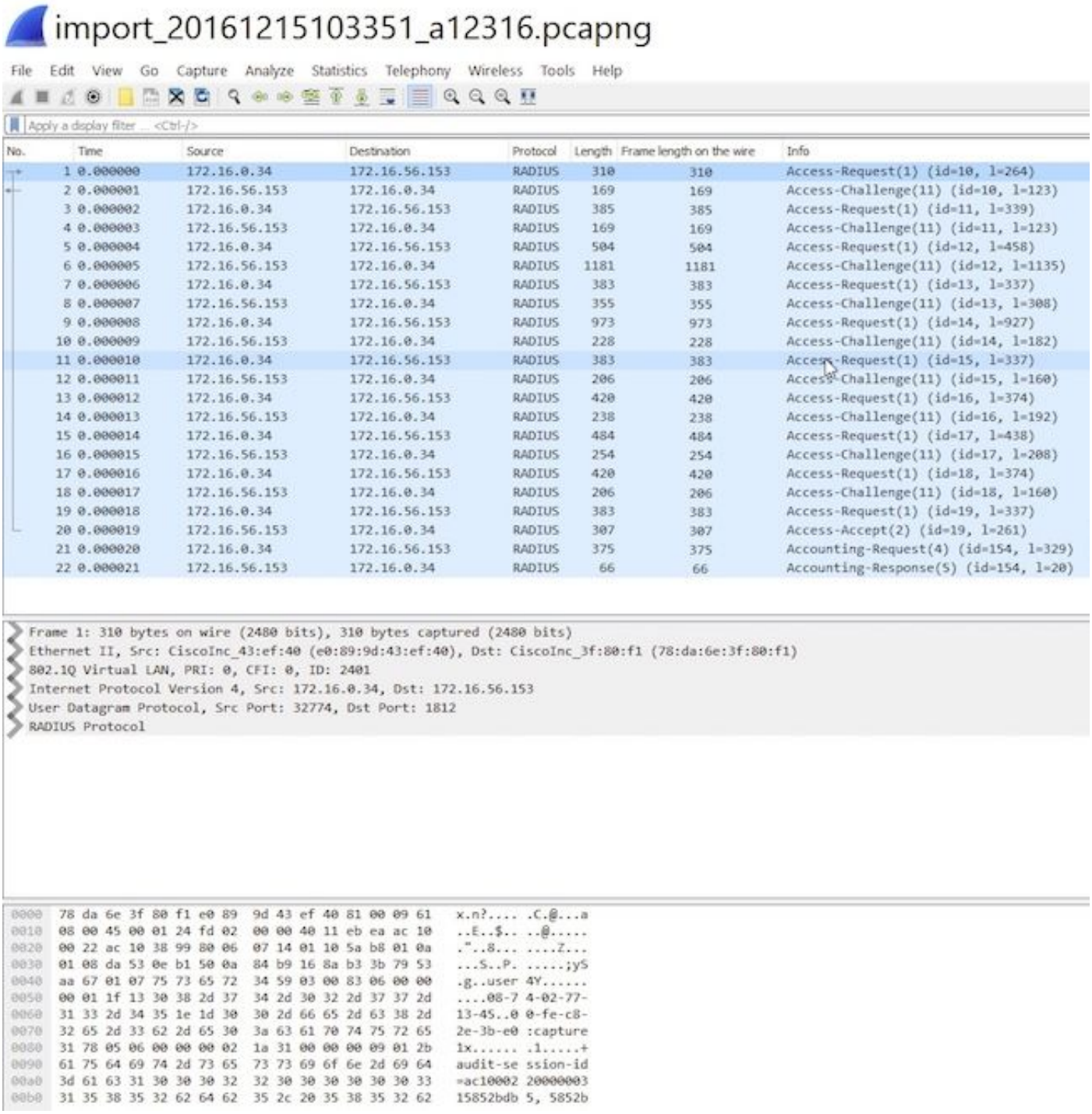
Stap 4. Selecteer het tekstbestand waarin u de pakketvastlegging-uitvoer hebt opgeslagen.



Stap 5. Klik op **Importeren.**



Wireshark toont het bestand als .pcap.



Opmerking: Let erop dat de tijdstempels niet accuraat zijn en dat de delta tijd tussen de frames niet nauwkeurig is.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- AP Packet Dump
- Basisfactoren van 802.11 draadloos snuffelen
- Technische ondersteuning en documentatie – Cisco Systems