

# Configurazione delle acquisizioni di pacchetti su AireOS WLC

## Sommario

[Introduzione](#)

[Requisiti](#)

[Componenti usati](#)

[Limitazioni](#)

[Configurazione](#)

[Abilita registrazione pacchetti in WLC](#)

[Verifica](#)

[Conversione dell'output di registrazione dei pacchetti in un file con estensione pcap](#)

[Risoluzione dei problemi](#)

## Introduzione

Questo documento descrive come eseguire un dump di pacchetto su un controller WLC (AireOS Wireless LAN Controller). Questo metodo visualizza i pacchetti inviati e/o ricevuti a livello di CPU del WLC in formato esadecimale, che vengono quindi convertiti in un file .pcap con Wireshark.

È utile nei casi in cui la comunicazione tra un WLC e un server RADIUS (Remote Authentication Dial-In User Service), un punto di accesso (AP) o altri controller devono essere verificati in modo rapido con un'acquisizione di pacchetti a livello WLC, ma un port-span è difficile da eseguire.

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso al WLC dall'interfaccia della riga di comando (CLI), preferibilmente SSH poiché l'output è più veloce della console.
- PC con Wireshark installato

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- WLC v8.3
- Wireshark v2 o successivo

**Nota:** questa funzione è disponibile dalla versione 4 di AireOS.

## Limitazioni

La registrazione dei pacchetti acquisirà solo i pacchetti bidirezionali da Control Plane (CP) a Data Plane (DP) nel WLC. I pacchetti che non vengono inviati dal piano dati WLC al/dal piano di controllo (ad es. traffico esterno verso il tunnel di ancoraggio, cadute DP-CP e così via) non vengono catturati.

Di seguito sono riportati alcuni esempi di tipi di traffico da/verso il WLC elaborati al CCP:

- Telnet
- SSH
- HTTP
- HTTPS
- SNMP
- NTP
- RAGGIO
- TACACS+
- Messaggi sulla mobilità
- controllo CAPWAP
- NMSP
- TFTP/FTP/SFTP
- Syslog
- IAPP

Il traffico da/verso il client viene elaborato nel Data Plane (DP) ad eccezione di: gestione 802.11, autenticazione 802.1X/EAPOL, ARP, DHCP e Web.

## Configurazione

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

### Abilita registrazione pacchetti in WLC

Passaggio 1. Accedere alla CLI del WLC.

A causa della quantità e della velocità dei log visualizzati da questa funzione, si consiglia di accedere al WLC tramite SSH e non tramite console.

Passaggio 2. Applicare un Access Control List (ACL) per limitare il traffico acquisito.

Nell'esempio riportato, l'acquisizione mostra il traffico da/verso l'interfaccia di gestione del WLC (indirizzo IP 172.16.0.34) e il server RADIUS (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
```

**Suggerimento:** Per acquisire tutto il traffico da/verso il WLC, si consiglia di applicare un ACL

che scarti il traffico SSH da/verso l'host che ha avviato la sessione SSH. Di seguito sono riportati i comandi che è possibile usare per compilare l'ACL:

```
>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 2
>debug packet logging acl ip 3 permette qualsiasi
```

Passaggio 3. Configurare il formato leggibile da Wireshark.

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

Passaggio 4. Abilitare la funzione di registrazione dei pacchetti.

Nell'esempio viene mostrato come acquisire 100 pacchetti ricevuti/trasmessi (supporta 1 - 65535 pacchetti):

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

Passaggio 5. Registrare l'output in un file di testo.

**Nota:** per impostazione predefinita, registra solo 25 pacchetti ricevuti con il comando `debug packet logging enable`.

**Nota:** Anziché **tutto**, è possibile utilizzare `rx` o `tx` per acquisire solo il traffico ricevuto o trasmesso.

Per ulteriori dettagli sulla configurazione della funzione di registrazione dei pacchetti, consultare questo collegamento:

[Guida alla configurazione di Cisco Wireless Controller, versione 8.3, uso della funzione di debug](#)

## Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Utilizzare il comando specificato per verificare la configurazione corrente della registrazione dei pacchetti.

```
> 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

```

Riprodurre il comportamento necessario per generare il traffico.

Viene visualizzato un output simile al seguente:

```

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...
```

## Rimozione di ACL dalla registrazione dei pacchetti

Per disabilitare i filtri applicati dagli ACL, usare questi comandi:

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

### Disabilita registrazione pacchetti

Per disabilitare la registrazione dei pacchetti senza rimuovere gli ACL, usare questo comando:

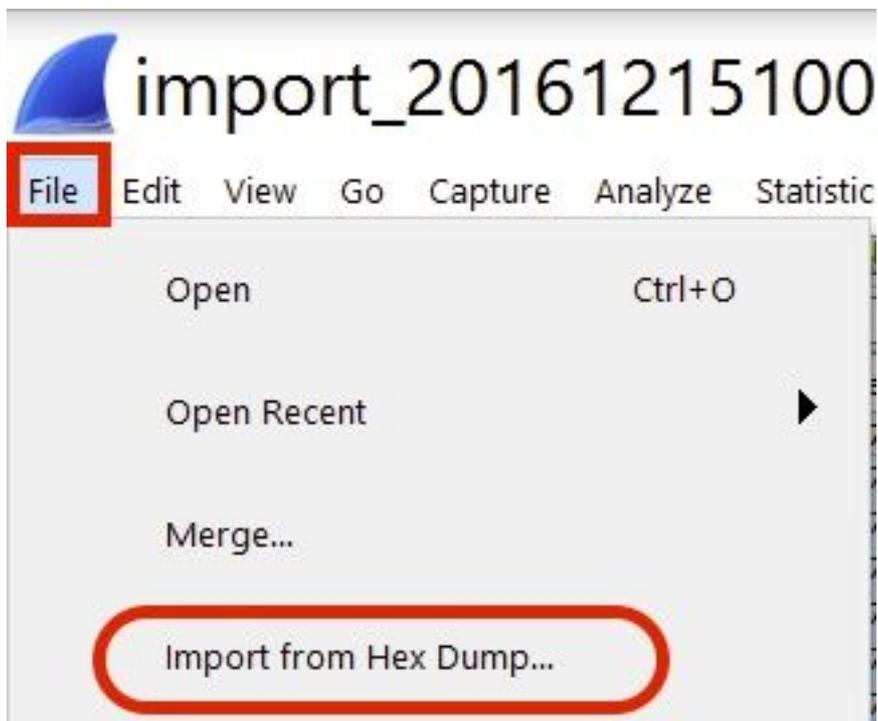
```
> debug packet logging disable
```

## Conversione dell'output di registrazione dei pacchetti in un file con estensione pcap

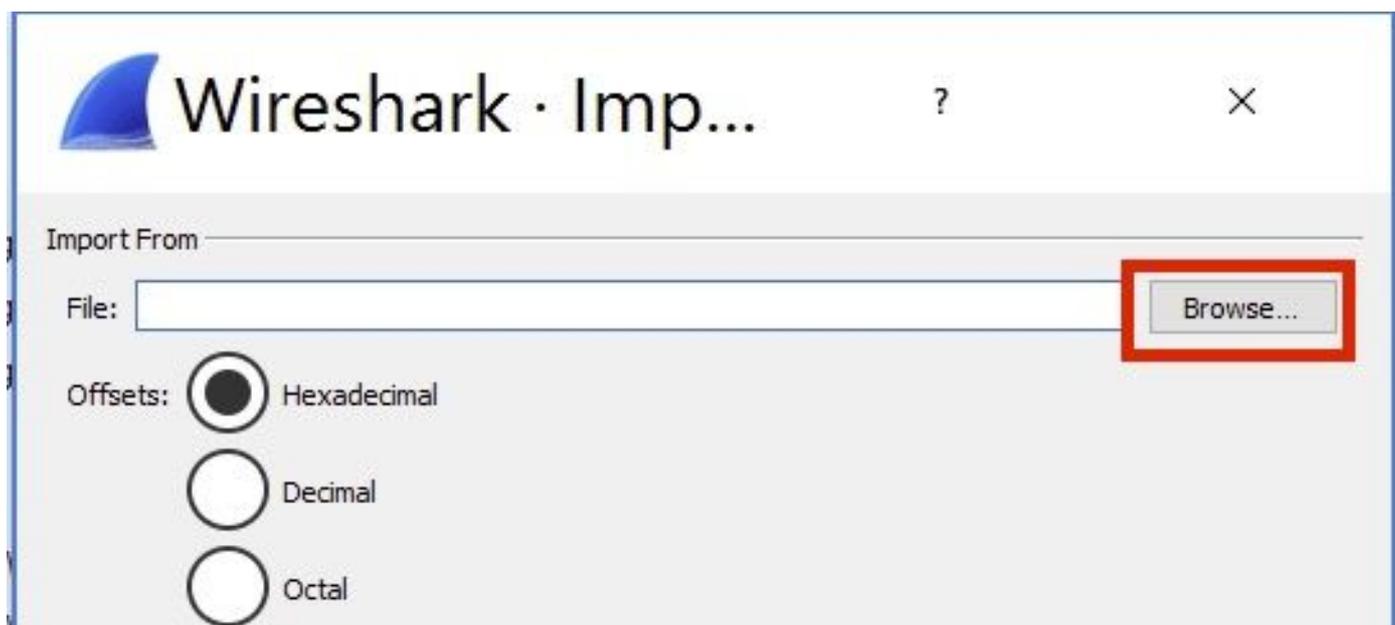
Passaggio 1. Al termine dell'output, raccoglierlo e salvarlo in un file di testo.

Verificare di aver raccolto un log pulito, altrimenti Wireshark potrebbe visualizzare pacchetti danneggiati.

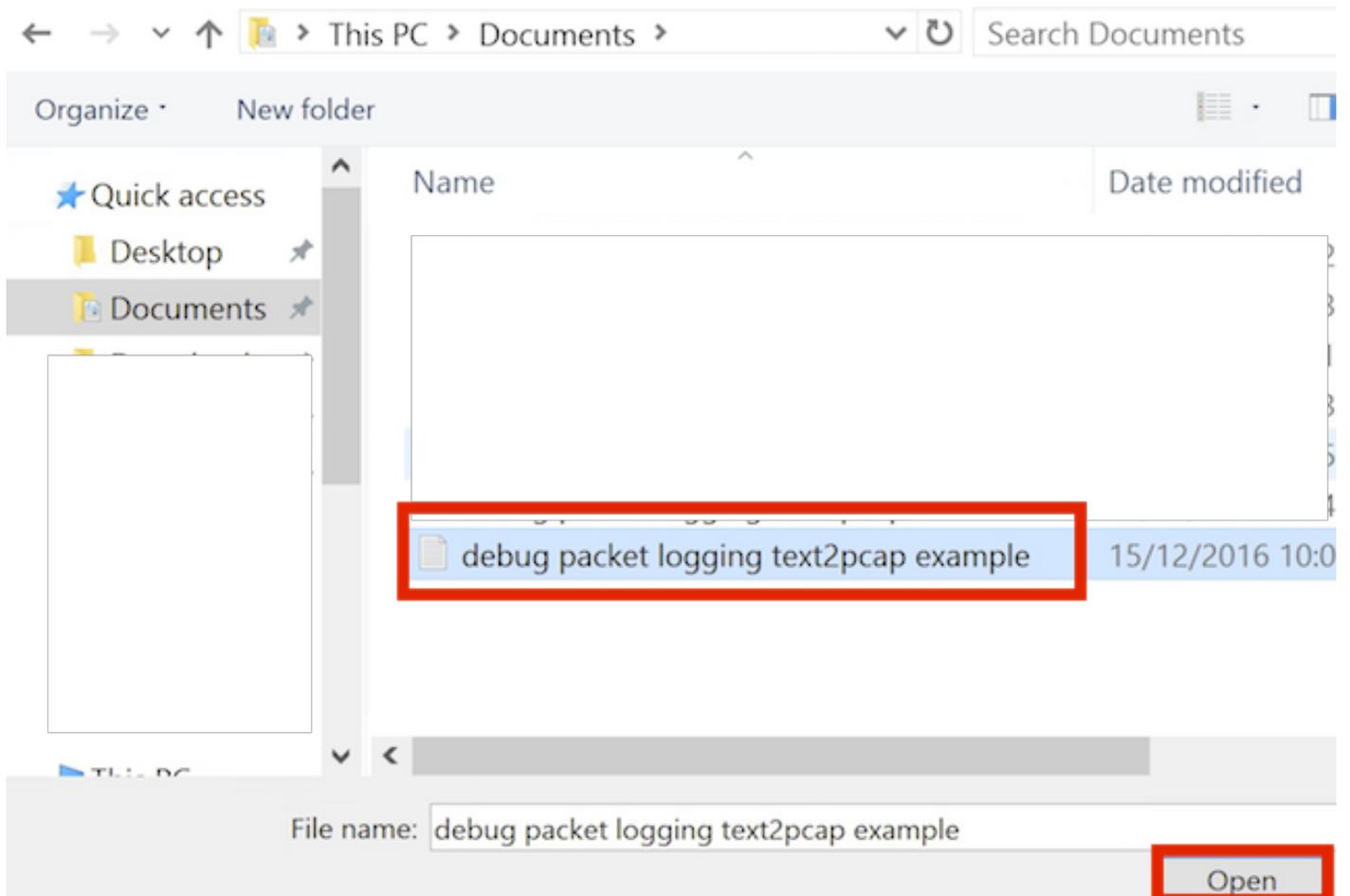
Passaggio 2. Aprire Wireshark e selezionare **File>Import from Hex Dump...**



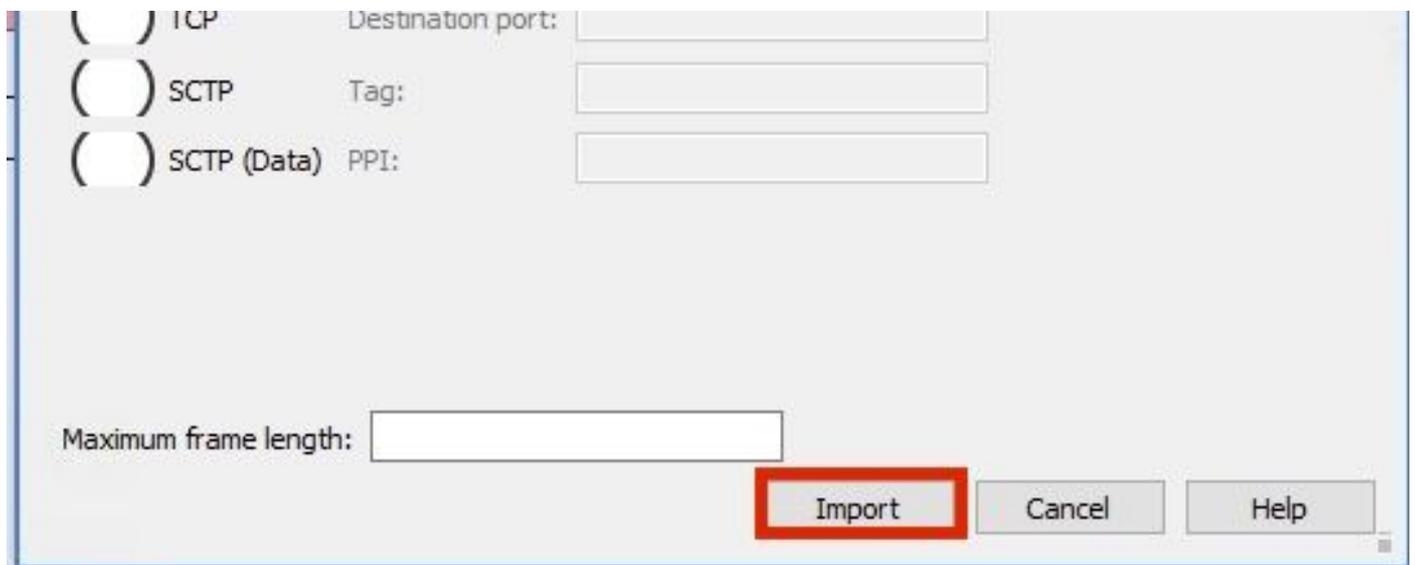
Passaggio 3. Fare clic su **Sfoglia**.



Passaggio 4. Selezionare il file di testo in cui è stato salvato l'output di registrazione dei pacchetti.



Passaggio 5. Fare clic su **Importa**.



Wireshark visualizza il file come .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
```

**Nota:** Tenere presente che i timestamp non sono accurati né il tempo delta tra i fotogrammi.

## Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

### Informazioni correlate

- [Dump pacchetto AP](#)
- [Nozioni fondamentali sullo sniffing wireless 802.11](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)