配置AireOS WLC的数据包捕获

目录

简介

本文描述如何运行在AireOS无线局域网Controller(WLC)的一数据包转储。此方法显示发送的数据包并且/或者接收在WLC的CPU级别在六角形的格式的，然后翻译到有Wireshark的一个.pcap文件。

是有用，在WLC和远程验证拨入用户服务(RADIUS)服务器、接入点(AP)或者其他控制器之间的通信在与数据包捕获的一快速方式需要验证在级处的WLC，但是波尔特SPAN是难实行。

要求

Cisco 建议您了解以下主题：

- 对WLC的命令行界面(CLI)访问，最好是SSH，因为输出比控制台快速。
- 有安装的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或以上

注意： 此功能从AireOS版本4是可用的。

限制

数据包记录日志将捕获仅双向控制层面(CP)到在WLC的数据层面(DP)数据包。没有从到/从控制层面即的那些数据包(外国的WLC数据层面被发送停住通道流量， DP-CP丢包等等)不会捕获。

流量类型示例到/从WLC的处理在CP是：

- Telnet

- SSH
- HTTP
- HTTPS
- SNMP
- NTP
- RADIUS
- TACACS+
- 移动性消息
- CAPWAP控制
- NMSP
- TFTP/FTP/SFTP
- Syslog
- IAPP

到/从客户端的流量在数据层面(DP)处理除了：802.11管理、802.1X/EAPOL、ARP、DHCP和Web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。如果您的网络实际，请保证您了解所有命令潜在影响。

启用登陆WLC的数据包

步骤1. WLC's CLI的洛金。

由于此数量和速度的日志功能显示它推荐登陆到WLC由SSH和不由控制台。

步骤2.应用访问控制表(ACL)限制哪个流量捕获。

在给的示例中捕获显示到/从WLC's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**：要捕获到/从WLC的所有流量丢弃到/从启动SSH会话的主机该的SSH流量推荐的应用ACL。这些是您能使用构件ACL的命令：
>
> >记录ACL ip 1的调试数据包拒绝<WLC-IP> <host-IP> tcp 22其中任一
> >记录ACL ip 2的调试数据包拒绝<host-IP> <WLC-IP> tcp任何22
> >调试数据包记录ACL任何ip 3的permit其中任一

步骤3.配置格式可读由Wireshark。

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

步骤4. Enable (event)数据包操作日志功能。

此示例显示如何捕获接收的100/已传输数据包(支持1 - 65535数据包) ：

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

注意：默认情况下，它只记录有debug packet命令**logging enable的**25个收到的信息包。

注意：而不是**所有**您能使用**rx**或**tx**捕获只已接收或已发送流量。

关于关于配置数据包操作日志功能的更详细的资料请参见此链路：

Cisco无线控制器配置指南，版本8.3，使用调试设备

验证

使用本部分可确认配置能否正常运行。

请使用给的命令验证数据包记录日志当前配置。

```
> 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
```

再生产需要的行为生成流量。

输出类似于此出现：

```
> 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
```

从数据包记录日志的删除ACL

为了禁用ACL应用的过滤器请使用这些命令：

```
> 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
```

禁用数据包记录日志

为了禁用数据包记录日志，无需删除ACL请使用此命令：

```
> 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
```

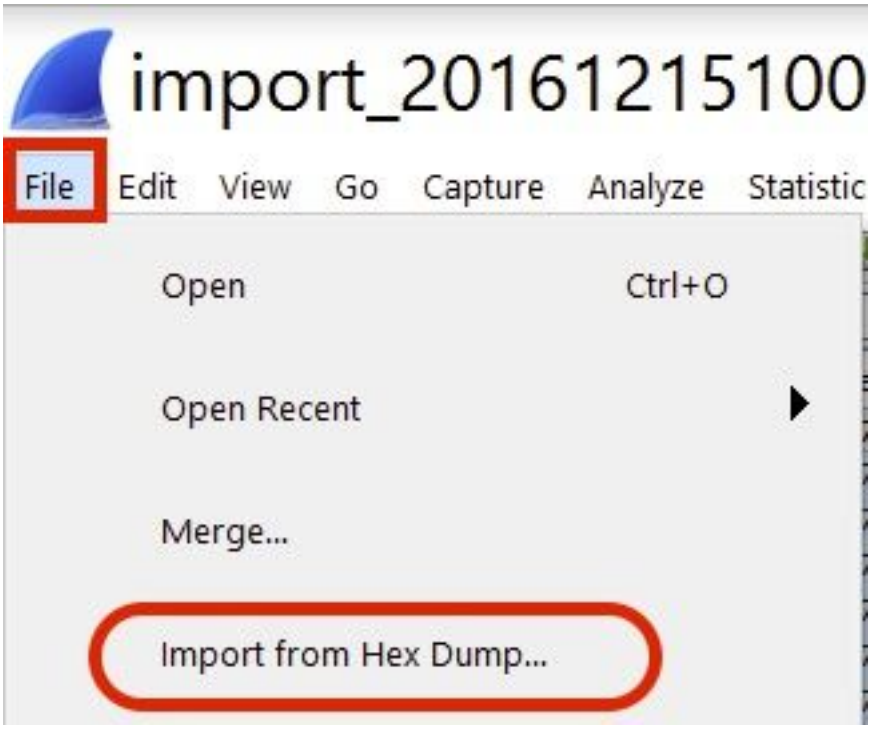
```
    [3]: disabled
    [4]: disabled
    [5]: disabled
    [6]: disabled
  LWAPP-IP ACL:
    [1]: disabled
    [2]: disabled
    [3]: disabled
    [4]: disabled
    [5]: disabled
    [6]: disabled
```

转换数据包操作日志输出到.pcap文件

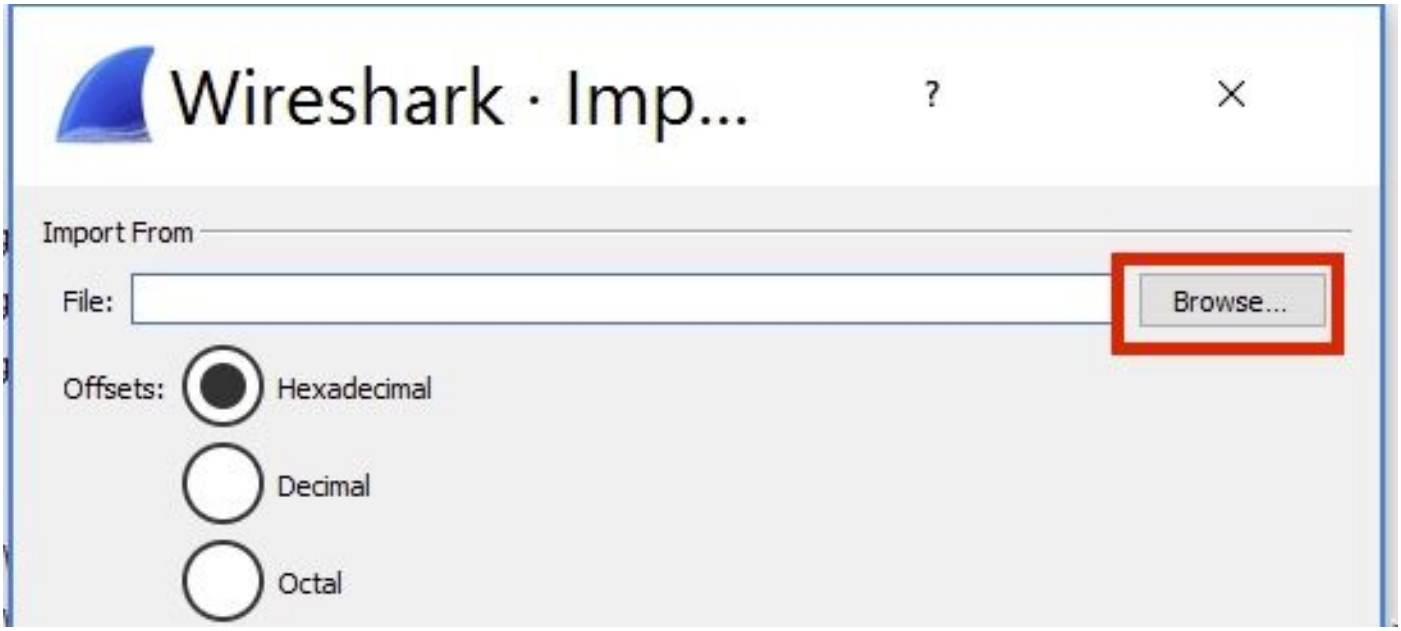
步骤1:一旦输出完成，请收集它并且保存它到文本文件。

保证您采集一本干净的日志，否则Wireshark也许显示损坏的数据包。

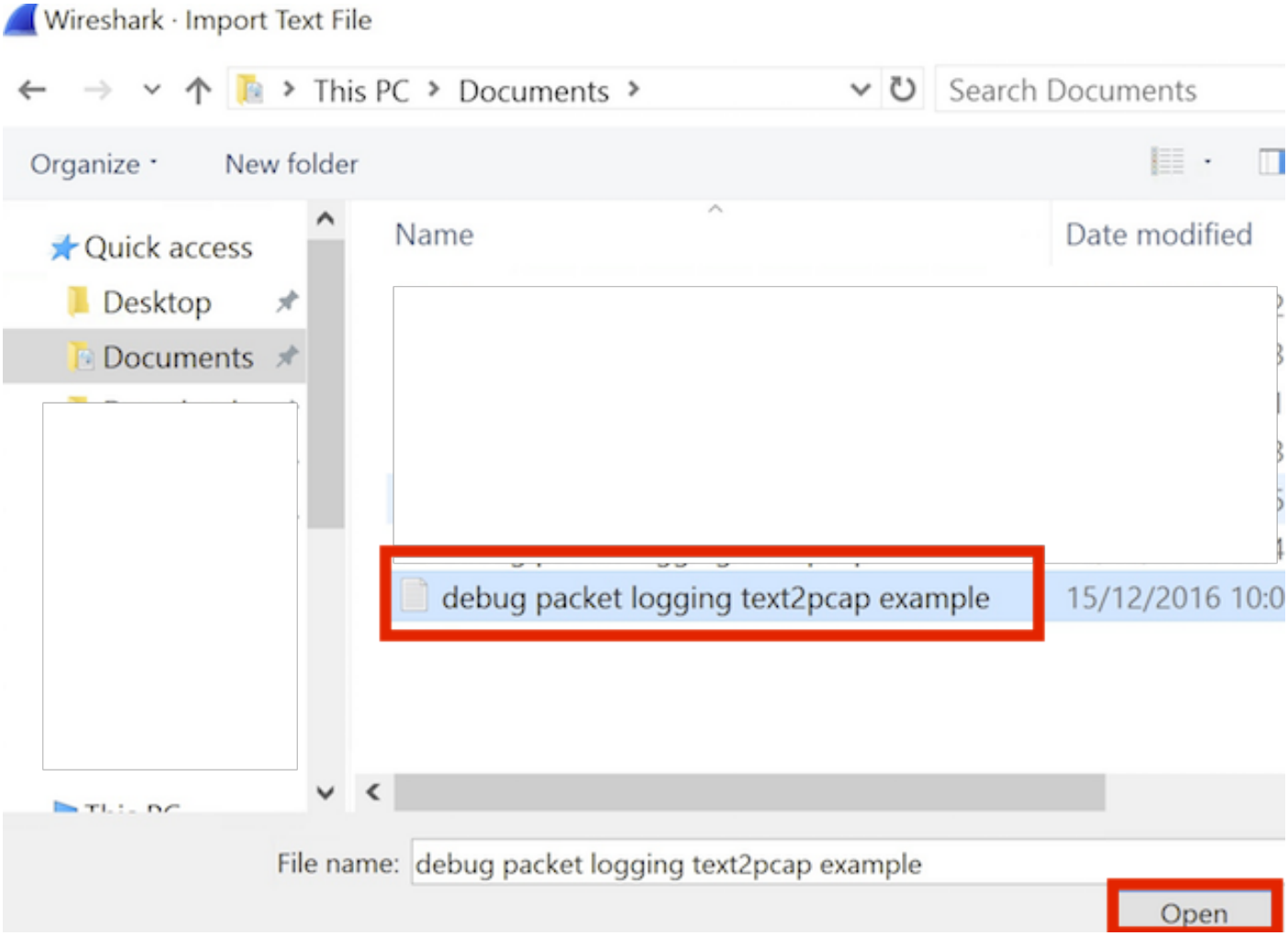
步骤2.打开Wireshark并且导航对**从HEX转储的文件>Import…**



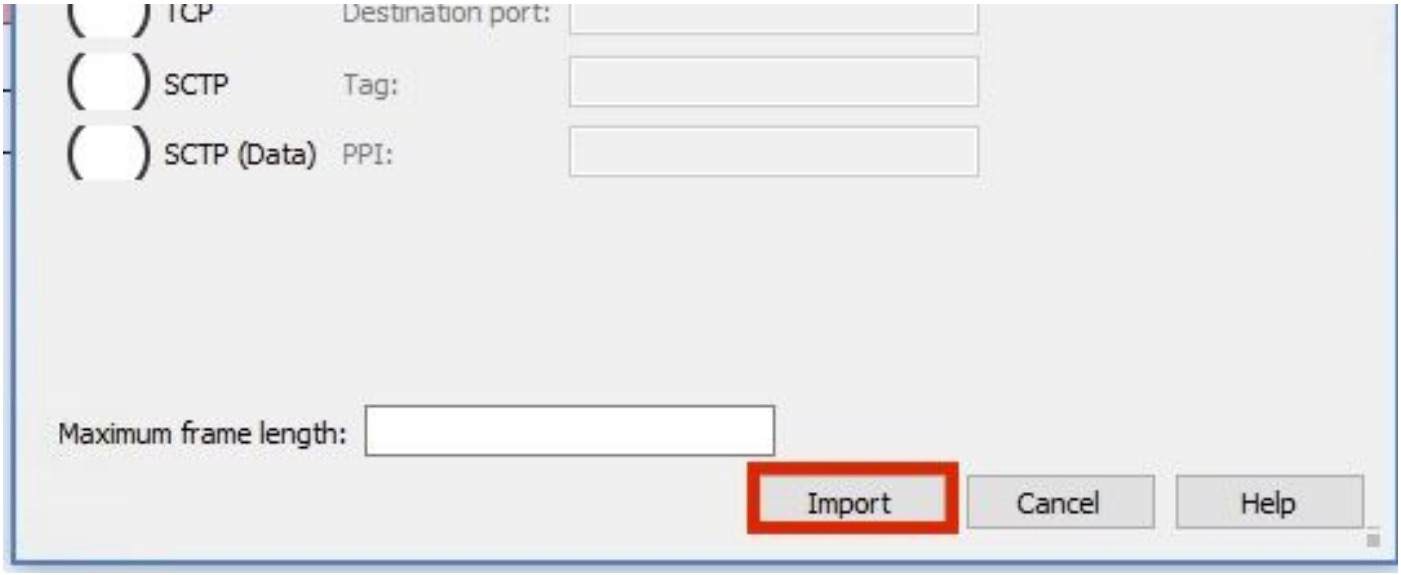
步骤3.单击**浏览。**



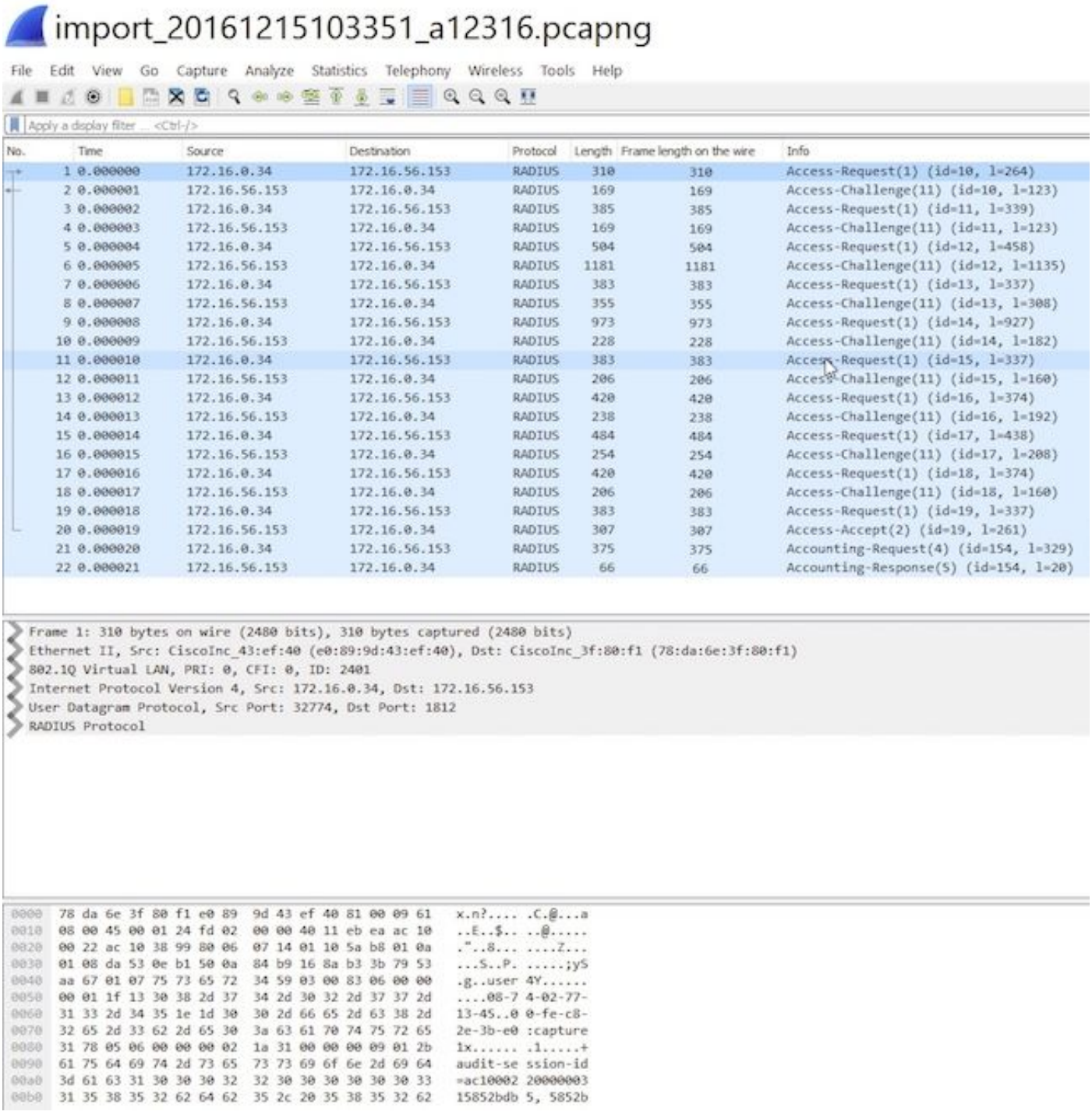
步骤4.选择您保存数据包操作日志输出的文本文件。



步骤5.点击**导入**。



Wireshark显示文件作为.pcap。



注意：注意时间戳不是准确亦不帧之间的delta时间。

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
- 基本802.11无线探测
- 技术支持和文档 - Cisco Systems