

AireOS WLC の設定 パケットキャプチャ

目次

[はじめに](#)

[要件](#)

[使用するコンポーネント](#)

[制限事項](#)

[設定](#)

[WLC のパケット ログ機能を有効にする](#)

[確認](#)

[パケット ログ出力を .pcap ファイルに変換する](#)

[トラブルシューティング](#)

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、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 ログイングを有効にする

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 ログ機能の有効にします。

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: すべての代わ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` が `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
```

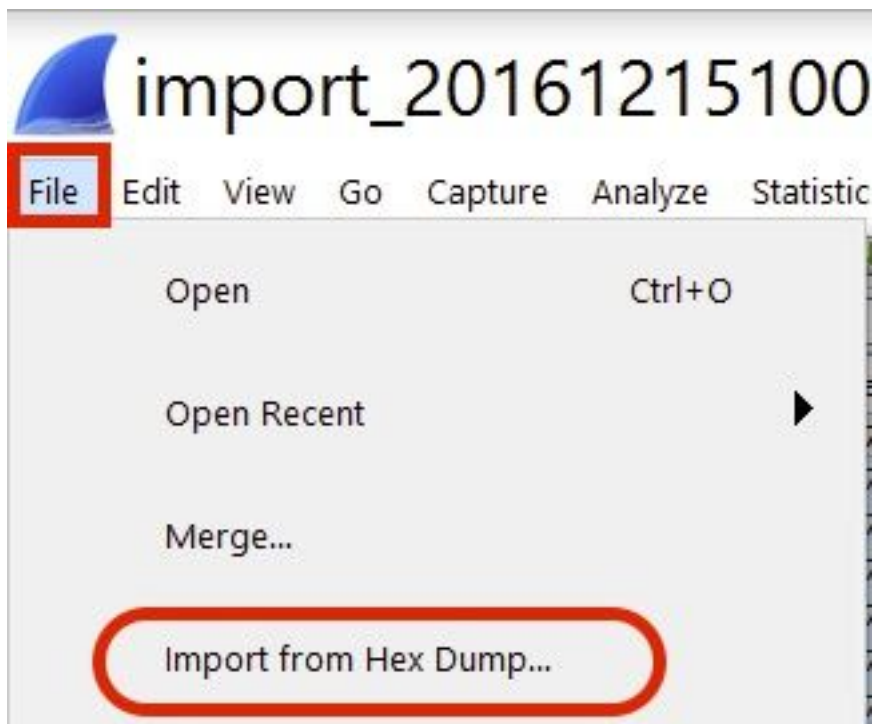
```
[4]: disabled
[5]: disabled
[6]: disabled
Ethernet ACL:
[1]: disabled
[2]: disabled
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled
IP ACL:
[1]: permit s=172.16.0.34 d=172.16.56.153 any
[2]: permit s=172.16.56.153 d=172.16.0.34 any
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled
EoIP-Ethernet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

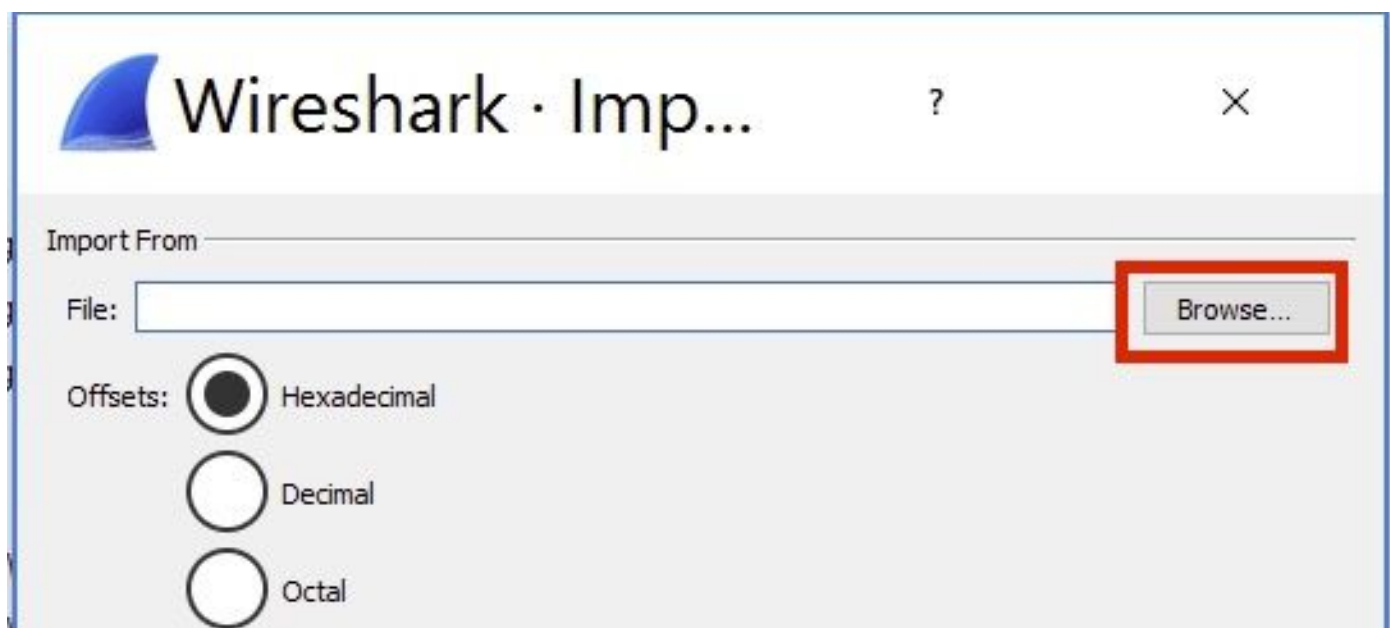
ステップ 1： 出力が完了したら、まとめてテキスト ファイルに保存します。

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。

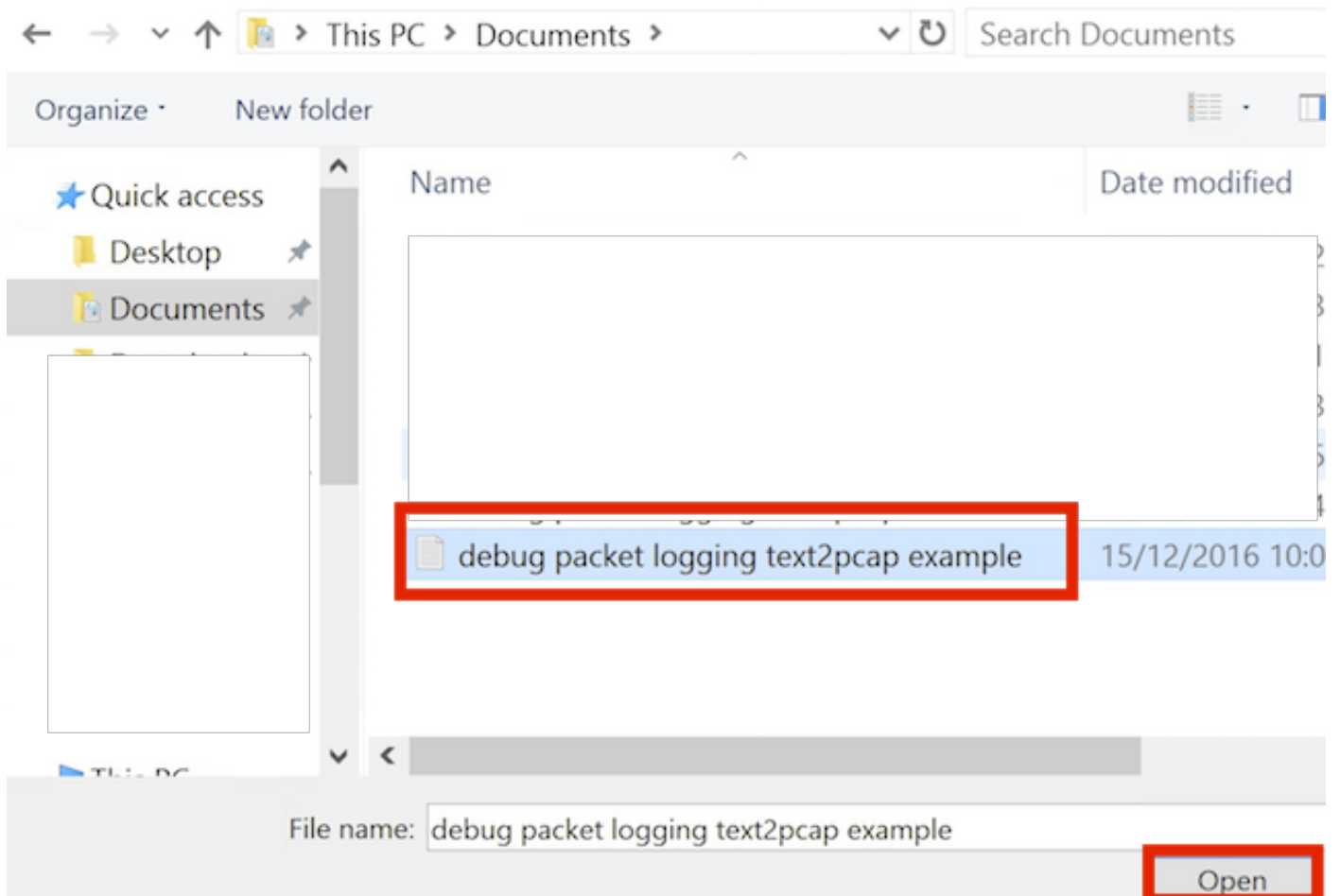
ステップ 2： Wireshark を開き、[File] > [Import from Hex Dump...] の順に開きます。



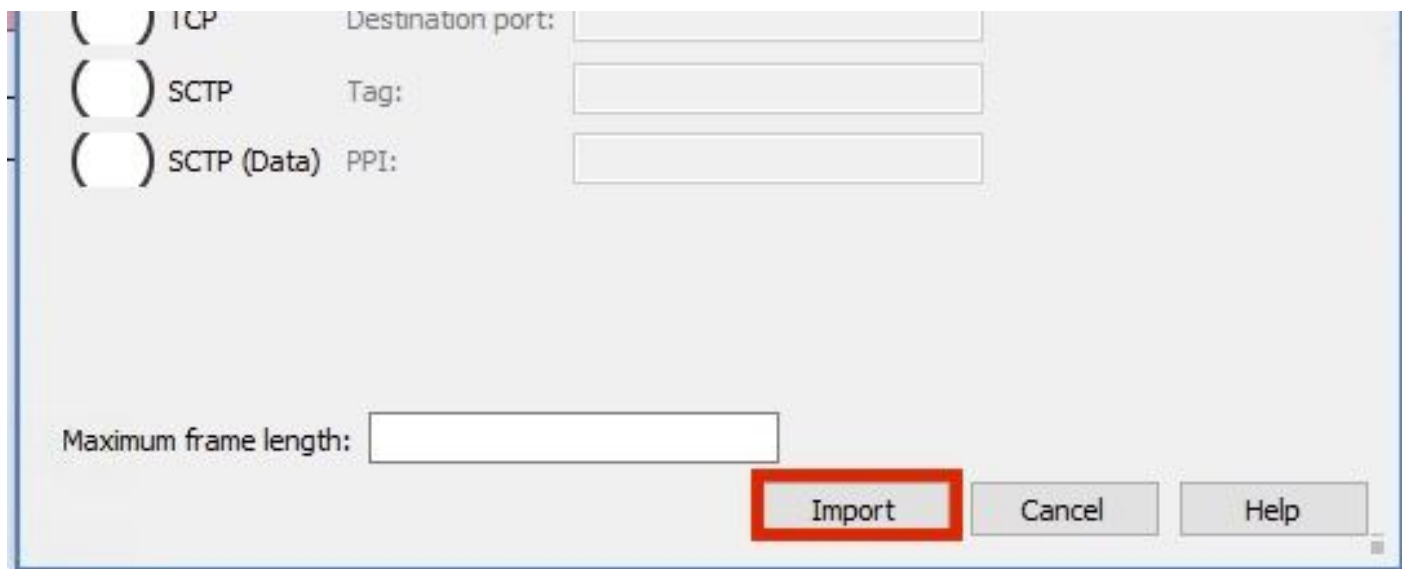
ステップ 3 : [Browse] をクリックします。



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。

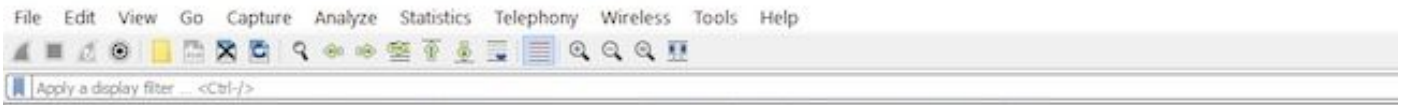


ステップ 5 : [Import] をクリックします。



Wireshark は .pcap としてファイルを表示します。

import_20161215103351_a12316.pcapng



No.	Time	Source	Destination	Protocol	Length	Frame length on the wire	Info
1	0.000000	172.16.0.34	172.16.56.153	RADIUS	310	310	Access-Request(1) (id=10, l=264)
2	0.000001	172.16.56.153	172.16.0.34	RADIUS	169	169	Access-Challenge(11) (id=10, l=123)
3	0.000002	172.16.0.34	172.16.56.153	RADIUS	385	385	Access-Request(1) (id=11, l=339)
4	0.000003	172.16.56.153	172.16.0.34	RADIUS	169	169	Access-Challenge(11) (id=11, l=123)
5	0.000004	172.16.0.34	172.16.56.153	RADIUS	504	504	Access-Request(1) (id=12, l=458)
6	0.000005	172.16.56.153	172.16.0.34	RADIUS	1181	1181	Access-Challenge(11) (id=12, l=1135)
7	0.000006	172.16.0.34	172.16.56.153	RADIUS	383	383	Access-Request(1) (id=13, l=337)
8	0.000007	172.16.56.153	172.16.0.34	RADIUS	355	355	Access-Challenge(11) (id=13, l=308)
9	0.000008	172.16.0.34	172.16.56.153	RADIUS	973	973	Access-Request(1) (id=14, l=927)
10	0.000009	172.16.56.153	172.16.0.34	RADIUS	228	228	Access-Challenge(11) (id=14, l=182)
11	0.000010	172.16.0.34	172.16.56.153	RADIUS	383	383	Access-Request(1) (id=15, l=337)
12	0.000011	172.16.56.153	172.16.0.34	RADIUS	206	206	Access-Challenge(11) (id=15, l=160)
13	0.000012	172.16.0.34	172.16.56.153	RADIUS	420	420	Access-Request(1) (id=16, l=374)
14	0.000013	172.16.56.153	172.16.0.34	RADIUS	238	238	Access-Challenge(11) (id=16, l=192)
15	0.000014	172.16.0.34	172.16.56.153	RADIUS	484	484	Access-Request(1) (id=17, l=438)
16	0.000015	172.16.56.153	172.16.0.34	RADIUS	254	254	Access-Challenge(11) (id=17, l=208)
17	0.000016	172.16.0.34	172.16.56.153	RADIUS	420	420	Access-Request(1) (id=18, l=374)
18	0.000017	172.16.56.153	172.16.0.34	RADIUS	206	206	Access-Challenge(11) (id=18, l=160)
19	0.000018	172.16.0.34	172.16.56.153	RADIUS	383	383	Access-Request(1) (id=19, l=337)
20	0.000019	172.16.56.153	172.16.0.34	RADIUS	307	307	Access-Accept(2) (id=19, l=261)
21	0.000020	172.16.0.34	172.16.56.153	RADIUS	375	375	Accounting-Request(4) (id=154, l=329)
22	0.000021	172.16.56.153	172.16.0.34	RADIUS	66	66	Accounting-Response(5) (id=154, l=20)

```
Frame 1: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface 0
Ethernet II, Src: CiscoInc_43:ef:40 (e0:89:9d:43:ef:40), Dst: CiscoInc_3f:80:f1 (78:da:6e:3f:80:f1)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 2401
Internet Protocol Version 4, Src: 172.16.0.34, Dst: 172.16.56.153
User Datagram Protocol, Src Port: 32774, Dst Port: 1812
RADIUS Protocol
```

```
0000 78 da 6e 3f 80 f1 e0 89 9d 43 ef 40 81 00 09 61  x.n?... .C.@...a
0010 08 00 45 00 01 24 fd 02 00 00 40 11 eb ea ac 10  ..E..$. .@.....
0020 00 22 ac 10 38 99 80 06 07 14 01 10 5a b8 01 0a  ."..8... ..Z...
0030 01 08 da 53 0e b1 50 0a 84 b9 16 8a b3 3b 79 53  ...S..P. ....;yS
0040 aa 67 01 07 75 73 65 72 34 59 03 00 83 06 00 00  .g..user 4Y.....
0050 00 01 1f 13 30 38 2d 37 34 2d 30 32 2d 37 37 2d  ...08-7 4-02-77-
0060 31 33 2d 34 35 1e 1d 30 30 2d 66 65 2d 63 38 2d  13-45..0 0-fe-c8-
0070 32 65 2d 33 62 2d 65 30 3a 63 61 70 74 75 72 65  2e-3b-e0 :capture
0080 31 78 05 06 00 00 00 02 1a 31 00 00 00 09 01 2b  1x..... .l.....+
0090 61 75 64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64  audit-se ssion-id
00a0 3d 61 63 31 30 30 30 32 32 30 30 30 30 30 33  =ac10002 20000003
00b0 31 35 38 35 32 62 64 62 35 2c 20 35 38 35 32 62  15852bdb 5, 5852b
```

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](#)