

Configurez les captures de paquet sur AireOS WLC

Contenu

[Introduction](#)

[Conditions requises](#)

[Composants utilisés](#)

[Limites](#)

[Configurez](#)

[Paquet d'enable ouvrant une session WLC](#)

[Vérifiez](#)

[Sortie de journalisation de paquet de conversion à un fichier .pcap](#)

[Dépannez](#)

Introduction

Ce document décrit comment exécuter un vidage mémoire de paquet sur un RÉSEAU LOCAL Sans fil Controller(WLC) d'AireOS. Cette méthode affiche les paquets envoyés et/ou reçus au niveau CPU du WLC dans le format hexadécimal, qui alors soit traduit à un fichier .pcap avec Wireshark.

Il est utile dans les cas où transmission entre un WLC et un serveur de Service RADIUS (Remote Authentication Dial-In User Service), un Point d'accès (AP) ou d'autres contrôleurs doit être vérifiés d'un moyen rapide avec une capture de paquet au niveau WLC mais il est difficile d'exécuter une port-envergure.

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès de l'interface de ligne de commande (CLI) au WLC, de préférence SSH puisque la sortie est plus rapide que la console.
- Le PC avec Wireshark a installé

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC v8.3
- Wireshark v2 ou plus tard

Remarque: Cette caractéristique est disponible depuis la version 4 d'AireOS.

Limites

Se connecter de paquet capturera seulement l'avion bidirectionnel de contrôle (CP) aux paquets du plan de données (DP) dans WLC. Ces paquets qui ne sont pas envoyés du plan de données WLC à/de l'avion de contrôle (c.-à-d. étranger pour ancrer le trafic percé un tunnel, des baisses DP-CP et ainsi de suite) ne seront pas capturés.

Les exemples des types de trafic à/de le WLC traités au CP sont :

- Telnet
- SSH
- HTTP
- HTTPS
- SNMP
- NTP
- RAYON
- TACACS+
- Messages de mobilité
- Contrôle CAPWAP
- NMSP
- TFTP/FTP/SFTP
- Syslog
- IAPP

Le trafic à/de le client est traité dans le plan de données (DP) excepté : Gestion de 802.11, 802.1X/EAPOL, ARP, DHCP et authentification Web.

Configurez

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Paquet d'enable ouvrant une session WLC

Étape 1. Procédure de connexion au CLI de WLC.

En raison de la quantité et de la vitesse des logs que cette caractéristique affiche il est recommandé pour ouvrir une session au WLC par SSH et pas par la console.

Étape 2. Appliquez une liste de contrôle d'accès (ACL) pour limiter que le trafic est capturé.

Dans l'exemple donné la capture affiche le trafic à/de l'interface de gestion du WLC (adresse IP 172.16.0.34) et le serveur de RAYON (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
```

Conseil : Pour capturer tout le trafic à/de le WLC il est recommandé pour appliquer un ACL qui jette le trafic de SSH à/de l'hôte qui a initié la session de SSH. Ce sont les commandes

que vous pouvez employer pour construire l'ACL :

- >le debug packet se connectant l'IP 1 d'acl refusent le TCP 22 de <host-IP> <WLC-IP>
- >le debug packet se connectant l'IP 2 d'acl refusent à TCP du <host-IP> <WLC-IP> n'importe quels 22
- >debug packet se connectant l'autorisation de l'IP 3 d'acl toute

Étape 3. Configurez le format accessible en lecture par Wireshark.

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

Étape 4. Fonctionnalité de journalisation de paquet d'enable.

Cet exemple affiche comment capturer 100 reçus/paquets transmis (il prend en charge 1 - 65535 paquets) :

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

Remarque: Par défaut, il se connecte seulement 25 paquets reçus avec le **logging enable de debug packet de commande**.

Remarque: Au lieu de **tous** vous pouvez employer le **rx** ou le **tx** pour capturer le trafic seulement reçu ou transmis.

Pour d'autres détails au sujet de configurer la fonctionnalité de journalisation de paquet consultez ce lien :

[Guide de configuration Sans fil de contrôleur de Cisco, version 8.3, utilisant l'installation de debug](#)

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Utilisez l'instruction donnée de vérifier la configuration en cours de se connecter de paquet.

```
> 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
```

Reproduisez le comportement nécessaire pour générer le trafic.

Un résultat semblable à ceci apparaît :

```
> 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
```

Retirez ACLs de se connecter de paquet

Afin de désactiver les filtres appliqués par l'ACLs utilisez ces commandes :

```
> 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
```

Se connecter de paquet de débranchement

Afin de désactiver le paquet se connectant sans retirer l'ACLs utilisez simplement cette commande :

```
> 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:
```

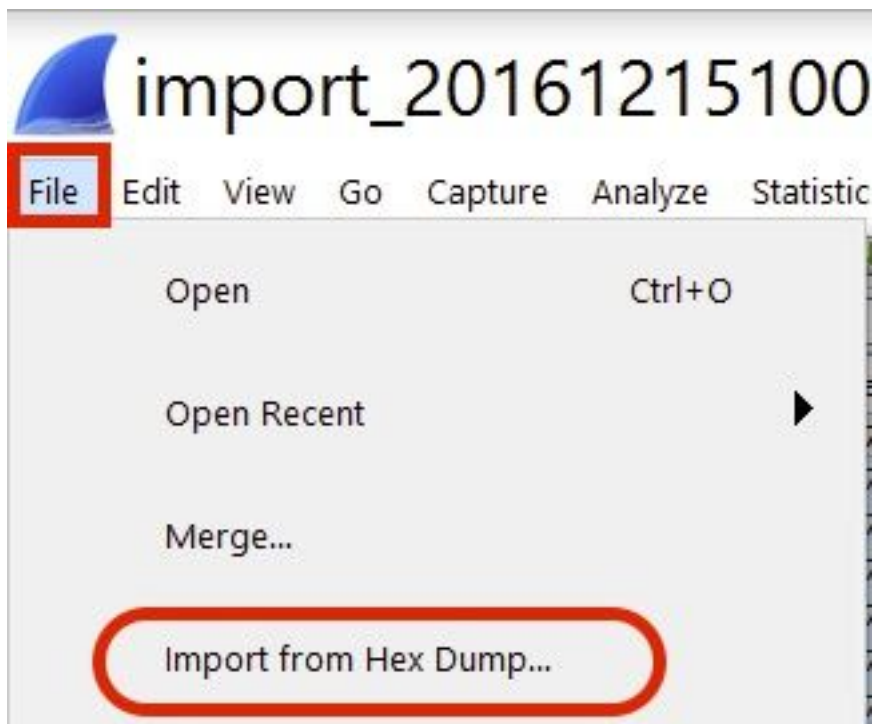
```
[1]: permit s=172.16.0.34 d=172.16.56.153 any
[2]: permit s=172.16.56.153 d=172.16.0.34 any
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled
EoIP-Ethernet ACL:
[1]: disabled
[2]: disabled
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled
EoIP-IP ACL:
[1]: disabled
[2]: disabled
[3]: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

Sortie de journalisation de paquet de conversion à un fichier .pcap

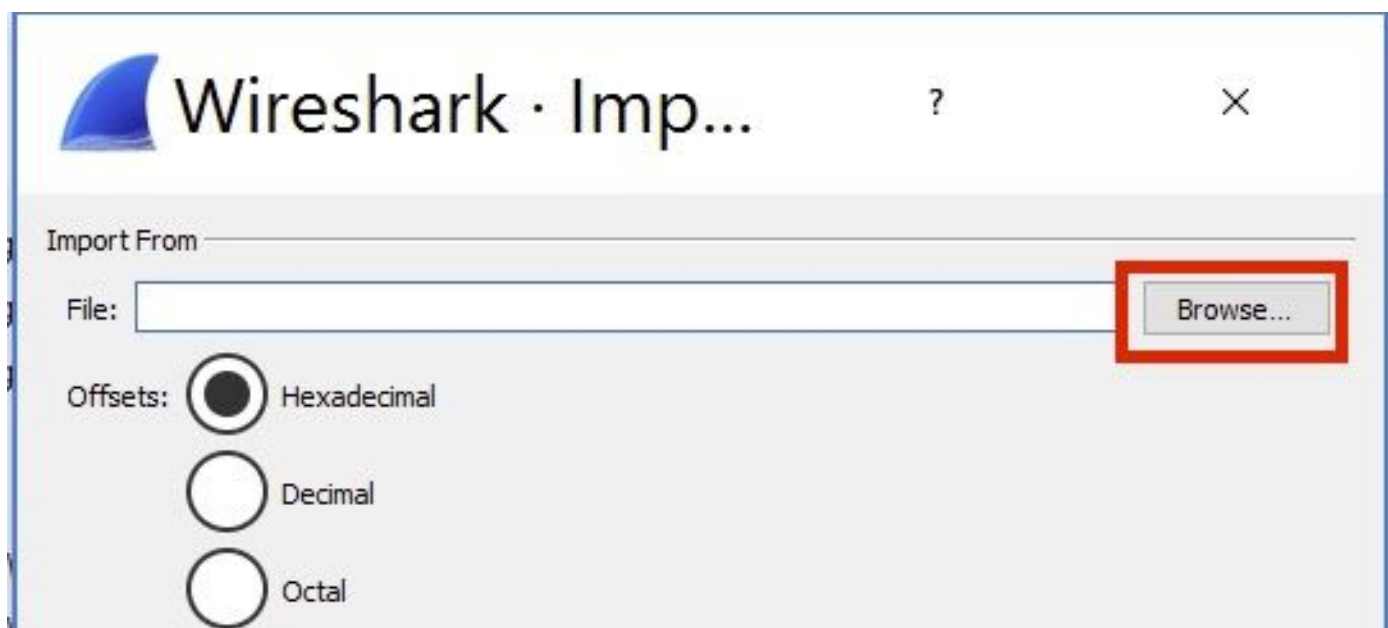
Étape 1. Une fois que la sortie termine, collectez-la et sauvegardez-la à un fichier texte.

Assurez-vous que vous recueillez un log propre, autrement Wireshark pourrait afficher les paquets corrompus.

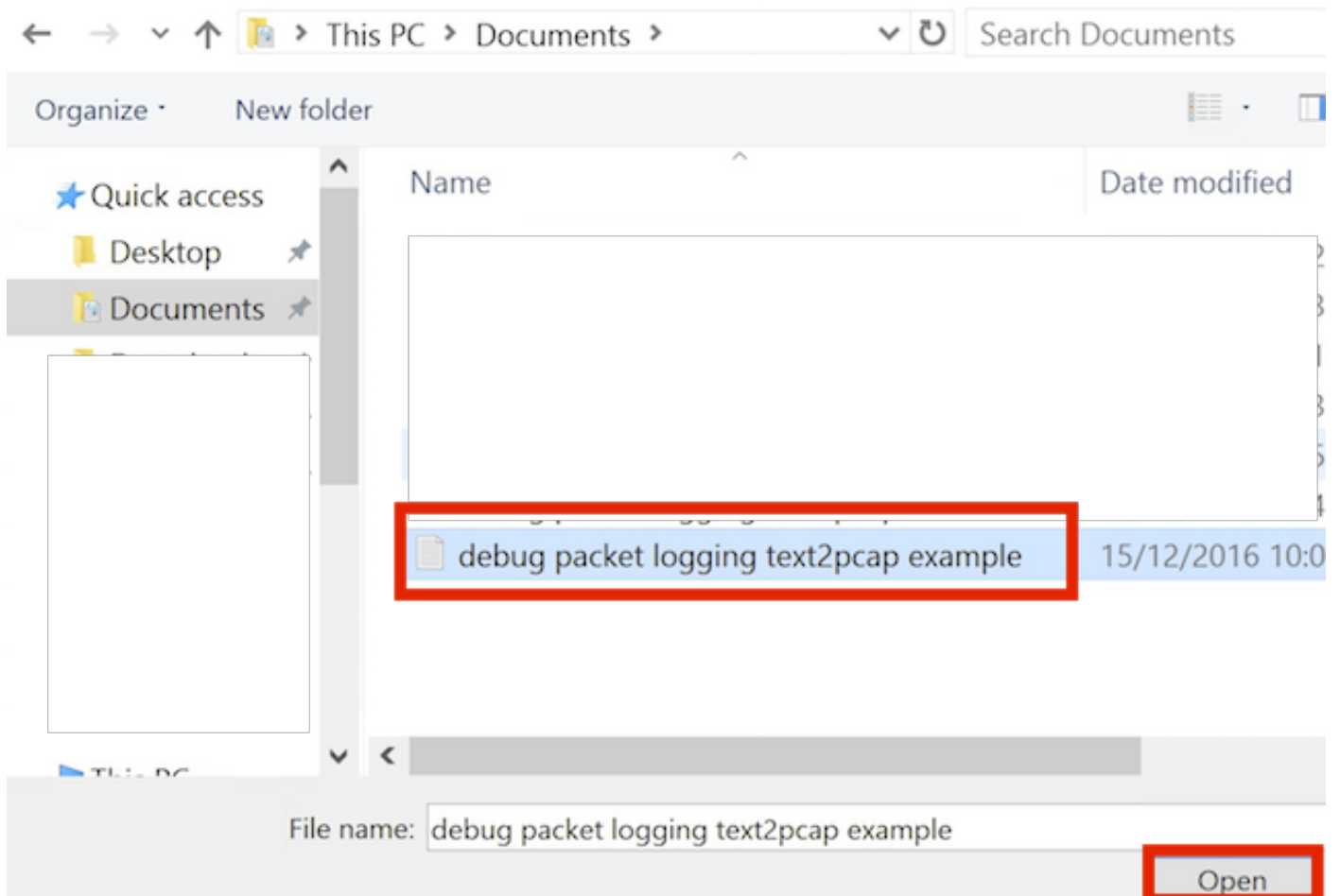
Étape 2. Ouvrez Wireshark et naviguez pour classer le >Import du vidage hexadécimal...



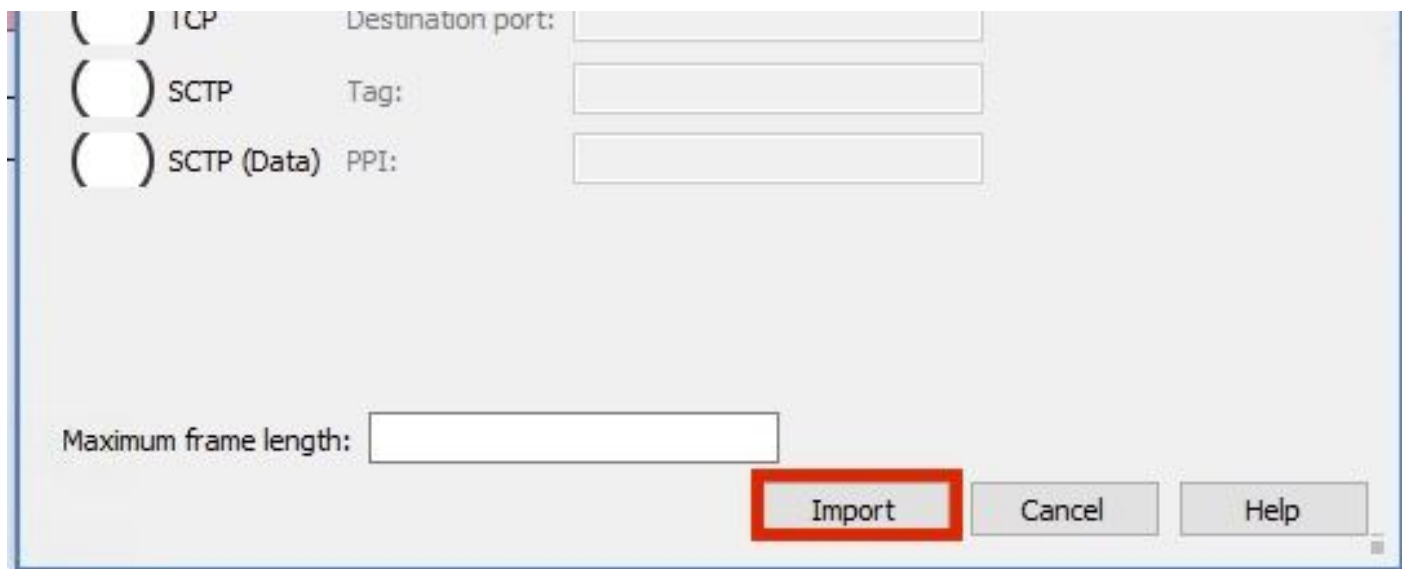
Étape 3. Le clic parcourt.



Étape 4. Sélectionnez le fichier texte où vous avez enregistré la sortie de journalisation de paquet.



Étape 5. **Importation de clic.**



Wireshark affiche le fichier comme .pcap.

import_20161215103351_a12316.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

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)

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
```

Remarque: Rendez-vous compte que les groupes date/heure ne sont pas précis ni le temps delta entre les trames.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

[Informations connexes](#)

- [Vidage mémoire de paquet AP](#)
- [Principes fondamentaux du reniflement Sans fil de 802.11](#)
- [Support et documentation techniques - Cisco Systems](#)