AireOS WLC の設定 パケットキャプチャ

目次

概要

この資料に AireOS Wireless LAN Controller（WLC）のパケット ダンプするを実行する方法を記述されています。 この方式は Wireshark と .pcap ファイルに変換される十六進形式の WLC の CPU レベルで送信されるおよび/または受信されるパケットを表示する。

それは WLC およびリモート認証ダイヤルイン ユーザ サービス（RADIUS） サーバ、Access Point （AP）または他のコントローラ間の通信が WLC レベルでパケットキャプチャが付いている簡単で確認される必要があればが、ポート スパンが実行しにくければ有用です。

要件

次の項目に関する知識が推奨されます。

- 出力がコンソールよりファーストであるので WLC への Command Line Interface （CLI） アクセス、できれば SSH。
- 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くものです。

- WLC v8.3
- Wireshark v2 以降

注: この機能は AireOS バージョン 4 以来利用できます。

制限事項

パケット 記録は WLC のデータ平面（DP）パケットに双方向 コントロール プレーンだけ（CP）キャプチャ します。 コントロール プレーン（すなわち外部 トンネルトラフィック、DP-CP ドロップを等固定するため）に出入する WLC データ平面から送信されないそれらのパケット

はキャプチャ されません。

CP で処理される WLC に出入するトラフィックの種類の例は次のとおりです:

- 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

クライアントに出入するトラフィックはデータ平面（DP）でを除いて処理されます: 802.11 管理、802.1X/EAPOL、ARP、DHCP および Web 認証。

設定

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

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。

このログの数量および速度が原因で機能 ディスプレイ SSH とないコンソールによって WLC にログインすることを推奨します。

ステップ 2.どのトラフィックがキャプチャ されるか制限するために Access Control List（ACL）を適用して下さい。

与えられた例でキャプチャは WLC のマネージメントインターフェイス（IP アドレス 172.16.0.34）および RADIUSサーバに出入するトラフィックを示します（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
```

> **ヒント**： WLC に出入するすべてのトラフィックをキャプチャ するためにホストに出入する 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 SSH セッションを始める。 これらは ACL を構築するのに使用できるコマンドです:

>ACL IP 1 拒否 <WLC-IP> <host-IP> TCP 22 を記録 する パケットをデバッグして下さい
>ACL IP 2 拒否 <host-IP> <WLC-IP> TCP を記録 する パケットをあらゆる 22 デバッグして下さい
>パケットをデバッグしまあらゆる ACL IP 3 割り当てを記録 します

ステップ 3. Wireshark によって読解可能な形式を設定して下さい。

```
> 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
```

> **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**の代りにキャプチャ するのに受信されたか、または送信されたトラフィックただ **rx** か **tx** を使用できます。

パケット ログ記録機能の設定についての更に詳しい情報についてはこのリンクを参照して下さい:

Ciscoワイヤレス コントローラ設定 ガイド、デバッグ ファシリティを使用するリリース 8.3、

確認

このセクションでは、設定が正常に機能していることを確認します。

パケット 記録の現在のコンフィギュレーションを確認するのにある特定のコマンドを使用して下さい。

```
> 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 して下さい。

次のような出力が表示されます。

```
> 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
```

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。

```
> 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
```

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。

```
> 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
```

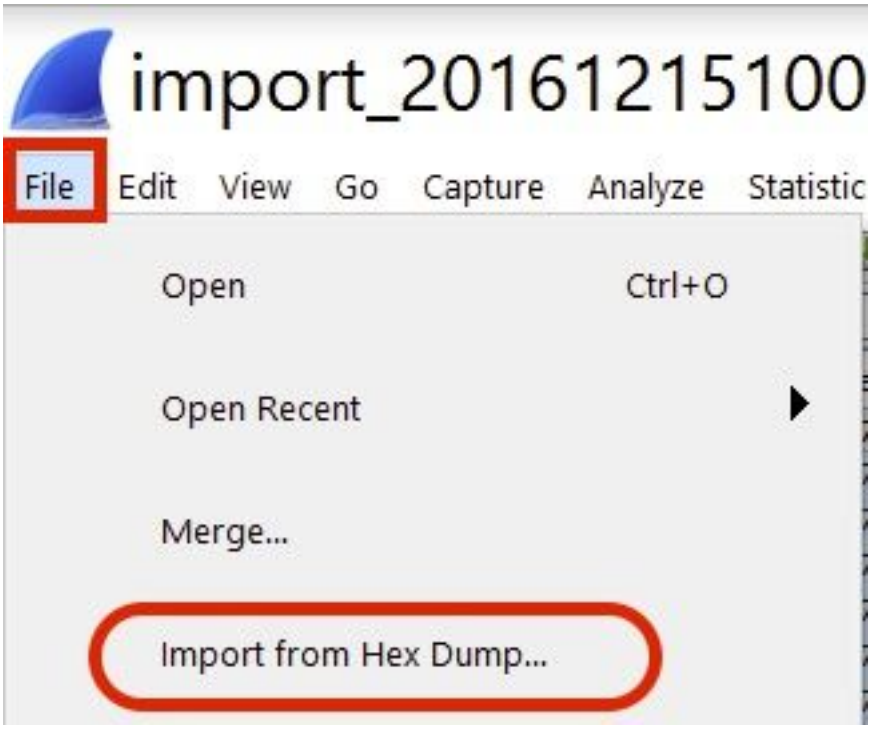
```
    [4]: disabled
    [5]: disabled
    [6]: disabled
  Ethernet ACL:
    [1]: disabled
    [2]: disabled
    [3]: disabled
    [4]: disabled
    [5]: disabled
    [6]: disabled
  IP ACL:
    [1]: permit s=172.16.0.34 d=172.16.56.153 any
    [2]: permit s=172.16.56.153 d=172.16.0.34 any
    [3]: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

パケット ログ出力を .pcap ファイルに変換する

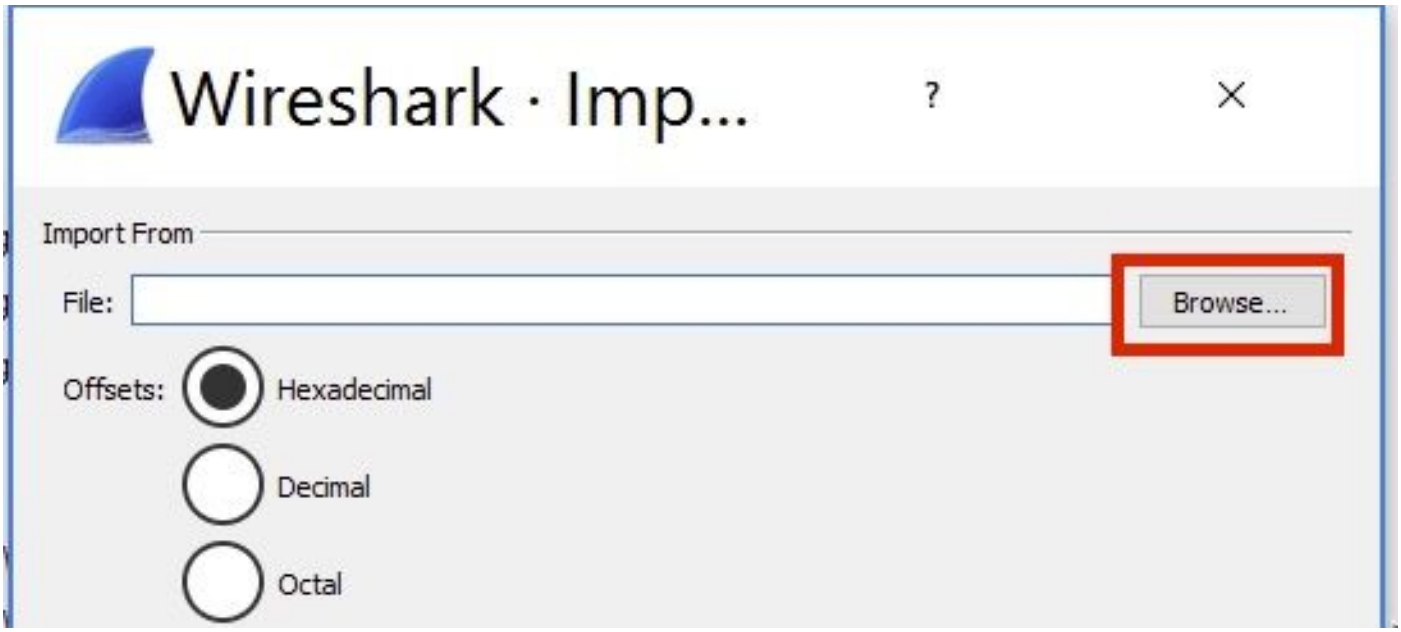
ステップ 1： 出力が完了したら、まとめてテキスト ファイルに保存します。

まとめる際はクリーンな口グになっていることを確認してください。クリーンな口グでないと 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。

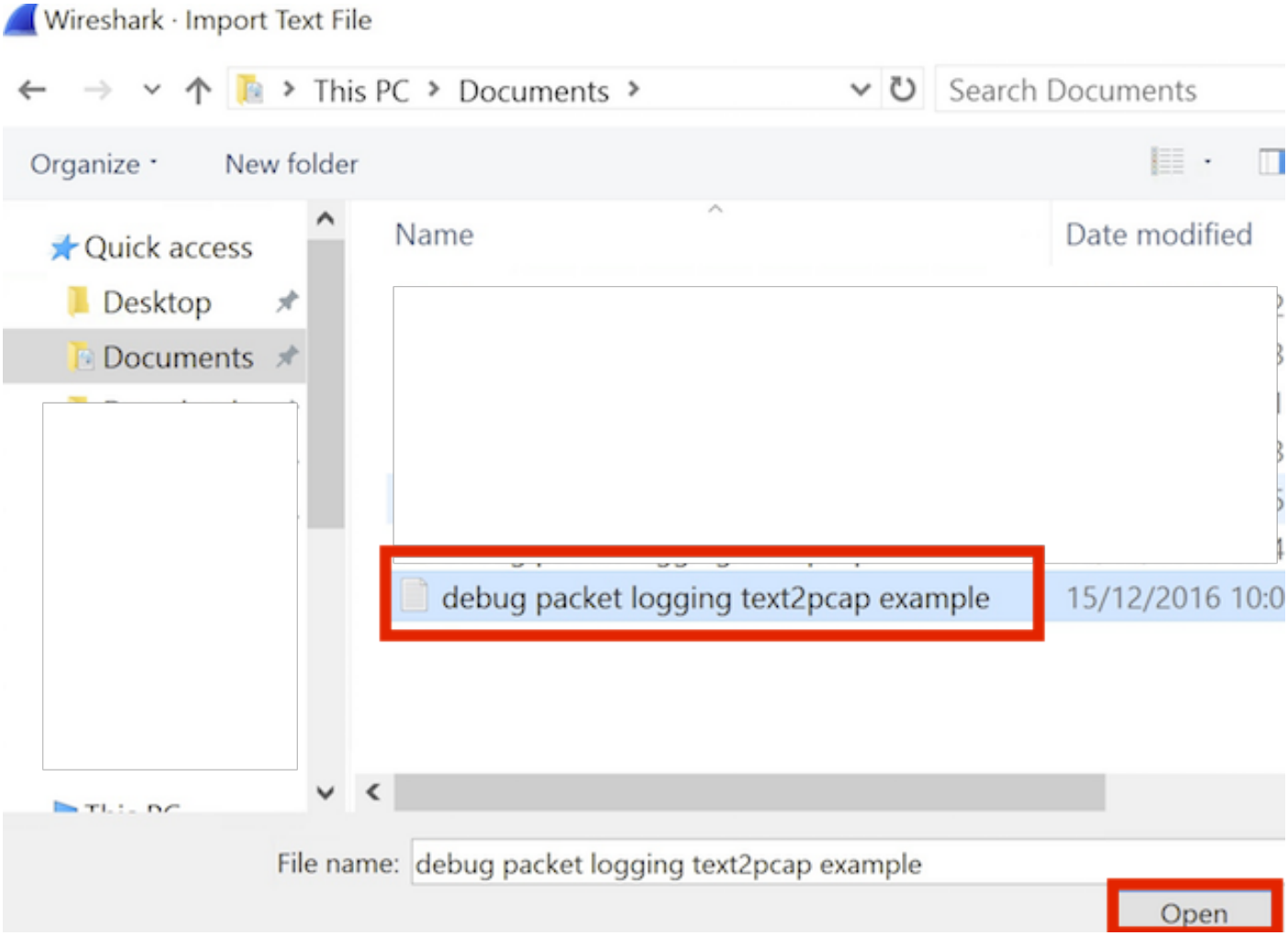
ステップ 2： Wireshark を開き、[File] > [Import from Hex Dump...] の順に開きます。



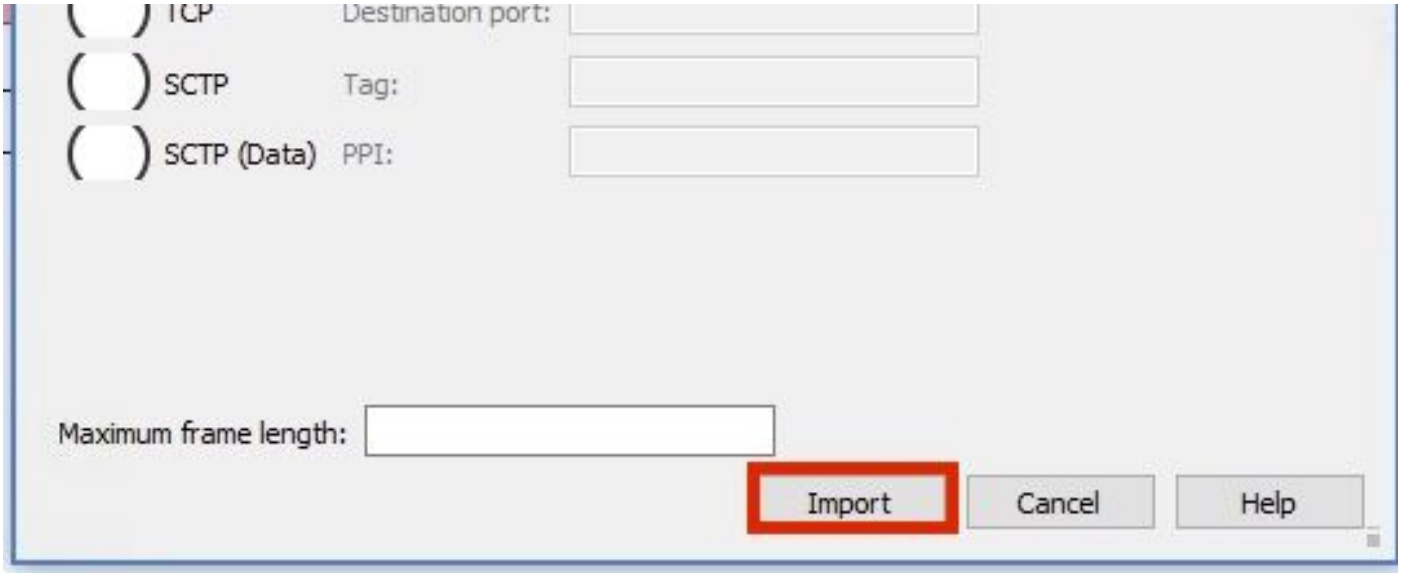
ステップ 3：[Browse] をクリックします。



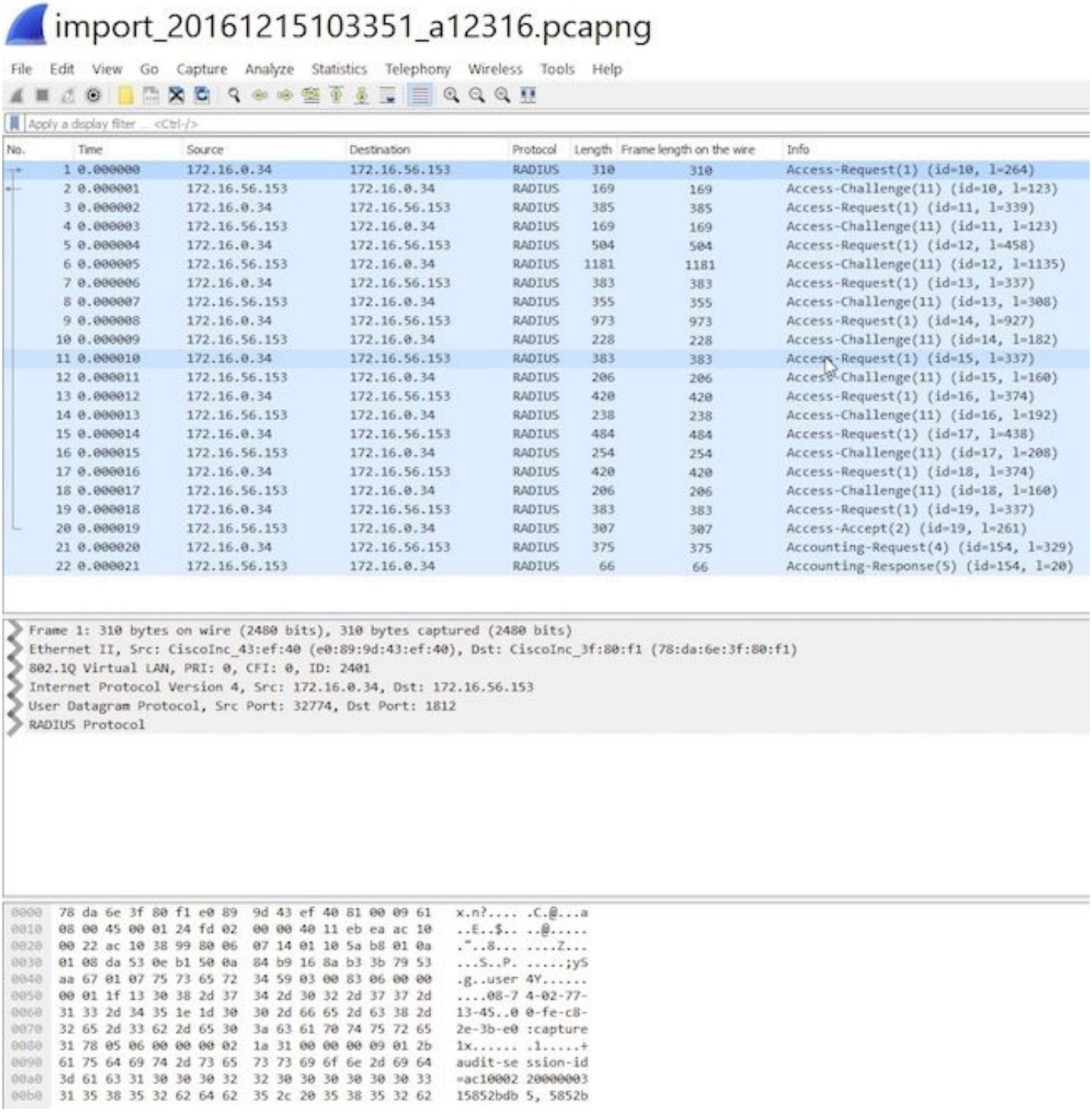
ステップ 4：パケット ログ出力を保存したテキスト ファイルを選択します。



ステップ 5：[Import] をクリックします。



Wireshark は .pcap としてファイルを表示します。



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。

トラブルシューティング

現在のところ、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