AireOS WLCでのパケットキャプチャの設定

内容

概要

このドキュメントでは、AireOSワイヤレスLANコントローラ(WLC)でパケットダンプを実行する方法について説明します。 この方式では、WLCのCPUレベルで送受信されたパケットが16進形式で表示されます。この形式は、Wiresharkを使用して.pcapファイルに変換されます。

WLCとリモート認証ダイヤルインユーザサービス(RADIUS)サーバ、アクセスポイント(AP)またはその他のコントローラ間の通信をWLCレベルでパケットキャプチャを使用して迅速に確認する必要があるが、ポートスパンが実行しにくい場合に役立ちます。

要件

次の項目に関する知識があることが推奨されます。

- WLCへのコマンドラインインターフェイス(CLI)アクセス。出力はコンソールよりも高速であるため、SSHが好ましい。
- Wireshark インストール済みの PC

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- WLC v8.3
- Wireshark v2 以降

注:この機能はAireOSバージョン4以降で使用できます。

制限

パケットロギングは、WLCで双方向コントロールプレーン(CP)からデータプレーン(DP)へのパケットのみをキャプチャします。WLCデータプレーンからコントロールプレーンに送受信されないパケット（トンネル化トラフィックをアンカーする外部パケット、DP-CPドロップなど）はキャ

プチャされません。

CPで処理されるWLCとの間のトラフィックの種類の例を次に示します。

- Telnet
- SSH
- HTTP
- HTTPS
- SNMP
- NTP
- RADIUS
- TACACS+
- モビリティメッセージ
- CAPWAP制御
- NMSP
- TFTP/FTP/SFTP
- Syslog
- IAPP

クライアントとの間のトラフィックは、次の点を除き、データプレーン(DP)で処理されます。802.11管理、802.1X/EAPOL、ARP、DHCP、およびWeb認証。

設定

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

WLC のパケット ロギングを有効にする

ステップ 1：WLC の CLI にログインします。

この機能が表示するログの数と速度が原因で、コンソールではなくSSHでWLCにログインすることを推奨します。

ステップ2：アクセスコントロールリスト(ACL)を適用して、キャプチャするトラフィックを制限します。

次の例では、WLCの管理インターフェイス(IPアドレス172.16.0.34)とRADIUSサーバ(172.16.56.153)との間のトラフィックをキャプチャで示しています。

```
> 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
```

> **ヒント**：WLCとの間のすべてのトラフィックをキャプチャするには、SSHセッションを開始したホストとの間のSSHトラフィックを廃棄するACLを適用することを推奨します。ACLの作成に使用できるコマンドは次のとおりです。

>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

ステップ3:Wiresharkで読み取り可能な形式を設定します。

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

ステップ 4：パケット ロギング機能を有効にします。

この例では送受信される 100 パケットをキャプチャする設定になっています（1 ～ 65535 パケットに対応）。

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

ステップ5：出力をテキストファイルに記録します。

注：debug packet logging enable コマンドは、デフォルトでは受信する 25 パケットのみロギングします。

注：すべての代わりに**rxまたはtx**を使用して、受信または送信されたトラフィックのみをキャプチャできます。

パケットロギング機能の設定の詳細については、次のリンクを参照してください。

Cisco Wireless Controllerコンフィギュレーションガイド、リリース8.3、デバッグ機能の使用

確認

ここでは、設定が正常に機能しているかどうかを確認します。

指定されたコマンドを使用して、パケットロギングの現在の設定を確認します。

```
> 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
```

トラフィックを生成するために必要な動作を再現します。

次のような出力が表示されます。

```
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...
```

パケット ロギングから ACL を削除する

ACL によって適用されるフィルタを無効にするには、次のコマンドを使用します。

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

パケット ロギングを無効にする

ACL を削除せずにパケット ロギングを無効にするには、次のコマンドを使用します。

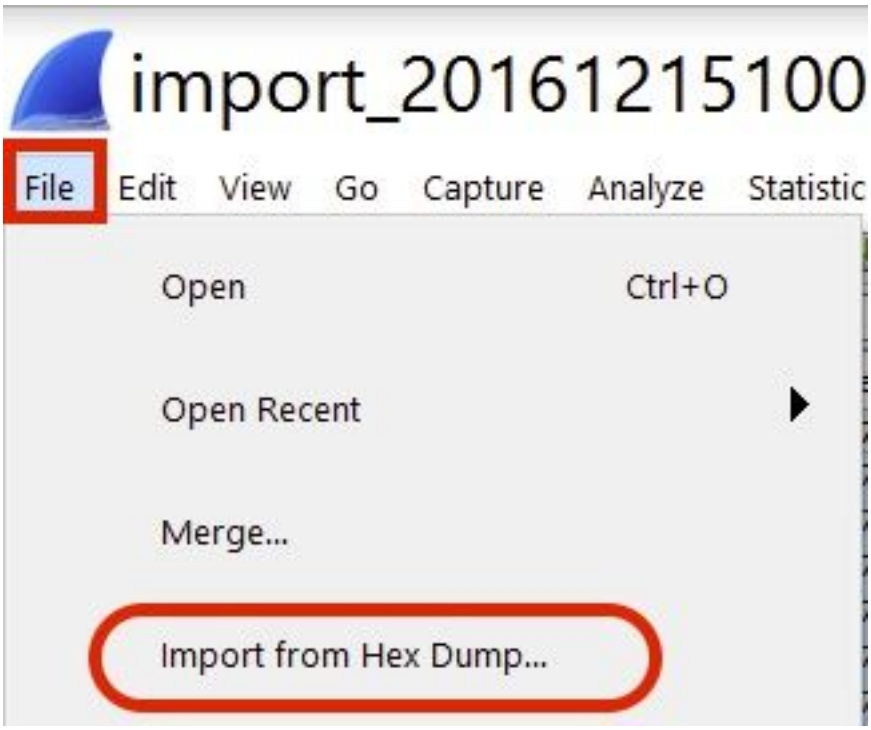
```
> debug packet logging disable
```

パケット ログ出力を .pcap ファイルに変換する

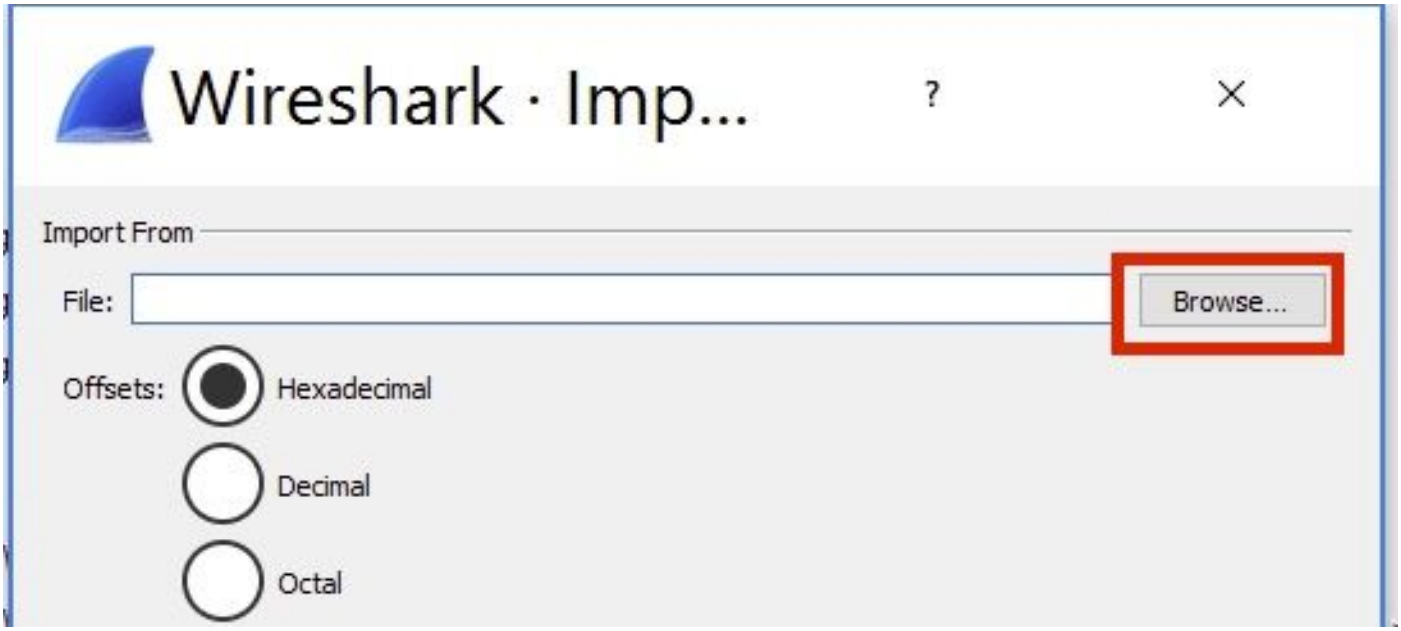
ステップ1：出力が終了したら、それを収集してテキストファイルに保存します。

まとめる際はクリーンなログになっていることを確認してください。クリーンなログでないと Wireshark で破損したパケットとして表示される場合があります。

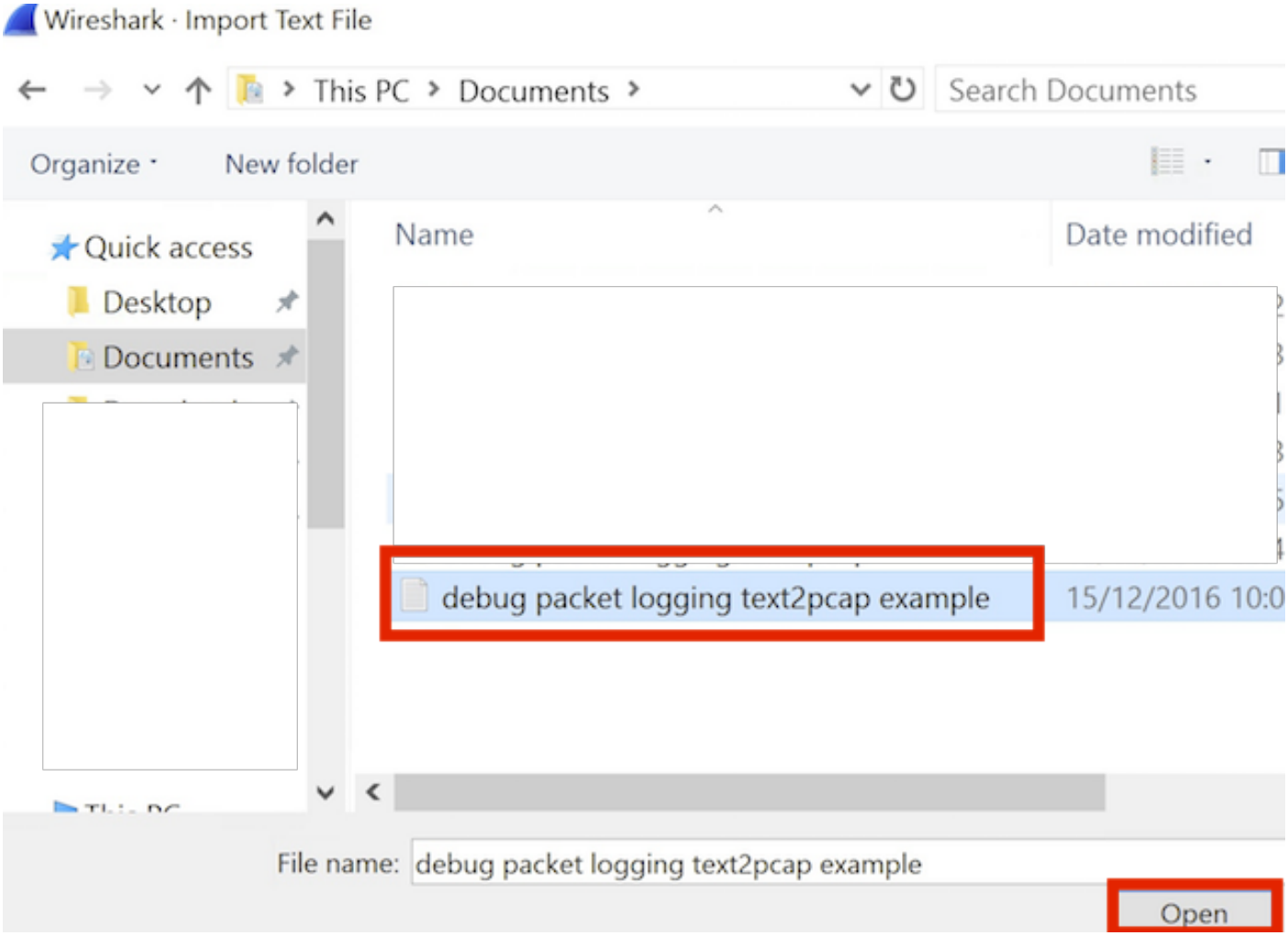
ステップ 2： Wireshark を開き、[File] > [Import from Hex Dump...] の順に開きます。



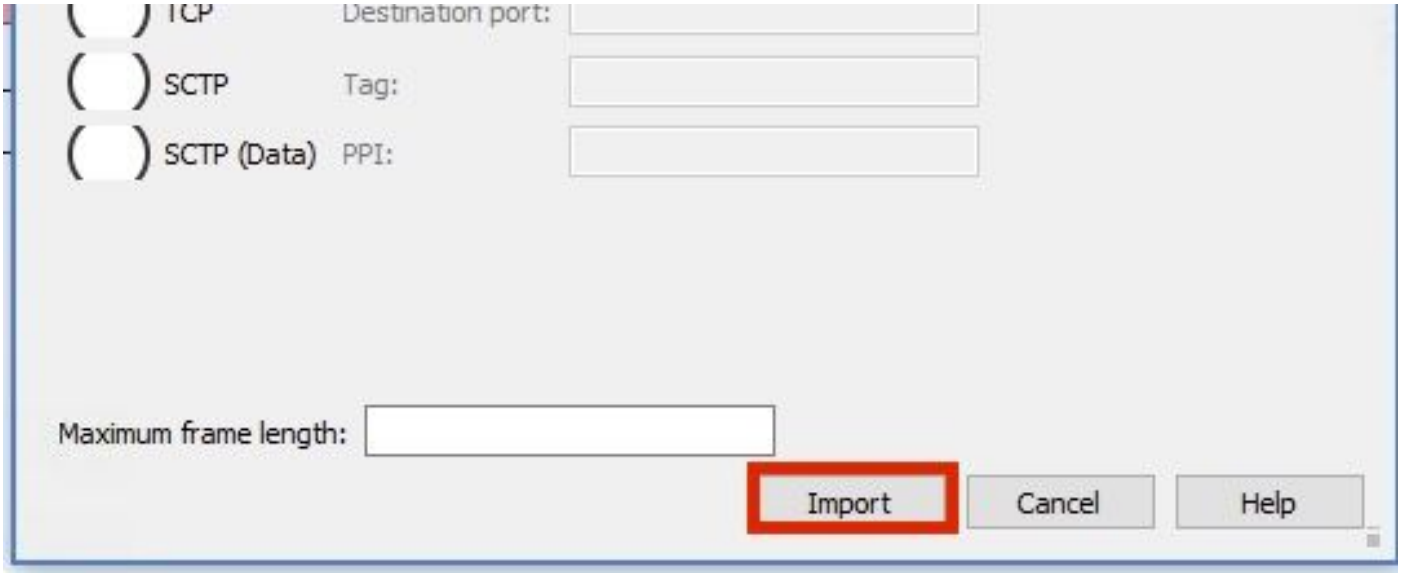
ステップ 3：[Browse] をクリックします。



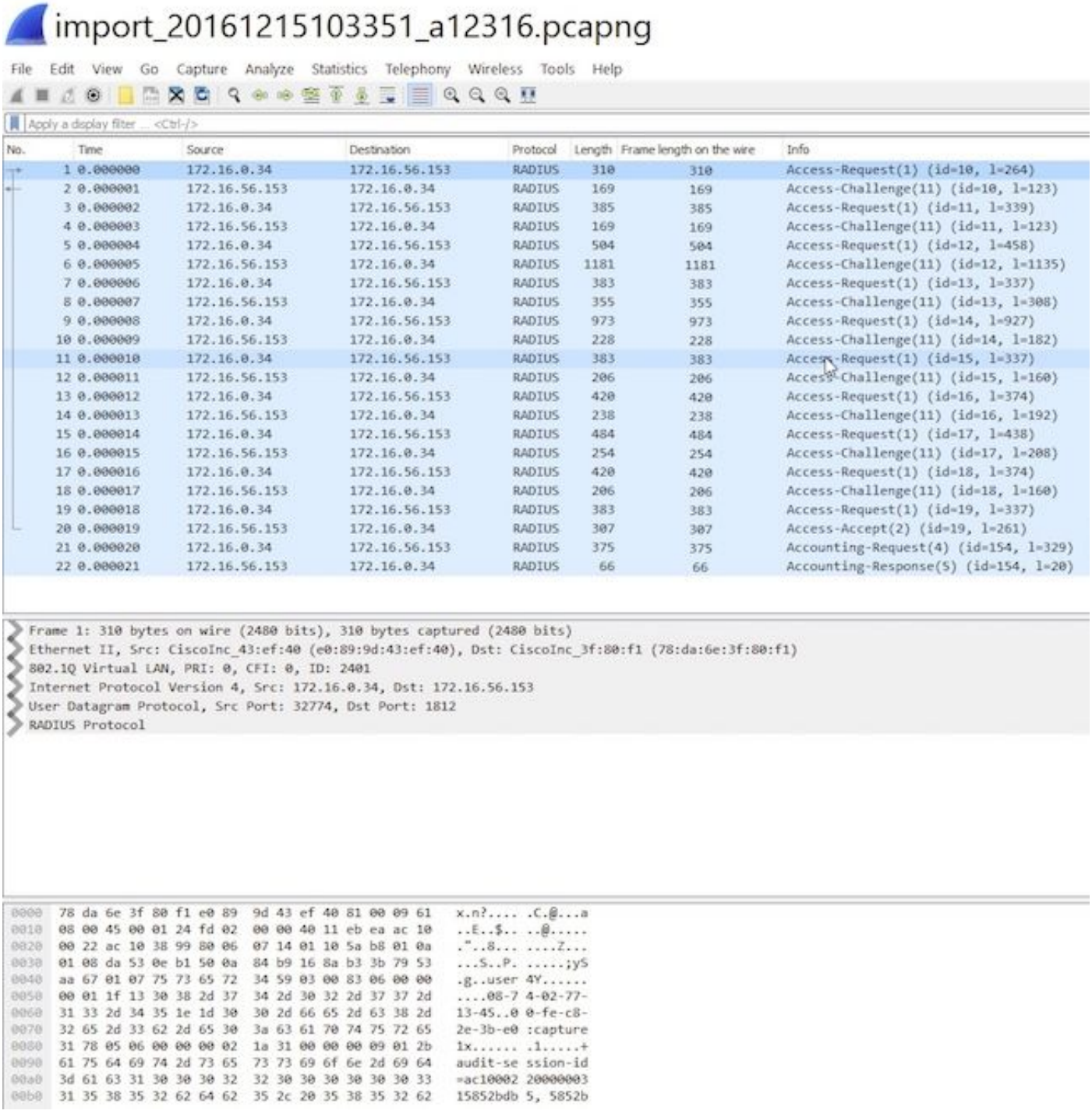
ステップ 4：パケット ログ出力を保存したテキスト ファイルを選択します。



ステップ 5：[Import] をクリックします。



Wiresharkでは、ファイルが.pcapとして表示されます。



注：タイム スタンプやフレーム間デルタ タイムは正確な時間ではありませんのでご注意ください。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- AP パケット ダンプ
- 802.11 ワイヤレス スニフィングの基礎
- テクニカル サポートとドキュメント – Cisco Systems