在AireOS WLC上配置数据包捕获

目录

简介

本文档介绍如何在AireOS无线LAN控制器(WLC)上运行数据包转储。 此方法以十六进制格式显示WLC的CPU级别发送和接收的数据包，然后使用Wireshark将其转换为.pcap文件。

在WLC和远程身份验证拨入用户服务(RADIUS)服务器、接入点(AP)或其他控制器之间的通信需要通过WLC级别的数据包捕获快速进行验证，但很难执行端口跨度时，此功能非常有用。

要求

Cisco 建议您了解以下主题：

- 命令行界面(CLI)访问WLC，最好是SSH，因为输出比控制台快。
- 安装了Wireshark的PC

使用的组件

本文档中的信息基于以下软件和硬件版本：

- WLC v8.3
- Wireshark v2或更高版本

注意：自AireOS第4版起，此功能可用。

限制

数据包日志记录将仅捕获WLC中的双向控制平面(CP)到数据平面(DP)数据包。未从WLC数据平面向控制平面发送/从控制平面发送的数据包（例如，外部到锚点隧道流量、DP-CP丢弃等）将不会被捕获。

在CP处理的WLC的流量类型示例包括：

- Telnet
- SSH
- HTTP
- HTTPS
- SNMP
- NTP
- RADIUS
- TACACS+
- 移动消息
- CAPWAP控制
- NMSP
- TFTP/FTP/SFTP
- 系统日志
- IAPP

进出客户端的流量在数据平面(DP)中处理，但：802.11管理、802.1X/EAPOL、ARP、DHCP和Web身份验证。

配置

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

在WLC中启用数据包日志记录

步骤1.登录WLC的CLI。

由于此功能显示的日志数量和速度，建议通过SSH而不是控制台登录WLC。

步骤2.应用访问控制列表(ACL)以限制捕获的流量。

在给定示例中，捕获显示进出WLC管理接口（IP地址172.16.0.34）和RADIUS服务器(172.16.56.153)的流量。

```
> 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
```

> **提示：**要捕获发往/来自WLC的所有流量，建议应用ACL，该ACL将SSH流量丢弃至/来自发起SSH会话的主机。以下是可用于构建ACL的命令：
>
> >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

步骤3.配置Wireshark可读的格式。

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

步骤4.启用数据包日志记录功能。

本示例展示如何捕获100个接收/传输的数据包(它支持1 - 65535个数据包):

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

步骤5.将输出记录到文本文件。

注意：默认情况下，它仅使用debug packet logging enable命令记录25**个收到的数据包**。

注意：而不**是**使用**rx** 或**tx** 仅捕获已接收或已传输的流量。

有关配置数据包日志记录功能的更多详细信息，请参阅以下链接：

[思科无线控制器配置指南，版本8.3，使用调试工具]

验证

使用本部分可确认配置能否正常运行。

使用给定命令检验数据包日志记录的当前配置。

```
> 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
```

重现生成流量所需的行为。

屏幕上将显示如下输出：

```
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...
```

从数据包日志记录中删除ACL

要禁用ACL应用的过滤器，请使用以下命令：

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

禁用数据包日志记录

要在不删除ACL的情况下禁用数据包日志记录，只需使用以下命令：

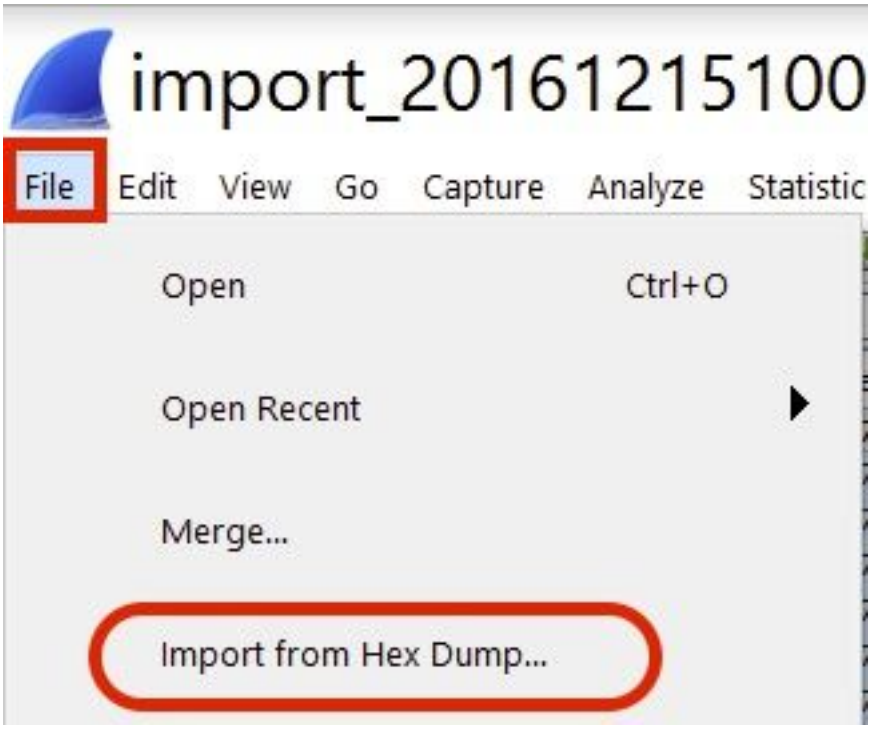
```
> debug packet logging disable
```

将数据包日志记录输出转换为.pcap文件

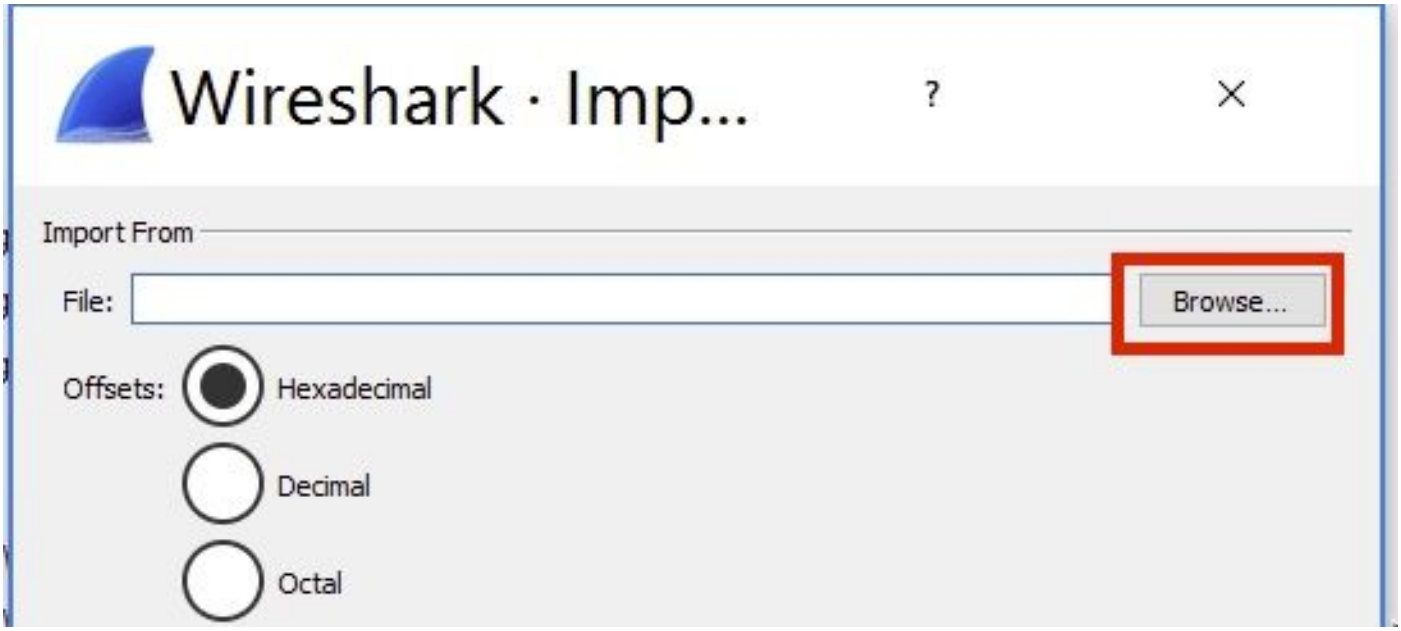
步骤1.输出完成后，收集并保存到文本文件。

确保收集干净的日志，否则Wireshark可能显示损坏的数据包。

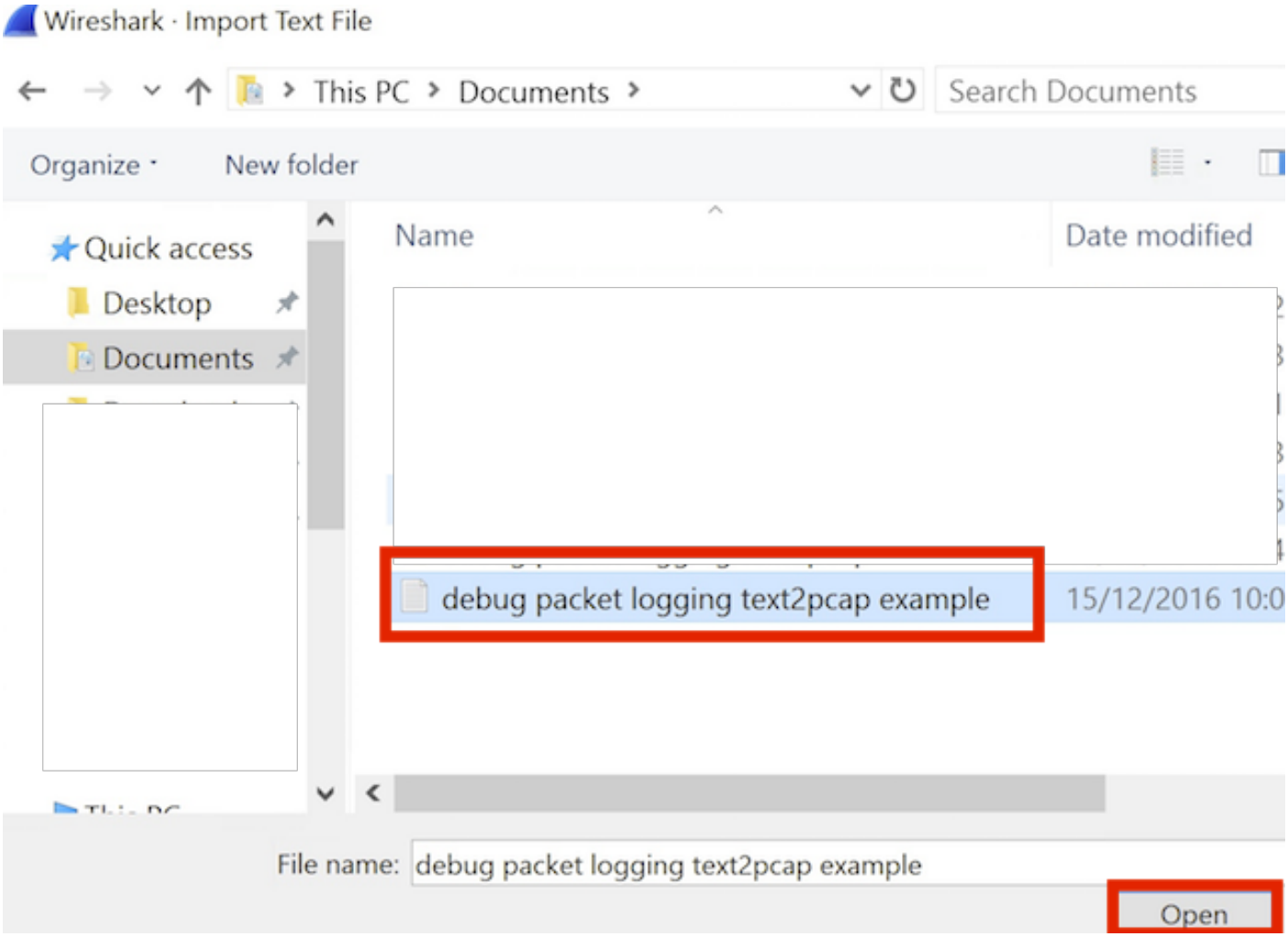
步骤2.打开Wireshark并导航至**File > Import from Hex Dump...**



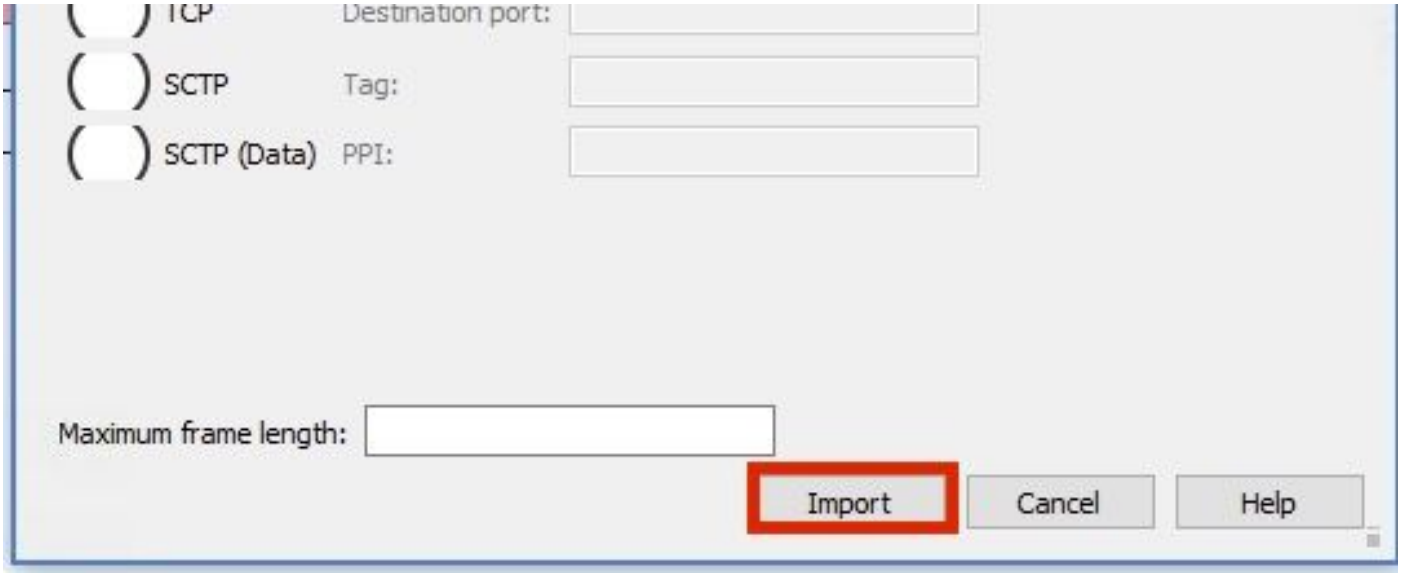
步骤3.单击“浏**览”。**



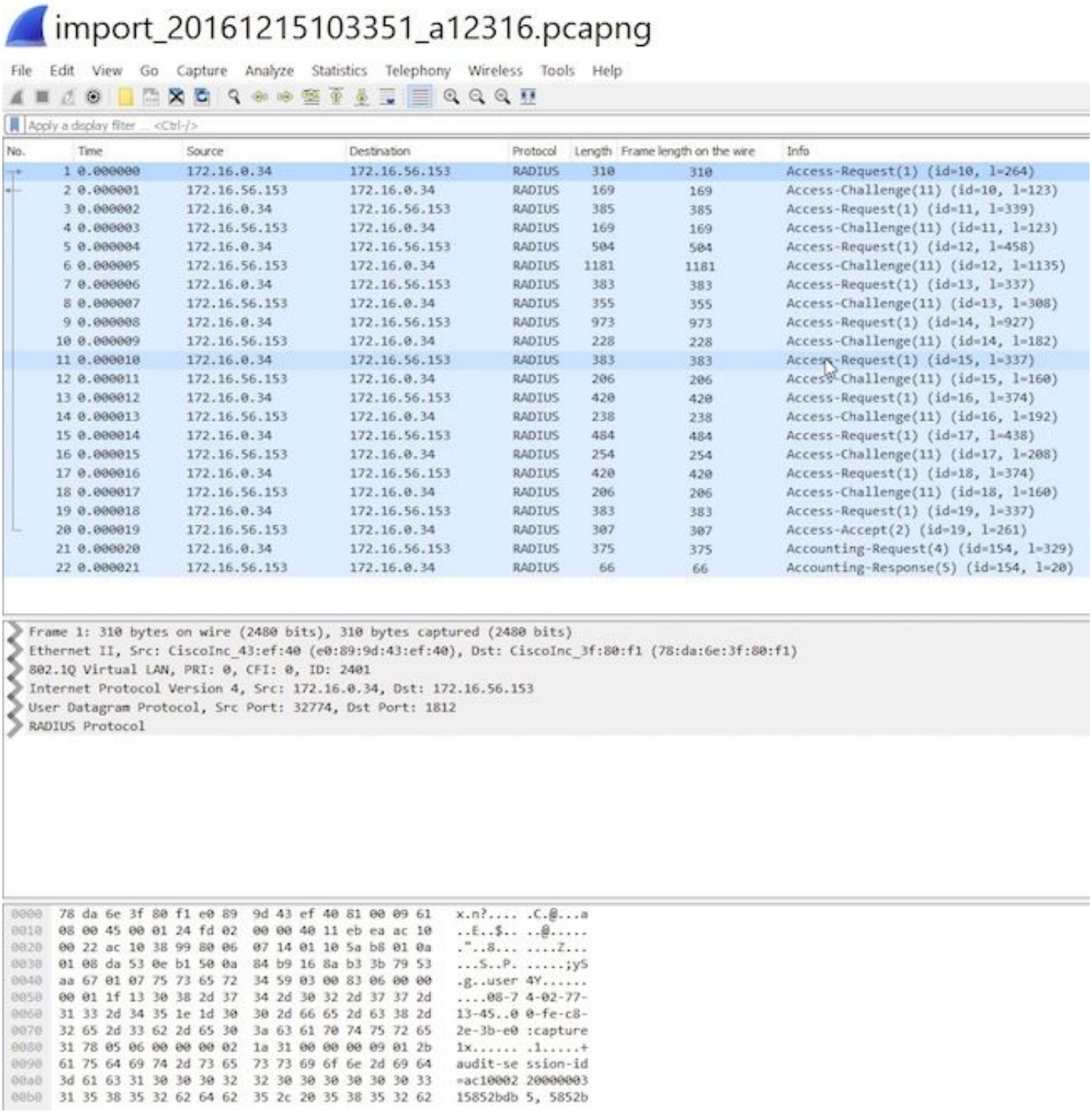
步骤4.选择保存数据包日志记录输出的文本文件。



步骤5.单击“导入”。



Wireshark将文件显示为.pcap。



注意：请注意，时间戳不准确，帧之间的增量时间也不准确。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- AP数据包转储
- 802.11无线嗅探的基础
- 技术支持和文档 - Cisco Systems