

# AireOS WLCでのパケットキャプチャの設定

## 内容

[概要](#)

[要件](#)

[使用するコンポーネント](#)

[制限](#)

[設定](#)

[WLCのパケットロギングを有効にする](#)

[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 ログイングから 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 ログイングを無効にする

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

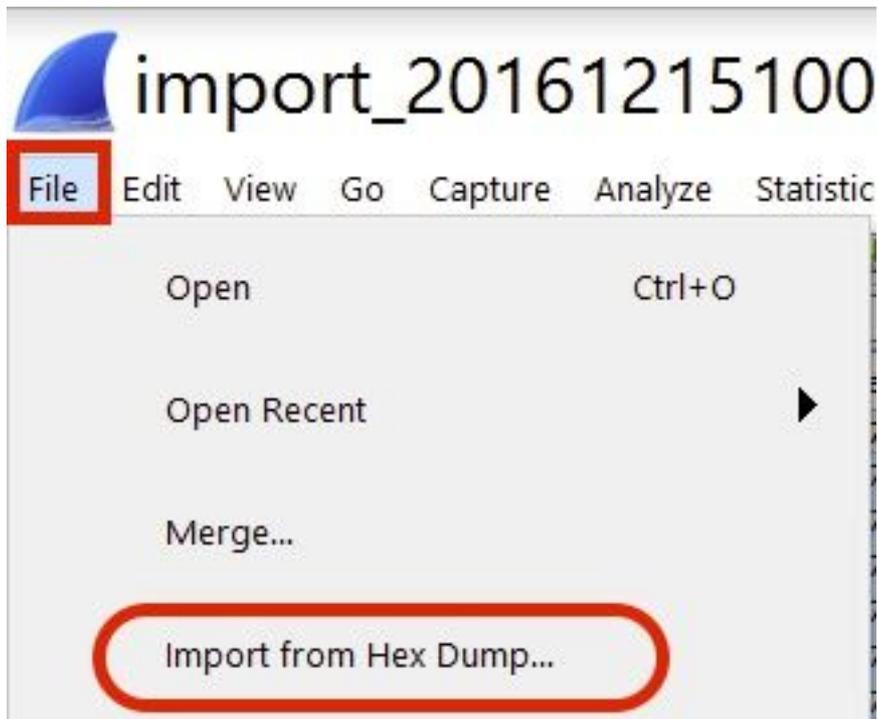
```
> debug packet logging disable
```

## パケット ログ出力を .pcap ファイルに変換する

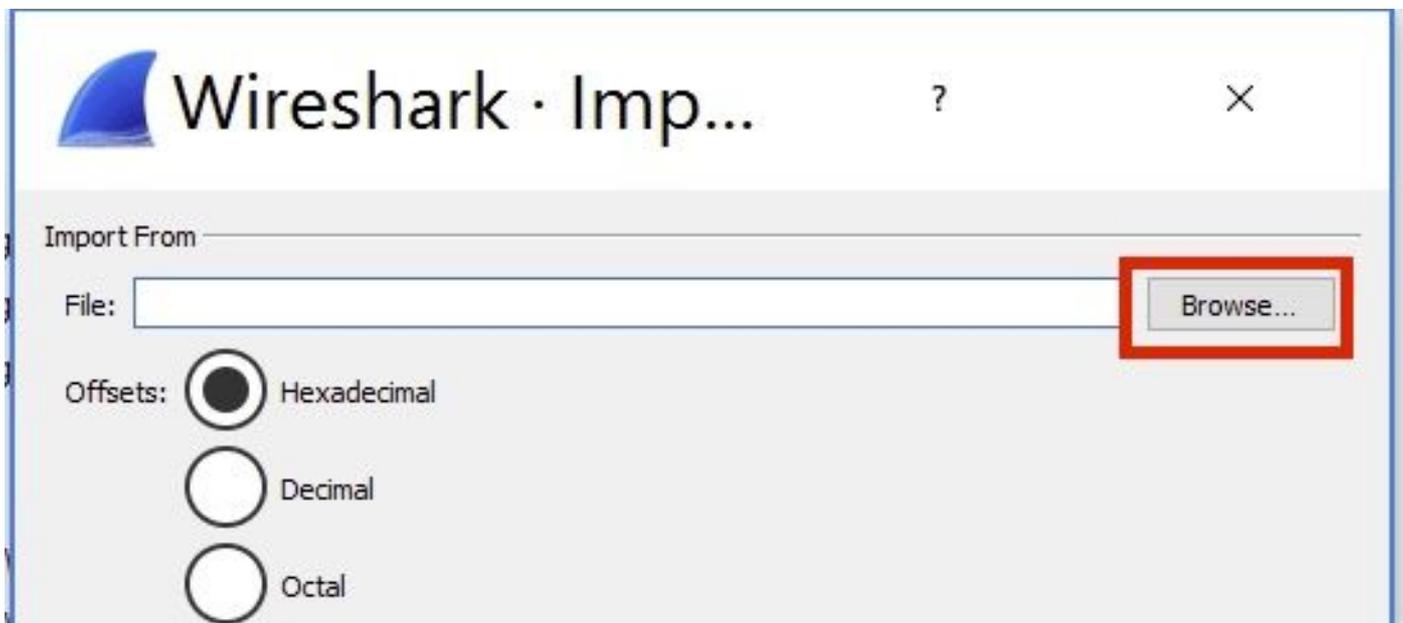
ステップ1：出力が終了したら、それを収集してテキストファイルに保存します。

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。

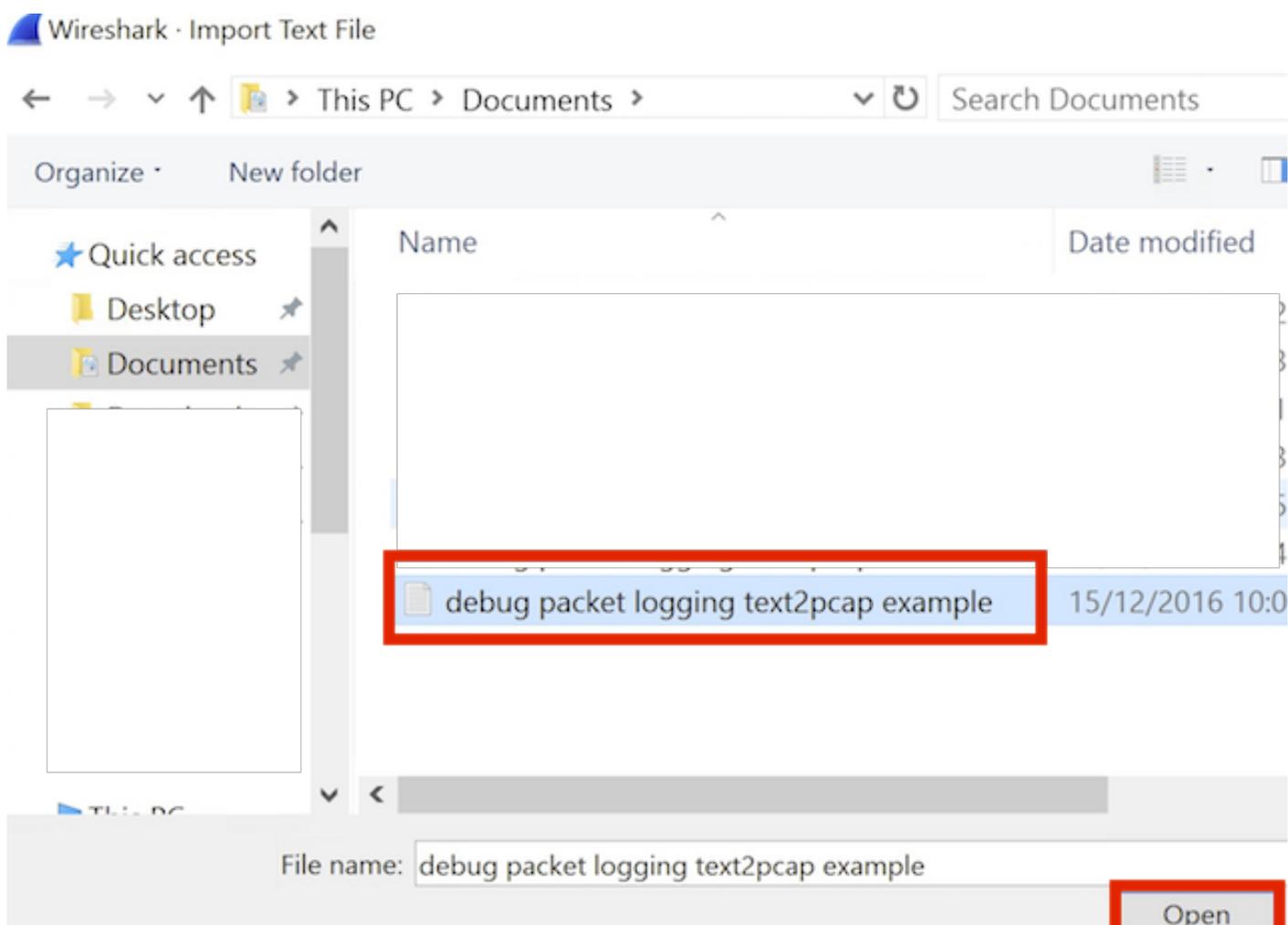
ステップ2：Wireshark を開き、[File] > [Import from Hex Dump...] の順に開きます。



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。

TCP Destination port:

SCTP Tag:

SCTP (Data) PPI:

Maximum frame length:

Wiresharkでは、ファイルが.pcapとして表示されます。

# 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、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](#)